EMC ControlCenter

Version 5.0

ONLINE HELP VOLUME 1

P/N 300-000-376
REV A01

EMC Corporation
171 South Street
Hopkinton, MA 01748-9103
Corporate Headquarters: (508) 435-1000, (800)424-EMC2
Fax: (508) 435-5374 *Service*: (800) SVC-4EMC

Copyright © 2001 EMC Corporation. All rights reserved.

Printed December, 2001

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Trademark Information

EMC^2, EMC, and Symmetrix are registered trademarks and EMC Enterprise Storage, The Enterprise Storage Company, ControlCenter, Connectrix, EDM, SDMS, SRDF, TimeFinder, PowerPath, InfoMover, FarPoint, EMC Enterprise Storage Network, E-Infostructure, and Celerra are trademarks of EMC Corporation.

All other trademarks used herein are the property of their respective owners.

Table of Contents

Introducing EMC ControlCenter

Welcome to EMC ControlCenter/Open Edition, your mission control center for your entire distributed storage environment. The EMC ControlCenter family of products enable you to monitor, configure, control, tune, and plan storage across an entire Enterprise Storage Network (ESN) from a single console. This powerful and flexible suite of tools provides end-to-end management of storage networks, storage devices, and other storage resources.

Where do you want to start?

Click your area of interest below to learn more about ControlCenter, perform a ControlCenter task, or examine your storage environment.

CONTROLCENTER

What's New?
Discover the features and benefits now available to you.

ControlCenter Architecture
Gain a deeper understanding of some of the background processes of this suite of tools.

Using the Console
Prepare yourself to use the power of this suite of tools.

CONTROLCENTER TASK

Storage Allocation
Examine or change your existing storage configuration.

Monitoring
Display the properties and status for all managed objects in your storage environment, set up alerts to warn of performance hot spots, and define alert autofixes.

Performance Management
Collect and archive statistics used for system tuning and future capacity planning.

ECC Administration
Define and control authorized users and user groups, and install or upgrade intelligent agents.

Data Protection
Address your disaster recovery needs and perform backups, data migration, and archiving.

STORAGE ENVIRONMENT

Properties
View the properties for selected objects.

Alerts
View the active alerts and alert definitions for managed objects.

Relationship
View the logical mapping for selected objects.

Performance
View the performance data for selected objects.

What's new in ControlCenter

ControlCenter provides a superior single product that combines the functionality of various storage management applications into an integrated application. This allows the user to manage objects, views, and actions together in an intuitive flow to achieve a particular task.

ControlCenter features

ControlCenter is easy to install, deploy, and maintain, and provides immediate access to the following features:

- Component status monitoring
- Configuration and monitoring of the storage environment
- Setting and sending of proactive alerts
- Performance tuning and optimization
- Security and auditing of the storage environment
- Administration of redundancy and failover
- Central management and multiuser support
- Painless installation and upgrade of independent and autonomous agents
- Central Repository for enterprise storage information

ControlCenter benefits

ControlCenter uniform user experience and quick problem resolution facilitation provides the following benefits.

- Business availability
- Recovery from failures
- Asset management
- Capacity planning
- Open framework approach
- Central services
- Independent agent and client

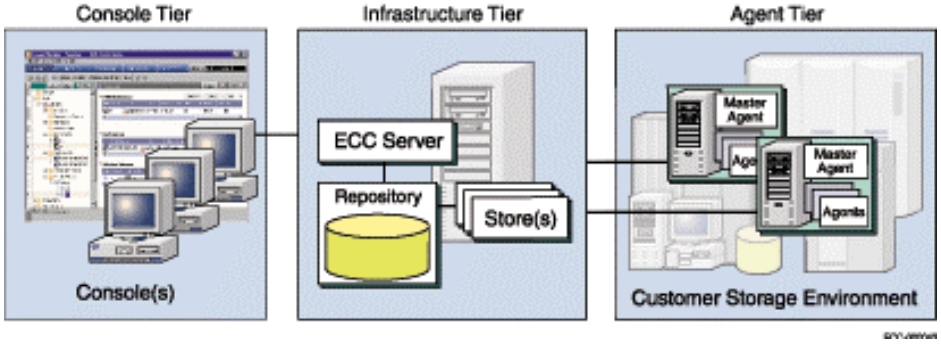
Related topics

- ControlCenter architecture
- ControlCenter agents
- Introduction to alerts

ControlCenter architecture

ControlCenter encompasses diverse areas such as communication between system components, data security, and storing and retrieving data. ControlCenter uses a central repository, distributed process, alert and event management, and reporting to achieve its mission.

ControlCenter has a three-tier architecture; Hosts at each tier run different ControlCenter components that perform specific roles. Click your area of interest in the figure below to get more information about that area.



Related topics

- What's new in ControlCenter
- ControlCenter agents
- Introduction to alerts

ControlCenter agents overview

An agent is a process that runs on a host and manages the customer's storage environment. Once the agent starts and initializes, it is constantly active, monitoring for configuration changes and alertable conditions, and is always waiting for transactions (pieces of work) to arrive. In addition, the agent publishes data to the store/server on periodic/as needed basis.

There are seven categories of agents.

- Common agents
- Storage agents
- Host agents
- Connectivity agents
- Database agents
- Backup Agent for TSM
- Tape agents

Common agents

Common agents must be present on a host to allow other agents or operations to function that are supported by that common agent.

- Master Agent
- Integration Gateway
- WLA Archiver

Storage agents

- Storage Agent for Symmetrix
- Storage Agent for CLARiiON
- Storage Agent for Celerra
- Storage Agent for Compaq StorageWorks
- Storage Agent for HDS
- Storage Agent for IBM ESS
- Storage Agent for RVA/SVA

Host agents

- Host Agent for Windows
- Host Agent for Solaris
- Host Agent for AIX
- Host Agent for HP-UX
- Host Agent for Novell
- Host Agent for MVS HSM
- Host Agent for MVS SMS
- Physical Agent for MVS
- Logical Agent for MVS

Connectivity agents

- Connectivity Agent for SDM
- Connectivity Agent for SNMP
- Connectivity Agent for Switches

Database agents

- Database Agent for Oracle
- Database Agent for DB2

Backup Agent for TSM

- Backup Agent for TSM

Tape agents

- Tape Agent for MVS

Related topics

- What's new in ControlCenter V5.0
- ControlCenter architecture
- ControlCenter alerts

Master Agent overview

The Master Agent must reside on each host running other agents and performs the following functions:

- Controls the installation, starting, and stopping of other agents on the host
- Serves as a single communication gateway/proxy for the agents
- Monitors agents' status
- Manages remote software distribution

All incoming commands and responses sent to or from the Master Agent are saved in a memory queue before they are processed.

Related topics

- Master Agent administration

Backup Agent for TSM overview

Overview Links

The Backup Agent for TSM allows you to monitor your TSM backup systems, looking for events, such as failed backups and increasing space utilization.

In managing your backup systems, four important areas are vital resources to be managed:

- Clientsthe machines with the data to be backed up
- Serversthe software, databases, and logs used for backups and restores
- Storagethe storage pools and volumes that hold the backups
- Policiesthe rules that govern the relationships between client files and the storage on which they are backed up

The Backup Agent for TSM helps you manage these four types of resources. You can ensure that your backups are completing. You can ensure that the TSM database and recovery logs are in optimal condition. You can ensure that storage is used efficiently and that clients backups remain within reasonable size limitations. You can monitor client licenses and invalid logons.

Ensuring backup completion

You can monitor backups and search logs to ensure backups are completing.

- Checking backup status
- Monitoring backups with alerts
- Viewing active processes
- Listing previous processes

Configuring backup policies, classes, and schedules

You can configure the objects that define what is backed up and when.

- Creating and editing classes and policies
- Creating and editing backup schedules
- Specifying included and excluded files
- Specifying storage units

Managing backup nodes

You can manage client systems whose backups are performed by the TSM server.

- Enforcing client storage limits
- Viewing client backup configuration
- Monitoring client licenses
- Adding a client or node to the backup server

Managing backup storage pools and volumes

You can manage the storage used for backups.

- Finding out about volume access problems
- Quantifying backup space use
- Adding capacity

Configuring and monitoring backup databases and logs

You can manage the critical databases and logs that TSM servers use to perform backups and restores.

- Monitoring databases and recovery logs for space problems
- Monitoring database performance
- Increasing database capacity
- Decreasing database capacity

Searching for files

- You can list backed up files for a node.

Related topics

- ControlCenter agents overview
- Backup Agent for TSM administration
- Starting and stopping agents

Connectivity Agent for SDM overview

The Connectivity Agent for Storage Device Masking (SDM Agent) monitors volume-access control information for Symmetrix systems. This agent allows you to regulate which host HBAs in a Fibre Channel environment can access specific Symmetrix volumes.

There are no user-defined alerts associated with the SDM Agent.

Related topics

- Connectivity Agent for SDM administration
- Connectivity Agent for SDM data collection policy
- Installing and configuring agents
- ControlCenter agents overview
- Topology discovery
- Discovery and monitoring requirements

Connectivity Agent for SNMP overview

The Connectivity Agent for SNMP allows you to discover and then monitor the connectivity devices in the SAN through the Simple Network Management Protocol. For example, when a configuration change occurs to a switch or hub, or when a known device cannot be detected, the Connectivity Agent for SNMP generates an alert to the Console. Alerts for this agent trigger automatically and do not have to be configured.

The Connectivity Agent for SNMP allows you to monitor the following types of information:

- Connectivity devices configured in the SAN
- Configuration and status changes to devices and their ports
- Device name changes
- System URLs to launch the device management software

Note: The Connectivity Agent for SNMP finds connectivity devices, including switches, in the SAN. To further discover switch topology information, you must perform switch discovery through the Search for Connectivity Devices dialog box. See Topology discovery.

Related topics

- Connectivity Agent for SNMP administration
- Connectivity Agent for SNMP data collection policies
- Connectivity Agent for SNMP alerts
- Installing and configuring agents
- ControlCenter agents overview
- Topology discovery
- Discovery and monitoring requirements

Connectivity Agent for Switches overview

The Connectivity Agent for Switches (Switch Agent) allows you to discover and monitor Fibre Channel switches and fabrics in your SAN. Fabrics are instrumental in partitioning your network into subsets of devices and work groups.

This agent allows you to monitor configuration and status changes for:

- Fibre Channel switches
- Fabrics, including:
  - Links
  - FAs
  - Switch ports
  - HBAs
  - WWNs

There are no user-defined alerts associated with the Switch Agent.

Related topics

- Connectivity Agent for Switches administration
- Connectivity Agent for Switches data collection policies
- Installing and configuring agents
- ControlCenter agents overview
- Topology discovery
- Discovery and monitoring requirements

Integration Gateway overview

The Integration Gateway provides an interface between the ECC Server and management framework applications, such as:

- CA Unicenter TNG
- HP OpenView Network Node Manager
- HP OpenView Vantage Point Operations
- Micromuse Netcool Omnibus
- Tivoli NetView
- Tivoli Enterprise Console

This interface propagates ControlCenter status information to these application event consoles and also appears as an icon for all ControlCenter managed objects. In addition, ControlCenter can be launched by clicking on an object for more active object management.

Note: A generic SNMP interface is available for integration with other management tools.

Related topics

- Integration Gateway administration

Database Agent for DB2 overview

The Database Agent for DB2 helps you explore the logical and physical storage elements of your DB2 subsystems.

Exploring

In the agent, you can explore DB2 resources that affect storage: Databases, table spaces, and tables; application plans and packages; DBRMs; and other DB2 resources. You can explore SQL statements, views, and aliases.

Monitoring

You can set alerts to monitor:

- DB2 storage utilization and trends
- DB2 database integrity
- Reorganization candidates
- Data collection

Running reports

Reports provide you with information about DB2 database and system tables. You can run reports to show:

- space utilization and allocation
- space trends
- history reports
- table space and index data sets

as well as other useful reports.

Running DB2 utilities

The agent allows you to execute DB2 utilities directly from the console, instead of having to submit a JCL job. Job results are returned directly to the console.

The agent uses a program called the *detector* that collects statistics on DB2's storage constructs and performance. You schedule when and how often the detector runs.

Summary

The Database Agent for DB2 allows you to:

- Manage physical database structures such as tablespaces, indexes, and their data sets
- Explore collections, databases, DBRMs, packages, and stored procedures
- Monitor space use and growth trends for tables, tablespaces, indexes, databases, and stogroups
- Create reports on most types of database objects

Related topics

- Database Agent for DB2 administration

Database Agent for Oracle overview

The Database Agent for Oracle runs on a host in the network and is responsible for:

- Provides local services or calls operating-system dependent services to interact locally with the host managed objects
- Accepts jobs or events from the ECC Server
- Runs Console jobs, collecting the results and output, and queues the results as required
- Checks for events, and queues the resulting event reports for the Console
- Cancels jobs or events as directed by the Console
- Handles Integration Gateway requests

A single Oracle Agent supports all the databases installed on one machine.

Related topics

- Database Agent for Oracle administration
- Database Agent for Oracle Environment alerts
- Database Agent for Oracle Space alerts
- Responding to Database Agent for Oracle Environment alerts
- Responding to Database Agent for Oracle Space alerts
- Database Agent for Oracle data collection policies

Host Agents for AIX, HP-UX, and Solaris overview

The Host Agents for AIX, HP-UX, and Solaris are local software components of ControlCenter that enable you to effectively manage UNIX storage hosts. In addition to providing shortcuts for most system management tasks, the agents pro-actively monitor your systems, looking for storage issues that you define as significant, and alerting you with detailed information so you can take corrective action. For more information about alerts, see UNIX: Monitoring hosts.

The agents can help you manage the following aspects of your AIX, HP-UX, and Solaris hosts:

- Operating systems
- File systems
- Logical volumes
- Physical volumes
- Volume groups
- Files and directories
- Processes
- Page spaces
- Storage devices
- Users and groups
- Space usage quotas

Starting points

- Administering UNIX hosts
- Monitoring Solaris, HP-UX, and AIX hosts
- Generating historical reports for UNIX hosts

Related alerts

- Solaris: VERITAS Disk Group Free Space alerts
- UNIX: Disk Space Free on a File System alert
- UNIX: Disk Space Percent Free on the File System alert
- UNIX: File and Directory Size alert
- UNIX: Hard Quotas: Free Disk Space or Files alerts
- UNIX: Inodes (files) Free on the File System alert
- UNIX: Soft Quotas: Free Disk Space or Files alerts
- UNIX: Swap Space Megabytes Free alert
- UNIX: Swap Space Percent Free alert
- UNIX: Volume Group Free Space alerts

Related topics

- Host Agents for AIX, HP-UX, and Solaris administration
- Installing agents
- ControlCenter agents overview
- Checking agent status
- How the UNIX Host Agents operate
- How open systems agents handle security
- Agent Inactive alert
- UNIX: Troubleshooting the UNIX Host Agents
- Generating historical reports for UNIX hosts
- Exploring host storage

Host Agent for MVS HSM overview

Host Agent for MVS HSM provides a complementary set of functions to aid you in using DFSMShsm, IBM's Hierarchical Storage Management technology on OS/390 servers.

MVS HSM allows you to:

- Evaluate migration and recall history
- List data sets migrated to tape
- List non-SMS managed data sets
- Search for specific HSM messages
- View information about ML1 and ML2 data sets
- Configure automation and backup rules for common HSM messages

MVS HSM must be installed and run on each logical partition of an OS/390 environment on which you use DFSMShsm to monitor all HSM activity. If you have a sysplex environment, the same rules apply.

Related topics

- Installing and configuring agents
- Host Agent for MVS HSM administration

Host Agent for MVS SMS overview

The Host Agent for MVS SMS allows you to retrieve current information on your DFSMS configuration for "at a glance" viewing. The agent also allows you to:

- Add volumes to an SMS-managed storage group
- Change the SMS status of a storage group
- Delete and drain volumes
- List datasets in a storage group
- Monitor storage group occupancy
- Monitor volume occupancy
- View SMS CDSs

You can also use the Host Agent for MVS SMS to do the following:

- Generate reports about storage and volume occupancy.
- Monitor dataset fragmentation.
- Create alerts to notify you when a storage group is getting full.
- Add an already-initialized volume to an SMS-managed storage group.
- Browse Automatic Class Selection (ACS) runtime source code from the Management Console.
- Drain and delete SMS-managed volumes.
- View the status of up to 32 systems and system group names in reports.

Related topics

- Installing and configuring agents
- Host Agent for MVS SMS administration

Host Agent for Novell overview

The Host Agent for Novell is a local software component of ControlCenter that enables you to effectively manage your Novell NetWare 4.x and 5.x servers. In addition to providing shortcuts for many system management tasks, the agent pro-actively monitors your NetWare servers, looking for storage issues that you define as significant and alerting you with detailed information so you can take corrective action. For more information about alerts, see Monitoring NetWare servers and file systems.

The agent can help you manage the following aspects of your Novell storage systems:

- NetWare 4.x and 5.x servers
- Volumes
- Directories
- Files
- NetWare Load Modules (NLM)
- Users and user space restrictions

Starting points

- Administering NetWare servers and file systems
- Monitoring NetWare servers and file systems (Alerts)

Related alerts

- Novell: Deleted File Space Threshold alert
- Novell: Large File alert
- Novell: Space Usage alert
- Novell: User Quota alert
- Novell: Volume % Free Space alert
- Novell: Volume Free Space alert

Related topics

- Host Agent for Novell administration
- How the Host Agent for Novell operates
- Checking the status of the Host Agent for Novell
- Agent Inactive alert
- Troubleshooting the Host Agent for Novell
- Authenticating on your Novell network
- Installing agents
- ControlCenter agents overview

Host Agent for Windows overview

The Host Agent for Windows enables you to effectively manage Windows NT and Windows 2000 systems. In addition to providing short cuts for most system management tasks, the agent proactively monitors your systems, looking for storage issues that you define as significant and alerting you with detailed information so you can quickly correct problems.

The agent can help you manage the following aspects of your Windows NT and Windows 2000 systems:

- Event logs
- Volumes
- Operating system
- Printers
- Processes
- Quotas
- Services
- Storage devices
- Users and groups

Event log management

- Browse event logs. This function removes the Windows NT and Windows 2000 restriction that you must be an Administrator on the remote machine whose logs you want to view.
- View the details of any event logged.
- Back up and clear the system, application, and security logs.
- Create alerts to notify you when the system logs specific events or when the system logs an event containing a specific text string.
- Create an alert to notify you when the size of an event log exceeds some threshold you define. This alert also includes an optional autofix that clears and optionally backs up the event log when the alert is triggered.
- Create alerts to notify you when events such as backing up or clearing an event log occur.

For more information, see Managing event logs, Monitoring event logs.

Volume management

- Explore Windows volumes and view important statistics on files and directories.
- Search for files or directories based on attributes such as name, size, owner, date, and other attributes.
- Monitor file I/O to see which users and processes are accessing a particular file or directory and at what times.
- View all the open files on a system and the processes that opened them.
- Compress or uncompress file systems, files, and directories on NTFS partitions.
- Move, remove, copy, and delete files and directories.
- Create new directories.
- View and change security attributes on NTFS partitions, including taking ownership of files.
- Control whether file systems or directories are shared with other network resources.
- View the contents of and empty the Recycle Bin.
- Receive notification when users install new software or change attributes of critical files through an alert that warns you when any attribute of a directory is changed, including all of the directory's files and subdirectories.
- Create alerts to monitor the size of files and directories.
- Map or disconnect network drives.

For more information, see Managing volumes, Monitoring volumes, Managing files and folders, Monitoring files and folders.

Operating system management

- Take snapshots of system, server, memory, paging file, and cache statistics to help diagnose performance problems.
- Schedule the recording of system statistics, enabling you to compile the trending information necessary for accurate capacity planning and system tuning.
- Identify which users are currently logged on to a Windows host.
- Monitor memory use by creating an alert to detect and alert you about memory bottlenecks.
- Receive notification when a paging file is not big enough to handle the hard pages occurring on a system.
- Identify when a system's processor is overloaded, based on an alert that monitors the processor's queue length.
- See which other systems are visible to a Windows host.

For more information, see Managing the Windows operating system, Monitoring performance.

Printer management

- Explore the printers defined on a system and view detailed properties.
- Start and stop printers and clear printer queues.
- View the details of specific print jobs and cancel, pause, or resume them.
- Create alerts to monitor printer changes to local printers, such as modifications to printer properties, jobs, ports, or drivers.

Fore more information, see Managing printers, Monitoring printers.

Process management

- Explore process statistics in a hierarchical tree that defines process relationships.
- Set process priorities.
- Stop processes.
- Create an alert to notify you when a process is either active or inactive.
- Take a snapshot of process statistics to help identify the source of performance problems.
- Schedule the recording of process information, enabling you to compile the trending information necessary to diagnose performance bottlenecks and tune system performance.
- View the shared libraries that a process currently has open.
- View the handles opened by a process.

For more information, see Managing processes, Monitoring processes.

Quota management

- Explore quota information for each volume on a system, including quota use, limits, and thresholds and account status.
- Display and set default volume quotas and states.
- Add and delete quota entries for users on a particular volume.
- Display, set, or modify user quota values on a particular volume.
- Create new user quota settings by copying the settings of an existing user.

Fore more information, see Managing quotas.

Service management

- View status information and other attributes for all services installed on a system.
- Start, stop, and alter the startup properties for services.
- Remove services from the Service Control Manager Database.
- Create an alert to warn you when a service is inactive and optionally attach an autofix to automatically restart the service.

For more information, see Managing services, Monitoring services.

Storage device management

- Explore storage device statistics, including viewing the partition table for the devices that support them. This can help you identify unused or misused space.
- Schedule recordings of storage device statistics, giving you the trending information you need to predict future storage needs.
- Identify current storage device problems by taking a snapshot of real-time storage device statistics.
- Monitor space use on a partition through an alert.
- Create an alert to warn you when physical disk bottlenecks are occurring, based on thresholds you define.
- Create an alert to identify when a storage device is exceeding a specified growth rate.

For more information, see Managing physical disks, Monitoring disk performance.

User and group management

- Explore group and user attributes.
- On Windows 2000 systems, display user quota allotments and use.

For more information, see Managing users and groups.

Related topics

- Host Agent for Windows administration
- Troubleshooting the Host Agent for Windows
- What's new in ControlCenter 5.0

Logical Agent for MVS overview

The Logical Agent for MVS monitors, generates reports, and automates activities affecting cataloged data throughout the OS/390 and MVS/ESA systems across your enterprise. The agent analyzes the condition of your catalogs, critical data sets, and allocation characteristics to provide a real-time view of all your data.

The agent:

Simplifies many routine maintenance tasks such as creating aliases and searching for, renaming, deleting, examining, and diagnosing data sets and catalogs. You can easily navigate data structures such as user catalogs, VTOCs, and VVDSs throughout your enterprise and monitor the logical interrelationships among these structures, all without using JCL. Additionally, the agent maps OS/390 UNIX System Services hierarchical file systems (HFSs) to reduce the effort of working with these data.

Prevents crisis situations from occurring. The agent detects potential logical storage management issues, and then alerts you to those requiring your attention, relaying the severity of the problem. You can define metrics that reflect your own management policies, directing the agent to scan volumes, catalogs, and storage groups at intervals you define. This way you can anticipate problems and proactively plan for them.

Enables you to monitor and manage your catalogs. Know exact relationships between catalogs, data sets, and aliases, or create new relationships. You can perform maintenance, run diagnostics, create reports, and carry out backup and recovery operations.

Helps you investigate space activity, allocation, and use. Alerts inform you when space activity increases for individual users and when space is allocated but not used. Space activity reports allow you to track down user IDs and jobs consuming space at a rapid rate. Space use reports let you define your applications to the agent for repeated use in generating reports. You can then compare space allocation and use among multiple applications.

Related topics

- Logical Agent for MVS administration
- Logical: Basic Setup
- Logical: Creating application IDs
- Logical: Defining new aliases
- Logical: Exploring MVS data sets
- Logical: Exploring OpenEdition files
- Logical: Generating reports
- Logical: Listing aliases in an MVS catalog
- Logical: Listing specific MVS data sets
- Logical: Running application space usage reports
- Logical: Using the CSL Scan utility
- Installing and configuring agents

Physical Agent for MVS overview

The Physical Agent for MVS allows you to:

- Create, delete, edit, and rename user volume groups
- Initialize volumes
- Search for data sets
- Vary volumes offline and online

In addition, Physical Agent includes alerts, so you can proactively track physical storage problems on MVS hosts. Physical Agent must be installed and run on each host in your data center. If you have a sysplex configuration, each host must have the agent installed and configured to run on it, too.

Related topics

- Physical Agent for MVS administration
- Updating MVS agent configuration
- Physical Agent for MVS: data collection policy

Storage Agent for Celerra overview

The Storage Agent for Celerra detects and monitors Celerra file servers status and performs the following:

- Continuously monitors the status of a single or multiple Celerra file servers
- Poll the Celerra file server status on the polling frequency set by the data collections policies of the ECC Server
- Uploads any Celerra file server status changes to the database

Right-click the Celerra file server object on the console tree to launch the Celerra File Server Manager.

Related topics

- Storage Agent for Celerra administration
- Storage Agent for Celerra alert
- Responding to the Storage Agent for Celerra alert
- Storage Agent for Celerra data collection policies

Storage Agent for CLARiiON overview

The Storage Agent for CLARiiON offers the user the ability to explore and view various components of their FC4700 storage system and its storage processors. It also provides displays of properties and statistics related to these components. The alert feature provides notification of free space utilization and storage array faults.

The EMC Fibre Channel FC4700 disk-array storage systems provide terabytes of disk-storage capacity, high transfer rates, flexible configurations, and highly available data at low cost.

A Fibre Channel storage system has three main components:

- Server component (host bus adapter driver package with adapter and software)
- Interconnect components (cables based on Fibre Channel standards, and optional switches)
- Storage components (storage system with Fibre Channel disks, storage processors (SPs), and power supply and cooling hardware)

You can use a storage system the following installation types:

- Unshared direct with one server is the simplest and least costly.
- Shared or clustered direct lets servers share storage resources with high availability.
- Shared switched, with one or two switch fabrics, lets multiple servers share the resources of several storage systems in a Storage Area Network (SAN). Shared switched installations are available in high-availability versions (multiple host bus adapters (HBAs) per server) or with one HBA per server.

Storage systems for any shared installation require EMC Access Logix software to control server access to the storage system LUNs. Using a storage system management utility, you combine LUNs into storage groups and connect each server to one storage group. A server can access only the LUNs in its storage group.

The storage system uses RAID (redundant array of independent disks) technology. RAID technology groups separate disks into one group, called a RAID Group on the FC4700, to improve reliability and/or performance.

The storage system supports five RAID levels and two other disk configurations, the individual unit and the hot spare (global spare). Using a storage system management utility, you create one or more RAID Groups and bind one or more LUNs on each RAID Group.

Navisphere products have two parts: a graphical user interface (GUI) and two agent types. The GUIs run on a management station, accessible from a common framework, and communicate with the FC4700 storage systems through an SP Agent application that runs on each SP in the storage system. Each FC4700 SP ships with the SP Agent already installed. A host agent runs on the server and communicates with the FC4700 storage system.

Navisphere CLI is optional software that ships with the host agent.

Related topics

- CLARiiON: Exploring storage processors
- CLARiiON: Exploring disks
- CLARiiON: Exploring RAID groups
- CLARiiON: Exploring LUNs
- CLARiiON: Exploring storage groups
- CLARiiON: Exploring software packages
- CLARiiON: Exploring SnapView
- Installing and configuring agents
- CLARiiON Agent administration
- CLARiiON: RAID Group Free Space alert
- CLARiiON: RAID Group Percent Free Space alert
- CLARiiON: Storage Array Fault alert

Storage Agent for Compaq StorageWorks overview

The Storage Agent for Compaq StorageWorks allows you to explore and monitor the configuration of StorageWorks subsystems. You explore a Compaq storage array through a Windows NT or Windows 2000 host that is connected to one or more arrays.

Exploring subsystem configuration

The agent provides access to the following configuration information:

- Subsystemsuch as the serial and model numbers and the count and type of disks
- Controllerincluding battery and cache status and port and terminal configurations
- Storagesetsuch as RAID configurations and devices assigned
- Remote copy sets
- Connections
- Units
- Spare and failed sets

In addition to manual exploration, the agent provides a data collection policy that collects subsystem configuration information automatically each day. The agent logs general information about the subsystem and unit information.

Monitoring the subsystem

The agent also provides alerts to help you monitor the following aspects of your storage subsystem:

- Controller cache battery life
- Unmapped devices
- Device counts for storagesets
- Device counts for the spare and failed sets

For more information, see the related topics below.

Related topics

- StorageWorks: Exploring subsystem configuration
- StorageWorks: Exploring storagesets
- StorageWorks: Monitoring subsystems
- StorageWorks: Monitoring storageset device counts
- Storage Agent for Compaq StorageWorks data collection policies
- Storage Agent for Compaq StorageWorks administration
- ControlCenter agents overview

Storage Agent for HDS overview

This Storage Agent for HDS enables you to perform operations on the disk array by issuing commands from the server host machine to the disk array subsystem. The software interfaces with the control software RAID Manager on the server host which communicates with the server on the subsystem.

RAID Manager utilities enable you to issue commands. These commands can be issued from the command line or built into a script. You can set up and execute many commands within a short period of time by using RAID Manager scripting. RAID Manager supports Business Copy (BC) to make the paired disks on one subsystem, or Continuous Access (CA) to make the paired disks cross multiple subsystems.

Note: Currently, Storage Agent for HDS supports BC only.

RAID Manager software allows you to create and maintain remote copies of the data stored on a local disk array. The copies can be stored on the same disk array (BC), another local disk array (CA), or a remote disk array (CA). This is useful for data duplication, backup, and disaster recovery purposes. RAID Manager displays subsystem processing information and allows you to perform operations through either the command line or a host script or batch file. The subsystem allows you to maintain up to nine internal copies of open system logical devices (LDEVs) on the disk array. These copies can be used for data backup, data duplication, or testing.

Related topics

- HDS: Exploring HDS/XP Agent
- HDS: Exploring BC volumes
- HDS: Exploring physical host devices
- HDS: Exploring physical ports
- HDS: Exploring physical subsystem devices
- HDS: Exploring volumes
- Installing and configuring agents
- Storage Agent for HDS administration
- ControlCenter agents overview
- Storage Agent for HDS data collection policies

Storage Agent for IBM ESS overview

The Storage Agent for IBM ESS enables you to monitor, from within ControlCenter, your IBM ESS system, including its subsystems, volumes, devices, and caching activity. The agent monitors backup performance and job failure issues that you define as significant, and alerts you with detailed information so you can take corrective action.

If a system error occurs, the Storage Agent for IBM ESS alerts notify you of the problem, while the IBM ESS system uses its call home feature to notify IBM technical support. When an alert triggers, right-click it and select **View alert Help** for information about the alert and how to respond to it.

Related topics

- Storage Agent for IBM ESS administration
- IBM ESS: Exploring the system
- IBM ESS: Viewing cache summary reports
- IBM ESS: Viewing detailed cache reports
- IBM ESS: Viewing status reports
- IBM ESS: Viewing system configuration and status reports
- IBM ESS: Exploring MVS volumes
- IBM ESS: Checking volumes for pinned tracks
- IBM ESS Data Collection policy
- Installing and configuring agents
- Starting and stopping agents
- ControlCenter agents overview

Storage Agent for RVA/SVA overview

Overview Links

Virtual storage disk subsystems have unique storage management needs. The IBM RAMAC Virtual Array (RVA) and the StorageTek Shared Virtual Array (SVA) each use virtual storage, which means that the logical entities as seen by MVS hosts do not map directly to the actual physical drives on which they reside in the RVA or SVA. Management of both logical and physical resources is essential to the success of RVA and SVA subsystems.

The Storage Agent for RVA/SVA shows you both types of resources. The agent allows you to test physical drives and to move them between different stages of availability, from spare status to accessibility by MVS hosts. The agent also allows you to configure MVS devices on the RVA or SVA and to modify them as needed. The agent makes both logical and physical configuration changes fast and convenient, even in difficult situations.

Because RVA and SVA subsystems compress all stored data, the concept of capacity has different implications. Their apparent storage capacity (in terms of files and databases stored) is far greater than the physical storage would seem to permit. Yet compression is unpredictable for different data types, and monitoring the actual physical capacity of the subsystems is critical to ensuring their performance and availability. The Storage Agent for RVA/SVA monitors Net Capacity Load, the key vital sign of capacity on the subsystem, and informs you as capacity approaches undesirable or dangerous limits.

The agent becomes even more useful when you set alerts for key events. You do not need to wait until problems cause a visible impact in your host systems' operations. Rather, you respond to pro-active alerts that come straight to a single window on your Windows display.

For example, the Storage Agent for RVA/SVA alerts you when:

- Net Capacity Load grows at an excessive rate.
- Space recovery measures are inadequate and MVS hosts are not properly informing the subsystem to recover data.
- The agent discovers a disabled MVS device.
- Communication channel interfaces from the RVA or SVA subsystem become disabled.

These and other alerts warn you of operational inefficiencies and risks to the continuous, robust use of RVA and SVA storage subsystems.

Beyond alerting and monitoring, the agent provides reports and status information to help you

- diagnose problems and irregularities
- make informed decisions about re-configuring storage, optimizing storage use, and purchasing additional hardware

Related topics

- Storage Agent for RVA/SVA administration

Storage Agent for Symmetrix overview

The Storage Agent for Symmetrix is responsible for populating the Symmetrix data for ControlCenter and should be run to view any Symmetrix properties. The agent is an executable that is installed on a host, but monitors and controls associated Symmetrix systems. It gathers real-time data that applies to the Symmetrix as a single unit, as well as to each component within the Symmetrix system. The agent tracks configuration and performance data for:

- Devices
- Ports
- Directors
- Physical drives
- Symmetrix system

The agent generates alerts relating to:

- Symmetrix performance, based on threshold settings
- Overall system and individual component status

The agent also supports operations in the following areas:

Data protection

- SRDF
- TimeFinder
- Management by device groups

Preformance

- Optimizer
- Quality of Service (QoS)

Configuration

- Symmetrix Disk Reallocation (SDR)
- Logical device configuration
- Port flag configuration
- Device type configuration
- Meta device configuration

Related topics

- ControlCenter agents overview
- Storage Agent for Symmetrix administration
- Storage Agent for Symmetrix data collection policies
- Introduction to alerts

Tape Agent for MVS overview

The Tape Agent for MVS is a local software component of ControlCenter that allows you to explore and manage the tape subsystems, both hardware and software, connected to or running on your MVS and OS/390 hosts. You can take a global approach and explore volumes and data sets across multiple devices and management systems, or you can take a component approach and manage the volumes and data sets particular to a specific device or piece of management software. In either case, the agent will help you better administer and understand your tape storage environment and its performance.

The Tape Agent for MVS can help you manage and identify conflicts between the following hardware and software components that you may have in your tape storage environment:

- IBM Removable Media Manager (DFSMSrmm)
- CA-1
- StorageTek Tape Library
- IBM 3494/3495 Tape Library and Virtual Tape Server

Tape Management Systems

IBM Removable Media Manager (DFSMSrmm)

For the DFSMSrmm tape management system, you can:

- Explore, add, modify, and delete data sets
- Explore, add, modify, delete, and count volumes
- Explore, add bins to, and remove bins from locations
- Explore, add, and delete volume record specifications (VRSs)
- Set alerts to monitor for operational problems

For more information and links: Managing the Removable Media Manager (DFSMSrmm)

CA-1

For the CA-1 tape management system, you can:

- Explore and modify the properties of data sets
- Explore, modify, and scratch a volume
- Explore CA-1 control data
- Set alerts to monitor for CA-1 operational problems

For more information and links: Managing CA-1

Tape Libraries

StorageTek Tape Library

For StorageTek tape libraries, you can:

- Explore Automated Cartridge Systems and Library Storage Modules
- Explore volumes, tape drives, Cartridge Access Ports, cells, scratch volumes, and cleaning cartridges
- Ensure sufficient free cells, cleaning cartridges, and scratch volumes
- Monitor ACS and LSM availability
- Manage volumes
- Manage tape drives
- Set alerts to monitor library resources, availability, and operational problems
- Set alerts to monitor mounts requiring operator intervention

For more information and links: Managing StorageTek tape libraries

IBM 3494/3495 Tape Library and Virtual Tape Server

For IBM tape libraries, you can:

- Enable and disable tape storage groups
- Explore tape libraries and VTSs
- Vary tape libraries and VTSs on and offline
- Vary real and virtual tape drives on and offline
- Create reports about VTS

For more information and links: Managing IBM 3494/3495 Tape Library and Virtual Tape Server

Starting points

- Exploring volumes using the Tape Agent for MVS
- Exploring data sets using the Tape Agent for MVS
- Identifying conflicts using the Tape Agent for MVS

Related topics

- Managing the Removable Media Manager (DFSMSrmm)
- Managing CA-1
- Managing StorageTek tape libraries
- Managing IBM 3494/3495 Tape Library and Virtual Tape Server
- Component Unavailable alert
- Installing agents
- ControlCenter agents overview
- MVS Tape Agent administration

WLA Archiver overview

The WLA Archiver processes and stores statistical data collected for Workload Analyzer (WLA) by individual ControlCenter agents.

Data collection policies are assigned to the Storage Agent for Symmetrix to collect Symmetrix statistics; to the Database Agent for Oracle to collect Oracle database statistics; and to host agents to collect host statistics.

As the agents collect statistical data, the data is transferred to the WLA Archiver, which processes and stores the data as performance archives, revolving collections, and analyst collections. The amount of data that is stored by the WLA Archiver is determined by the WLA Retention policy.

There are also alerts associated with the WLA Archiver host and functionality. You can enable/disable these alerts or change the assigned severity levels.

The following alerts are available for the WLA Archiver host and functionality:

- Disk Space Status to inform you when you are running out of disk space
- Archive Errors an error occurred while generating the data collections
- Archive Process Status a data collection has been successfully generated
- Automation Errors an error occurred while processing an automation job

Related Topics

- Installing and configuring agents
- WLA Archiver administration
- Responding to WLA Archiver alerts
- WLA Archiver data collection policy

Getting help with Help

This topic includes information about:

- Using the contents
- Using the index
- Using search
- Printing help topics
- Displaying a topic in a new window
- Docking and undocking
- Adjusting topic window font size
- Getting dialog box help
- Getting view help
- Navigating Help
- Copying Help

Using the contents

Click the Contents tab in the Help Navigator to display the table-of-contents tree.

To browse the tree:

- Double-click a closed book to expand the next lower level of topics and books.
- Double-click an open book to collapse all levels below it.
- Select a book and then select Expand, Expand All, Collapse, or Collapse All from the File menu.

To display a topic from the tree:

- Double-click a topic.
- Select a topic and then click  .
- To display a topic in a new window, select a topic and then click  , or right-click a topic in the tree and select **Display in New Window** from the Context menu.

To print from the tree:

- To print a topic, select the topic and select **Print Topics** from the File Menu.
- To print multiple topics at once, select a book icon and select **Print Topics** from the File menu. All the topics within that book will be printed.
- To print the table-of-contents tree, select Print Tree from the File menu. The tree will be printed in its current state. Only the tree will be printed; the contents of the topics will not be printed.

Note: The table-of-contents tree highlights whichever topic is displayed in the currently selected topic window.

Using the index

Click the Index tab in the Help Navigator to display the keyword index.

To find a topic using the index:

1. In the field at the top, type the first few letters of a keyword for which you want to search. The keyword list scrolls to the relevant keywords as you type. As keywords are selected, one or more topics appear in the topics list.
2. Display a topic from the topics list:
3. Double-click a topic.
4. Select a topic, and then click Open.
5. Select a topic, and then click  .
6. To display a topic in a new window, select a topic, and then click  .

Using search

Click the Search tab in the Help Navigator to display the full-text search.

1. Enter your search criteria and click Search.
2. Type the word or words for which you want to search in the field at the top.
3. Select Case-sensitive to match the case of these words.
4. Select one of the following:
   - Any of these words — displays topics that contain at least one of the search words.
   - All of these words — displays only the topics that contain all of the search words.
   - This boolean expression — uses the search words as a boolean expression. Help recognizes AND, OR, and NOT operators.
   - Matching topics appear in the topics list sorted by relevance — indicated by the following icons:
     — indicates a high level of relevance
     — indicates a medium level of relevance
     — indicates a low level of relevance

     Note: Click Relevance, TopicTitle, or Source to sort the results.
5. To display a topic from the topics list, double-click a topic or select a topic, and then click Open.
6. Select a topic, and then click  .
7. To display a topic in a new window, select a topic, and then click  .

   Note: You can use previous search criteria by selecting the keywords from the drop-down list where you enter the word or words for the search.

Printing help topics

To print from the topic window, click  or choose Print Topic from the File menu.

To print from the Contents:

- To print a topic, select the topic and select **Print Topics** from the File menu.
- To print multiple topics at once, select a book icon and select **Print Topics** from the File Menu. All the topics within that book will print.
- To print the table-of-contents tree, select **Print Tree** from the File menu. The tree will print in its current state.
- Note that only the tree will print; the contents of the topics will not print.

Displaying a topic in a new window

In the Index or Search tabs, select a topic, then click  .

In the Contents tab:

- Select a topic then click  .
- Right-click a topic in the Contents tree and choose Display in New Window from the Context Menu.

Docking and undocking

To undock the Navigator and topic window, click  in the topic window or choose Dock from the topic window's Tools menu. The Navigator connects to the left side of the topic window.

You can move, resize, undock, or close the docked pair.

To undock the Navigator and topic window, click  in the topic window or choose Undock from the topic window's Tools menu. The two panes separate and return to their default positions.

Adjusting topic window font size

To increase the size of the fonts used in a particular topic window, select the window and press the PLUS SIGN on the numeric keypad.

To decrease the size of the fonts used in a particular topic window, select the window and press the MINUS SIGN on the numeric keypad.

Getting dialog box help

To get Help in a dialog box click the Help button.

A topic window with information about that dialog box will display.

Getting view help

To get Help in an information Panel view click the ? icon in the view title bar.

A topic window with information about that view will display.

Navigating Help

As you view different topics in Help, Back and Forward will become available for use.

To view topics that you have already seen, click  in the topic window or choose Back from the topic window's Go menu. The topic window will display the previous topic.

Click  in the topic window or choose Forward from the topics window's Go menu to display the topic from which you just retreated.

Copying Help

To copy information from a Help topic, highlight the information you want to copy and type Ctrl+c.

In the document where you want the information to appear, click the place where you want to put the information and click Paste.

Related topic

- Contacting EMC
- Troubleshooting context-sensitive help

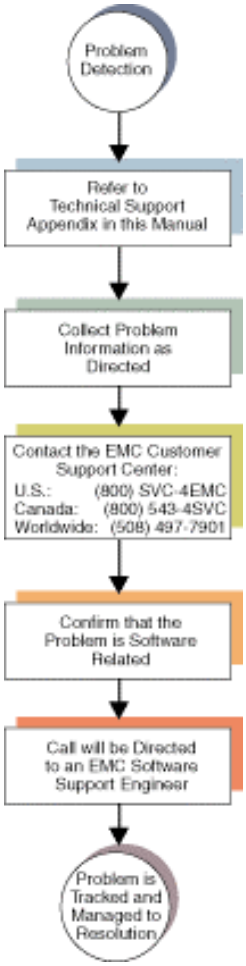
Contacting EMC

This topic reviews the EMC process for detecting and resolving software problems, and provides essential questions that you should answer before contacting the EMC Customer Support Center.

- Overview of detecting and resolving problems
- Troubleshooting the problem
- Before calling the customer support center
- Documenting the problem
- Reporting a new problem
- Sending problem documentation

Overview of detecting and resolving problems

EMC software products are supported directly by the EMC Customer Support Center in the United States. EMC uses this process to resolve customer problems with its software products.



Troubleshooting the problem

Please perform the following diagnostic steps before you contact the EMC Customer Support Center:

1. Read the documentation carefully.
2. Reconstruct the events leading up to the problem and describe them in writing.
3. Run some test cases to reproduce the problem.

If you encounter a problem that requires technical programming or analysis, call the nearest EMC office or contact the EMC Customer Support Center at one of the following numbers:

- United States: (800) 782-4362 (SVC-4EMC)
- Canada: (800) 543-4782 (543-4SVC)
- Worldwide: (508) 497-7901

Please do not request a specific support representative unless one has already been assigned to your particular system problem.

Before calling the customer support center

Have the following information available before calling the Customer Support Center or your support representative (if one has been assigned to you):

- Your company name
- Your name
- Your phone number
- For an existing problem, the problem tracking system ID, if one was previously assigned to the problem by a support representative
- For an MVS problem, the JESLOG, SYSPRINT, all STDOUT DD members of the server job output and similar output for the client, and the relevant portion of the SYSLOG

Documenting the problem

If the EMC Customer Support Center requests information regarding the problem, please document it completely, making sure to include the following information:

- Your company name and address
- Your name
- Your telephone number
- The importance of the problem, so that it can be assigned a priority level

To expedite the processing of your support request, you can photocopy this list and include it with the package.

Reporting a new problem

For a new problem, please provide the following information:

- Release level of the software that you are running
- Software installation parameters
- Host type on which you are running
- Operating system you are running and its release number
- Functions of the software that you are running
- Whether you can reproduce the problem
- Previous occurrences of the problem
- Whether the software has ever worked correctly
- Time period that the software did work properly
- Conditions under which the software worked properly
- Changes to your system between the time the software worked properly and the problem began
- Exact sequence of events that led to the system error
- Message numbers and complete text of any messages that the system produced
- Log file dated near the time the error occurred
- Results from tests that you have run
- Other related system output
- Other information that may help solve the problem

Sending problem documentation

Use one of the following methods to send documentation of the problem to the EMC Customer Support Center:

- E-mail
- FTP
- U.S. mail to the following address:

EMC Customer Support Center

45 South Street

Hopkinton, MA 01748-9103

If the problem was assigned a number or a specific support representative, please include that information in the address as well.

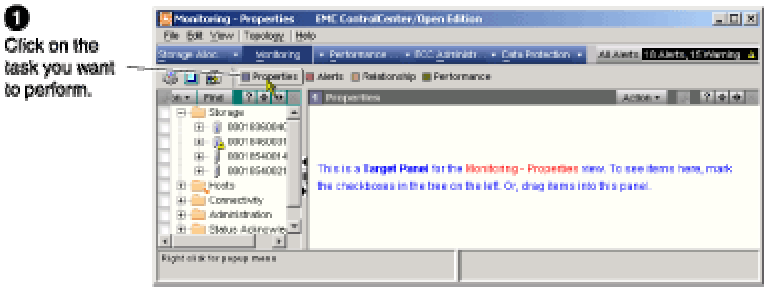
Related topic

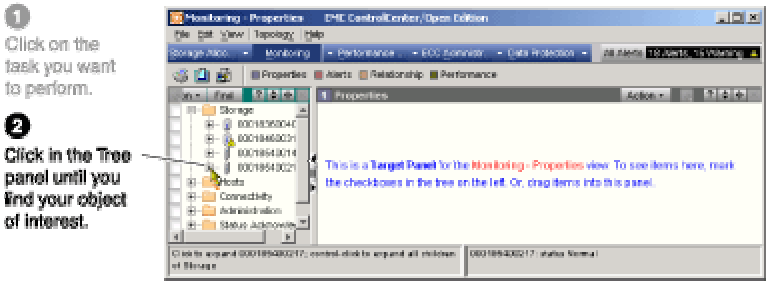
- Getting help with Help
- Troubleshooting context-sensitive help

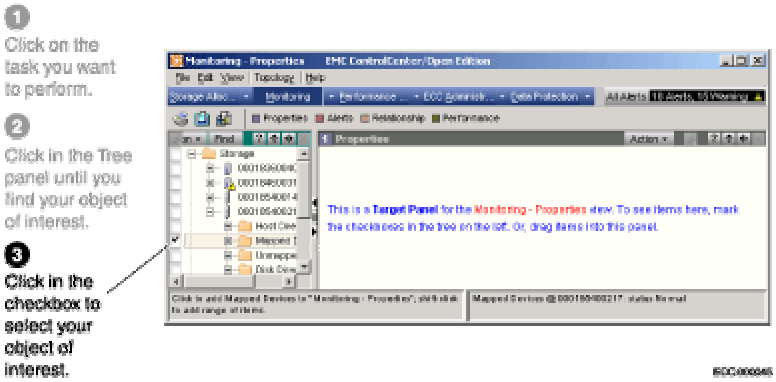
Using the Console

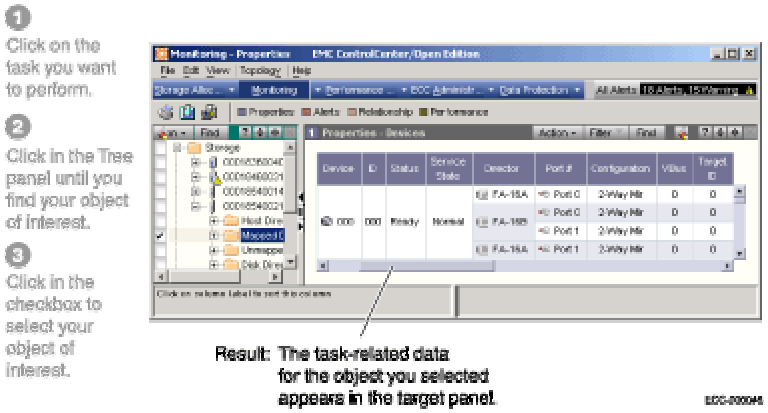
The Console design reflects an attention to detail that promotes task-based user functions. These functions are accessed through Console commands as demonstrated by this example.

Follow the numbered sequence below for a quick introduction to basic console command use.









Related topics

- Using the Console menu bar
- Using the Console task bar
- Using the Console Tree Panel
- Using the Console Target Panel
- Using the Console toolbar
- Understanding ControlCenter icons

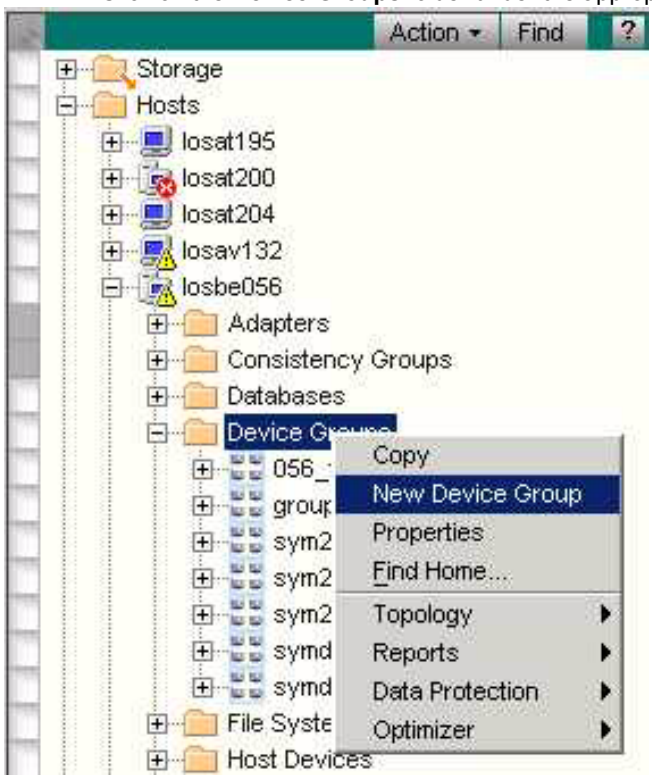
Device group operations

You can create device groups to support operations with multiple devices. In some cases, the devices must be members of groups before certain operations can be performed.

Note: The Symmetrix agent must be running on the host (or proxied to another host) in order to perform these operations. Refer to Proxy Discovery for more information.

Creating a device group

1. Click on the **Device Groups** folder under the appropriate host.



2. From the right-click menu, select **New Device Group**. The following dialog box appears:

3. Specify a name and the type of devices (STD, R1, or R2) for the group.
4. Click **OK**. The new device group is created and added to the tree panel.

Adding a device

Members are added to the folders within the device group by dragging and dropping from the appropriate section of the tree panel.

Note: If a device is inappropriate for a particular folder, ControlCenter will not allow it to be added.

Deleting a device

Select the device group member and then select **Delete Devices from the Group** from the right-click menu.

Renaming a device

Select the device group member and then select **Rename a device from the Group** from the right-click menu.

Deleting a device group

Select the device group and then select **Delete** from the right-click menu.

Renaming a device group

Select the device group and then select **Rename** from the right-click menu.

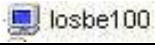
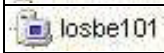
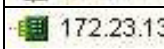
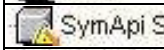
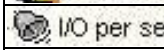
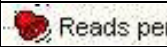
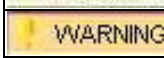
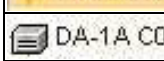
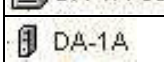
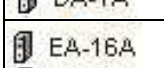
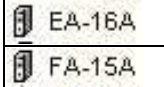
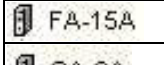
Related topics

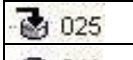
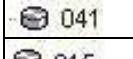
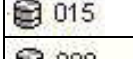
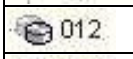
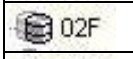
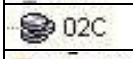
- TimeFinder device group operations
- SRDF device group operations
- SRDF consistency groups
- SRDF concurrency

Understanding ControlCenter icons

The following table describes many of the icons used in EMC ControlCenter.

Icon	Description
	Status indicator for a Fatal or Critical alert. This icon overlays the icon for an object.
	Status indicator for a Warning or Minor alert. This icon overlays the icon for an object.

	Red downward arrow indicates an alert status applies to a nested object
	Objects selected in the tree panel have a checkmark in the left column and are highlighted in tan.
	Symmetrix 4.0 (3330, 5330) Symmetrix 4.8 (3630, 5630) Icon often displayed with Symmetrix ID
	Symmetrix 4.0 (3430, 5430) Symmetrix 4.8 (3830, 5830) Icon often displayed with Symmetrix ID
	Symmetrix 4.0 (3700, 5700) Symmetrix 4.8 (3930, 5930) Icon often displayed with Symmetrix ID
	Symmetrix 5.5 (8230) Icon often displayed with Symmetrix ID
	Symmetrix 5.0 (8730), Symmetrix 5.5 (8830) Icon often displayed with Symmetrix ID
	Symmetrix 5.0 (8430), Symmetrix 5.5 (8530) Icon often displayed with Symmetrix ID
	Symmetrix 5.0 (8130) Icon often displayed with Symmetrix ID
	Host
	Mainframe
	Mainframe Host
	UNIX host with name
	Windows host with name
	Adapter with IP address
	Agent with name
	Agent with name and pending alert
	Alert with name
	Alert with name and triggered threshold
	Alert with fatal status
	Alert with information status
	Alert with warning status
	Disk icon with director number
	Disk director
	ESCON adapter
	Fibre Channel director
	SCSI director

	Remote Link Director used by SRDF
	Symmetrix front end port with number
	TimeFinder and SRDF R1 source volume
	SRDF R1 device
	SRDF R2 device
	Symmetrix logical volume standard (STD) device
	Meta device
	Meta device with members
	Mirrored device
	Mirrored meta device
	DRV device
	Report with name
	Clear selections in the tree panel

Related topics

- Using the Console tree panel

Using the Console menu bar

The Console menu bar displays the most frequently used actions for a selected task.

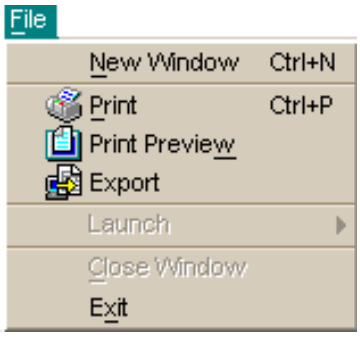
When you use the Console menu bar you will be:

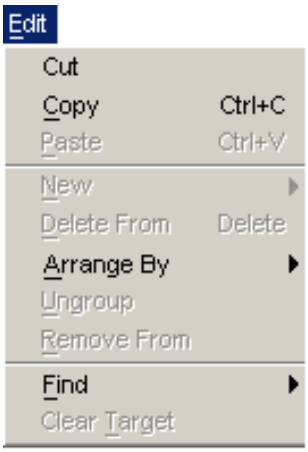
- Selecting menu commands
- Using the Task-associated menu bar

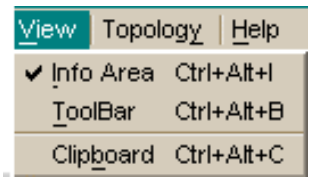
Selecting menu commands

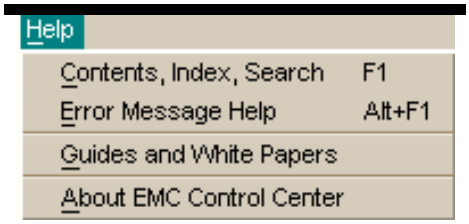
The File, Edit, View, and Help menus are always available on the Console menu bar

Click a menu command for more information about that command.









Using the Task-associated menu bar

When you select a user-task button with a single mouse-click the Console menu bar changes to reveal the menus associated with that task.

The Console menu bar will change and display the relevant commands for the selected user task.

For example, when you select Storage Allocation in the task bar, the Configure menu will displays.

When you select:

- Monitoring the menu item Topology displays.
- Performance Mgt. the menu items QoS and Optimizer display.
- ECC Administration the menu items Topology, Alerts, Repository, Collection, Install, Report Management, Reports, Security, and Agents display.
- Data Protection the menu items Timefinder, SRDF, and QoS display.

This provides quick and easy access to a set of views and actions that are frequently needed to perform the task at hand.

Related Topics

- Using the Console
- Using the Console task bar
- Using the Console Tree Panel
- Using the Console Target Panel
- Using the Console toolbar
- Understanding ControlCenter icons

Using the Console task bar

The Console task bar consists of 5 user-task buttons.

When you use the Console task bar you will be:

- Using the task-associated menu bar
- Using the task menu commands
- Using common commands

Using the task-associated menu bar

When you select a user-task button with a single mouse-click the Console menu bar changes to reveal the menu item(s) associated with that task.

For example, when you select Storage Allocation the menu item Configure displays.

When you select:

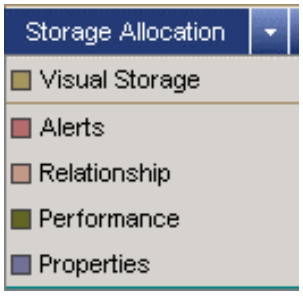
- Monitoring the menu item Topology displays.
- Performance Mgt. the menu items QoS and Optimizer display.
- ECC Administration the menu items Topology, Alerts, Repository, Collection, Install, Report Management, Reports, Security, and Agents display.
- Data Protection the menu items Timefinder, SRDF, and QoS display.

This provides quick and easy access to a set of views and actions that are frequently needed to perform the task at hand.

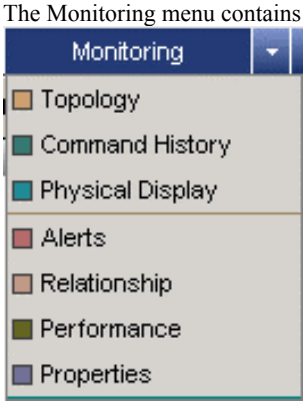
Using the task menu commands

Each user-task button also contains its own menu commands that create read-only views in the target panel.

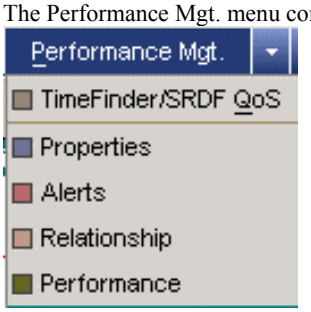
The Storage Allocation menu contains the Visual Storage command.



The Monitoring menu contains the Topology, Command History, and Physical Display commands.

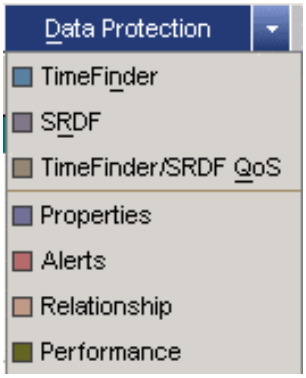


The Performance Mgt. menu contains the TimeFinder/SRDF QoS command.



The ECC Administration menu contains the Authorization, Agents, and Policies commands.

The Data Protection menu contains the TimeFinder, SRDF, and TimeFinder/SRDF QoS commands.



Using common commands

Each user-task menu also contains the following common commands.

- Properties
- Alerts
- Relationship
- Performance

Related Topics

- Using the Console
- Using the Console menu bar
- Using the Console Tree Panel
- Using the Console Target Panel
- Using the Console toolbar
- Understanding ControlCenter icons

Using the Console tree panel

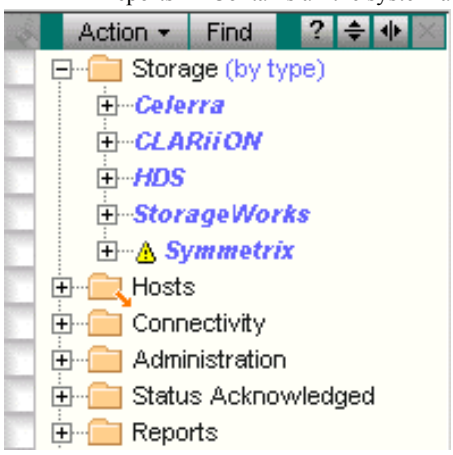
The Console tree panel contains a view of all the managed objects available in the monitored system. When you use the Console tree panel you will be:

- Using the six main tree folders
- Expanding and collapsing tree items
- Checking tree items
- Using common toolbar commands
- Using the Action menu
- Using Find
- Using the right-click menu

Using the six main tree folders

The tree contains the following six main items represented as folders:

- Storage — Contains all the available storage and storage devices visible throughout the network .
- Hosts — Contains all the hosts and host devices available throughout the network.
- Connectivity — Contains all the connectivity devices available throughout the network.
- Administration — Contains all the agent information and data collection policies used throughout the network.
- Status Acknowledged — Contains all the alarmed objects that you have placed here.
- Reports — Contains all the system and user-defined reports for the network.



Creating user-defined groups

You can also create user-defined folders and group object into that folder.

Right-click anywhere in the tree panel and select New. A folder called New Group appears in the tree. You can rename this group and drag-and-drop copies of objects from elsewhere in the tree into this folder to create groups based upon your business needs and practices.

Expanding and collapsing tree items

You can expand or collapse any tree item that has a plus (+) or minus (-) sign next to its icon.

Checking tree items

Using the check boxes

Click in any check box located on the far left side of the tree panel to check any tree item. Click again to un-check that item. Notice that the cursor changes to a checkmark for check-marking and an eraser for un-check-marking.

It is possible to make multiple selections. Click the eraser at the top of the check boxes to un-check multiple selections.

Checking a tree item adds that item to a target panel view.

Using Drag-andDrop

An alternate method to using the check boxes is to click on the object in the tree panel, continue to hold down the mouse button, and 'drag' the object into the target panel. This will also put a check in the check box of that object.

Double-Click

You can also double-click on an object in the tree panel to add that object to the target panel.

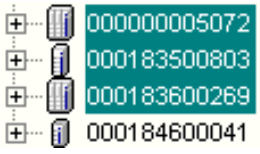
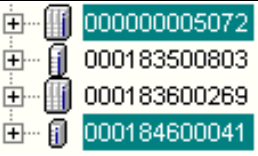
Right-Click

You can also right-click on an object in the tree panel to add that object to the target panel. From the right-click menu choose **Add to View** to add the object to an active target panel view, or choose **Properties** to create a properties view for that object.

Using Highlighting

Click on any tree item to highlight it. Click again to un-highlight it. It is possible to make multiple selections by holding the shift key when clicking to make contiguous selections and by holding the control (Ctrl) key when clicking to make non-contiguous selections.

Highlighting objects in the tree panel when you want to use relevant menu commands to change that object.

	
contiguous selections	non-contiguous selections

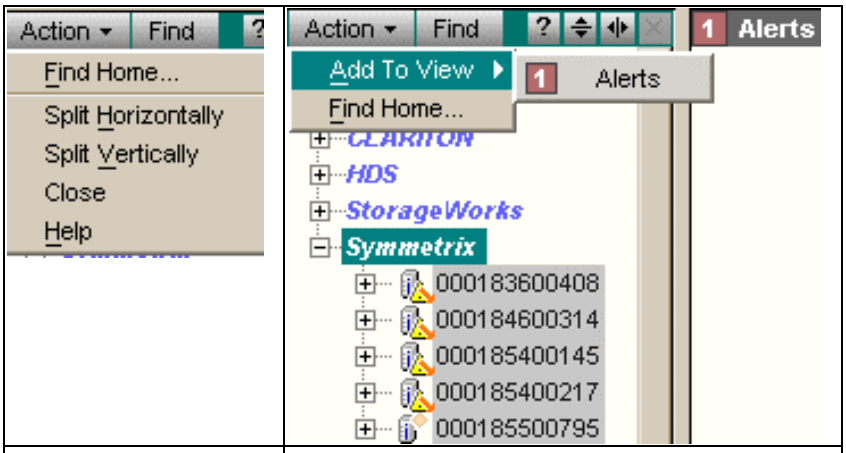
Using common toolbar commands

The following common commands are available in the tree panel.

- Selecting the question mark button (far left) provides access to this help system.
- Selecting the Split horizontally button (middle left) splits the tree panel horizontally.
- Selecting the Split vertically button (middle right) splits the tree panel vertically.
- Selecting the Close panel button (far right) closes the tree panel.
- You can close tree panel views after you have created tree panel views using the split horizontal and vertical buttons. You cannot close the last tree panel view.

Using the Action menu

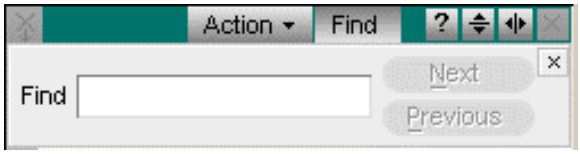
The Action menu is available as a pull-down from the top of the tree panel and changes depending upon which object is highlighted in the tree.



no object highlighted	object highlighted

- Click Add to View to add the highlighted object to the target panel. Notice that the object will be added using the view that the target panel is currently using.
- Click Find Home... to navigate in the tree to the default home location of the object.
- Click Split Horizontally to split the tree panel horizontally.
- Click Split Vertically to split the tree panel vertically.
- Click Close to close the tree panel.
- You can close tree panel views after you have created tree panel views using the split horizontal and vertical buttons. You cannot close the last tree panel view.
- Click Help for access to this help system.

Using Find



Click Find to toggle the Find feature and type in the exact name of the object for which you are searching.

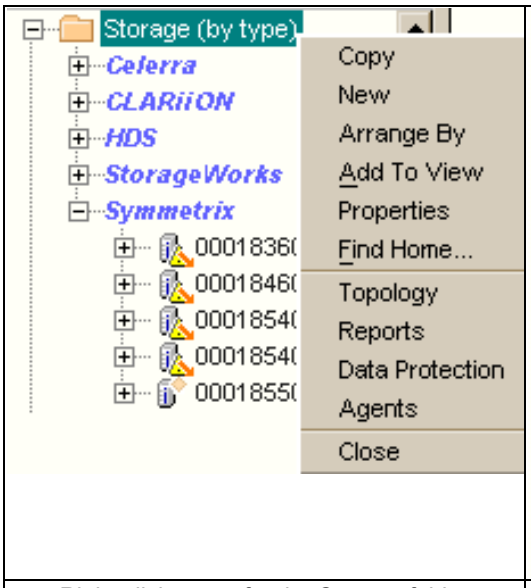
Click Next and Previous to navigate from instance to instance of an object by that name.

Using the right-click menu

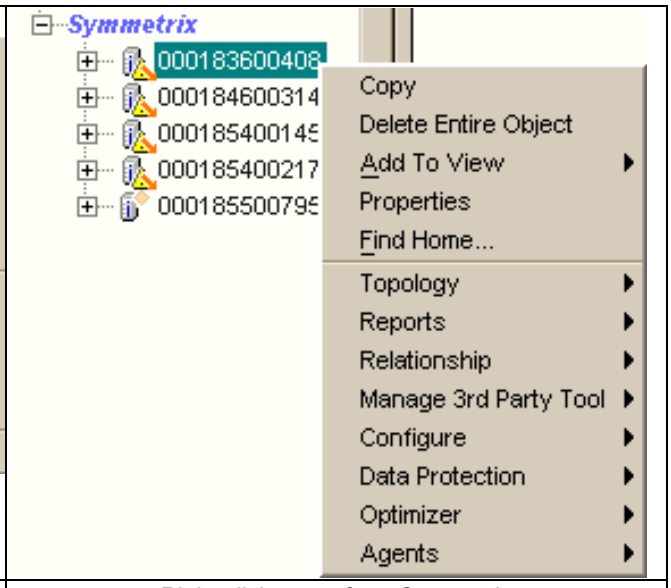
The right-click menu is available for use with any selectable managed object.

The commands visible in the right-click menu vary depending upon what is selected anywhere in the console.

For example, the right-click menu for the Storage folder has fewer commands available than the right-click menu for a Symmetrix.



Right-click menu for the Storage folder



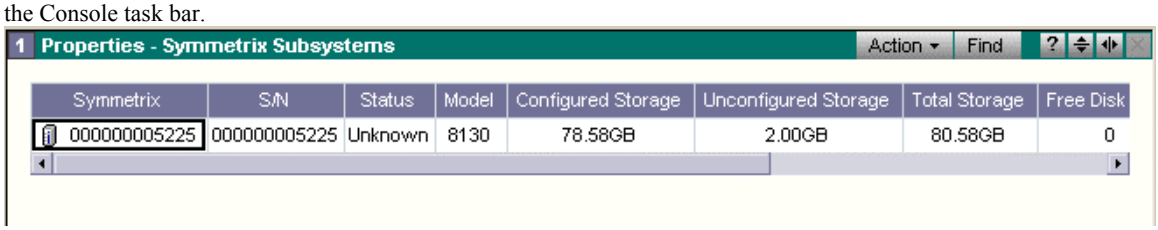
Right-click menu for a Symmetrix

Related topics

- Using the Console
- Using the Console menu bar
- Using the Console task bar
- Using the Console Target Panel
- Using the Console toolbar
- Understanding ControlCenter icons
- Using the Status Acknowledge Folder

Using the Console target panel

The Console target panel changes according to what is checked in the tree panel combined with what view is chosen in the Console task bar.



When you use the Console target panel you will be:

- Using common commands
- Using the Action menu
- Creating table views
- Creating special views
- Using the current view
- Using Find
- Using the right-click menu

Using common commands

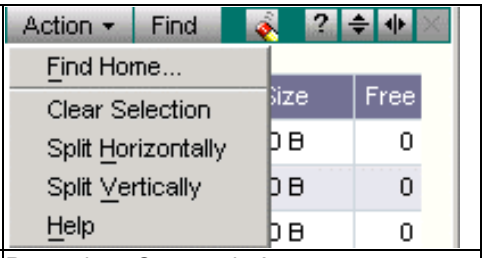
The following commands are common in the target panel views.

- Clicking the question mark button (far left) provides access to help on the active view.
- Selecting the Split horizontally button (middle left) splits the target panel horizontally.
- Selecting the Split vertically button (middle right) splits the target panel vertically.
- Selecting the Close panel button (far right) closes the target panel.
- You can have multiple target panel views in differing modes

Using the Action menu

The Action menu is available as a pull-down from the top of the target panel. The Action menu changes depending upon what is in the target panel.

Empty target panel



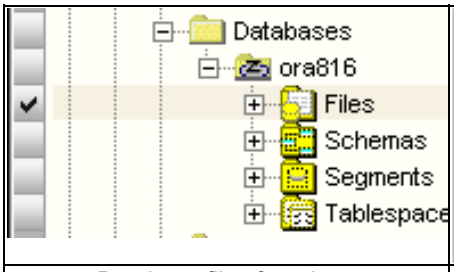
Properties - Symmetrix Arrays

- Click Split Horizontally to split the target panel horizontally.
- Click Split Vertically to split the target panel vertically.
- Click Help for access to this help system.

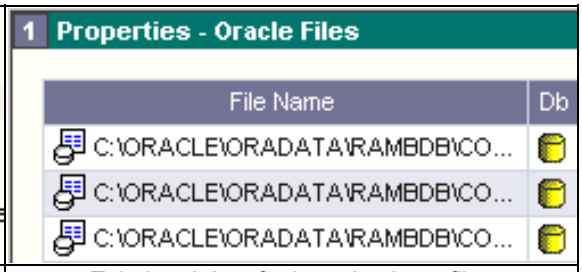
Creating table views

This view enables you to sort ascending/descending any column, filter the table by columns and rows, and change order of columns.

For example, checking the database files for a host in the tree panel and selecting Properties from any task menu generates tabulated properties data for those host database files in the target panel.



Database files for a host



Tabulated data for host database files

Creating special views

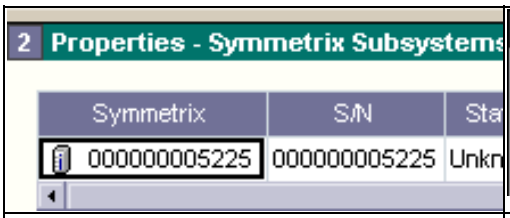
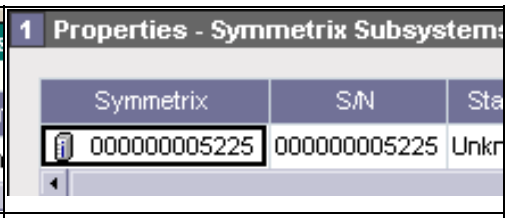
Special views appear for certain tasks.

For example, checking a Symmetrix in the tree panel and selecting Physical Display from the Monitoring menu generates a Symmetrix Front and Rear Views display in the target panel.

Using the current view

If the title bar of a target panel is your system default color and the background is white, this panel is current. This means it will automatically update its contents as you select items in the tree panel. The background of a current panel is white.

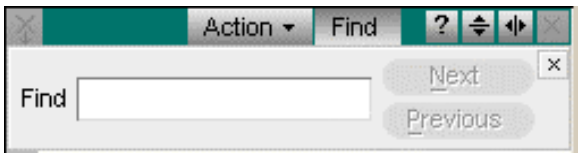
If the title bar and background of a target panel are, gray this panel is not current. Only one panel can be current at a time. A panel that is not current has frozen contents and will not update as you change your check boxes in the tree panel.

	
Current Target Panel	Non-current Target Panel

Using Find

Click Find to toggle the Find feature and type in the exact name of the object for which you are searching.

Click Next and Previous to navigate from instance to instance of an object by that name.

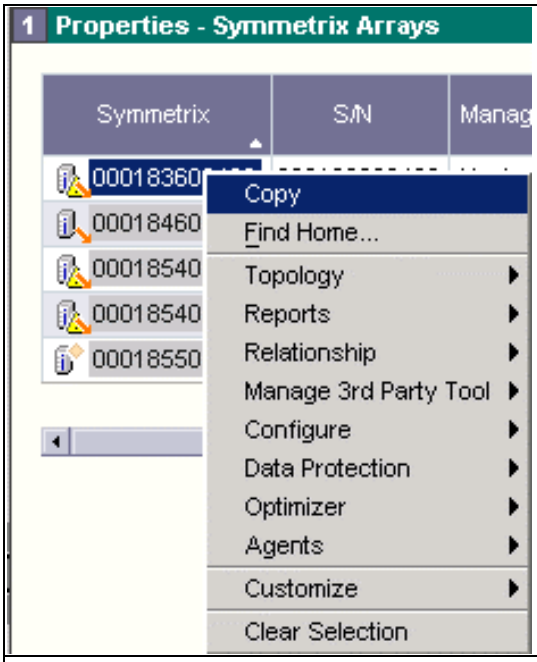


Using the right-click menu

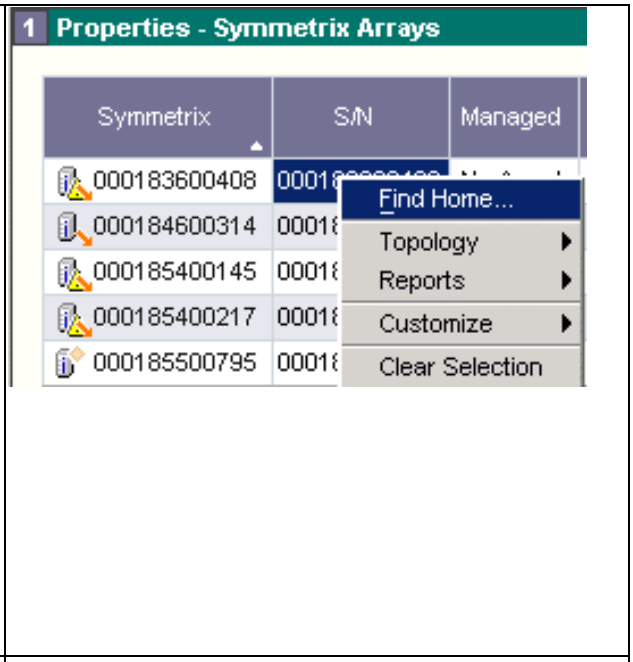
The right click menu is available for use with any selectable target panel item.

The commands visible in the right click menu vary depending upon where you right-click in the target panel.

For example, the right-click menu for Symmetrix in the Properties - Symmetrix Subsystems table has more commands available than the right-click menu for Status in the same table.



Right-click menu for Symmetrix in the Properties - Symmetrix Subsystems table



Right-click menu for Status in the Properties - Symmetrix Subsystems table

Related topics

- Using the Console
- Using the Console menu bar
- Using the Console task bar
- Using the Console Tree Panel
- Using the Console toolbar
- Understanding ControlCenter icons

Using the Console toolbar

The Console toolbar is divided to three areas:

- File menu commands
- Common commands
- Custom commands

File menu commands

The following file menu commands are available on the toolbar: printing, print preview, and export.

These commands are available regardless of which task is selected in the taskbar.

See Using the Console menu bar for more information about the File menu commands.

Common commands

The following common commands are available on the toolbar: Alerts, Relationship, Performance, and Properties. These commands are available regardless of which task is selected in the taskbar.

See Using the Console task bar for more information about the Common commands.

Custom commands

Custom commands change to reflect the task selected in the task bar.

Storage Allocation

With the Storage Allocation task selected on the task bar the following custom commands display.


SRD


Meta Device Configuration

Monitoring

No custom commands are available for the Monitoring task.

Performance Mgt.

With the Performance Mgt. task selected, the Set TimeFinder/SRDF QoS custom command displays.


Set TimeFinder/ SRDF QoS

ECC Administration

With the ECC Administration task selected, these custom commands display.


New Alert


New User


User New Rule

Data Protection

With the Data Protection task selected, these custom commands display.


Establish BCV pairs


Split BCV pairs


Establish SRDF pairs


Split SRDF pairs


Set TimeFinder/SRDF QoS

Related topics

- Using the Console
- Using the Console menu bar
- Using the Console task bar
- Using the Console Tree Panel
- Using the Console Target Panel
- Understanding ControlCenter icons

Using the Performance command

The Performance command displays performance statistics about various objects available within the ControlCenter interface.

For each object, real-time data can be displayed in chart or table form. You can configure the interface to display both the chart and table side by side for multiple types of managed objects.

The table view is displayed by default.

The chart view can be displayed by clicking on the **Chart** button along the top edge of the target panel.

You can toggle between these two views.

Displaying performance statistics

1. Click on the **Performance** button.
2. Select a performance enabled object within the tree panel, such as components within a Symmetrix.

Note: Performance statistics cannot be retrieved from a remote Symmetrix.

Related topics

- Performance management

Using the Properties command

The Properties command provides tabulated information for many objects in the Tree panel.

To create a Properties view in the Target Panel:

1. Click the Properties command in the common command toolbar or select the Properties command from any task menu.
2. Click in the checkbox next to your object of interest in the Tree Panel.

Using the Relationship command

The Relationship command provides a map and table view of the logical mapping of file systems and databases to storage devices and disks.

To create a Relationship view in the target panel:

1. Click the Relationship command in the common command toolbar or select the Relationship command from any task menu.
2. Click in the checkbox next to your object of interest in the tree panel.
3. Toggle between the views by clicking Map or Table in the target panel title bar.

Related topics

- Relationship table view
- Relationship map view

Alerts View

Introduction to Alerts View

The Alerts View provides you with a high level view of the active alerts in your Storage Network. The Alerts view may be in one of two modes, tabular or graphical. On initial selection the default mode is tabular, this presents the user with the Active Alerts and Alert Definition tables. The Alert details contained in the tables relate to the nodes selected on the tree, unless All Alerts selected.

The user may also select the Alerts button on the top right hand side of the ECC Console. This creates a new view, in table mode, with all the alerts for the system. Tree selection is empty for this view. The user can toggle between table/chart displays of the alerts. Table displays the table of alerts and alert definitions, while Chart displays the relevant bar chart and the table of related alerts.

Related topics

- Bar Charts of Alerts
- Displaying the Active Alert Table

Active Alert Table

The Active Alert table displays detailed information about the alerts in the storage network. This information can be based on the entire network (All Alerts) or on your selection of tree nodes.
Alerts in the table are associated with the selected managed objects in the tree, indicated by the highlighted managed object in the chart title.

Icons and colors are also used in the table to aid instant identification of the alert severity. These are shown in the table below.

ICON	COLOR	SEVERITY
		Fatal
		Critical
		Warning
		Minor
		Information

The table headings under which the alerts are listed are explained in the table below.

Headings	Explanation
Note	Paper clip icon, indicates if a note is attached
Severity	Severity of alert
Object Name	Name of the object to which the alert is related
Message	Brief explanation of the alert
Date	Date and Time the alert was issued.
Agent	Name of the agent

The table headings can be used to sort the displayed alerts.

Related topics

- Displaying the Active Alert Table
- Sorting Alerts

Bar Charts of Alerts

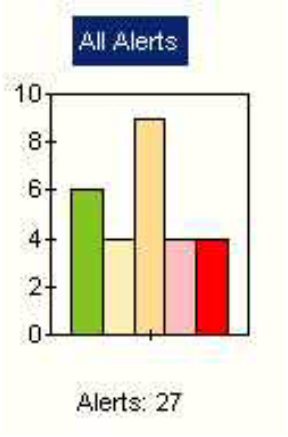
The Alerts view allows you to view a bar chart(s) of Active Alerts in the content pane of the ECC Console.
The bar charts are displayed by clicking on the Chart button, located on the task bar. This provides you with a graphical representation of the number of alerts and their severity. The graph(s) are constructed on the selected Managed Objects (MO) and there may be one or more charts displayed at any one time. A table of the Active Alerts is displayed beneath the charts.

If multiple bar charts are displayed, the table of alerts displayed beneath the bar charts will be, by default, of the leftmost bar chart.

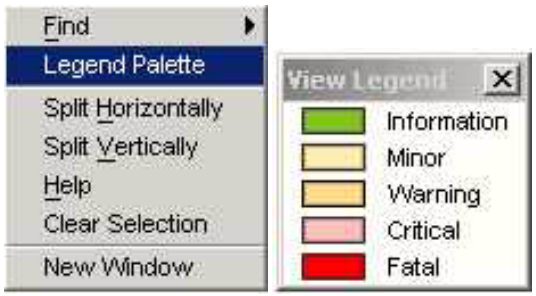
When the Alerts view is active the bar chart(s) indicates the number and severity of Alerts that relate to the entire storage network (All Alerts) or each node in your selection, i.e. for each Managed Object (MO) or MO grouping there will be an associated bar chart. You can see the current status of each MO (or MO grouping) by looking at its associated bar chart.

The bar chart is a graphical representation of the alerts from the Active Alert table. The y -axis of the bar chart displays the total number of alerts, while the x -axis displays the severity of the alert.

The All Alerts bar chart is the graphical representation of the alerts present over the entire storage network.



The **Legend Palette** for explaining the link between the bar colors and the alert severity can be viewed by right clicking on the content pane, a pop up menu displays and the **Legend Palette** option is presented (see below). The Legend Palette is also displayed as an option from the **Actions** button drop down menu.



When an individual bar from the chart is selected, a blue arrow points at the selected bar. The total number of alerts is displayed under the bar chart.

Detailed information about the alerts is displayed in the Active Alert table.

Related topics

- Displaying the Active Alert Table
- Displaying Alerts for a Bar Chart
- Displaying Alerts for a Specific Bar
- Displaying All Alerts

Displaying Active Alert Table

The Active Alerts table displays the details of the current active alerts. The leftmost bar chart is the default selection.

Displaying all Alerts in the Active Alert table

Click the **All Alerts title** of the All Alerts bar chart.

Related topics

- Active Alert Table

Displaying Alerts for a Bar Chart

The alerts that are graphed to a particular bar chart can be displayed in the alert table. The selected chart is indicated by a highlighted Managed Object title. The table is displayed showing the alerts related to that chart.
If multiple bar charts are displayed, the table of alerts displayed beneath the bar charts will be, by default, of the leftmost bar chart.

Displaying alerts for a specific bar chart

Click the **Managed Object title** of the bar chart.

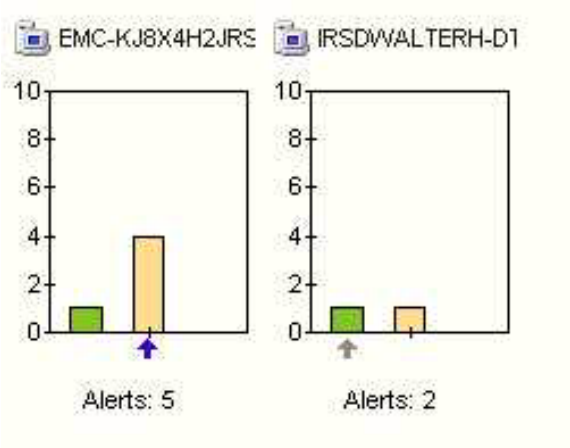
Related topics

- Bar Charts of Alerts
- Active Alert Table

Displaying Alerts for a Specific Bar

Each colored bar, in a bar chart, represents alerts of that severity for a managed object. The color code legend shows the link between the severity and its associated color. The selected bar in the chart is identified by the arrow beneath the bar turning from gray to blue. Selecting a specific bar in a chart displays a table of active alerts, of the severity of that bar, related to the managed object.

The chart below shows the selection of the Warning bar and this will display a table of the alerts of severity type - Warning, for that managed object. The gray arrow indicates other possible selections.



Displaying a table of alerts for a specific bar

Click on or above the bar, within the bar chart. Ensure that the arrow, indication selection, has turned from gray to blue.

Related topics

- Active Alert Table
- Bar Charts of Alerts

Displaying All Alerts

The alerts that are graphed to a particular bar chart can be displayed in the alert table. The selected chart is identified by the bar chart label being highlighted. The table is displayed showing the alerts related to that chart.

The All Alerts bar chart is the graphical representation of the alerts present over the entire storage network. Clicking the All Alerts button removes any previous tree selection and displays the bar chart for All Alerts.

Displaying All Alerts

Click **All Alerts** button, 

.

Related topics

- Bar Charts of Alerts
- Active Alert Table

Sorting Alerts

When the active alert table is displayed on the Console, the table below shows the order in which the headings sort the alerts.

Headings	Sort Order
Severity	Fatal to Information
Object Name	Alphabetical (A-Z)
Message	Alphabetical (A-Z)
Date	Most recent to least recent
Agent	Alphabetical (A-Z)

Note: Clicking again on the heading will reverse the order of the sort, e.g. Take an alphabetically sorted heading, like Agent, clicking once on the heading will sort the alerts in the order (A-Z), clicking a second time on the heading and the sort order reverses to (Z-A).
This applies to all sorting by heading.

Sorting alerts by table headings

Click on the required **table heading** to sort the active alerts.

Related topics

- Active Alert Table

Command History

Introduction to Command History

Command History is an application within the EMC ControlCenter (ECC) Console Monitoring group. Command History provides a tabular view of the ECC Active Commands, associated with selected objects, which were issued by the ECC user through the Console. Active Commands are requested from the repository, which is a component of the ECC infrastructure.

The Command History details are displayed across the 9 fields of the table . These commands are sorted by Start Date. Command History allows filtering on Command attributes. For example, to show only those commands issued by a specified user on a specific date.
All commands can be viewed by, Show All Commands or commands specific to particular managed object can be displayed either by:

- Tick on hierarchical tree
- Drag and drop an object from the tree to the view panel
- Filtering the results of the Show All Commands

Related topics

- Command History Table
- Sorting Command History
- Filter Dialog Box

Command History Table

The Command History details are displayed in a table, located in the content pane of the console.
In the table, Commands are sorted by Start Date.
The Command History details are displayed under the following headings.

Heading	Explanation
Command ID	Command ID number
Associated Object	Managed Object associated with the command
Operation Name	Operation Type
Name	Command Name
User Name	Name of user who issued the command
Start Date	Start Date and Start Time of command
End Date	End Date and End Time of command
Outcome	Outcome of command
State	State of command

Note: The **Print** option requires that you click on the table that you wish to print.

Related topics

- Sorting the Command History Table

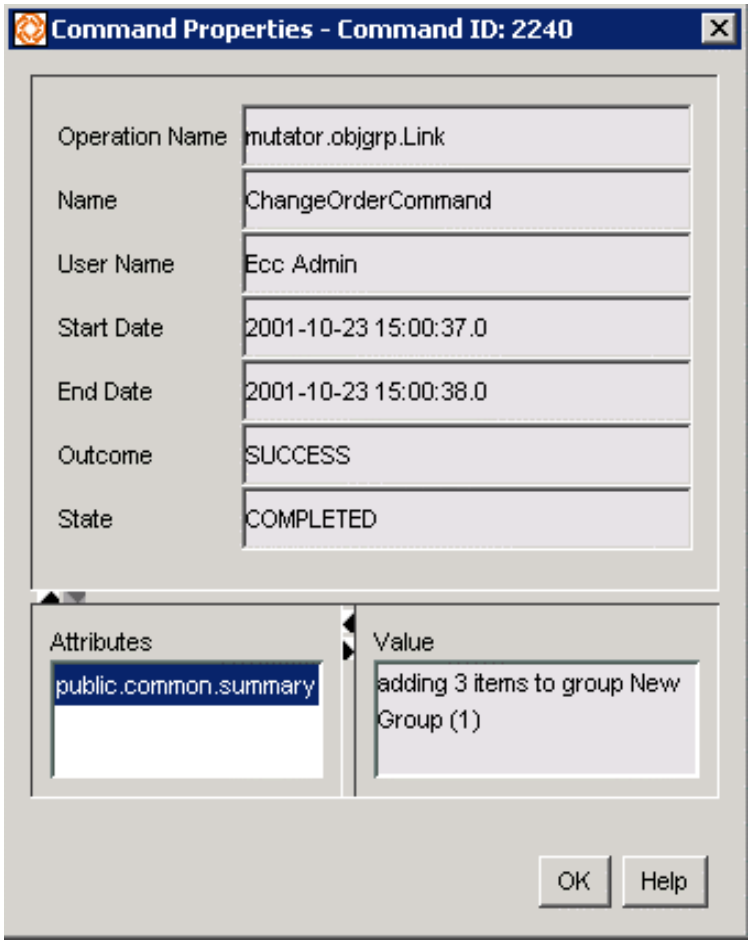
Command Properties

You can display the Command History Properties for each command. The Command ID is displayed in the heading of the Command Properties dialog box.

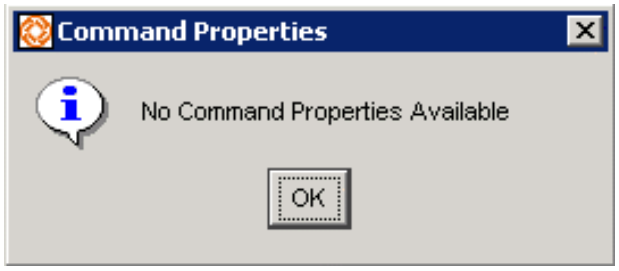
These details are displayed, in the Command Properties dialog box, after the following headings:

- **Operation Name**
- **Name**
- **Outcome**
- **Start Date**
- **End Date**
- **User Name**
- **State**

The **Attributes** and **Values** of the Command are also displayed



If there are no Command Properties logged, then the Command Properties dialog box is displayed stating " No Command Properties Available".



Related topics

- Displaying Command Properties

Displaying the Command Properties

Displaying the Command Properties for a specific command, in the Command Properties dialog box.

1. Right click on the required row in the Command History table.
2. Select **Command Properties** from the pop up menu

Related topics

- Command Properties
- Command History Table

Showing All Commands

The **Show All Commands** option displays all active commands issued to all managed objects.
Showing all Commands can be achieved by either of the two listed procedures.

Procedure One

1. Click on **Actions** arrow on the task bar
2. Select **Show All Commands** from the drop down menu

Procedure Two

1. Right click on the table
2. Select **Show All Commands** from the drop down menu

Related topics

- Command History Table
- Sorting the Command History Table

Refreshing the Commands

The **Refresh Commands** option reposts the Command History details from the server.
Refreshing Command History details can be achieved by either of the two listed procedures.

Procedure One

1. Click on **Actions** arrow on the task bar
2. Select **Refresh Commands** from the drop down menu.

Procedure Two

1. Right click on the table
2. Select **Refresh Commands** from the drop down menu

Related topics

- Command History Table

Sorting the Command History table

When the Command History table is displayed, the Command History details are sorted by Start Date. The list shows how clicking on the headings will sort the commands.

Note. You can not sort by Associated Object

Heading	Sort Order
Command ID	Numerical
Operation Name	Alphabetical
Name	Alphabetical
User Name	Alphabetical
Start Date	Chronological
End Date	Chronological
Outcome	Alphabetical
State	Alphabetical

Note: Clicking again on the heading will reverse the order of the sort, e.g. Take an alphabetically sorted heading, like User Name, clicking once on the heading will sort the commands, by User Name in an A-Z order.

Click a second time on the heading and the sort order reverses to (Z-A).

This applies to all sorting by heading.

Sorting Command History by table headings

Click on the required table heading to sort the Commands by that column.

Related topics

- Command History Table

Filter

ECC Filter

The Filter dialog box is comprised of three panes:

- **Attribute**
- **Attribute value**
- **Filter Summary**

The left pane of the Filter dialog box contains a list of all the associated Attributes.
The right pane of the Filter dialog box, displays all the possible attribute values of a selected attribute.
The selected attribute values are used as the filter criteria.
Selection of multiple values of an attribute are displayed as an OR condition in the Filter Summary.
The selected filter criteria details are displayed in the Filter Summary section of the Filter dialog box.

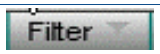
The table below identifies and explains the functions of the buttons displayed on the Filter dialog box.

Button	Function
Add	Allows you to add additional attribute values as filter criteria, where applicable
Reset	Deselects all attribute values selected from a particular attribute
OK	Applies the filter criteria and closes the dialog box
Reset All	Deselects all attribute values for all selected attributes and clears the Filter Summary.
Apply	Applies the filter criteria and keeps the dialog box open
Cancel	Does not apply the selected filter criteria and closes the dialog box.

Related topics

- Filter Functions
- Filter Configuration Prompt

Filter Dialog Box

The Filter dialog box is displayed when the Filter button 

is selected from the task bar.
The Filter dialog box is comprised of three sections:

- **Command History Attributes**
- **Attribute Values**
- **Filter Summary**

The Command History Attributes are displayed in the left pane of the Filter Dialog box.
The attributes for Command History are:

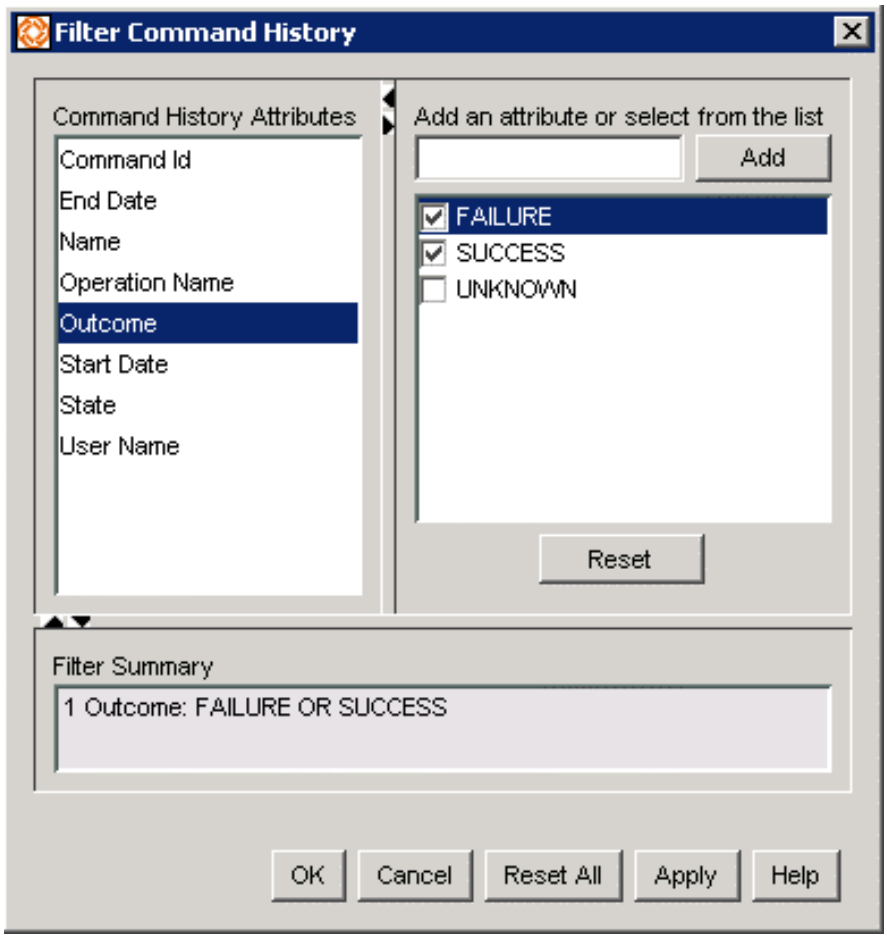
- **Command ID**
- **Operation Name**
- **Name**
- **User name**
- **State**
- **Outcome**
- **Start Date**
- **End Date**

The attribute values, of the selected attribute, are displayed in the right pane of the Filter dialog box. These attribute values can be selected as filter criteria. The selection is shown by a tick in the checkbox, located to the left of the value.

If a filter has not been previously applied, the filter dialog box will appear. Otherwise the Filter Configuration Prompt will display.

Filter Configuration Prompt	Explanation
Switch Filter Off	Turns off the filter, but does not reset the filter criteria
Show Filter Dialog	Display Filter Dialog box
Cancel	Cancel, but not reset filter
Help	Display online help

The filter criteria details are displayed in the Filter Summary section of the Filter dialog box.



Note: The **Find** option can only be used for Associated Objects in the Command History table.

Related topics

- Using the Filter
- Command History Table

Using the Filter

The listed procedures describe how to use the filter.

Selecting Command History attributes.
Click on the required attribute and it will be highlighted to show selection.

Selecting attribute values as filter criteria.
Click on the required attributes to display the associated attribute values. These attribute values are displayed in the right pane of the Filter dialog box and can be selected as filter criteria by clicking on them. Their selection is shown by a tick in the checkbox.

Deselecting specific attribute values as filter criteria.
Click on the selected attribute value and the tick in the checkbox is removed.

Deselecting all selected attribute values for a particular attribute.
Click **Reset**

Deselecting all attribute values for all selected attributes.
Click **Reset All**

Applying the filter criteria and close the Filter dialog box.
Click **OK**

Applying the filter criteria and keep the Filter dialog box open.
Click **Apply**

Canceling the filter criteria selection and close the Filter dialog box.
Click **Cancel**

Opening the Filter Help.
Click **Help**

Related topics

- Filter Dialog Box
- Command History Table

Filter Functions

The following list of procedures describe the functions of the ECC Filter.

Selecting attributes
Click on the required attribute, which becomes highlighted to show it is selected.

Selecting attribute values as filter criteria
Click on the required attributes to display the associated attribute values. These attribute values are displayed in the right pane of the dialog box and can be selected as filter criteria by clicking on them. Their selection is shown by a tick in the checkbox or by a mark in the radio button, depending on the attribute type: date, string or size.

Use of wild card * to aid selection.
The use of the wild card * is allowed in the filter. If you added T* to the attribute value list for the command history attribute Operation Name and applied this as filter criteria, then all commands which have an Operation Name beginning with T will be displayed in the command history table.

Wild Card Usage	Commands displayed in Command History table
*A	Commands ending with the letter A
A	Commands with the letter A between the first and the last letter
A*	Commands starting with the letter A

Deselecting specific attribute values as filter criteria
Click the selected attribute value and the tick in the checkbox or radio button is removed.

Deselecting all selected attribute values for a particular attribute
Click **Reset**.

Deselecting all selected attribute values for all attributes
Click **Reset All**.

Applying the filter criteria and close the dialog box
Click **OK**.

Applying the filter criteria and keep the dialog box open
Click **Apply**.

Retain the filter criteria selection and close the dialog box
Click **Cancel**.

Related topics

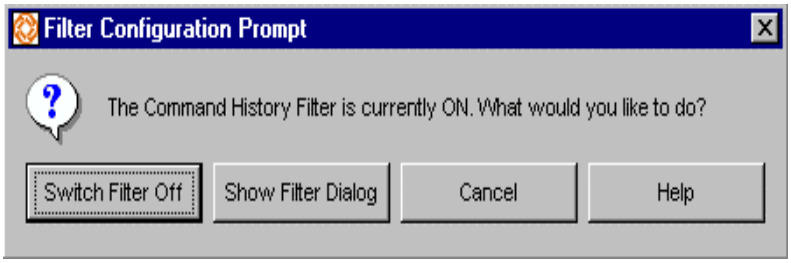
- ECC Filter
- Filter Configuration Prompt

Filter Configuration Prompt

The Filter button on the console can be displayed in either of the following states depending on whether it is on or off. The table shows the different states.

Button	Explanation
	Filter not defined (turned off)
	Filter is defined (turned on)

If the filter has been defined and the Filter button is selected, the Filter Configuration Prompt will be displayed. Stating in the leftmost button that the Filter can be either switched ON or OFF and giving you the choice of the following options:



Button	Explanation
Switch Filter On/OFF	Turn On/Off the Filter
Show Filter Dialog	Display Filter Dialog Box
Cancel	Cancel Configuration Prompt
Help	Display online help

Related topics

- ECC Filter
- Filter Functions

Storage Allocation

ControlCenter storage allocation operations allow you to view available storage throughout the network and within a single Symmetrix unit, as well as perform a variety of configuration tasks. The available operations include:

- **SDR** Control mapping of devices to Symmetrix front-end ports.
- **Logical Device Configuration** Define additional Symmetrix devices from unconfigured physical disks within a Symmetrix unit.
- **Meta Device Configuration** Create new meta devices and support adding and removing members of meta devices.
- **Port Flag Settings** Configure the flag settings on Symmetrix Fibre and SCSI front end ports associated with a host.
- **Device Type Definition** Define the identity of a device as BCV or STD.
- **Visual Storage** Display Symmetrix configuration details, including all directors, channels, cache, ports, and volumes, as well as the links between them. This graphical display is highly configurable.
- **Exploring host storage** Determine how much and what kind of storage can be seen from the host perspective.
- **Adding and removing host storage** Map and unmap storage from a particular host perspective.

You can reach these configuration tools from the **Configure** menu.

Related topics

- Physical Display

Visual Storage

Visual Storage: Overview

Visual Storage provides a highly configurable graphical display of Symmetrix configuration details that can be matched to your specific needs. Visual Storage can show all directors, channels, cache, ports, and volumes, as well as the links between them. For example, Visual Storage can display:

- The disk devices that are serviced by any disk director
- Volumes in RAID-S groups
- Which volumes are accessible to any host and from which Symmetrix port.

Related topics

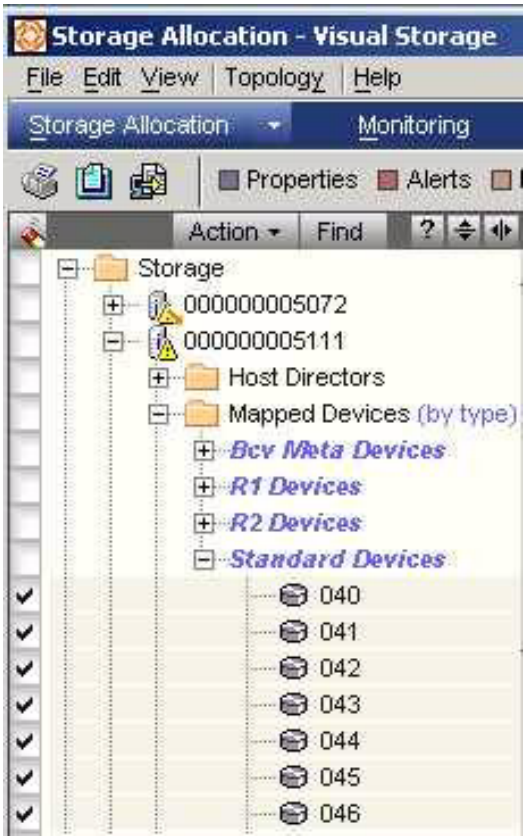
- Displaying Visual Storage
- Showing Hyper Detail
- Filtering the display

Visual Storage: Displaying

Visual Storage supports an interactive display of logical and hyper devices, and their relationship to front end and back end directors.

Displaying Visual Storage

1. In the tree panel, select the Symmetrix unit or components you want to inspect. To do so, check the corresponding checkbox.



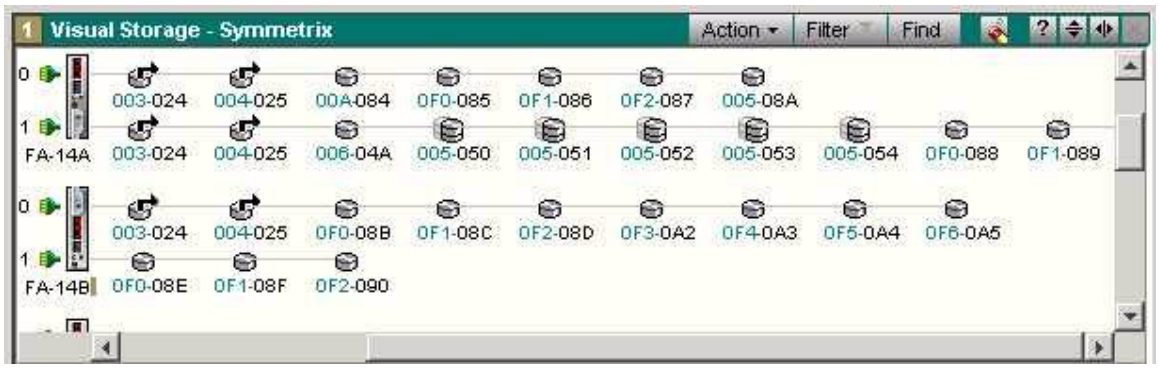
2. Select **Visual Storage** from the **Storage Allocation** menu. The Visual Storage display will now occupy the target panel.

Notes on using Visual Storage

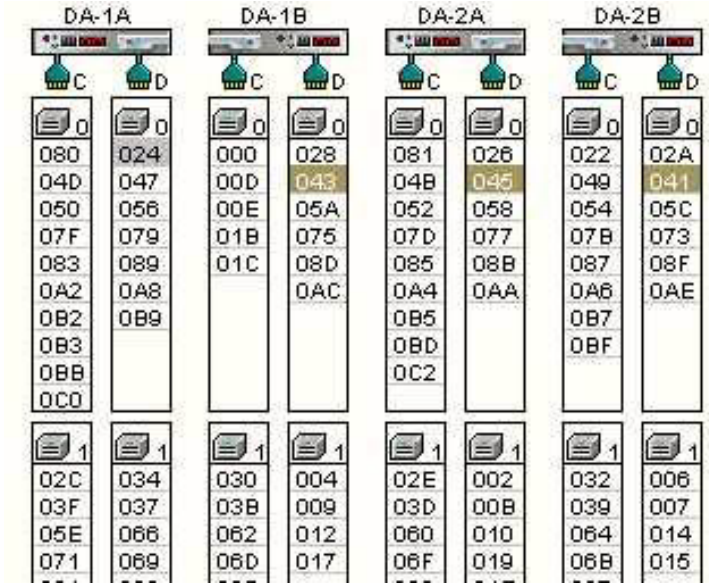
- If you are only interested in information relating to a specific device, right-click the device and select **Only Show Selection**.
- Use the Find button to locate a specific device. You should specify a logical device number, not the address.
- The device names are in two parts; The device address is the first three digits in green, and the device number is the last three digits.
- You can drag and drop any object into a new panel to perform other operations, such as displaying properties of a logical device.
- Selections in the tree panel (left side of console) are synchronized with the display in Visual Storage.
- Inside each device icon area, the device address and device number is displayed. You can highlight a hyper volume with a single mouse click, and all the hyper volumes with same volume number as well as all front-end devices associated with that hyper volume are highlighted.
- You can specify what types of volumes to display by selecting Set Filter from the right click menu. Refer to Visual Symmetrix — Filtering for more information.

Visual Storage panels

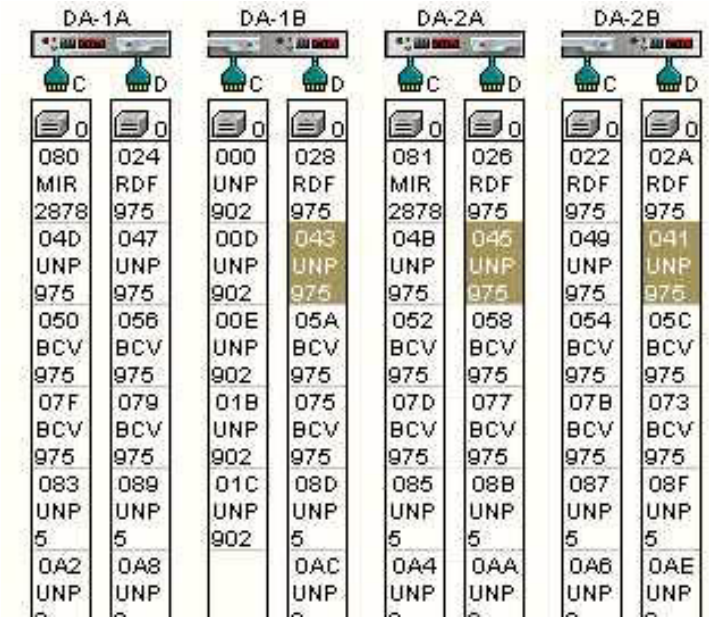
Visual Storage has three panels. The top panel displays the storage devices from the front end perspective, with the SCSI and Fibre Channel Directors as the basis for display.



The middle panel displays the storage devices from the back end perspective, with the disk directors as the basis for display.



Right click and select **Show Hyper Detail** to expand the cells to include information about device configuration and capacity in MBs.



Depending upon the specific device covered by the mouse pointer at each point in time, the bottom panel is a table of dynamically changing information about:

- the logical device mapped to a host director
- the back end disk director
- the physical disk associated with the back end director
- the hyper device associated with the physical disk
- the front end director

Front end (host) director table

Column Heading	Description
Director	Director ID
Status	Status of the device. Possible values are: Ready Not ready
# Ports	Number of ports associated with this director
# Devices	Number of logical devices associated with this director

Displaying Detailed Configuration

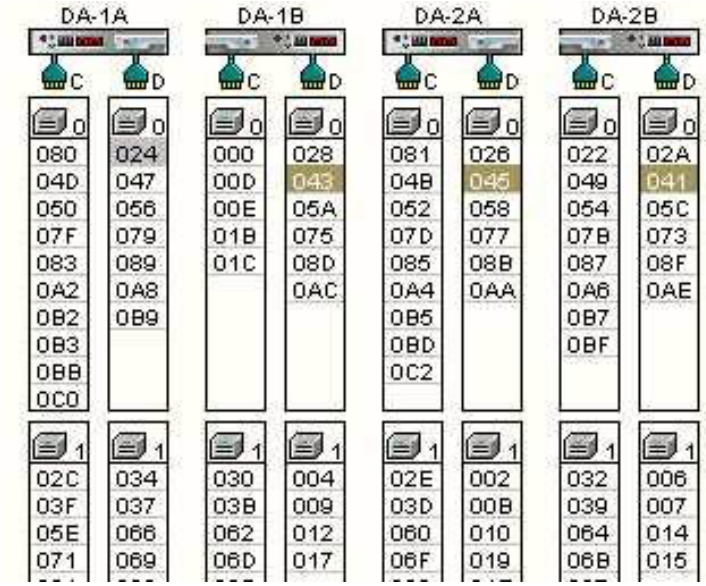
Inside each device icon area, only the device number is displayed. When you click a hyper volume, all the hyper volumes with same volume number, as well as all front-end devices associated with that hyper volume, are highlighted.

Filtering the display

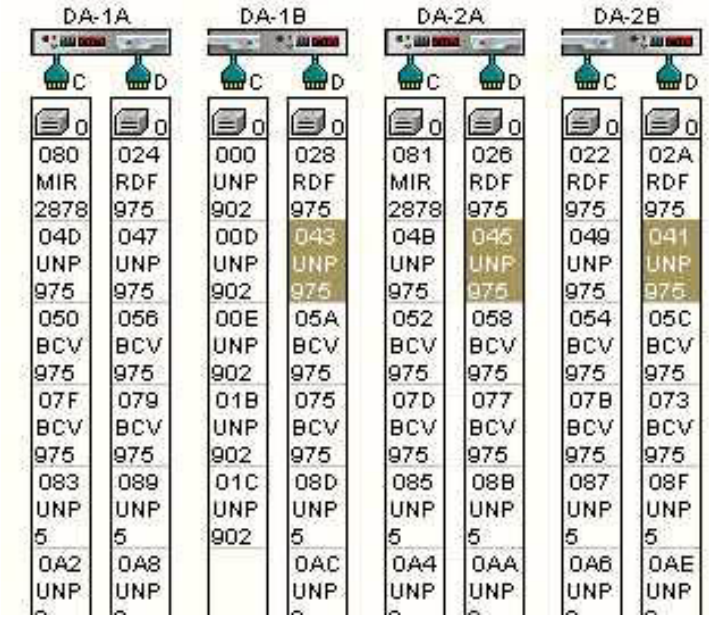
To specify the types of volumes to display, right click on the display and select **Set Filter**. Refer to Visual Storage: Filtering for more information.

Visual Storage: Show Hyper Detail

Once you have displayed the Visual Storage view of a Symmetrix unit, and the target panel is active, the normal display of the back end is as follows:

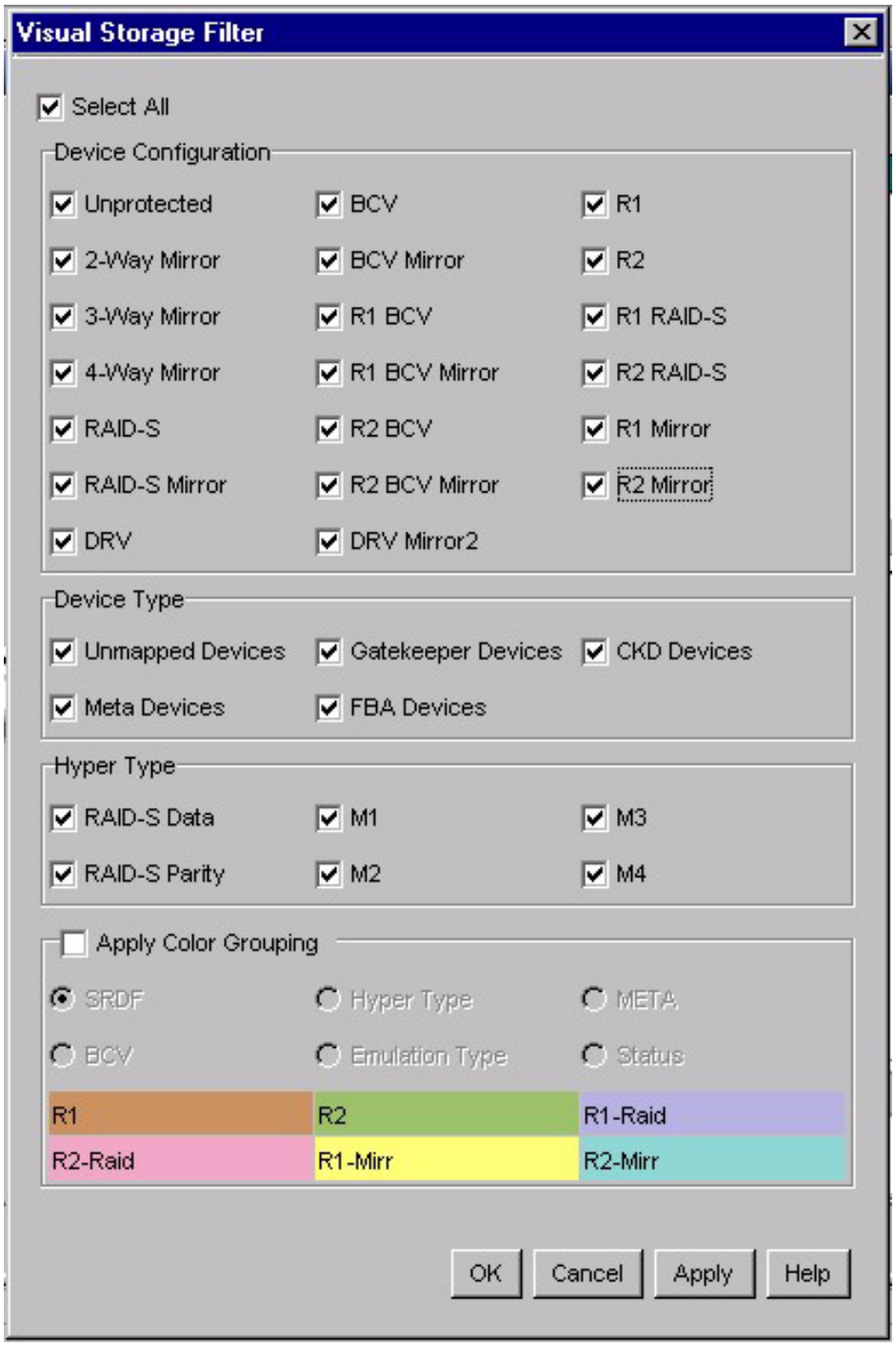


To enhance the display, right-click and select **Show Hyper Detail**. The additional information includes the device configuration and size in MB. The enhanced display is as follows:



Visual Storage: Filtering

Once you have displayed the Visual Storage view of a Symmetrix unit, and the target panel is active, you can filter the display. To do so, right-click and select **Set Filter** from the right click menu. The following Visual Storage Filter dialog box appears:



Device Configuration

Select the device configurations you want to display.

Device Type

Select the type of device you want to display.

Hyper Type

Select the type of hyper volume to display.

Apply Color Grouping

If Apply Color Grouping is selected, you can select one of the group color schemes. Color coding helps increase the visibility of certain devices in the information panel.

Changing Color Choices

To change a particular color within a group, click on one of the color blocks. The Pick A Color dialog box appears. You have a choice of three different methods for editing the color associated with a color group: Swatches, HSB, and RGB.

If you are unsatisfied with your edits to a color, click **Reset** to return to the default setting.

Related topics

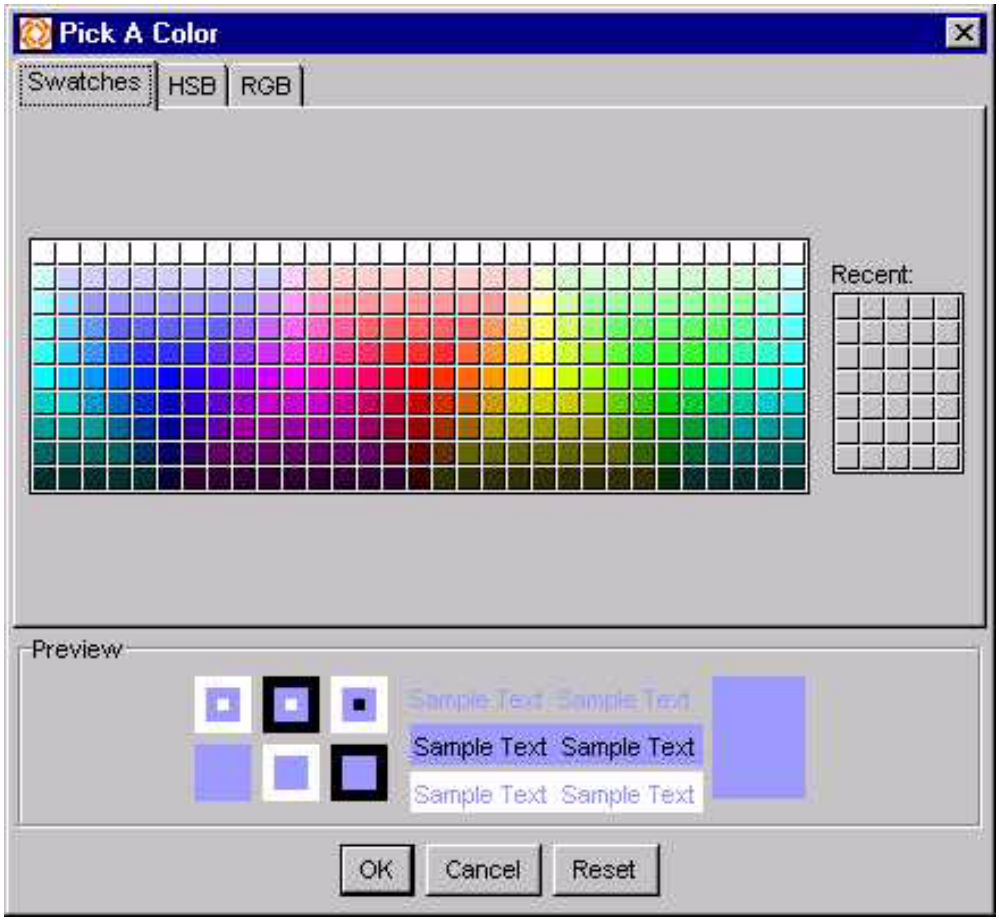
- Visual Storage: Overview

Pick A Color: Swatches

The Swatches Pick A Color dialog box allows you to choose from among a variety of sample colors for use within a color group.

Click a tile of color to select it. Your choices are temporarily stored in the Recent: display panel, so you can revert to a previous color if a later choice is unsatisfactory.

The Preview panel provides dynamically updated examples of how these colors will look in the interface.



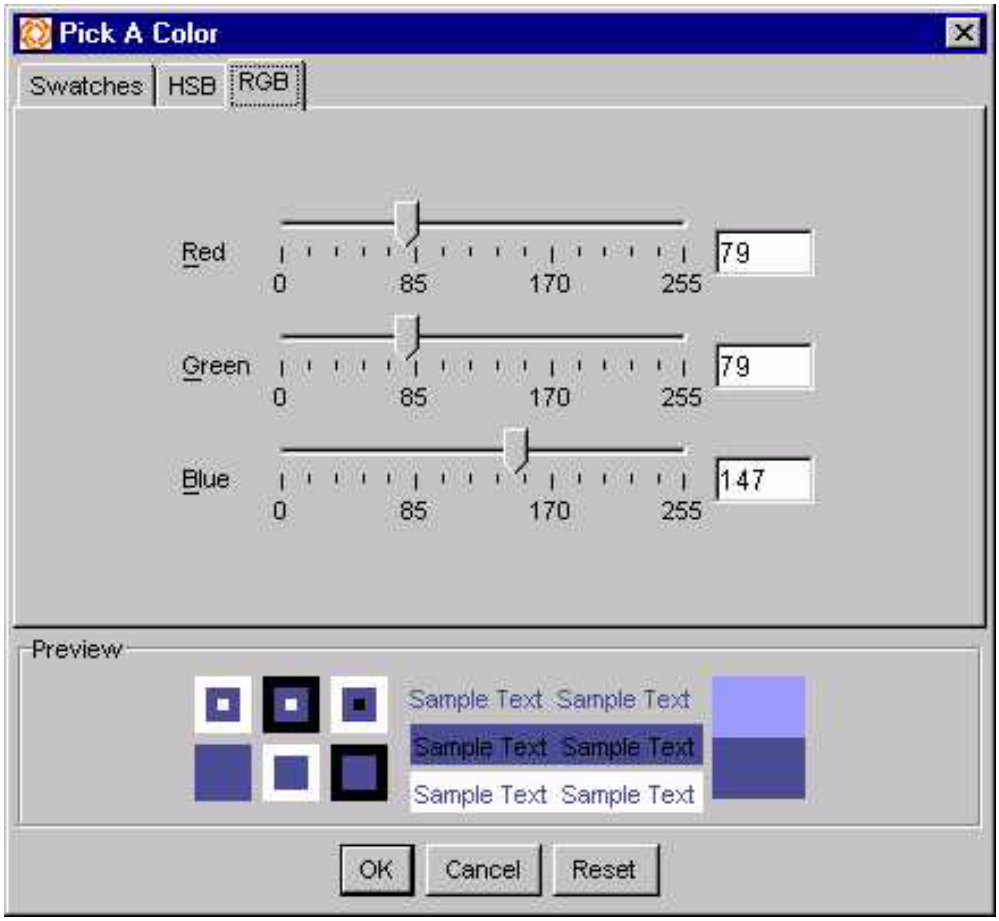
Pick A Color: RGB

The RGB (Red, Green, Blue) Pick A Color dialog box allows you to specify the exact color used within a color group.

There are two ways to set each primary color:

- Move the Red, Green, or Blue slide control left or right
- Type a numerical value in the corresponding number entry box

The Preview panel provides dynamically updated examples of how these colors will look in the interface.



Pick A Color: HSB

The HSB (Hue, Saturation, Brightness) Pick A Color dialog box allows you to specify the exact color used within a color group.

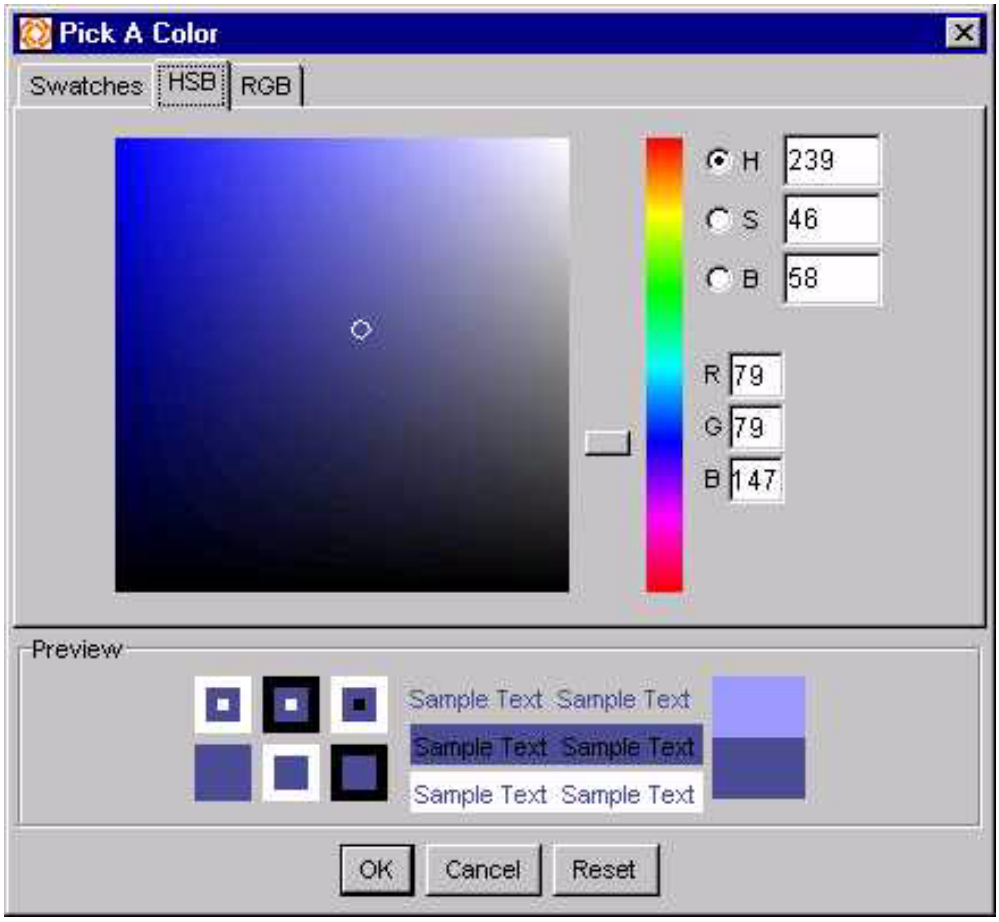
Hue defines the color itself, and can be changed in two ways:

- Move the Hue slide control up and down the color bar
- Type the numerical value in the H number entry box

Saturation indicates the degree to which the hue differs from a neutral gray and Brightness indicates the level of illumination. These values can be changed in two ways:

- Click anywhere in the colorfield square
- Type the numerical values in the S and B number entry boxes

The Preview panel provides dynamically updated examples of how these colors will look in the interface.



Configure

Configuration Manager: Overview

ControlCenter Configuration Manager allows you to modify the configuration of a Symmetrix unit. The controllable areas include:

- **SDR** Map and unmap devices to Symmetrix front-end ports.
- **Logical Device Configuration** Create additional storage capacity from unused physical disks within a Symmetrix unit.
- **Meta Device Configuration** Create new and configure existing members of meta devices.
- **Port Flag Settings** Configure the flag settings on Symmetrix Fibre Channel and SCSI front-end ports.
- **Device Type Definition** Define a device as either BCV or STD.

You can reach these configuration tools from the **Configure** menu.

SDR

SDR: Overview

Symmetrix Disk Reallocation (SDR) allows you to reconfigure Symmetrix logical volumes by mapping and unmapping devices to and from open system front-end director ports. The following operations are supported:

- Unmapping Remove devices from open system front-end director ports
- Moving Unmap devices from open system front-end director ports (Fast-Wide or Ultra SCSI director (SA) or Fibre Channel director (FA)) and map them to a different open system front-end director port.
- Copying Map devices to an open system front-end director port. The devices can originally be mapped to other front-end director ports or they can be unmapped.
- Changing an Address Modify the channel address (target/LUN) of a device.

Related topics

- Starting SDR
- Copying devices
- Moving devices
- Unmapping devices
- Changing addresses
- Updating hosts in general
- Updating Windows NT systems
- Updating Sun SPARC systems
- Updating HP/9000 systems
- Updating IBM RISC System/6000
- Updating NCR 34xx/35xx systems
- Updating DEC Alpha systems
- Updating Sequent systems
- Updating SGI systems
- Updating Siemens systems

Starting SDR

Displaying the Configuration Manager (SDR) dialog box

1. Select a Symmetrix unit from the Storage folder in the tree panel.
2. Click **Storage Allocation**, and then select **SDR** from the **Configure** menu.
3. After an initial warning, the Configuration Manager (SDR) dialog box appears.

The following operations are supported:

- Unmapping Remove devices from open system front-end director ports
- Moving Unmap devices from open system front-end director ports (Fast-Wide or Ultra SCSI director (SA) or Fibre Channel director (FA)) and map them to a different open system front-end director port.
- Copying Map devices to an open system front-end director port. The devices can originally be mapped to other front-end director ports or they can be unmapped.
- Changing an Address Modify the channel address (target/LUN) of a device.

Notes

- When you move, add, delete, or modify a device, any data stored on the device is still on that device until it is reformatted. Back up any data that you want to retain before reallocating Symmetrix devices using SDR.
- ControlCenter allows you to move, delete, or modify a device while I/O operations are occurring on the device. There is a warning message before the SDR session starts, but it is your responsibility to ensure I/O operations have stopped.
- At commit time, devices unmapped from any port will first be write-disabled to ensure data integrity.
- There is no Undo capacity for SDR operations. Verify your actions before proceeding.
- After you reallocate Symmetrix devices, you must update the host on which devices have been reallocated so that the host recognizes the new Symmetrix device configuration.

Related topics

- Overview of Configuration Manager
- Copying devices
- Moving devices
- Unmapping devices
- Changing addresses
- Updating hosts in general

SDR: Copying devices

Copying a device associates it with an additional port.

Copying a device

To copy a device:

1. Select a device or group of devices from the tree panel.
2. Click **Storage Allocation**.
3. Select **SDR** from the **Configure** menu. The SDR dialog box appears.
4. Select the devices to be copied from the Host Directors folder in the Source-Select Devices panel. You can select devices from more than one front-end director port.
5. In the target panel, click the front-end director port to which the devices are to be copied.
6. Click **Copy**.
   Note: There is no Undo capacity for this operation, although you can click **Cancel** or perform an operation in the same session to revert to a previous state. Verify your actions before proceeding.
7. Click **Commit** to commit the actions listed in the **Proposed Configuration/Result** panel to the Symmetrix unit.

Notes

- Copying devices to front-end director ports other than SCSI or Fibre ports is not allowed.
- Certain devices cannot be copied from any front-end director ports, including SCSI and Fibre ports.
- If the action is successful, the devices will be mapped to the target location without being removed from the ports to which they were originally mapped. The next available channel address will be automatically assigned to the new mapping as a default. To change the default address settings, see Changing addresses.
- Copying a device maps it to an additional front-end director port, which has no impact on the ports to which it was originally mapped.

Related topics

- SDR overview
- Starting SDR
- Moving devices
- Unmapping devices
- Changing addresses
- Updating hosts

SDR: Moving devices

Moving a device associates it with a different port.

Moving a device

To move a device:

1. Select a device or group of devices from the tree panel.
2. Click **Storage Allocation**.
3. Select **SDR** from the **Configure** menu. The SDR dialog box appears.
4. Select the devices to be moved from the Host Directors folder in the Source-Select Devices panel. You can select devices from more than one front-end director port.
5. In the target panel, click the front-end director port to which the devices are to be moved.
6. Click **Move**.
   Note: There is no Undo capacity for this operation, although you can click **Cancel** or perform an operation in the same session to revert to a previous state. Verify your actions before proceeding.
7. Click **Commit** to commit the actions listed in the **Proposed Configuration/Result** panel to the Symmetrix.

Notes

- Moving devices from the Unmapped Devices groups is not allowed.
- Moving devices to or from front-end director ports other than SCSI or Fibre ports is not allowed.
- Certain devices cannot be moved from any front-end director ports, including SCSI and Fibre ports.
- If the action is successful, the devices will be moved from their corresponding source locations to the target location. The next available channel address will be automatically assigned to the new mappings as default. To change the default address settings, see SDR: Changing device addresses.
- For devices that are mapped to more than one front-end director port, moving of the devices from one of their source locations to a target location has no impact on the other source locations to which the devices are mapped.

Related topics

- Starting SDR
- Copying devices
- Unmapping devices
- Changing addresses
- Updating hosts

SDR: Unmapping devices

Unmapping a device removes it from the host view.

Unmapping a device

To unmap a device:

1. Select a device or group of devices from the tree panel.
2. Click **Storage Allocation**.
3. Select **SDR** from the **Configure** menu. The SDR dialog box appears.
4. Select the devices to be unmapped from the Host Directors folder in the **Source-Select Devices** panel. You can select devices from more than one front-end director port.
5. Click **Unmap**. The action is added to the **Proposed Configuration/Result** panel.
   Note: There is no Undo capacity for this operation, although you can click **Cancel** or perform an operation in the same session to revert to a previous state. Verify your actions before proceeding.
6. Click **Commit** to commit the actions listed in the **Proposed Configuration/Result** panel to the Symmetrix unit.

Notes

- If more than one device is selected, a dialog box asks for confirmation.
- Selection of devices from more than one front-end director port is allowed.
- Unmapping of devices from the Unmapped Devices groups is not allowed.
- Unmapping of devices from front-end director ports other than SCSI or Fibre ports is not allowed.
- Certain devices cannot be moved from any front-end director ports, including SCSI and Fibre ports.
- If the last copy of a device is unmapped from a front-end port, the devices will automatically be removed from the Mapped Devices group and added to the Unmapped Devices group.
- If the action is successful, the devices will be unmapped from their corresponding front-end director ports.
- For devices that are mapped to more than one front-end director port, removal of the devices from one port has no impact on the other ports to which the devices are mapped.

Related topics

- Starting SDR
- Copying devices
- Moving devices
- Changing addresses
- Updating hosts

SDR: Changing device addresses

Changing a device address means modifying the target/LUN value of an FBA, BCV, or meta device.

Changing a device address

To change a device address:

1. Select a device or group of devices from the tree panel.
2. Click **Storage Allocation**.
3. Select **SDR** from the **Configure** menu. The SDR dialog box appears.
4. In the **Address** column, double-click the tree cell corresponding to the address of the device to modify. The current address is highlighted, the cell enters edit mode, and the cursor is displayed.
5. Enter a valid channel address for the device in the tree cell.
   Note: There is no Undo capacity for this operation, although you can click **Cancel** or perform an operation in the same session to revert to a previous state. Verify your actions before proceeding.
6. Click **Commit** to commit the actions listed in the **Proposed Configuration/Result** panel to the Symmetrix unit.

Notes

- The addresses of devices can only be changed sequentially, one at a time.
- You can change the address of a device mapped to SCSI or Fibre front-end director ports only.
- Addresses of certain devices cannot be changed.
- If the action is successful, the new address is displayed.

Related topics

- Device properties
- Starting SDR
- Copying devices
- Moving devices
- Unmapping devices
- Updating hosts

SDR: Updating hosts in general

Whenever devices are added to the Symmetrix system or device channel addresses are changed, you need to introduce the new devices to the host system.

The exact procedures vary with each host hardware architecture, and sometimes vary with revisions of the operating systems.

The help topics included with this release attempt to document the procedures for the more common host types, but if you cannot find your host in the list, consider one of the following options:

Additional information on updating host views of attached storage may be available from the following sources:

- the *Open Systems Host Environment Product Guide*, which is available in PDF format on the documentation CD included with this product
- your host vendor documentation
- the EMC Customer Support Center

Related topics

- Updating Windows NT systems
- Updating Sun SPARC systems
- Updating HP/9000 systems
- Updating IBM RISC System/6000
- Updating NCR 34xx/35xx Systems
- Updating DEC Alpha Systems
- Updating Sequent Systems
- Updating SGI Systems
- Updating Siemens Systems

SDR: Updating Windows systems

Whenever devices are added to the Symmetrix system or device channel addresses are changed, you need to perform the actions described below in order to introduce the new devices to the system.

To add new Symmetrix devices while the system remains on-line, perform these steps:

Windows NT

1. Run Disk Administrator. The new devices will have a free space designation.
2. Partition and format the new devices as described in the Windows chapter of the *Open Systems Host Environment Product Guide*, which is available in PDF format on the documentation CD included with this product.

Windows 2000

1. Go to **Control Panel**, **Administrative Tools**, **Computer Management**.
2. Run **Disk Management**. The new devices will have a free space designation.
3. Partition and format the new devices as described in the Windows chapter of the *Open Systems Host Environment Product Guide*, which is available in PDF format on the documentation CD included with this product.

Additional information on updating host views of attached storage may be available from your host vendor documentation. You may also contact the EMC Customer Support Center.

Related topics

- SDR: Overview
- Configuration Manager: Configuring devices

SDR: Updating Sun SPARC Systems

Whenever devices are added to the Symmetrix system or device channel addresses are changed, you need to perform the actions described below in order to introduce the new devices to the system.

To add new Symmetrix devices while the system remains on line, perform these steps:

1. Add the new Symmetrix devices into the Symmetrix configuration using the AutoInstall utility.
   Note: Always consult the EMC PSE Configuration Group for assistance when working with a system with live data.
2. Locate the host adapter port to which the new Symmetrix devices are attached by typing:
   `autoconf -l`
3. Type:
   `iosreprobe eisa1/sport80`
   The host displays a message that you may now power on the devices attached to this port. You may choose to do so or quit.

4. To introduce new devices to the host environment, follow the instructions in the Sun chapter of the *Open Systems Host Environment Product Guide*, which is available in PDF format on the documentation CD included with this product.

Additional information on updating host views of attached storage may be available from your host vendor documentation. You may also contact the EMC Customer Support Center.

Related topics

- Configuration Manager: Configuring devices
- SDR: Overview

SDR: Updating HP/9000 Systems

Whenever devices are added to the Symmetrix system or device channel addresses are changed, you need to perform the actions described below in order to introduce the new devices to the system.

You can define newly-connected physical volumes to the system without rebooting the host. This requires use of the `insf` command in a statement similar to the following:

`insf -e`

Alternatively, you can use the `ioscan` command in a statement similar to the following:

`ioscan -fnC disk`

Additional information on updating host views of attached storage may be available from the following sources:

- the *Open Systems Host Environment Product Guide*, which is available in PDF format on the documentation CD included with this product
- your host vendor documentation
- the EMC Customer Support Center

Related topics

- Configuration Manager: Configuring devices
- SDR: Overview

SDR: Updating IBM RISC System/6000

Whenever devices are added to the Symmetrix system or device channel addresses are changed, you need to perform the actions described below in order to introduce the new devices to the system.

1. From the SMIT menu, select **Devices**, **Fixed Disk**, **Add a Disk**.
2. Choose the EMC SYMMETRIX definition from the disk table.
3. Select the SCSI bus on which the new disk resides.
4. Specify the connection address for the new device (target, LUN).
5. Select **EXECUTE**.
6. Repeat steps 2 through 5 for each new device being added to the configuration.

Additional information on updating host views of attached storage may be available from the following sources:

- the *Open Systems Host Environment Product Guide*, which is available in PDF format on the documentation CD included with this product
- your host vendor documentation
- the EMC Customer Support Center

Related topics

- Configuration Manager: Configuring devices
- SDR: Overview

SDR: Updating NCR 34xx/35xx systems

Whenever devices are added to the Symmetrix system or device channel addresses are changed, you need to perform the actions described below in order to introduce the new devices to the system.

When configuring new devices on a live system, it is best to minimize the amount of disk activity the host is performing.

To inform the host about new devices:

1. Run the **mktable** command as follows:

```
% /usr/sadm/sysadm/mktable
```

This command may take several minutes to execute (depending on the number of resources on the host). This command updates the host's table of resources. If not executed, **sysadm** or **dskconfig.NCR** may not be able to work with a new device.

2. Once **mktable** has completed, determine which devices are the new ones by comparing the old list of devices using the **prtconf** command.
3. Continue with the instructions in the NCR chapter of the *Open Systems Host Environment Product Guide* to introduce the new devices to the host.

Additional information on updating host views of attached storage may be available from the following sources:

- the *Open Systems Host Environment Product Guide*, which is available in PDF format on the documentation CD included with this product
- your host vendor documentation
- the EMC Customer Support Center

Related topics

- Configuration Manager: Configuring devices
- SDR: Overview

SDR: Updating DEC Alpha systems

Whenever devices are added to the Symmetrix system or device channel addresses are changed, you need to perform the actions described below in order to introduce the new devices to the system.

Digital UNIX V3.2x

1. At the prompt, type:
   scu
2. At the scu prompt, type one of the following:
   scan edt
   scan edt bus<#>.
   The host scans the target bus (controller specified by bus <#>) or all busses (controllers) and reconstructs the Equipment Device Table (edt).
3. To add the Symmetrix disk names to the system, perform the steps described in the Digital UNIX chapter of the *Open Systems Host Environment Product Guide*, which is available in PDF format on the documentation CD included with this product.

Digital UNIX V4.0

When using Digital UNIX V4.0, you can introduce the new devices to the system as described for Digital UNIX V3.2x above, or perform these steps:

1. At the prompt, type:
   scsimgr -scan_bus bus=BUSNUM
2. Repeat for each LUN:
   a. Write a label to the device you are defining:
   disklabel -rw rz<*lun letter***><***unitID***> <***label***>**
   b. Change the ownership on the device to a particular application:
   chown <*owner***>:<***group***> *rz<***lun letter***><***unitID***>***

Additional information on updating host views of attached storage may be available from your host vendor documentation. You may also contact the EMC Customer Support Center.

Related topics

- Configuration Manager: Configuring devices
- SDR: Overview

SDR: Updating Sequent systems

Whenever devices are added to the Symmetrix system or device channel addresses are changed, you need to perform the actions described below in order to introduce the new devices to the system.

When configuring new devices on a live system, it is best to minimize the amount of disk activity the host is performing.

To add new Symmetrix devices while on line in the DYNIX/ptx V4.4.0 and above environment, perform the following steps:

1. Use the `devctl` command with the `-c` option, as follows:
   devctl -c scsibus*yy*
   where *yy* is the bus number to which the new device is attached.
2. Type:
   devctl -N

If you are running a version of DYNIX/ptx lower than V4.3.0, you will need to reboot the host in order to see the new devices.

Additional information on updating host views of attached storage may be available from the following sources:

- the *Open Systems Host Environment Product Guide*, which is available in PDF format on the documentation CD included with this product
- your host vendor documentation
- the EMC Customer Support Center

Related topics

- Configuration Manager: Configuring devices
- SDR: Overview

SDR: Updating SGI Systems

The SGI operating system currently does not support adding devices on line.

The EMC PSE Configuration Group can add new devices to the Symmetrix configuration while the Symmetrix system remains on line to the host. Once this is complete, stop all host activity and reboot the host using:

```
shutdown -y -g0 -i6
```

Additional information on updating host views of attached storage may be available from the following sources:

- the *Open Systems Host Environment Product Guide*, which is available in PDF format on the documentation CD included with this product
- your host vendor documentation
- the EMC Customer Support Center

Related topics

- Configuration Manager: Configuring devices
- SDR: Overview

SDR: Updating Siemens Systems

Whenever devices are added to the Symmetrix system or device channel addresses are changed, you need to perform the actions described below in order to introduce the new devices to the system.

To add new Symmetrix devices while the system remains on line, perform these steps:

1. Add the new Symmetrix devices into the Symmetrix configuration using the AutoInstall utility.
   Note: Always consult the EMC PSE Configuration Group for assistance when working with a system with live data.
2. Locate the host adapter port to which the new Symmetrix devices are attached by typing:
   ```
   autoconf -l
   ```
3. Type:
   ```
   iosreprobe eisa1/sport80
   ```
   The host displays a message that you may now power on the devices attached to this port. You may choose to do so or quit.
4. To introduce new devices to the host environment, follow the instructions in the Siemens Nixdorf chapter of the *Open Systems Host Environment Product Guide*, which is available in PDF format on the documentation CD included with this product.

Additional information on updating host views of attached storage may be available from your host vendor documentation. You may also contact the EMC Customer Support Center.

Related topics

- Configuration Manager: Configuring devices
- SDR: Overview

Logical Device Configuration

Configuration Manager: Configuring devices

Logical device configuration is process of defining what sections of a physical disk will be used for a particular Symmetrix logical device. To display the Logical Device Configuration dialog box:

1. Select a Symmetrix unit (or any component) from the tree panel.
2. Click **Storage Allocation**.
3. Select **Logical Device Configuration** from the **Configure** menu. The Logical Device Configuration dialog box appears.

Note the following points before proceeding:

- If you receive a message referring to the configuration server, such as "`Access to the configuration server could not be established!`", the message is referring to the service processor on the Symmetrix. Contact EMC Customer Support for help.
- You can configure multiple logical devices of the same type by specifying the appropriate number for the Count parameter.
- You can specify multiple logical devices of different types by adding them consecutively to the **Requested Configuration** table.
- If you create an unprotected device, it should be used only as a BCV or an SRDF device, not as a standard (STD) device.

Configuring a logical device

To configure a logical device:

1. Use the values available in the **Configuration Parameter** panel to define each logical device.
2. Once you have specified the desired configuration, click **Add** to place it in the Requested Configuration review table.
3. If you want to save the summary of proposed configuration changes listed in the Results tab, you should use the Export or Print commands before proceeding.
4. The actual configuration update does not commence until you click **Commit**. The configuration can take several minutes.

Dialog box features

The options in the Logical Device Configuration dialog box are described in the following table.

Feature	Description
Count	Specifies the number of devices to allocate. For a device with no protection, specify the actual number of devices to be allocated. For mirrored devices, specify the number of mirror sets to be allocated.
Emulation	Specifies the type of device emulation. In release 5.0, the only supported type is FBA.
Type/Host	For FBA emulation, this field shows the recommended preset configuration. In release 5.0, the only supported type is Open System.
Size	Specifies the size of the logical device. For FBA devices, the default size is shown in MBs. Each emulation type has different default values. You can edit the displayed value or choose from the pull-down menu.
Unit	Specifies the device size in cylinders or megabytes. For FBA, the sizes are shown in MB units by default.
Protection	Specifies the type of device protection. Possible values are: UNPROTECTED and M2. ControlCenter will calculate the configuration capacity. For example, if the selected device has M2 protection, ControlCenter will multiply the device capacity by two and show the result in the Configuring: field.
Configuring	Shows the current configuration capacity in MB units.
Requested Configuration	Displays the configuration entries that have been submitted but not yet committed to the Symmetrix unit. You can add and remove items from the list. The table can be sorted based on heading. The table sorting will automatically reset if you add another item to the table.
Result tab	Displays a history of commands and messages for the entire configuration session.
Add	Adds a configuration entry to the request table.
Remove	Removes an entry from the request table.

After the logical devices have been created, they are added to the Unmapped Devices folder in the tree panel.

Related topics

- Defining BCV devices
- Configuring meta devices
- Updating hosts after adding new devices
- Device properties

Meta Device Configuration

Concatenated and striped devices

Addressing of data contained in a meta volume can be organized in two different ways:

- Concatenated
- Striped

Concatenated volumes

Concatenated volumes are volume sets that are organized with the first byte of data at the beginning of the first volume. Addressing continues to the end of the first volume before any data on the next volume is referenced. When writing to a concatenated volume, the first slice of a physical disk device is filled, then the second, and so on, and on to the next and subsequent physical disk devices.

Striped Data

Meta volume addressing by striping also joins multiple slices to form a single volume. However, instead of sequential address space, addresses are interleaved between slices. When writing to a striped volume, equal size stripes of data from each participating drive are written alternately to each member of the set.

Striping data across the multiple drives in definable cylinder stripes was designed to benefit “random reads” by avoiding stacking multiple reads to a single spindle and disk director. This scheme creates a large volume, but additionally balances the I/O activity between the disk devices and the Symmetrix disk directors.

The following table defines the data stripe sizes and capacities for Symmetrix meta volumes.

Meta volume stripe sizes

Stripe Size	Stripe Capacity (512 byte blocks)
2 Cylinders	1,920
4 Cylinders	3,840
8 Cylinders	7,680
16 Cylinders	15,360
32 Cylinders	30,720
64 Cylinders	61,440

Related topics

- Configuration Manager: Configuring meta devices
- Moving meta devices
- Defining BCV devices
- Logical device configuration

Configuration Manager: Configuring meta devices

Meta devices are Symmetrix devices concatenated together to form a larger device. The Symmetrix devices forming the meta device are all accessed through the same target/LUN value. Configuration Manager reports the Symmetrix meta device number as the device number of the first device in the group, which is also known as the *meta head*.

The Meta Device Configuration dialog box allows you to modify existing meta devices as well as create new meta devices.

Note: Meta device configuration can be performed only on a local Symmetrix unit.

Displaying the Meta Device Configuration dialog box

To display the Meta Device Configuration dialog box:

1. Select a Symmetrix unit from the Storage folder in the tree panel.
2. Click **Storage Allocation**.
3. Select **Meta Device Configuration** from the **Configure** menu. The Meta Device Configuration dialog box appears.

   If you receive a message referring to the configuration server, such as "`Access to the configuration server could not be established!`", the message is referring to the service processor on the Symmetrix. Contact EMC Customer Support for help.

Two panels are used to support meta device creation and configuration:

- a table containing the available unmapped Symmetrix devices
- a table containing the existing meta devices divided into Concatenated and Striped

Displaying information about a meta device

The left-hand panel (Source - Select Devices) depicts the configuration for the unmapped devices on the selected Symmetrix unit. The columns also indicate which devices have been selected, the size of each device, and the protection type. This display of devices has been pre-filtered to prevent the selection of the following:

- meta devices
- DRV devices
- SRDF devices
- devices smaller than 20 MB in size
- CKD devices

The right-hand panel (Target - Select Meta Type for New Meta or Meta Head to Extend) displays all the configured meta devices on the specified Symmetrix unit, along with the meta device type, stripe size, member size, and protection type.

Creating a meta device head

Note: If you select multiple devices before performing step 2 and step 3, a meta device will be created with the first device as the meta head and the remaining devices will become meta members.

1. Click an available device in the left-hand source panel.
2. Control-click either the Striped Metas folder or the Concatenated Metas folder in the right-hand target panel.
3. Click **Create Meta**. This creates the device as a meta head to the appropriate meta device type.

Drag and Drop procedure

Select devices from the left-hand source panel, then drop onto either the Striped Metas folder or the Concatenated Metas folder in the right-hand target panel.

Adding a meta device member

Note: Members can be added to - or removed from - striped meta devices only at meta device creation time.

1. Click the device to be added in the left-hand source panel.
2. Control-click the appropriate meta head device under either the Striped Metas folder or the Concatenated Metas folder in the right-hand target panel.
3. Click **Add Members**.

Drag and Drop procedure

Select devices from the left-hand source panel, then drop onto the appropriate meta head device under either the Striped Metas folder or the Concatenated Metas folder in the right-hand target panel.

Removing a meta device member

Notes

- Delete only a meta device that is completely unmapped. The deletion of the meta device will make all members available for individual mapping.
- Concatenated metas: You must remove the last added member (the tail) first. When removing multiple members, they have to be in contiguous order, and the last member must be one of them.

1. Click the meta device member to be deleted in the right-hand target panel.
2. Click **Remove**.

Removing a meta device head

1. Remove all meta device members.
2. Click the meta device head.
3. Click **Remove**.

Saving configuration changes

If you want to save the summary of proposed configuration changes listed in the Proposed Configuration/Results tab, you should use the Export or Print commands before clicking Commit.

Configuration Errors

While unusual, it is possible to receive an error when performing one of the configuration operations. If you receive an error message such as

```
The SymConfigChangeControl VALIDATE failed
```

You should perform the following actions:

1. Go to the host where Storage Agent for Symmetrix is running, and open the SYMAPI log file. On Windows, the default location is C:\Program Files\EMC\symapi\log. On UNIX, the default location is var/emc/symapi/log.
2. Perform a search for the error string.
3. Refer to either the *SymmAPI-Configuration Programmer's Manual* or the *EMC Solutions Enabler SYMCLI Configuration Component Product Guide* for the error message.
4. The Symmetrix Service Processor is designed to call home to EMC in the case of configuration errors, but you may want to contact EMC Customer Support to determine the resolution.

Related topics

- Displaying meta device properties
- Moving devices
- Defining BCV devices
- Logical device configuration
- Updating hosts after adding new devices
- Concatenated and striped devices

Port Flag Settings

Configuration Manager: Setting port flags

Use the Port Flag Settings command to control the settings on Symmetrix SCSI and Fibre Channel front end ports. The flags are used to customize the negotiation done between the HBA on the host and the Symmetrix unit. Each host type to which the Symmetrix unit connects may implement the SCSI or Fibre protocol slightly differently. The port flag settings tell the Symmetrix unit how to communicate with each host type and behave in certain situations.

Setting port flags automatically

ControlCenter provides you with the ability to set all the flags automatically for a specified host.

1. Click **Storage Allocation**.
2. Select one or more Symmetrix host directors, ports, or the Symmetrix itself from the tree panel.
3. Select **Port Flag Settings** from the **Configure** menu. The Port Flags Default Settings dialog box is displayed.
4. Select the desired host type from the **Select Host Policy** panel, and the desired port from the **Select Port** panel, then click **Add**. The proposed configuration is displayed in the **Selected** panel. Repeat this operation for other ports, as required.
5. If you want to save the summary of proposed configuration changes, you should use the Export or Print commands before proceeding.
6. When you are satisfied with the proposed configuration, click **Commit** to commit the actions to the Symmetrix unit.

Setting the port flags manually

ControlCenter allows you to fine tune the characteristics of the front-end port by selecting each flag independently.

1. Once the Port Flags Default Setting dialog box is displayed, click **Expert Mode**. The Port Flag Settings dialog box is displayed.
2. Select the director and port to be configured, then edit the flag values as required.

Editing tips: The table columns are checkboxes representing the value for each setting that is possible.

- A bullet in the column indicates that the flag is set to true.
- A white cell indicates you can change that value;
- A gray cell indicates no edits are possible.
- A blue cell indicates that the cell value has changed from the initial value when the dialog first opened.

Cautions

- You should not manually change these settings without consulting EMC Customer Support. Failure to configure these values properly can result in a host no longer being able to communicate with a Symmetrix unit.
- There is no Undo capacity for this operation, although you can perform an operation in the same session to revert to a previous state. Verify your actions before proceeding.

SCSI port flag descriptions

SCSI Port Flag Settings dialog box

Except for DILC, all of the SCSI flags are also used for the Fibre settings. The settings are defined as follows:

SCSI Flags	Description
A4S = IF_SERVER_ON_AS400	When enabled for AS/400 platforms, this flag indicates that the port is to behave as a server returning server inquiry data rather than AS/400 data.
AB = IF_AUTO_BUSY	When enabled for Unisys A-series platforms only, this flag enables the auto-busy mechanism so that the Symmetrix unit returns a Busy to all Unisys host requests.
AFN = IF_AVOID_FORCE_NEG	When enabled for Sequent V4.2.3 and below, the Symmetrix unit never initiates negotiations. Normal behavior of the Symmetrix unit is to initiate negotiations after an off-line to on-line transition. This is for hosts that do not handle negotiations.
ARB = IF_AVOID_RESET_BROD	When this flag is enabled, a SCSI bus reset only occurs to the port that received the reset (not broadcast to all channels).
B = HP_3000_MODE	When enabled for HP MPE 5.0 and microcode levels of 5062 and below, this flag causes the Symmetrix port to return a SCSI Busy state instead of a 0B44 sense code when a xx3C error occurs.
C = COMMON_SN	This flag should be enabled for multipath configurations or hosts that need a unique serial number to determine which paths lead to the same device.
D = DIS_Q_RESET_ON_UA	When this flag is enabled, a Unit Attention (UA) that is propagated from another director does not flush the queue for this device on this director. Used for hosts that do not expect the queue to be flushed on a 0629 sense (only on a Hard Reset).
DFD = DISABLE_FALSE_DISC	When enabled for debugging, this flag prevents the port from performing a False Disconnect operation. Default is disabled.
DILC = DISABLE_INTRLVD_CMD	When enabled (always), meta volume command interleaving is being supported. This allows multiple meta members to operate at the same time on the same volume. Used for SCSI, but not for Fibre.
DMQ = DISABLE_MINI_Q	When enabled for debugging, this flag disables the use of the Mini Queue on the port. Default is disabled.
E = ENVIRO_SET	When enabled, this flag enables the environmental error reporting by the Symmetrix unit to the host on the specific port.
L = LINK_CMDS	When enabled, this flag enables support of SCSI linked commands. It allows a host to chain SCSI commands in a manner similar to mainframe Channel Command Words (CCWs). Default is enabled.
N = NEGO_REST	When enabled for AS/400 hosts, this flag forces a SCSI negotiation by the Symmetrix unit after a: • SCSI reset • Error • Bus device reset This flag has a default setting of off.

P = CYL_NAME	When this flag is enabled, the Symmetrix unit via the specified port embeds the cylinder count into the product ID returned in the SCSI Inquiry command. Enabled for Pyramid only when it is desirable to embed the Symmetrix support into the Pyramid kernel.
Q = PBAY_MONITOR	When enabled for Sequent platforms, this flag enables low-level polling of the SCSI bus in order to intercept the nonstandard SCSI opertions required for a Sequent PBAY disk subsystem. Must be used for the Sequent cluster operation for the Symmetry system for V4.2.x operating systems only. Must not be used on versions later than V4.2.x or for any NUMA-Q systems and also not used for Fibre Channel.
R = ENABLE_C_REORDER	When this flag is enabled with Tag Command Queueing in use, the incoming SCSI commands become reordered to Simple Queueing. The default is enabled, and should only be disabled upon a request from EMC.
S = SOFT_REST	When enabled for Bull/GCOS-7 host, the Symmetrix port supports SCSI Soft Reset option.
SC3 = IF_SCSI_3	When enabled, the Inquiry data is altered when returned by any device on the port to report that the Symmetrix supports SCSI 3 protocol. When this flag is disabled, the SCSI 2 protocol is supported.
SCL = ENABLE_SUNAPEE	When enabled for Sun PDB clusters, this flag enables the Sunapee option on the port.
SEQ = IF_ENABLE_SEQUENT	When this flag is enabled for Sequent DYNIX/ptx V4.4.2 and above, the Symmetrix unit on the specified port does not force wide or synchronous negotiations and sets the task timeout window to be 15 seconds before aborting a process. Also, a busy status is returned instead of a 0B44h when aborting a command on a timeout.
SM = IF_ENABLE_SIEMENS	For Siemens R-Series (RM/400-RM/600) platforms only. When this flag is enabled for Siemens, the Symmetrix unit returns in the sense data error 0B48 instead of 0B44 for normal behavior.
T = TAGD_COMMANDS	When enabled, this flag enables support for tagged commands. Default is enabled.
U = DISABLE_ULTRA	When enabled, this flag disables Ultra SCSI on an Ultra-capable SA port. Default is disabled.
W = WIDE_TRNS	When enabled, this flag enables SCSI Wide operation. Default is enabled.
Y = SYNC_TRNS	When enabled, this flag enables SCSI synchronous negotiations. Default is enabled.
Z = SET_QERR	This flag should be enabled for SGI platforms only to flush the queue on a contingent allegiance condition (CAC). Must be used for V5.3 and V6.2 SGI operating systems and cluster environments. Not used on versions later than V6.2.

Fibre Channel port flag descriptions

Fibre Channel Port Flag Settings dialog box

The Fibre Channel port flag settings are defined as follows:

Fibre Channel Flags	Description
A = DISK_ARRAY	When enabled (default), the port is represented as a disk array. This port information appears in the Inquiry data.
C2S = CLASS_2_SERVICE	Enabled for a Class 2 fibre protocol connection that requires an acknowlegement for each frame transmitted.
GVSA = GENERIC_VSA	When enabled, the generic volume set addressing mode is selected. GVSA mode allows hexadecimal addressing.
H = HARD_ADDRESS	When enabled (default), the FA director attempts to get the loop_id specified when it initializes on the loop (hard-assigned addressing). When disabled, soft addressing is being used.
NP = NON_PARTICIPATE	When enabled along with the HARD_ADDRESS flag, the Fibre channel director only uses hard-assigned addressing when it initializes on the loop. Otherwise, soft-assigned addressing is used during loop initialization (the default).
OVMS = OPEN_VMS	Enabled for an OpenVMS fibre connection.
PP = PT_TO_PT	When enabled for microcode 5x65 and above at configuration time, specifies a point-to-point (direct or switched) topology in the initialization sequence. When disabled (default), it is initialized as an arbitrated loop.
UWN = UNIQUE_WWN	When enabled (default) for all environment reconfigurations and new environments, ensures unique World Wide Names (WWN) within the Fibre Channel environment (uses Symmetrix serial numbers and port numbers). When disabled, you do not have to change WWN.
V = VOL_SET_ADDR	When enabled along with the Disk_Array flag for HP-UX hosts, the volume set addressing mode is selected. VSA mode allows octal addressing.
VCM = VCM_ENABLED	Enabled for the Volume Logix software which provides volume configuration management controls to handle access to Symmetrix volumes. Default is disabled.
TP = GLOBAL_TPRLO	When enabled (default) for microcode 5x65 and above, an extension is provided to the existing third party logout required by the standard. In addition to logging out the hosts that are logged in to the port receiving the third-party logout, the logout propagates to other Symmetrix Fibre Channel ports that share volumes with the port that received the logout.

Related topics

- Updating hosts to recognize new devices

Device Type Definition

Configuration Manager: Device type definition

The Configuration Manager allows you to define the following Symmetrix devices:

- STD A standard Symmetrix storage device used for direct data storage.
- BCV Business Continuance Volume device which functions as a mirror to a standard device to create a protected storage environment. The BCV device can also be independently addressed.

Defining a Symmetrix device

To define a Symmetrix device:

1. Select a Symmetrix unit (or any component) from the tree panel.
2. Click **Storage Allocation**, then select **Device Type Definition** from the **Configure** menu.
   Note: If you receive a message referring to the configuration server, such as "`Access to the configuration server could not be established!`", the message is referring to the service processor on the Symmetrix. Contact EMC Customer Support for help.

   The Device Type Definition dialog box appears with a list of unmapped devices on the Symmetrix. There are four columns, each of which can be sorted by clicking on the column header. This display of devices has been pre-filtered to prevent the selection of the following devices:
   - SRDF
   - DRV
   - SFS (Symmetrix File System)
   - VCM (Volume Control Manager can have dedicated devices for Volume Logix)
   - CKD
   - meta
   - RAID-S
3. Select a device from the Device column.
4. Click **BCV** or **STD** to redefine the device. Note that once you redefine a device, the type is displayed in *blue italics*. Illegal operations are flagged in the **Result** tab.
5. Repeat this operation as required.
6. If you want to save the summary of proposed configuration changes listed in the Results tab, you should use the Export or Print commands before proceeding.
7. The configuration update does not commence until you click **Commit**. The actual device definition may take several minutes.

Note: If you are redefining an unprotected device, it should be used only as a BCV or an SRDF device, not as a standard (STD) device.

Creating SRDF devices

SRDF devices can be created using SYMCLI.

Related topics

- Configuring logical devices
- Configuring meta devices
- Updating hosts after adding new devices

Monitoring

ControlCenter supports a variety of methods for monitoring the devices and activities on your storage network. The **Monitoring** menu provides the following commands.

Topology command Monitors the topology and populates the Repository with discovered data.

Command History command Provides a tabular view of the ControlCenter Active Sessions/Commands, associated with selected objects, which were issued by the ControlCenter user through the Console.

Physical Display command Provides a photo-realistic, dynamically changing view of the Symmetrix internals.

Physical Display

Physical Display display a dynamically changing view of the physical layout of a Symmetrix unit, follow these steps:

1. Select a Symmetrix unit from the Storage folder in the tree panel.
2. Click **Monitoring** and select **Physical Display** from the resulting menu.

A dynamically changeable view of the front and rear views of a Symmetrix is displayed.

As you interactively select and deselect devices in the tree panel, the display changes to reflect your selections.

This functionality can serve a wide range of purposes, including locating a physical device in your Symmetrix, when you know only the logical device identifiers.

Note: ControlCenter does not report on physical disks that do not have associated volumes.

Topology

The topology is a description of the physical and logical configuration of devices within the storage area network (SAN), including ports, fabrics and connecting links.

This topic provides a brief overview of some of the topology management features provided by ControlCenter. For more information, see Discovery and monitoring requirements.

The following sections are included:

- Topology discovery
- Monitoring connectivity devices
- Connection settings
- Creating user-defined objects
- Identifying unknown ports
- Topology map
- Login history table viewer
- Supported devices
- Monitoring Symmetrix volume-access control

Topology discovery

Topology discovery is the process of identifying the various elements and their relationships to each other.

Discovering hosts and storage arrays

Hosts and storage arrays are discovered automatically by ControlCenter agents. For more information on host agents and storage agents, see ControlCenter agents overview.

Discovering connectivity devices

Connectivity devices are used to connect hosts and storage systems. Connectivity devices may also connect to other connectivity devices. They include switches, hubs, bridges, extenders, patch panels, and so on.

ControlCenter first searches for connectivity devices and then discovers the topology information for the switches found. Topology information refers to the ports, links, neighbors and logical relationships of switches and fabrics.

For more information on discovering the topology, see Topology discovery.

Monitoring connectivity devices

ControlCenter can be set to monitor all of the connectivity devices in the SAN. For example, you can monitor:

- Addition, removal and swapping of connectivity devices
- Configuration and status changes to devices and their ports
- Switch topology changes
- Name changes
- System URLs used to launch the device management software

Specific devices can be selectively monitored. For example, you may want to monitor the startup of a new hub or switch.

For more information on monitoring the topology, see the following topics:

- Connectivity Agent for SNMP overview
- Connectivity Agent for Switches overview

Connection settings

You can check or modify the connection settings of switches and fabrics in the topology. They typically include an IP address for management purposes and may also include a User ID and password. Connection settings vary among switch vendors as well as what users provide to the Switch Agent for connecting to a switch.

For more information, see Connection settings.

Creating user-defined objects

An object may remain undiscovered, and therefore unrepresented in the Console if ControlCenter cannot identify any of its following attributes:

- IP address
- director
- ports
- serial number
- type
- management information base (MIB)
- Fibre Channel adapter (FA) port
- Neighboring switch
- world wide name (WWN)

ControlCenter's topology editing utility allows you to manually depict objects in the topology that cannot be discovered, and further, to display these undiscoverable objects in the topology map.

The Create/identify wizard prompts you to manually enter some basic object properties and it's relationship to other devices in the topology. The information you provide through the wizard is entered into the Repository, where it persists, the same as data received from all ControlCenter and third-party agents.

For more information on depicting undiscoverable objects in the topology, see Topology editing.

Identifying unknown ports

Unassociated ports are stored in the Unknown Ports folder in the tree panel. The topology editing utility can be used to identify these unknown ports with user-defined objects.

For more information, see Identifying unknown ports.

Topology map

ControlCenter's topology map is a pictorial rendering of devices in the topology. Tree-selected elements and the connectivity relationships between them appear in a graphical display in the Console's target panel. Many ControlCenter operations can be executed from the topology map.

For more information on viewing the topology, see Topology map.

Login history table viewer

The Login history table (LHT) viewer displays the login history tables for all Symmetrix units in the SAN. You can use the login history tables to verify connections between hosts and Symmetrix units and to track volume-access configuration changes in Symmetrix systems.

For more information on viewing Symmetrix login history tables, see Login history table viewer.

Supported devices

ControlCenter discovers a wide range of FibreAlliance-compliant devices in the topology and renders them accessible in both the Console tree and the topology map.

When ControlCenter encounters a supported switch during discovery, it automatically attempts to discover the topology information for that switch, prompting for connectivity information as needed. Supported switches are listed in the following table:

Switch Vendor	Organization Unique Identifier (OUI)
Brocade Communications Systems	006069
McData / EMC	080088 006048
QLogic	00C0DD

Monitoring Symmetrix volume-access control

ControlCenter starts monitoring volume-access control configurations within Symmetrix systems upon installation of the SDM Agent. For more information, see Connectivity Agent for SDM overview.

Related topics

- ControlCenter agents overview
- Connectivity Agent for SNMP overview
- Connectivity Agent for Switches overview
- Connectivity Agent for SDM overview
- Topology discovery
- Connection settings
- Topology editing
- Topology map
- Login history table viewer
- Discovery and monitoring requirements

Topology discovery

ControlCenter automatically discovers and monitors the hosts, storage arrays and connectivity devices in the topology via the agents installed through the Console. In addition, you can initiate discovery of connectivity devices any time you wish. Once a connectivity device is discovered, ControlCenter monitors those devices.

Notes

- For information on preparing your environment for discovery, see Discovery and monitoring requirements.
- For more information about monitoring connectivity devices, see Connectivity Agent for SNMP overview
- For more information about monitoring switch topology, see Connectivity Agent for Switches overview

User-initiated discovery includes the following steps:

1. Finding the connectivity devices switches, hubs, bridges, converters, extenders, patch panels, gateways, and so on.
2. Discovering switch topology the ports, links, neighbors and fabric configurations of the switches found.

top

Finding connectivity devices

Finding connectivity devices is the first step of topology discovery. Connectivity devices are the devices that indirectly connect hosts to storage systems, including connecting to other connectivity devices. This step does not include discovering topology information for switches and fabrics.

You find connectivity devices by entering an IP address or range into the Search panel of the Search for Connectivity Devices dialog box. The Connectivity Agent for SNMP finds these devices and ControlCenter displays them in the Results panel.

Discovering switch topology

Discovering switch topology is the second step of topology discovery and is performed by the Connectivity Agent for Switches (Switch Agent). An option in the Search panel of the Search for Connectivity Devices dialog box enables ControlCenter to discover topology information for all switches found in step one. If selected, the Switch Agent discovers the switch links, neighbors, logical relationships and fabrics associated with these switches.

Unconfigured switches and switches configured incorrectly cannot be discovered. A second option in the Search panel enables ControlCenter to prompt for the connection settings of switches that require setup. After supplying the missing connectivity information, you can discover topology information for these switches.

The Details panel displays detailed information on the switches selected in the Results panel. A dynamic **Import** button appears when more information is available on supported switches displayed in the Details panel.

To discover the topology of your SAN, see Discovering the topology.

Related topics

- Topology
- Discovering the topology
- Discovery and monitoring requirements
- Search for connectivity devices dialog box
- Connectivity Agent for SNMP overview
- Connectivity Agent for Switches overview

Discovery and monitoring requirements

The following agents must be installed and running before you can use ControlCenter to discover, monitor or set up devices in the SAN.

Agent	Comments
Master Agent	Manages all agents. Typically installed on each host during ControlCenter installation. Cannot be installed through the Console.
Connectivity Agent for SNMP	Discovers and monitors connectivity devices in the SAN. Typically installed during ControlCenter installation.
Connectivity Agent for SDM	Monitors volume-access control in Symmetrix systems. Install on your computer through the Console.
Connectivity Agent for Switches	Discovers and monitors switch topology information. One installation is necessary per ECC Server. Can be installed on any user's computer.
host agent	Helps manage a host's storage activities. Install one of the following on your computer through the Console. • Host Agent for Windows • Host Agent for AIX • Host Agent for HP-UX • Host Agent for Solaris • Host Agent for Novell • Host Agent for MVS HSM • Host Agent for MVS SMS • Physical Agent for MVS • Logical Agent for MVS

storage agents	Manages storage arrays. Install one or more on your computer through the Console. • Storage Agent for Symmetrix • Storage Agent for CLARiiON • Storage Agent for Celerra • Storage Agent for StorageWorks • Storage Agent for HDS • Storage Agent for RVA/SVA • Storage Agent for IBM ESS
Oracle Agent	Manages an Oracle database instance. Install on hosts where your Oracle databases are installed (not necessary for ECC Repository).
vendor agents	See documentation provided by device vendors.

It may be necessary to edit the data collection policies associated with some of these agents before the agent can function in the SAN.

Related topics

- Connectivity Agent for SDM administration
- Connectivity Agent for Switches administration
- Connectivity Agent for SNMP administration
- Installing agents
- Topology
- Topology discovery

Discovering the topology

Note: Before you can fully discover the topology, certain agents must be installed in your environment and on your host. For more information, see Discovery and monitoring requirements.

To find connectivity devices and discover topology information for switches and fabrics:

1. Click the **Monitoring** or **ECC Administration** task and select **Discover** from the Topology menu. The Search for Connectivity Devices dialog box appears.
2. In the Search panel, select **Search for a single device** or **Search for a range of devices**.
3. Enter a device name or IP address/range under the selected option.
4. Click **Advanced Options** and adjust the default Read/Write Community and SNMP Port settings, if necessary.
5. Clear **Discover fabric for switches** to find connectivity devices only, or select this option to discover fabric information for supported switches.
6. If **Discover fabric for switches** is selected, select **Prompt for missing connectivity information** to cause ControlCenter to prompt for missing connectivity information during discovery of switches. Clear this option to ignore devices with missing connectivity information.
7. Click **Search Now** after you have selected all your search options. The status field in the lower right corner of the dialog box displays the progress of discovery. The devices found and switches discovered appear in the Results panel as progress is made.
8. Click **Stop Search** to stop discovery.
9. In the Results panel, select **Show Only Search Results** to display only the connectivity devices found at the IP addresses entered in the Search panel. Select **Show All Connectivity Devices** to display the connectivity devices found plus the connectivity devices connected to switches.
10. Click a device in the results table to select it and display its details in the details panel below.
11. If an undiscovered supported switch is displayed in the Details panel, an **Import** button appears with the message: `There is more information available for this switch. Press the import button to retrieve it.` Click **Import** to retrieve additional information for this switch.
12. Click **Help** to launch the Help topic for this dialog box.
13. Click **Close** to close the dialog box.

Related topics

- Topology discovery
- Discovery and monitoring requirements
- Search for connectivity devices dialog box
- Connection settings dialog box

Topology map

The topology map is a pictorial rendering of elements in the storage network that depicts tree-selected objects and the connectivity relationships between them. This topic contains the following sections:

- Features
- Categories rendered
- Customization
- Map tools

Features

You can use the topology map to:

- **Display the physical configuration of the storage network:** When a storage container, adapter, port, host, or fabric is placed in the map, the object and the elements to which it is connected appear in the map.
- **Display paths between host HBA and Symmetrix FA ports:** Paths are anchored by hosts on the left side of the map and by Symmetrix systems on the right side. Connectivity devices configured between hosts and storage appear in the middle section of the map. If the connectivity device is a switch, the fabric associated with the switch is shown as the switch parent. If the fabric is collapsed, the fabric icon is displayed. When expanded, the fabric is displayed as a colored box that contains the switches and switch ports making up the fabric.
- **Arrange hosts and storage by name:** The devices in the hosts and storage folders in the map can be arranged by name. When one hundred or more hosts or storage arrays appear in the map, they are automatically arranged by name.
- **Create and associate objects in the SAN:** Using the Create/identify wizard, host Fibre Channel adapters can be added to hosts; connectivity Fibre Channel ports can be added to switches; and unknown ports can be identified with user-defined objects. All user-defined objects created in the tree panel can be displayed in the map.
- **Display updated status of objects monitored in the SAN:** The topology map is updated in much the same way as the Console tree panel. Object status, relationships, and alerts displayed in the tree are also displayed the map. When an object is expanded so that it is displayed in both the tree panel and the map, selecting that object in one place also selects it in the other.
- **Display object type:** The floating legend palette makes it easy to identify all of the objects displayed in the map. Just like in the tree panel, you can right-click an object displayed in the map to access its properties and relationships.
- **Perform ControlCenter tasks:** Many of the tasks you can performed from the tree panel you can also perform in the map. For example, you can access the management URLs of depicted devices; check and modify switch and fabric connection settings; and associate unidentified ports with user-defined objects.

Categories rendered

The following categories of elements can be rendered in the topology map:

- hosts
- storage systems
- adapters
- ports
- links
- fabrics

Containers, switches, HBAs and other objects can be nested in the topology. The final rendition in the topology map contains ports and physical links. As you drill down by expanding nested icons in the map, logical links between elements in the map are displayed.

Mousing over a link in the map changes the color of the link to blue, displays the status of the link in the status area, and elicits a tool tip that displays the endpoints of the link. Physical links display the link name and both end port names. If one or both endpoints of a link are not fully expanded in the map, the link is logical, and the name of the parent container(s) displays as a logical endpoint in the tool tip. Broken links are indicated in the map.

Customizing the map

You can customize the topology map by:

- Expanding and collapsing parent icons in a complex depictions
- Toggling on and off logical links
- Moving parent containers vertically in the map
- Moving end ports within confines of the parent box within which they are displayed
- Zooming in and out of the map
- Arranging a link so that its end ports appear in the same screen for easy viewing

Map tools

The topology map has a Hide / Show Links button that toggles on and off all logical links in the map.

The find tool is used to locate objects in the map.

You can launch a floating tools palette containing a set of map tools that can also be accessed through the topology map menus. The tools palette contains the following map tools:

- Move Move objects around in the map. You can manipulate complex map depictions to display the end ports of a link and its intermediary connectivity devices in the same plane for easy viewing.
- Zoom box Draw a box around any section of the map to magnify it. Use in conjunction with the overview tool to roam around the entire map and magnify any section of it.
- Zoom in Point and click to magnify any section of the map.
- Zoom out Point and click to reduce the magnification of the map.
- Default size Reset the map to the default 100% magnification setting.
- Overview Open a small window depicting the entire topology map with a selection box drawn around the section of the map that is currently magnified. Drag the selection box around in the overview window to magnify any section of the map.

Objects displayed in the map can be renamed.

The map can be printed and exported to an external file.

Related topics

- Viewing the topology
- Topology
- Topology editing

Viewing the topology

The topology map appears in the Console target panel and adheres to the selection and update rules outlined in Using the Console target panel. Object status, relationships, and alerts displayed in the Console tree panel are also displayed in the map.

When a storage container, adapter, port, host, or fabric is placed in the map, its connected elements also appear. Objects cannot be deleted from the map. However, when an object that is displayed in the map is deleted from ControlCenter, the object and its children are removed from the map, along with any associated links.

Hosts are displayed in the left column of the map and storage elements in the right column. Connectivity devices are displayed in the middle column. If the connectivity device is a switch, the fabric associated with the switch is shown as the switch parent. If the fabric is collapsed, the fabric icon is displayed. When expanded, the fabric is displayed as a colored box that contains the switches and switch ports making up the fabric.

ControlCenter provides a suite of tools and features that create flexibility in viewing the topology through the map. When an object is expanded so that it is displayed in both the tree panel and the map, selecting that object in one place selects it in the other. The find tool can also be used to locate objects in the map. Mousing over a link highlights it so you can easily follow it to the end port. Turning off logical links with the Hide/Show Links button frees up space in the map and makes it easier to work. The move tool can be used to bring a link and its connectivity devices into the same horizontal plane. The options on the tools palette allow you to roam around a large map area while zooming in and out. Many SAN management operations can be performed in the map.

Select the task you want to perform from the list below.

Note: Many of the procedures in this topic include accessing the topology map Customize submenu. You can access this submenu from the right-click context menu and the Action menu in the topology map title bar. The tools accessed on the Customize submenu can also be accessed from the tools palette.

- Opening the topology map
- Displaying objects in the map
- Launching the legend palette
- Arranging hosts and storage by name
- Using the move tool
- Using the zoom box
- Using the zoom in tool
- Using the zoom out tool
- Using the actual size tool
- Using the overview tool
- Using the tools palette
- Hiding and showing links in the map
- Finding objects in the map
- Printing the map
- Exporting the map

To open the topology map:

- Click the **Monitoring** task drop-down menu and select **Topology Map**. The Topology map displays in the target panel.

To display objects in the topology map:

1. In the tree panel, select an object(s) to display in the map. The object and all its connected elements and links appear in the map.
2. Expands objects to display their children.

Note: For Help using the tree panel, see Using the Console tree panel.

To launch the legend palette:

- Right-click in the topology map and select, **Legend Palette**. The floating legend palette appears. You can use it to identify the icons displayed in the topology map.

To arrange host or storage containers by name:

1. Right-click the Host or Storage top-level directory in the map and select **Arrange By, Name**. The objects in the directory are arranged in alphanumeric order. When 100 or more hosts or storage arrays are displayed in the map, they are automatically arranged them by name.

To move objects in the topology map:

1. Right-click in the topology map and select, **Customize, Move Node**. The cursor turns into a hand.
2. Drag the icons to the desired location in the map. You can move parent icons up and down in the map. End ports can be relocated within the confines of their parent container. The host and storage directories can be moved horizontally to another column in the map.
3. Right-click in the topology map and select, **Customize, Move Node**. The move tool is turned off and the cursor returns to normal.

To use the zoom box to magnify the map:

1. Right-click in the topology map and select, **Customize, Zoom Box**. The cursor turns into a selection tool.
2. Draw a box around the area in the map that you want to magnify. The selection is magnified, retaining full functionality.
3. Use the zoom box in conjunction with the overview tool to roam and magnify any section of the map.
4. Right-click in the topology map and select, **Customize, Actual Size** to restore the map to its normal size.

To zoom in on the map:

1. Right-click in the topology map and select, **Customize, Zoom In**. The map is magnified by a factor of 1.5.
2. Repeat step 1 to continue magnifying.
3. Use the zoom in tool in conjunction with the overview tool to roam and magnify any section of the map.
4. Right-click in the topology map and select, **Customize, Actual Size** to restore the map to its normal size.

To reduce the map in magnification with the zoom out tool:

1. Right-click in the topology map and select, **Customize, Zoom Out**. The map is reduced in magnification by a factor of 1.5.
2. Repeat step 1 to continue reducing magnification.
3. Right-click in the topology map and select, **Customize, Actual Size** to restore the map to normal.

To use the actual size tool to restore the map to its normal size:

- Right-click in the topology map and select, **Customize, Actual Size**. The map is restored to normal in magnification. The actual size tool is also known as the default size tool.

To roam and magnify the map with the overview tool:

1. Right-click in the topology map and select, **Customize, Overview**. A miniature window appears depicting the entire topology map with a selection box drawn around the section of the map that is currently magnified.
2. Drag the selection box around in the overview window to magnify any section of the map.

To launch and use the tools palette:

1. Click **Action** in the topology map title bar and select **Tools Palette**. The floating tools palette appears.
2. Select one of the buttons to activate one of the following tools:
    - move
    - zoom box
    - zoom in
    - zoom out
    - default size
    - overview

To hide and show links in the map:

1. Select **Hide Links** in the topology map title bar. All the logical links in the topology map disappear.
2. Select **Show Links** in the topology map title bar. All the logical links in the topology map reappear.

Broken links are designated in the map by a small icon breaking the link.

To find objects in the map:

1. Select **Find** in the topology map title bar. The find tool appears.
2. Enter the full name of an object you want to find in the map and click **Next**. An object with that name is selected and displayed in the map.
3. Continue clicking **Next** until you find the correct object.

When an object is displayed in both the tree panel and the map, selecting that object in one place selects it in the other.

To print the map:

1. With the map in focus, select **File, Print**. The Print dialog box appears.
2. Make your selections and click **OK**.

A Print Preview option is also available on the **File** menu.

To export the map to an existing file:

1. With the map in focus, select **File, Export**. The Export dialog box appears.
2. Enter the path and file name where the exported information will reside, or click **Browse** to locate the file. Any information in the existing file will be overwritten.

Related topics

- Topology map
- Discovery and monitoring requirements
- Topology
- Topology discovery
- Using the Console tree panel
- Using the Console target panel

Topology editing

The topology editing utility allows you to manually depict elements in the topology that cannot be discovered by ControlCenter. The Create/identify wizard is used to create these user-defined objects.
For example, some elements do not have software-based management interfaces and are wholly hardware entities. The Create/identify wizard allows you to depict these undiscoverable objects in the topology by providing some basic object properties. The user-defined object and its information are entered into and persist in the Repository, just like discovered object information.
The Create/identify wizard:

- Creates user-defined objects
- Identifies unknown ports

Topology editing and discovery

User-defined objects may be created, and then later discovered as having properties that do not match those that a user had defined earlier. To avoid inconsistencies, you must enter valid properties for the user-defined object when you create it. ControlCenter uses these properties to correlate a user-defined object with a discovered element. If a user-defined element exists with the same properties as the discovered element, ControlCenter overwrites any inconsistent properties and notifies the user of these inconsistencies via an alert. An object's properties include its relationship to other objects.

User-defined objects created

You can depict the following objects in the topology with the *Create/identify wizard*:

Containers

All ESN containers fall into one of these three categories:

- storage clients Any device that requests data from a target and generates data for application use such as a host or a physical server.
- storage targets Any hardware media that stores data persistently such as a storage array or a tape device.
- connectivity devices Any device that indirectly connects hosts with storage systems, including devices that connect to other connectivity devices. For example, switches, hubs, bridges, extenders, patch panels, and so on.

Adapters

An adapter generally refers to the card that is plugged into a container's slot (bus). An adapter may contain one or more ports. Adapters can be of the following types:

- client SCSI adapter
- client Fibre Channel adapter
- target SCSI adapter
- target Fibre Channel adapter

Ports

The port refers the point of physical connection to an adapter. The adapter has a one-to-many relationship with the port. Port types are:

- client Fibre Channel
- client SCSI
- target Fibre Channel
- target SCSI
- connectivity Fibre Channel

The wizard constrains the order of association. For example, a port cannot be presented before an adapter.

Physical associations

- Associate a container with an adapter.
- Associate an adapter with a port.

To create user-defined objects with the Create/identify wizard, see Creating user-defined objects.

Identifying ports

Unknown ports are ports that are not associated with an adapter. You can use the Create/identify wizard to identify unknown ports with user-defined objects. For more information, see Identifying unknown ports.

Related topics

- Identifying unknown ports
- Creating user-defined objects
- Create/identify wizard

Creating user-defined objects

The Create/identify wizard is used to depict undiscoverable objects in the topology.

To create a user-defined object:

1. In the tree panel, right-click the Connectivity, Hosts or Storage folder, or an adapter, and select **New, *element***. The Create page of the Create/identify wizard displays with the object type preselected as context.
2. Enter required information into the wizard fields for the object you want to create, clicking **Next** until you get to the Associate Ports page.
3. Select the ports that you want to associate with the new object on the **Associate Ports** page and click **Next**. The Associate Ports page contains a list of all the unknown ports in the ControlCenter Repository.
4. On the final page of the wizard review all the fields and ports that are to be set for the new object and click **Finished,** or click **Back** to make changes.
5. Verify that the new element displays in the tree.

Related topics

- Identifying unknown ports
- Topology editing
- Create/identify wizard

Identifying unknown ports

Unknown ports are ports that are not associated with an adapter, yet are known to exist. They can be accessed in the Unknown Ports folder in the tree panel.

To identify an unknown port with a user-defined objects:

1. In the ControlCenter tree, expand the Connectivity folder, and then expand the Unknown ports folder.
2. Right-click an unknown port in the tree, and select **Identify Port**. The Identify page of the Create/identify wizard displays with the port WWN and vendor displayed.
3. From the drop-down list, select the type of user-defined object you want to identify with the unknown port, and click **Next**.
4. Select the container you want to identify with the unknown port, and click **Next**.
5. On the final page of the wizard review all the fields and ports that are to be set for the new object and click **Finished,** or click **Back** to make changes.
6. Verify that the new element displays in the tree.

Note: If you have mistakenly identified a port, you can use the Create/identify wizard to re-identify the port with the correct device.

Related topics

- Creating user-defined objects
- Topology editing
- Create/identify wizard

Deleting objects from the topology

The delete operation permanently removes an object from the topology, including its related elements such as associated adapters and ports, alerts and command history.

Associated discovered adapters and ports that were deleted from the Repository with an object can be rediscovered through topology discovery.

You can delete objects only in the tree panel. You can delete the following types of objects:

Storage systems	Fibre Channel adapters
Hosts	Fabrics
Unknown ports	Links
Generic hardware ports	Network-attached storage
Connectivity devices	File systems
Databases	

To delete an object from the topology:

1. Right-click the object you want to delete in the tree panel, and select **Delete**. A confirmation dialog box appears. **Note:** Before the confirmation dialog box appears, ControlCenter checks to see if the delete operation is in compliance with the business rules for deleting objects. If these preliminary checks stall, a dialog box appears. Click **Cancel** to halt the delete operation, or do nothing and the dialog box will dismiss when the stall ends. If the preliminary checks fail, a dialog box appears. Click **OK** to cancel the delete operation and then consult your ECC administrator.
2. If you want to be notified when the delete process is complete, select the **Notify me when delete is done** checkbox.
3. Click **OK** to proceed or **Cancel** to abandon the delete operation. ControlCenter permanently deletes the entire object from the Repository. If you requested notification, you are notified when the deletion is complete.
4. If the delete operation fails, a dialog box appears. Click **OK** and consult your ECC administrator.

Business rules for deleting objects

Business rules categorized in this section may restrict the deletion of some objects. In addition, you must have the appropriate permissions before you can delete objects from ControlCenter.

Rules for deleting all objects

You cannot delete an object if an agent that discovers data for that object is running.

Note: Some objects are discovered and monitored by multiple agents.

Rules for deleting hosts

You cannot delete a host on which there is an active ECC Server or Store.

Rules for deleting file systems

You can only delete file systems that are reported as being *undiscovered* by the storage agent.

Related topics

- Delete confirmation dialog box

Login history table viewer

The Login history table viewer displays information from the login history tables (LHTs) of all VCM-enabled Symmetrix systems. LHTs store current and historical login information for all Fibre Channel adapters (FAs) in a Symmetrix system. When a host HBA logs in to a Symmetrix system, a record is created in the LHT. Each FA port on a Symmetrix contains its own row in the login history table.

You can use the information in the LHT Viewer to:

- Verify connections between hosts and Symmetrix systems.
- Track configuration changes. For example, you can view a list of host bus adapters (HBAs) that were once connected to an FA, and see if they were connected through a switch.

The LHT Viewer can be minimized, maximized, placed behind the main console window, and can run multiple sessions.

Notes

- You must have the Connectivity Agent for SDM installed and running on the host connected to Symmetrix systems in order to read the current login information.
- To enable volume configuration management (VCM) on a Symmetrix system, see the *ESN Manager Product Guide*.

Related topics

- Viewing the login history table viewer
- Topology discovery
- Topology

Viewing the login history

To view the login history table:

1. Click **Monitoring** on the task bar.
2. Select **View Login History** from the **Topology** menu. The Login history table viewer appears.
3. Select a Symmetrix from the list to view its login history in the table.

Field descriptions

Status	Time stamp. Displays when the LHT Viewer is opened.
List	Displays the VCM-enabled Symmetrix systems in the SAN.
Login history table	Displays the login history table of the object selected in the list. The table is sortable and supports row selection and multi-selection but does not allow cells to be edited. **FA** Fibre Channel adapter or director **Node** name or serial number of a host machine or Symmetrix system **Port** FA port number of a Symmetrix system or HBA port WWN of a host machine **Port WWN** FA port WWN of a Symmetrix system or HBA port WWN of a host machine **Node WWN** WWN of a host machine, Symmetrix system, or a switch **Vendor** manufacturer of HBA or Symmetrix system **Source ID** of agent that entered this record (table row) **Logged In** True if logged on; False if not logged on **On Fabric** True if entire path is through a fabric; false if entire path is not through a fabric
Show only active entries	Displays only FAs and ports that are logged on when selected. Displays all FAs and ports in the SAN when cleared.
Refresh	Retrieves the latest LHT data directly from the Connectivity Agent for SDM. Information for each Symmetrix is retrieved the first time a Symmetrix is selected. When the selection is changed, and then reselected, the login history data changes instantly. The status at the top of the LHT Viewer reflects the time that the data was actually retrieved from the Connectivity Agent for SDM. If the topology changes, and you wish to see the changes in the LHT Viewer, you must **Refresh** to view the new data. The progress of data retrieval is displayed in the status at the bottom of the viewer. When the new data is acquired, status at the top of the viewer reflects the time the refresh operation was performed.
Close	Close the LHT Viewer.
Help	Launches context-sensitive Help topic.
Status bar	Displays data retrieval status.

Related topics

- Login history table viewer

Connection settings

The Connection settings dialog box prompts you for connectivity information that is needed to connect to supported switches. It appears dynamically during switch discovery.

You can also launch this dialog box from ControlCenter for the purpose of checking or modifying the connection settings of a switch or fabric.

To check or modify the connection settings of a switch or a fabric in the SAN:

1. Select a switch or fabric in the tree panel.
2. Click the **Monitoring** or **ECC Administration** task and select **Connection Settings** from the **Topology** menu. The Connection Settings dialog box appears.

Field descriptions

Switch	Name of the switch selected in the tree panel. Default name is WWN. If a fabric is selected, all switches in the fabric are listed. A check indicates that the switch is connected with the current settings displayed in the dialog box.
Choose a vendor	Supported vendors shown in a drop-down list.
Proxy IP address	The IP address of the switch proxy to which you want to connect. (McData, QLogic)
Switch WWN	A valid WWN for the switch to which you want to connect. (McData, QLogic)
Target IP address	The IP address of the switch to which you want to connect. (Brocade)
Username	The host username. (Brocade)
Password	The host password for the switch to which you want to connect. (Brocade)
Revert	Resets all fields for the selected switch to the values that were displayed when you opened this dialog box.
Apply to all switches in fabric checkbox	Applies connectivity information to all the switches in the fabric when selected.
Also import fabric information checkbox	Imports fabric information for the switch when selected.

Related topics

- Topology
- Topology discovery
- Discovering the topology
- Search for connectivity devices dialog box

Performance Management

ControlCenter performance management supports a wide variety of software options designed to improve performance and maximize data availability.

Performance view

The common task Performance can be used to display both tables and charts.

See Using the Performance command

Quality of Service

Quality of Service (QoS) allows you more flexibility in managing the performance of your Symmetrix. By reducing the resources allocated for BCV or SRDF copy operations on selected logical devices, you increase the overall performance of the other I/O operations.

See QoS for TimeFinder and SRDF

Optimizer

Optimizer spreads I/O activity evenly across the physical disks. By balancing highly active logical devices (hot spots) and lower activity logical devices (cold spots) across drives, seek activity is balanced, and contention among drives is reduced.

See Optimizer Overview

Quality of Service: TimeFinder/SRDF

QoS for TimeFinder/SRDF allows you more flexibility in managing your Symmetrix system's performance. By controlling the pace of BCV or SRDF copy operations on selected devices, you can increase the performance of selected BCV or SRDF devices within those groups, or increase the performance of primary devices relative to BCV and SRDF devices.

You can specify a BCV or SRDF Quality of Service performance setting for each device in your Symmetrix unit. This setting, 0 (fastest copy rate, which is the default) to 10 (lowest copy rate), affects the service that the Symmetrix unit provides to copy operations associated with the device.

Choose the appropriate settings for each device based on its priority within your storage system. Quality of Service settings can be changed at any time to adjust for changes in your system I/O requirements.

The default Quality of Service performance setting of 0 allows the device to receive full service as resources are available within the Symmetrix unit. Applying an incremental value from 1 to 10 introduces an associated delay time before each track is copied between standard and BCV devices or SRDF R1 and R2 devices.

The delay time ranges in a nonlinear scale from 1 millisecond to 1 second as shown in the following table.

Performance Setting	Inter-track Delay (ms)
0	Default, no delay
1	1
2	8
3	27
4	64
5	125
6	216
7	343
8	512
9	729
10	1000 (1 second)

Starting TimeFinder/SRDF QoS

To start TimeFinder/SRDF QoS:

1. Specify the BCV or SRDF devices that you want to manage in the tree panel.
2. Click **Data Protection.**
3. Select **TimeFinder/SRDF QoS** from the **QoS** menu. The TimeFinder/SRDF QoS dialog box appears.
4. Select a device from the table; then use either the TimeFinder or SRDF Performance slide control to specify the degree of resource allocation for those operations.

Related topics

- Optimizer overview
- TimeFinder overview
- SRDF overview

Optimizer: Overview

Optimizer helps you increase the performance of a Symmetrix system by spreading I/O activity evenly across the physical disks. When a particular drive is in high demand, there is excessive head movement on that drive. This movement slows down read and write activity. By balancing highly active logical devices (hot spots) and lower-activity logical devices (cold spots) across drives, seek activity is balanced, and contention among drives is reduced. Throughput within the overall Symmetrix system is improved, and you experience optimal response times.

Optimizer performs self-tuning of Symmetrix data configurations from the Symmetrix service processor by:

1. Analyzing statistics about Symmetrix logical device activity.
2. Determining which logical devices should have their physical locations swapped to enhance Symmetrix performance.
3. Swapping logical devices and their data using internal Dynamic Reallocation Volumes (DRVs) to hold customer data while reconfiguring the system (on a device-to-device basis).

Topics for Optimizer include:

- Managing Optimizer
- Setting parameters
- Specifying logical device attributes (setting priority)
- Setting Time Windows
- Viewing log files
- Rolling back swaps
- Manually approving swaps
- Swapping logical devices
- Overview of Time Windows

Related topics

Quality of Service is a related software product that allows you to specify the proportion of time allocated to primary task I/O as compared to other operations.

- QoS and TimeFinder/SRDF operations

Managing Optimizer

Before you start

Once you start an Optimizer configuration session, you will have exclusive control of Optimizer commands.

Notes

- Configuration settings are persistent; they are maintained on the service processor after reboot.
- Optimizer requires Ingenuity (microcode) 5x67.

Displaying the Optimizer dialog box

To display the Optimizer dialog box:

1. Select the appropriate Symmetrix system in the tree panel or the target panel.
2. Select **Setting** from the **Optimizer** menu or the right-click menu. The Optimizer settings dialog box appears.

Related topics

- Setting general configuration
- Setting device attributes
- Configuring time windows
- Viewing log information
- Rolling back swaps
- Manually approving swaps
- Swapping logical devices (process overview)
- Time windows (concept overview)

Optimizer: Setting general configuration

The Parameter tab of the Optimizer configuration dialog box provides both status information and configuration capabilities for Optimizer.

Note: Optimizer must be stopped in order to change parameters.
The following functionality is supported:

Feature	Description
Optimizer Status	Indicates the current state and activity of Optimizer. **State** can be: • Stopped • Stopping • Started • Starting **Activity** can be: • Idle • Fetching statistics • Generating swap suggestion • Swapping
Client Status	**Lock:** - Indicates if the client holds a lock on this Symmetrix **Mode:** - Read-Write if this client holds the lock, meaning it can change the parameters displayed on this panel. Read-only indicates this client does not hold the lock.
Startup Mode	Allows you specify a manual start, or the **Automatic** option, which will start Optimizer automatically when the service processor in the Symmetrix is started.
Workload Analysis Settings	**Workload Analysis Period** — Specifies the amount of workload sampling that Optimizer should maintain for sample analysis. The minimum is one hour and the maximum is 672 hours. The default is 168 hours (per week). **Initial Period** — Specifies the minimum amount of workload sampling that Optimizer should complete before analyzing the samples for the first time. This parameter exists in case you do not want to wait until the entire workload period has elapsed before Optimizer commences its analysis and swap activity. The minimum is 0 and the maximum is the Workload Analysis Period, which is the default.
Time Windows	Displays the Time Windows dialog box that allows you to configure the time periods used by Optimizer for statistical analysis and swapping.
Swap Mode	**Automatic** — Performs each swap suggestion without user confirmation. **User Approved** — Prompts for approval before each swap.
Swap Settings	**Max Number of Swaps per Day** — Specifies the maximum number of swaps that can be performed in a 24 hour period, starting at midnight. **Max Simultaneous Swaps** — Specifies the number of swaps that can be performed at one time. The default value is equal to the number of available DRV devices, which is the maximum.
Device Attributes	Displays a dialog box that allows you to assign priority attributes to specific logical volumes. These attributes assist Optimizer during sample analysis.
Start/Stop Optimizer	Starts or stops Optimizer immediately. Optimizer must be stopped in order to change parameters.
Clear Statistics	Resets the statistics database and starts collecting new data.
Set Defaults	Resets all displayed values to their default settings, including device attributes and time windows.
Apply	Applies the specified configuration changes, but maintains the dialog box display.
Progress Bar	Displays the communication status between the Optimizer client and the Optimizer Service Process and the swap status if the Optimizer Service Process is swapping.

Related topics

- Setting device attributes
- Configuring time windows
- Viewing log information
- Rolling back swaps
- Manually approving swaps
- Swapping logical devices (process overview)
- Time windows (concept overview)

Optimizer: Setting device attributes

The Device Attributes dialog box allows you to assign priority attributes to specific logical devices. These attributes assist Optimizer during sample analysis and swapping operations. Defined attributes are:

- High Priority — Assign this device the highest priority because it contains crucial data. Optimizer attempts to achieve the best performance for this device without sacrificing the performance of other devices in this high-priority group.
- Normal Priority — This device is eligible for swap, but assign it an normal priority.
- No Swap — Do not swap.

Setting device priority

To set logical device priority:

1. Select one or more logical device rows. **Note:** To sort the table, click on any of the column headers.
2. Click one of the priority buttons to set the priority for the selected rows.
3. Click **OK** to save the changes

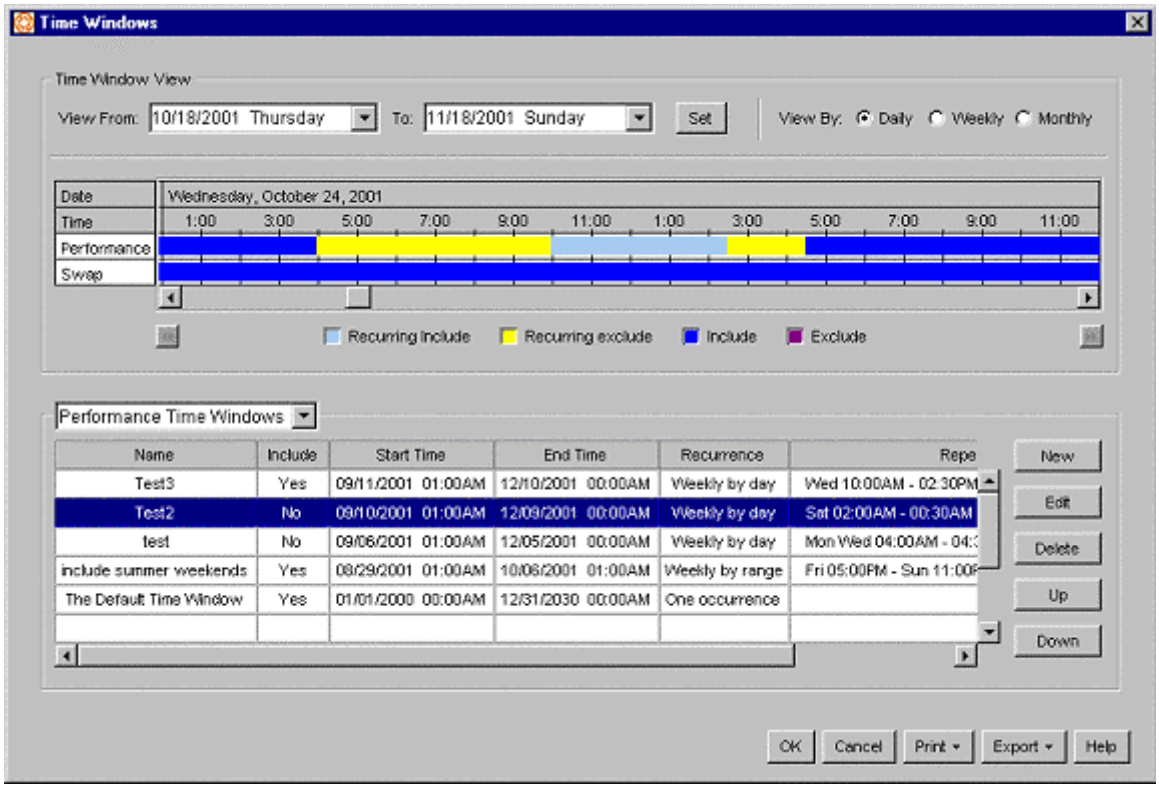
Related topics

- Setting general configuration
- Configuring time windows
- Viewing log information
- Rolling back swaps
- Manually approving swaps
- Swapping logical devices (process overview)
- Time windows (concept overview)

Optimizer: Configuring time windows

For overview information about time windows and their characteristics, read Time Window Overview.

The Time Windows dialog box contains two information tables.



The upper table

The upper table is a read only composite of all the existing applicable analysis and swap time windows, color coded for clarity.
There are four colored attributes:

Time Window Attribute	Description
Recurring Include	Perform activity during this period. Recur as specified.
Recurring Exclude	No activity during this period. Recur as specified.
Include	Perform activity for this one period.
Exclude	Except this one time period.

Notes

- You can specify the size of the time range you want to evaluate by changing the values in the **View From:** and **To:** panels, and then clicking **Set.**
- If the time range exceeds 30 days, the double arrow buttons below the upper table become active, allowing you to shift left or right to adjacent months.
- You can specify a daily, weekly, or monthly view of the time windows by making the appropriate selection in the **View By:** panel.

The lower table

The lower table is an editable summary of either the performance or swap time windows. The type of list is controlled by the drop-down menu on the left side. Time windows are listed according to priority, with the time window on the first row having the highest priority. If multiple time windows have time ranges that overlap each other, the higher-listed time window will override the others. Therefore, the order of time windows in the list resolves conflicts between overlapping time windows. Conflict resolution only applies to time windows of the same type.

Adding a new time window

1. Select **Swap Time Window** or **Performance Time Window** from the pulldown menu on the left side.
2. Click **New**.
3. The Optimizer - Select a period dialog box is displayed.
4. Specify the values you require for the new time window.
5. Click **OK**. The new time window is now added to the lower table list.

Editing an existing time window

1. Select your target row in the lower table.
Note: You can also double-click the time window bar in the upper table or the target row in the lower table.
2. Click **Edit**.
3. The Optimizer - Select a period dialog box is displayed, with the existing values displayed.
4. Edit the values you need to change.
5. Click **OK**. The revised time window values are now displayed in the lower table list.

Deleting a time window

To delete or clear a Time Window, select one or more time windows from the lower tables and then click **Delete**. The default time window cannot be deleted. Be cautious of what you choose to remove, there is no undo for this action.

Note: Press and hold Shift to select multiple time windows.

Click **OK** to save all edits and close the dialog box.

Changing priority for a time window

1. Select your target row in the lower table.
2. Click **Up** or **Down** to move this row.

Note: The time window on the first row has the highest priority. The default time window is always on the bottom and has the lowest priority.

Related topics

- Setting general configuration
- Setting device attributes
- Configuring time windows
- Viewing log information
- Rolling back swaps
- Manually approving swaps
- Swapping logical devices (process overview)
- Time windows (concept overview)

Optimizer: Selecting periods for performance or analysis

There are six versions of the **Select a period ...** dialog box. Both the performance and the analysis time windows can be configured for the following time frames:

- a single occurrence
- recurring weekly by range
- recurring weekly by day

All six dialog boxes share the following options:

Option	Description
Name	User-defined name for this time window
Include in Analysis/Performance	**Yes** includes data from this period. **No** excludes data from this period.
Effective Range	For a single occurrence, this is the time window period. For *recurring weekly by range* and *recurring weekly by day*, this is the overall range in which to use this time window
Occurrence	There are three choices to set the frequency: • One occurrence • Recurring Weekly by range • Recurring Weekly by Day

Single occurrence time window

There are no other options for the single occurrence time window.

Recurring weekly by range time window

The weekly recurrence allows you specify the starting and ending day and time for a single time window that is to recur weekly

Recurring Weekly by Day time window

The weekly by day recurrence allows you specify the starting and ending time for a time window and which of the seven days it should be used in.

Related topics

- Setting general configuration
- Setting device attributes
- Configuring time windows
- Viewing log information
- Rolling back swaps
- Manually approving swaps
- Swapping logical devices (process overview)
- Time windows (concept overview)

Optimizer: Viewing log information

The Logging tab of the Optimizer dialog box lets you retrieve current and past state information on Optimizer activities and errors.

Viewing log information

To view log information:

1. Select either **All Activity Log** or **Error Log**.
2. Specify the **Start** time and the **End** time.
3. Click **Get Log**. The log is displayed in the lower section of the dialog box.

Note: Log data is kept in memory, not files, by Optimizer. You can use the **Export** button to save the current log as a file.

Related topics

- Setting general configuration
- Setting device attributes
- Configuring time windows
- Rolling back swaps
- Manually approving swaps
- Swapping logical devices (process overview)
- Time windows (concept overview)

Optimizer: Swap history and rolling back swaps

The Swap History/Rollback tab of the Optimizer dialog box allows you to display a history of all successful swaps between the current date and a specified rollback date, as well as the ability to roll back selected swaps. You may want to do this if you suspect that performance has degraded since the original swap.

Notes

- Any command or operation issued to Optimizer while the rollback is in progress is rejected, except to cancel the rollback.
- You will receive an error message if any Symmetrix configuration changes made since the specified date prevent the rollback from proceeding.

Displaying swap history

The history of swaps is automatically displayed in the Swap History panel.

The Swap Time column displays the date and time that various swaps were completed.

Click **Refresh** to refresh the view.

The **Analysis** button opens a browser-based display of the comparative performance before and after the swapping process.

Rolling back a swap

To roll back a swap:

1. Click **Refresh** to get the current list of swaps that were successfully performed.
2. Specify the date and time to roll back to in the **Rollback To** panel.

   or
3. Determine which swap you want to roll back to in the Swap Time column. Click on the *previous* swap above it. The completion date and time for the previous swap appears in the **Rollback To** panel.
4. Click **Rollback**.

Related topics

- Analyzing performance
- Setting general configuration
- Setting device attributes
- Configuring time windows
- Viewing log information
- Manually approving swaps
- Swapping logical devices (process overview)
- Time windows (concept overview)

Optimizer: Manually approving swaps

If you have selected the User Approved swap mode in the Parameter tab, then you can access the User Approval tab to manage the manual approving or vetoing of the current swap list.

The User Approval Swap Mode table has four columns:

Column Header	Description
Group	Name of the swap group
Hyper	Name of the hyper to be swapped
From	The address location the hyper is being moved from
To	The address location the hyper is being moved to

You have the following actions available by clicking the corresponding button :

Action	Description
Refresh	Displays the list which represents the current swap suggestions, but the swaps have not executed yet.
Reject	Rejects the swap list.
Approve or Re-Schedule	Authorizes Optimizer to execute the swaps on the list after an optional specified delay. Optimizer will not generate a new swap list until after the approved swap has executed. However, the approval operation can be denied if the list has become “stale” by the time Optimizer receives the approval. This happens when you approve a list after Optimizer has already generated a new list. You can also re-schedule the swap execution time after you have approved it.
Analysis	Compares performance before and after swapping.

Related topics

- Setting general configuration
- Setting device attributes
- Configuring time windows
- Viewing log information
- Rolling back swaps
- Swapping logical devices (process overview)
- Time windows (concept overview)

Optimizer: Swap status

The Swap Status tab of the Optimizer dialog box displays a dynamically updated list of the ongoing swap operations. The table columns are defined as follows:

Swap Status List Column	Description
Group	Number of the swap group
Hyper	Name of the hyper
From	Address location from which the hyper device is being moved
To	Address location to which the hyper device is being moved
Status	Possible values are: Pending Before, or during, swap initialization Swapping Swap is in progress Completed Swap has completed

The **Analysis** button opens a browser-based display of the comparative performance before and after the swapping process.

You can use the **Export** or **Print** buttons to save the results.

Related topics

- Analyzing performance
- Setting general configuration
- Analyzing disk performance
- Viewing log information
- Rolling back swaps
- Manually approving swaps

Optimizer: Analysis

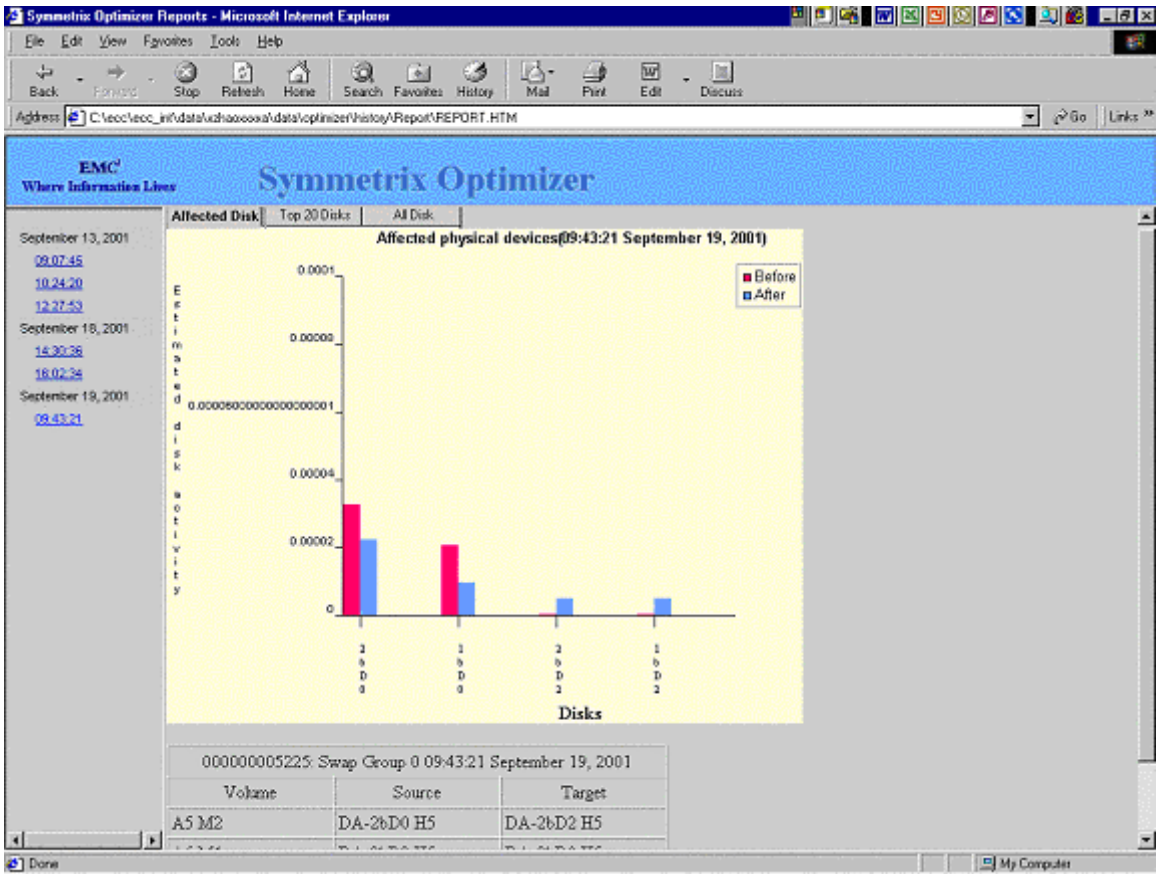
You can display a collection of charts and tables analyzing disk performance by clicking on the **Analysis** button within any of the following Optimizer dialog box tabs:

- Swap History/Rollback tab
- User Approval tab
- Swap Status tab

The charts and tables are displayed within the default browser available on your client workstation. The left panel lists the time windows when the swap is executed, while the right panel offers a tabbed display of the following three charts.

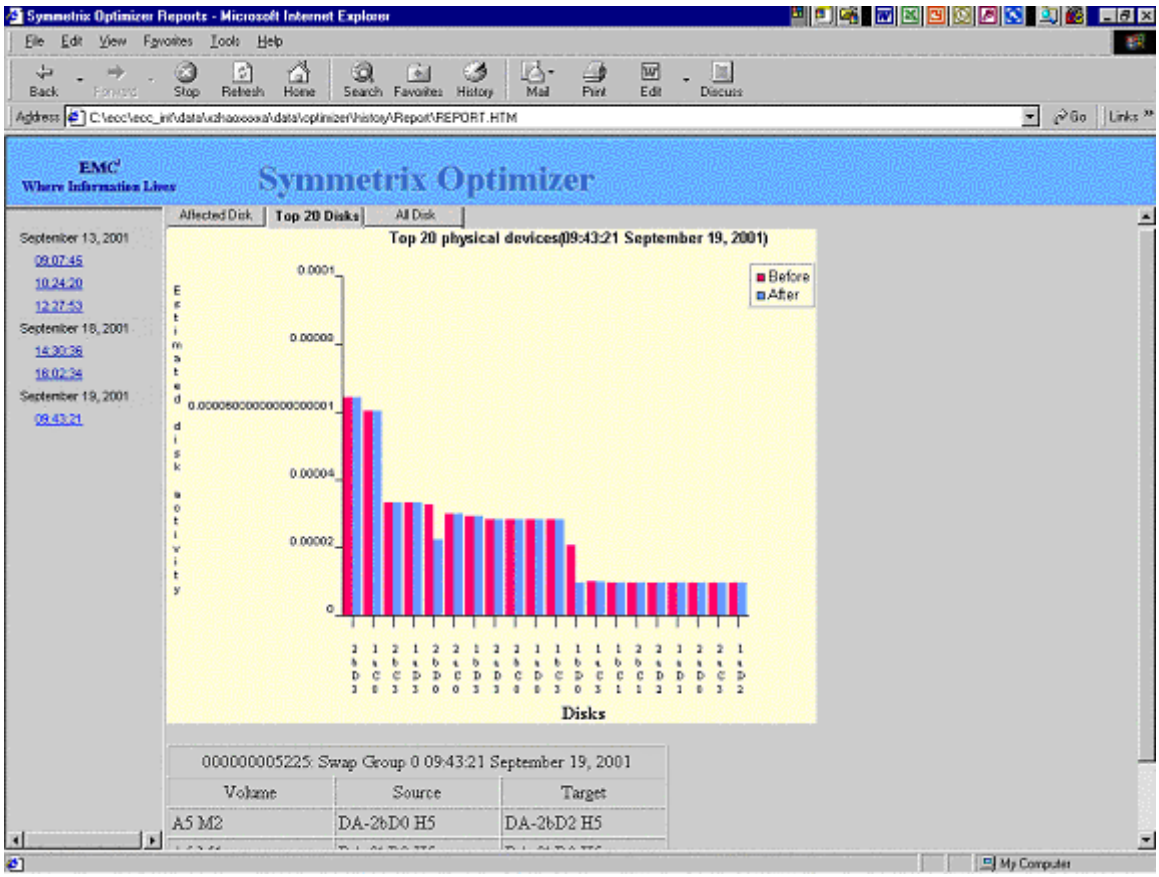
Affected Disk

The **Affected Disk** chart displays all the disks affected by the current swaps. Normally, two disks are affected for each swap.



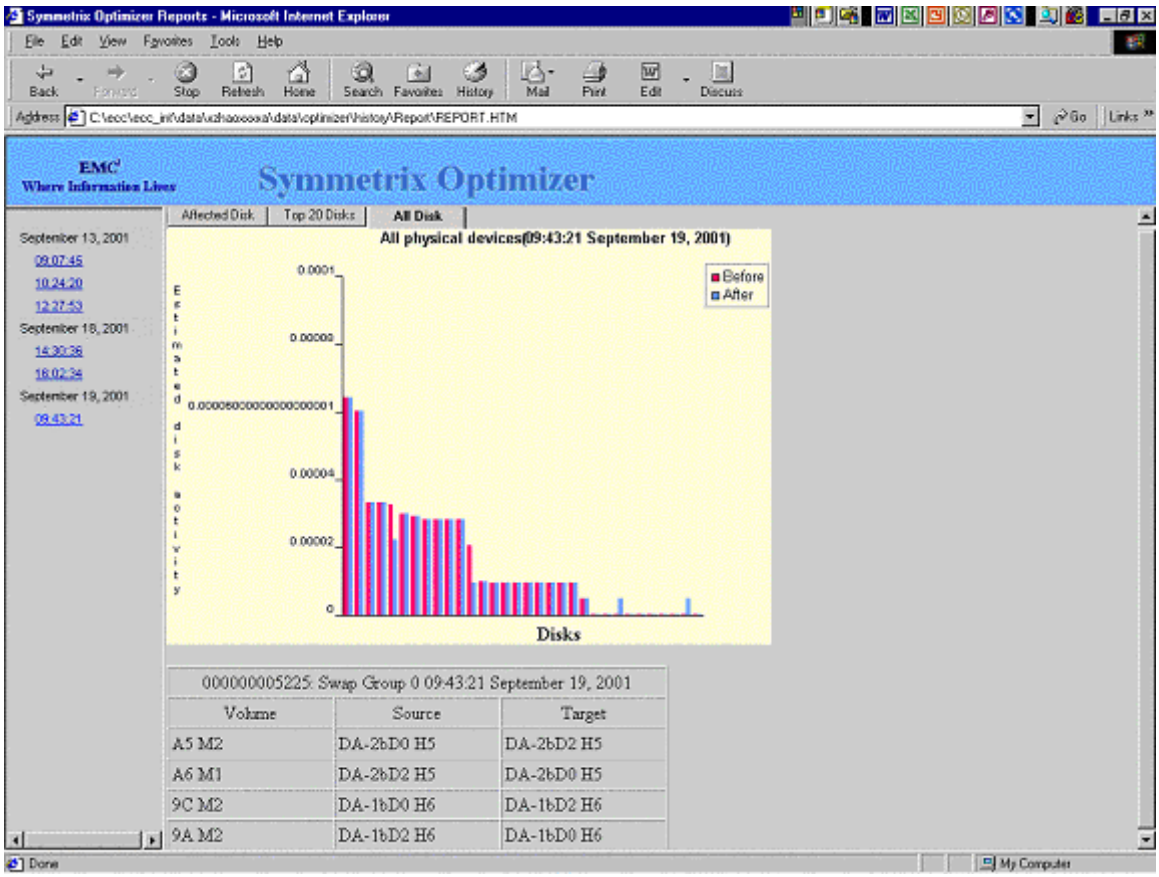
Top 20 Disks

The Top 20 Disks display is produced by first calculating the current load of all disks on the Symmetrix, than sorting the disks by activity. The 20 most active disks in the work period (with a default of one week) are displayed.



All Disk

The All Disk display shows all of the physical disks on the Symmetrix.



Related topics

- Setting general configuration
- Configuring time windows
- Viewing log information
- Rolling back swaps
- Swapping logical devices (process overview)
- Time windows (concept overview)

Optimizer: The process of swapping logical devices

Prerequisites

The following requirements must be met before two logical devices can be swapped by the Optimizer. The devices must:

- be the same size
- be the same emulation
- reside on the same system bus pair (Top high/Bottom low or Top low/Bottom high)
- not be configured as RAID or BCV devices, nor as AS400 devices

You must have DRVs configured on your Symmetrix unit.

Process overview

The logical device swapping process has five main steps:

1. Identify a pair of logical devices for swapping.
2. Designate each logical device to a DRV and copy data from the logical device to the designated DRV.
3. Swap the address locations of the logical devices.
4. Copy data back from the DRVs to the designated logical devices in their new locations.
5. Split the DRVs from the logical devices.

Related topics

- Setting general configuration
- Setting device attributes
- Configuring time windows
- Viewing log information
- Rolling back swaps
- Manually approving swaps
- Time windows (concept overview)

Optimizer: Overview of time windows

A time window is a period in time during which an aspect of Optimizer's behavior is controlled. Time windows have the following characteristics:

- A start time and end time (may be infinite in either direction) in increments of 30 minutes, and aligned on the half-hour
- A periodicity (once, weekly by day, weekly by range)
- A type of behavior to control
- The ability to include or exclude the behavior during the time window

Optimizer allows you to set as many time windows as you like. However, it maintains the list of existing time windows as a single entity (it is fetched and set as one unit). You can read the list, modify the list, and then apply the list after changing it. Optimizer provides a default time window.

Types of time window behavior

Optimizer supports two types of time window behavior: performance and swap.

Performance

Specifies which samples to consider when executing the Optimizer's swap generation algorithm. Performance time windows do not dictate when sampling takes place – they only identify which time windows are to be considered when the Optimizer's algorithm executes. This allows you to change the past or future times you want Optimizer to optimize on.

Inclusion analysis time windows instruct Optimizer to consider samples taken during their time range when making swap suggestions.

Exclusion analysis time windows instruct Optimizer to ignore samples taken during their range when making swap suggestions.

The default is a 30-year inclusion type.

Swap

Specifies when Optimizer can perform swap activity and when it cannot. The range is from the present into the future.

Inclusion swap time windows instruct Optimizer to perform swap activity during the specified time range.

Exclusion swap time windows instruct Optimizer to not perform swap activity during the specified time range.

The default is a 30-year exclusion type.

Related topics

- Setting general configuration
- Setting device attributes
- Configuring time windows
- Viewing log information
- Rolling back swaps
- Manually approving swaps
- Swapping logical devices (process overview)

Data Protection

ControlCenter supports the following Symmetrix data protection operations:

- TimeFinder Provides a Business Continuance solution that allows customers to use special devices (BCVs) that contain copies of Symmetrix devices while the primary devices are online.
- SRDF Supports the remote mirroring of a Symmetrix device to allow the highest degree of disaster recovery ability.
- QoS for TimeFinder and SRDF Allows you more flexibility in managing the performance of your Symmetrix unit. By controlling the copy pace on selected logical devices, you free Symmetrix resources and increase the overall performance of the other Symmetrix devices.
- Symmetrix Access Control Provides security controls that protect configuration and management of Symmetrix resources.

You can access most of these data protection tools from the **Protection** menu.

Symmetrix Access Control

The primary goal of storage administrators is to manage user access to data. Administrators control and monitor the activity of all of the hardware and software components of the storage network in order to protect the information on the storage subsystem. They design a physically secure topology, divide the network into subsets of devices, and implement volume access controls to manage the ESN environment.

Customers want to manage their own pool of information, but providing them all with management privileges jeopardizes the security of the entire environment. EMC created Symmetrix Access Controls to provide management capabilities in these situations.

Symmetrix Access Controls provide security controls that limit configuration and management of Symmetrix resources in an ESN environment. This functionality is available in 5567 microcode or later, and requires EMC ControlCenter v4.3 or later.

Symmetrix Access Controls allow a storage administrator to restrict management control to specific device pools for various systems. When enabled, they limit functions such as SRDF, TimeFinder, SDR, and Optimizer. They can be established for an entire Symmetrix system or a subset of Symmetrix devices.

Configuring Symmetrix Access Controls is a three-step process that involves:

1. Creating device pools
2. Creating access groups
3. Assigning actions

The configuration operations are available through the Symmetrix Command Line Interface (SYMCLI) and included as part of Symmetrix Manager, which is a component of ControlCenter. All security definitions are stored internal to the Symmetrix system, so enforcement is independent of any single host.

Creating device pools

The first step to creating Symmetrix Access Controls is to define device pools. Device pools represent the lowest level of granularity for which management security is established. Device pools contain one or more Symmetrix volumes, located in a single Symmetrix array. These pools can be defined by specifying each of the Symmetrix logical volumes or an existing SYMCLI device group.

Creating access groups

The second step in setting up Symmetrix Access Controls is to establish access groups. Access groups consist of one or more host systems. Each host is defined by a unique host ID calculated by Symmetrix Access Control. Access groups are used to define which hosts are allowed to perform specific management operations against explicit device pools. In situations where a host system contains a ControlCenter or SYMAPI Agent, all clients performing management operations through that agent inherit the security defined for the host where the agent resides.

Assigning actions

The final step is to define the actions each access group can perform on specific device pools. Actions include active management functions such as disk reallocation, volume configuration, Optimizer, and SRDF and TimeFinder controls. Hosts that have not been granted privileges have no management control, even though they may have read/write access to the volumes.

Accessing Symmetrix Access Control

Use the procedures outlined in your Solutions Enabler documentation to install, configure and enable the Symmetrix Access Control component.

Before attempting to apply any of the SYMCLI commands that perform control operations on your Symmetrix storage systems, you first should have an understanding of the SYMCLI command set, how to get online help, and how to work with the Symmetrix host database and other associated files.

Prior to starting to use the SYMCLI commands, you need to run the `symcfg` discover command in order to build your configuration database. This needs to be done once after installation, and after any changes are made to your Symmetrix configuration.

Configuring Symmetrix Access Control for ControlCenter

Use the following procedure to set up each Symmetrix system to work with ControlCenter:

1. Each Symmetrix unit that has Access Control enabled must set up an accgroup for the ECC application with the ECC PIN added as a user ID. Use the following command to set up access rights:

   ```
   symacl -sid 1166 commit -file setUpECC.txt
   ```

   Where `setUpECC.txt` contains the following Access Control commands:

   - Create a group for the ECC application:

     ```
     create accgroup ECC_APP;
     ```

   - Add an access PIN for ECC applications:

     ```
     add user accid ECCPIN name ECC_PIN to accgroup ECC_APP;
     ```

   - Grant ALL or BASE access to the ECC application group:

     ```
     grant access=ALL to accgroup ECC_APP for ALL DEVS;
     ```

2. Next, each host running a Symmetrix agent monitoring this Symmetrix must have ECC access rights. Set up an access group that contains all of the Symmetrix agent hosts and give that group the Base and ECC rights.

   ```
   symacl -sid 1166 commit -file setUpECC_Hosts.txt
   ```

   Where setUpECC_Hosts.txt contains the following Access Control commands:

   - Create an access group for hosts running ECC Agents

     ```
     create accgroup ECC_HOST;
     ```

   - Add an access ID for an ECC agent-running host to the group where <UNIQUE ID> is the unique ID of the host returned by running `symacl -unique` on that host and <HOST NAME> is the name of the host:

     ```
     add host accid <UNIQUE ID> name <HOST NAME> to accgroup ECC_HOST;
     grant access=BASE,ECC to accgroup AdminGrp for ALL DEVS;
     ```

   When you finish, the entries in the access database display as follows:

   ```
   admin# symacl list -acl
   Symmetrix ID: 000000001166
   Group Name Pool Name Access Type
   ---------- --------- -----------
   ECC_HOST   ALL_DEVS  BASE
   ECC_HOST   ALL_DEVS  ECC
   ECC_APP    ALL_DEVS  ALL
   or
   ECC_APP    ALL_DEVS  BASE
   ```

3. Symmetrix Access Control configuration is complete. Repeat this procedure for each Symmetrix requiring ControlCenter access.

Related documentation

Refer to the following documents for information about using Symmetrix Access Control with ControlCenter 5.0 to set up security on your network:

- *EMC ControlCenter Version 5.0 User Guide*, EMC Corporation
- *EMC Symmetrix Storage Concepts Guide*, EMC Corporation

Refer to the following documents for detailed information about installing, configuring, and using Symmetrix Access Control:

- *EMC Solutions Enabler SYMCLI Access Control Component Product Guide*, EMC Corporation
- *EMC Solutions Enabler Installation Guide*, EMC Corporation
- *EMC Solutions Enabler SYMCLI Base Component Product Guide*, EMC Corporation

TimeFinder: Overview

TimeFinder manages the relationship between a standard storage device (STD) and separately addressable mirrored volumes (BCVs) within the local Symmetrix system.

These mirrored volumes contain a copy of the data while the original device is online for regular I/O operation. After the mirror image is established, you can split it from the standard device, manipulate the data (back it up or perform applications testing), and later reestablish the mirror image with the standard device.

Before using TimeFinder, some of the disks in the Symmetrix system must be configured (through the Storage Allocation task) as special disks known as Business Continuance Volumes (BCVs). Each BCV device has its own host address, and is configured as a stand-alone device. You then pair the BCV with a standard Symmetrix volume.

TimeFinder device types

In addition to the STD and BCV devices, TimeFinder also supports two other device types:

RBCV This is a BCV device that is both mapped to an R2 SRDF device, viewing it as a STD, as well as acting in the role of an R1 SRDF device for another remote R2 SRDF device.

BRBCV This is a BCV device that is both mapped to an R2 SRDF device, viewing it as a STD, as well as acting in the role of an R1 SRDF device for another remote R2 SRDF device.

The TimeFinder process

1. Define a device as a BCV using Configuration Manager.
2. Establish a new pair relationship between an STD device and the BCV device. Once the BCV is established as a mirror of the standard device, it is not accessible through its original device address.
3. Split the BCV device from the standard device with which it was previously paired. After a split, the BCV device has valid data and is available for backup or other host processes through its original device address.

Once host processes on the BCV device are complete, the BCV may again be mirrored to a standard device (either the same device to which it was previously attached or a different device). It can then acquire new data for other BCV processes or update the standard device with any new data from the completed BCV processes.

Related topics

- Defining devices as BCV
- Establishing a new BCV pair
- Attaching a preferred device
- Splitting a BCV pair
- Establishing a BCV pair
- Restoring a BCV pair
- Displaying TimeFinder devices

TimeFinder: Displaying data about BCVs

To display a table listing all the BCV devices and their characteristics:

1. Select a Symmetrix system from the tree panel.
2. Click **Data Protection**, and then select **TimeFinder** from the corresponding menu.
3. The TimeFinder table appears in the information panel.

The following table describes the columns in the TimeFinder table.

Column Headings	Description
STD Host-Dev Grp	Name of the device group containing the specified STD device
Symmetrix	Symmetrix ID
STD	Device ID of the STD device
BCV	Device ID of the BCV device
BCV Host-Dev Grp	Name of the device group containing the specified BCV device
State	Current state of the BCV pair
Last Action	Date and time of the last TimeFinder operation.
STD inv trks	Number of invalid tracks on the STD device
BCV inv trks	Number of invalid tracks on the BCV device
MBs left	Remaining storage capacity, measured in MBs.
MBs/sec	Data flow rate between the BCV pair, measured in MB per second.
Time left (sec)	Time remaining to complete a data transfer

You can right-click in the table area to display a menu that allows you to show and hide columns and move to a specified row.

Related topics

- Defining devices as BCV
- Establishing a new BCV pair
- Splitting a BCV pair
- Establishing a BCV Pair
- Restoring a BCV pair

TimeFinder: Device group operations

A BCV device must be associated with a device group before it can be paired with a standard device in the group. Device groups are groups of devices that can be managed using a single device group name.

TimeFinder device group operation notes

- A BCV device cannot be associated with more than one group at the same time. All the devices in a device group must belong to the same Symmetrix unit.
- You can associate a BCV with a device group, even if it has already been paired with another device. You should avoid doing this, as this situation requires the use of the **Force** option during establish operations, and can produce many warning messages when associating BCVs in large drag-and-drop operations.

  To avoid this problem, associate the paired BCV device with this group, thereby eliminating the need for the **Force** option. You may want to use the TimeFinder, SRDF or Device properties tables to determine if a device is already a member of a device group.
- You may find that drag and drop group operations are easier to perform if you split the Source panel into two views, one showing the available devices, and the other showing the group folders.

Creating a device group

1. Click on the **Device Groups** folder under the appropriate host.
2. From the right-click menu, select **New Device Group**. The following dialog box appears:

3. Specify a name and the type of devices (STD, R1, or R2) for the group.
4. Click **OK**. The new device group is created and added to the tree panel.

Pairing an STD device and a BCV device without synchronizing data

1. Create a device group, if one does not yet exist.
2. Add STD devices to the Group Members folder and BCV devices to the Local BCVs folder.
3. After populating the group folders, select the **Attach** command from the right-click menu or from the TimeFinder menu.
4. Refer to Attaching a preferred device for a description of the **Attach** dialog box.

Note: You can pair devices only if they are of the same size and same emulation.

Related topics

- General device group operations
- Device properties table
- TimeFinder properties table
- SRDF properties table
- Attaching a preferred device
- Establishing new pairs
- Establishing pairs
- SRDF device group operations

TimeFinder: Attaching a preferred device

A standard (STD) device can have multiple BCV devices paired with it.

Attaching BCV pairs is the process of defining a specific BCV device as the *preferred* BCV device. This eliminates the need to specify a device for each subsequent establish and restore operation.

The preferred pair attachment operation is an optional step in the management of BCV pairs that eliminates the need to specify a device for each subsequent full establish and full restore operation. Starting with 5x66 microcode levels, this pairing also applies to incremental establish and restore operations.

Notes

- The attach operation is normally performed on an ad hoc basis before performing a specific operation, such as a restore. The identification of a particular BCV device as *preferred* may vary over time and depends upon a variety of conditions.
- The attach operation requires a populated device group. If you do not have a populated BCV group, refer to Device group operations for more information.
- You can attach devices only if they are the same size and same emulation.

Pairing an STD device and a BCV device without synchronizing data

The following section describes how to pair an STD device and a BCV device without synchronizing data, which is also known as attaching a preferred device.

Attaching a preferred device

To attach a preferred device:

1. Click **Data Protection**.
2. Create a device group in **Hosts**, **Device Groups**, if one does not yet exist.
3. Select the target Symmetrix.
4. Display the TimeFinder Properties table in the target panel. Use this table to determine which STD and BCV devices can be added to the device group. **Note:** You can pair devices only if they are of the same size and same emulation.
5. Add STD devices to the Group Members folder and BCV devices to the Local BCVs folder.
6. After populating the group folders, select the **Attach** command from the right-click menu or from the TimeFinder menu. The TimeFinder Attach dialog box appears. All the STD devices that are members of the group appear in the **Select device** pane.
7. Select a device from the left panel. The corresponding devices (from the set of locally associated devices) of same size and emulation type are shown in the middle **Select BCV** device panel.
8. Select a BCV device, and click **Add** to add your pair to the proposed configuration pane on the right side.
9. When you finish specifying pairs to add, click **OK** to implement the pairing.

The following option is available:

Option	Description
Force	Overrides some of the normal checking for TimeFinder operations. For the establish and restore operations, an STD device will not be processed if an appropriate BCV device cannot be found. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.

The changes made to the TimeFinder device relationships are not activated until you click OK. If you do not click OK, the settings remain as they were before the changes were made. If you do not want to save the changes you made, click Cancel.

Disassociating a pair

To disassociate a particular BCV device from an STD device, you must use the SYMCLI.

Using the detach action, you can remove the preferred matched-pair association from the devices that was initially defined with the attach action. For example, to detach the existing preferred attachment of various BCVs from their standard devices in the prod group, enter:

```
symmir -g prod detach
```

To detach the attached BCV preference on standard device (DEV001) in the prod group, enter:

```
symmir -g prod detach DEV001
```

Related topics

- General device group operations
- TimeFinder device group operations
- Defining devices as BCV
- Establishing a new BCV pair
- Splitting a BCV pair
- Restoring a BCV pair
- Displaying TimeFinder devices

TimeFinder: Establishing new BCV pairs

Establishing new BCV pairs is the process of pairing an STD device with a BCV device. This process copies the entire contents of the standard device to the BCV. This operation may be used with either local or remote BCV pairs.

Establishing new BCV pairs creates the original relationship between an STD device and a BCV device, then initially copies the STD data to the BCV device. By comparison, *establishing BCV pairs* assumes that the relationship has been established, and has since undergone an operation such as a split, which now requires synchronization of the data between the two devices.

Establishing new BCV pairs

To establish new BCV pairs:

1. Select one or more ports, directors, devices, or Symmetrix systems from the tree panel or from the target panel TimeFinder table. It does not matter what level you select, because all the devices associated with the selected Symmetrix system will be displayed.
2. Select **Establish New Pairs** from the **TimeFinder** menu. The TimeFinder Establish New Pairs dialog box appears.

The following option is available:

Option	Description
Force	Override some of the normal checking for TimeFinder operations. For the establish operation, an STD device will not be processed if an appropriate BCV device cannot be found. **Note:** Exercise extreme caution when using this flag as it may result in data loss if used improperly.

3. Select a mapped device from the Select device panel and a corresponding BCV device from the Select BCV device panel. You may also select them in the reverse order. Note that after you select a device of one type, all corresponding devices of the same size and emulation type are displayed in the other window.
4. Click **Add** to add your pair to the table pane.
5. When you finish adding pairs, click **OK** to start the process.

Related topics

- Defining devices as BCV
- Splitting a BCV pair
- Establishing a BCV pair
- Restoring a BCV pair
- Displaying TimeFinder devices

TimeFinder: Splitting a BCV pair

Splitting a BCV pair makes each device available to hosts through their separate device addresses. The split command can be applied to either local or remote BCV pairs.

Splitting a BCV pair

To split a BCV pair from the Symmetrix perspective:

1. Select a BCV device.
2. Select **Split** from the **TimeFinder** menu. The TimeFinder Split dialog box appears.

To split a BCV group from the host device group perspective:

1. Select a device group in **Hosts**, **Device Groups**.
2. Right-click and select **Split** from the **TimeFinder** menu. The TimeFinder Split dialog box appears.

   Note: If the Storage Agent for Symmetrix is not operating on the host, device group-based operations cannot be performed.

The following options are available:

Option	Description
Differential	Starts a differential synchronization between the first mirror of a BCV device and its additional mirrors (local or remote). This option is available for locally or remotely mirrored BCVs with microcode level 5265 or later. This option copies only the updated tracks to a BCV's local or remote mirror on second and subsequent differential splits. All mirrors of the BCV are rapidly synchronized to the associated standard device to the point in time that the differential split command was issued. The differential split can significantly reduce the time required for the split process because only changed tracks need to be synchronized.
Bypass lock	Bypasses Symmetrix exclusive locks for the local and/or remote units during this operation. Use this only if you are sure that no other TimeFinder operation is in progress to the local and/or remote Symmetrix units. This option bypasses SCSI reservations on the STD devices. This option is valid only for split or restore operations.
Remote data copy	Indicates the BCV control operation is targeted at the remote standard mirrors of the device group and the remote BCV devices that are associated with the device group.
Reverse split	After the split operation is complete, initiates a reverse data copy from the rest of the BCV mirrors to the first (moving) mirror of the BCV.
Remote mirror	The split operation will be targeted at the remote standard mirrors of the device group and the remote BCV devices that are associated with the device group. This option only applies if the device group is an SRDF group.
Force	Does not process devices that are not properly synchronized with BCVs. In addition, this option may reject devices in an invalid state. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
Sym force	Forces the Symmetrix system to split all BCV pairs in the group even though one or more may be in the SYNC_IN_PROG or RESTORE_IN_PROG state. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
Instant split	Improves the performance of a typical split operation by performing a quick foreground BCV split. It returns a more immediate successful status back to the host, allowing applications to continue. Supported in microcode 5x66 versions and later.
Target not ready	After the split operation is complete, sets each BCV device to Not Ready.
BCV remote mirror	The split operation will be targeted at the remote side of any R1 BCVs associated with the group and BCV remote BCV device(s) that are associated with the device group. Only applies to device group operations.

3. Select the appropriate option or options, and then click **OK**.

The wait icon appears while the split command is transferred to and accepted by the Symmetrix system. Once the split command is executed, the BCV pair(s) label changes to indicate the current BCV device status.

Related topics

- Defining devices as BCV
- Defining a preferred device
- Establishing a new BCV pair
- Establishing a BCV pair
- Restoring a BCV pair
- Displaying TimeFinder devices

TimeFinder: Establishing BCV pairs

Establishing BCV pairs is the process of copying data from the STD device to the BCV device until both devices are identical. Once they contain exactly the same data, normal TimeFinder operations can commence. This operation may be used with either local or remote BCV pairs.

Establishing new BCV pairs creates the original relationship between an STD device and a BCV device, then initially copies the STD data to the BCV device. By comparison, *establishing BCV pairs* assumes that the relationship has been established, and has since undergone an operation like a split, which now requires synchronization of the data between the two devices.

Establishing a BCV pair

To establish a BCV pair from the Symmetrix perspective:

1. Select one or more Symmetrix devices from the tree panel.
2. Select **Establish** from the **TimeFinder** menu. The TimeFinder Establish dialog box appears.

To establish a BCV group from the host device group perspective:

1. Select a device group in **Hosts**, **Device Groups**.
2. Right-click and select **Establish** from the **TimeFinder** menu. The TimeFinder Establish dialog box appears.

   Note: If the Storage Agent for Symmetrix is not operating on the host, device group-based operations cannot be performed.

The following options are available:

Option	Description
Incremental	Copies from the STD device to the BCV device only that data that has changed since the split operation.
Sym force	Forces the Symmetrix system to perform the current operation even though it may be in the SYNC_IN_PROG or RESTORE_IN_PROG state. **Note**: Exercise extreme caution when using this option as it may result in data loss if used improperly.
Optimize	Optimally pair each BCV with an STD device, without regard to its previously paired BCV. If this option is not used, the devices are paired with their previous mates. Only applies to device group operations.
Remote mirror	This operation is targeted at the remote standard mirrors of the device group and the remote BCV devices that are associated with the device group. This option only applies if the device group is an SRDF group.
Force	Overrides some of the normal checking for TimeFinder operations. For the establish operation, an STD device will not be processed if an appropriate BCV device cannot be found. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
Verify Reverse Split	Verify that the establishing of this pair will support a reverse split operation in the future. If it cannot, an error message is displayed.
Exact pairing	The STD devices and BCV devices are paired in the exact order in which they are listed in the device group. Only applies to device group operations.
BCV remote mirror	The establish operation will be targeted at the remote side of any R1 BCVs associated with the group and BCV remote BCV device(s) that are associated with the device group. Only applies to device group operations.

3. Select the desired BCV device and appropriate options, and click **OK**.

The changes made to the TimeFinder device relationships are not activated until you click **OK**. If you do not click **OK**, the settings remain as they were before the changes were made. If you do not want to save the changes you have made, click **Cancel**.

Related topics

- Defining devices as BCV
- Establishing a new BCV pair
- Splitting a BCV pair
- Restoring a BCV pair
- Displaying TimeFinder devices

TimeFinder: Restoring from BCVs

The restore command copies the entire contents of the BCV device to the standard (STD) device.

Restoring does the following:

- Check command validity. For example, the BCV and STD devices must be the same size.
- Define the BCV device as "Not Ready" to the host.
- Copies the entire contents of the BCV device to the standard device and to all of its mirrors.

Restoring from BCVs

To perform a restore action on a device pair from the Symmetrix perspective:

1. Select a Symmetrix from the tree panel.
2. Select **Restore** from the **TimeFinder** menu. The TimeFinder Restore dialog box appears.

To perform a restore on a BCV group from the host device group perspective:

1. Select a device group in **Hosts**, **Device Groups**.
2. Right-click and select **Restore** from the **TimeFinder** menu. The TimeFinder Restore dialog box appears.

   Note: If the Storage Agent for Symmetrix is not operating on the host, device group-based operations cannot be performed.

The following options are available::

Option	Description
Incremental	Copies to the STD device only data which has been written to the BCV device while it was split from the STD device. **Note:** Any updates made to the standard device while the BCV pair was split are discarded.
Bypass lock	Bypasses Symmetrix exclusive locks for the local and/or remote units during SRDF operations. Use this only if you are sure that no other SRDF operation is in progress to the local and/or remote Symmetrix units. This option will bypass SCSI reservations on the STD devices.
Remote data copy	Indicates that the BCV control operation is targeted at the remote standard mirrors of the device group and the remote BCV devices that are associated with the device group.
Verify reverse split	Verify that the establishing of this pair will support a reverse split operation in the future. If it cannot, an error message is displayed.
Remote mirror	This operation is targeted at the remote standard mirrors of the device group and the remote BCV devices that are associated with the device group. This option only applies if the device group is an SRDF group.
Force	Overrides some of the normal checking for TimeFinder operations. For the restore operation, this means that it will skip, but not reject, devices in the group that are NEVER_ESTABLISHED, or are not properly paired and split with BCVs associated with the group. This will also allow devices that are SPLIT_BEFORE_RESTORE to be restored. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
Sym force	Forces the Symmetrix system to perform a restore operation on all the BCV pairs in the group even though one or more may be in the state of SYNC_IN_PROG or RESTORE_IN_PROG. **Notes:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
Protective restore	Restores data from the BCV to the STD, but write-disables the BCV so that any new writes to the STD do not propagate to the BCV. Available with 5x67 microcode levels and later.
Exact pairing	The STD devices and BCV devices are paired in the exact order in which they are listed in the device group. Only applies to device group operations.
BCV remote mirror	The restore operation will be targeted at the remote side of any R1 BCVs associated with the group and BCV remote BCV device(s) that are associated with the device group. Only applies to device group operations.

3. Select the desired BCV device and appropriate options, and click **OK**.

Related topics

- Defining devices as BCV
- Defining a preferred device
- Establishing a new BCV pair
- Splitting a BCV pair
- Establishing a BCV pair
- Displaying TimeFinder devices

SRDF: Overview

SRDF creates and maintains a mirror image of one or more logical volumes on a remote Symmetrix system. Before you can use SRDF, the local and remote Symmetrix systems must each be set up with at least two Remote Link Directors (RLD) through which the two systems are linked. The Symmetrix system being mirrored is designated as the *source (R1)*; the Symmetrix system maintaining the remote mirror is designated as the *target (R2)*. Data is transferred across the SRDF link from the source to the target system. SRDF systems can be up to 12,000 miles apart.

By maintaining real-time copies of data in different physical locations, SRDF enables you to perform the following operations with minimal impact on normal business processing:

- Disaster recovery
- Recovery from planned outages
- Remote backup
- Data center migration

Local vs. remote mirroring

Local mirroring protects data by maintaining data on both a production volume and a mirror volume within the same storage unit. SRDF, however, uses *remote mirroring*, which is similar to local mirroring, except that the production volume resides in one storage unit while its mirror resides in a different storage unit.

Related topics

- Starting SRDF
- Establishing SRDF pairs
- Splitting SRDF pairs
- Restoring SRDF pairs
- Suspending SRDF links
- Resuming SRDF links
- Failover (target takeover)
- Failback (source takeover)
- Changing the mode of operation
- Updating Source Volumes (R1)

Starting SRDF

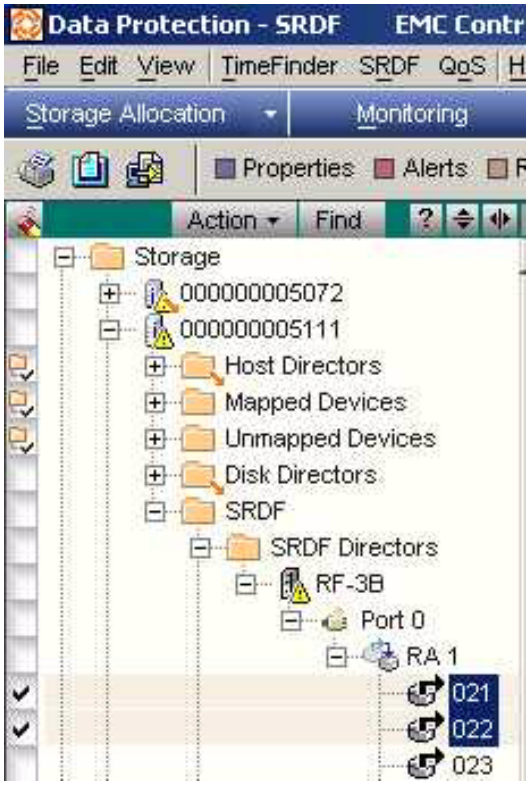
Note: Before you can perform the SRDF operations described in this section, SRDF must be installed and configured by an EMC representative. This configuration includes the mapping between the R1 and R2 devices.

Displaying SRDF Information in table view

SRDF devices can be found in the tree panel, in **Storage**, *SymmetrixID,* **SRDF**. After you select one or more SRDF devices, you can click Properties to display a full range of information about them in the table view, as shown in the SRDF Properties table:

To perform an SRDF operation:

1. Click **Data Protection**.
2. Select the appropriate Symmetrix or SRDF devices in the tree panel, as shown in this figure:



3. Click **Properties** to display a table describing the device configuration.
4. Select **SRDF** from the menu bar.
5. Specify the SRDF operation you want to perform.

Related topics

- Displaying table data

SRDF: Displaying table data about SRDF

To display data about the status of SRDF devices, select the appropriate Symmetrix system, then select **SRDF** from the **Data Protection** menu.

The SRDF table displays all relevant information relating to SRDF configuration and operational status.

Column Heading	Description
R1 Host - Dev Grp	Name of the host and SRDF device group for the R1 device
R1 Symmetrix	ID of the Symmetrix housing the R1 device.
R1	ID of the R1 device.
R2	ID of the R2 device.
R2 Symmetrix	ID of the Symmetrix housing the R2 device.
R2 Host - Dev Grp	Name of the host and SRDF device group for the R2 device
R1 State	State of the R1 device. Possible values are: Ready, Not Ready, Write Disabled, NA, and MIXED.
Pair State	State of the pair. Possible values are: Invalid, SYNCINPROG, Synchronized, SPLIT, SUSPENDED, FAILED_OVER, PARTITIONED, R1_UPDATED, R1_UPDINPROG, and MIXED.
R2 State	State of the R2 device. Possible values are: Ready, Not Ready, Write Disabled,, NA, and MIXED.
Rem inv on R1	Number of R2 remote invalid tracks on the R1 side.
Rem inv on R2	Number of R1 remote invalid tracks on the R2 side
Loc inv on R1	Number of R1 invalid tracks on the R1 side
Loc inv on R2	Number of R2 invalid tracks on the R2 side
R1 RA Grp	I/O of the R1 RA group. Possible values start at 1 and increase from there.
R2 RA Grp	I/O of the R1 RA group. Possible values start at 1 and increase from there.
Mode	Level of synchronization between R1 and R2 devices. Possible values are: SYNCHRONOUS, SEMI_SYNCHRONOUS, ADAPTIVE_COPY, and MIXED.
Domino	State of the Domino attribute which forces data on the R1 and R2 devices to be synchronized. Possible values are: ENABLED, DISABLED, and MIXED.
Ad. Copy	Adaptive Copy - Disk Mode and Adaptive Copy - Write Pending Mode Possible values are: • Disabled • Enabled: WP Mode • Enabled: Disk Mode • Mixed
AC Skew	Number of invalid tracks allowed when in Adaptive Copy mode. Possible values range from 1 to 65535.
Link Status	Status of the link. Possible values are: Ready, Not Ready, Write Disabled, NA, and MIXED.
R1 SA Status	SA status of R1. Possible values are Ready, Write Disabled, and NA (if there is no front end director)
R2 SA Status	SA status of R2. Possible values are Ready, Write Disabled, and NA (if there is no front end director)
RA Status	Status of the Remote Link Director. Possible values are: Ready, Not Ready, Write Disabled, NA, and MIXED.
Dev SRDF Status	Status of the SRDF device. Possible values are: Ready, Not Ready, Write Disabled, NA, and MIXED.

Related topics

- Screen capture of table

SRDF: Consistency groups

A *consistency group* is a group of Symmetrix SRDF devices specially configured to act in unison to maintain the integrity of a database distributed across multiple SRDF units. Consistency groups maintain coherency for an SRDF configuration by monitoring data propagation from the source (R1) devices in a consistency group to their corresponding target (R2) devices.

Note: Consistency groups require PowerPath 2.1 or greater.

When a typical DBMS application updates a database, it first writes to the disk containing a log, it then writes the data to the actual database datafiles, and finally writes to the log volume to indicate these write I/Os (log, database) are related, and each I/O is not issued until the prior I/O has successfully completed.

Even in a remote disk copy environment, data consistency cannot be ensured if one of these I/Os was remotely mirrored, but its predecessor was not remotely mirrored. This could occur, for example, in a rolling disaster where there is a communication loss that affects only a portion of the disk controllers that are performing the remote copy function.

SRDF-established consistency groups can prevent this situation by using the PowerPath pseudo-device driver to intercept any I/O to a disk device that cannot communicate to its remote mirror. The consistency protocol is to then suspend the remote mirroring for all devices defined to the consistency group before the intercepted I/O and return control to the application. In this way, consistency groups prevent dependent I/O from getting out of sync, thus ensuring the integrity and consistency of the data at the remote site.

Creating groups and adding devices

You must use the SYMCLI to create consistency groups and add members.

The ControlCenter console provides the capability to monitor the status of these groups.

Related topics

- Consistency group table properties
- Domino Effect
- Device group operations

SRDF: Concurrent SRDF

In an SRDF configuration, a single source (R1) device can be concurrently remotely mirrored to two target (R2) devices. This feature is known as *concurrent SRDF* and is supported with ESCON and Fibre Channel interfaces. Concurrent SRDF is valuable for duplicate restarts or disaster recovery, or for increased flexibility in data mobility and migrating applications.

Note: Concurrent SRDF is supported in microcode levels 5567 and later.

Operating mode restrictions

Concurrent SRDF supports each of the two remote target devices operating independently (but concurrently) in any of the following SRDF modes:

- synchronous
- semi-synchronous
- Adaptive Copy Disk mode
- Adaptive Copy Write Pending mode

While the modes for the two remote target devices can be the same or different, the following restrictions apply:

- Each of the two concurrent mirrors must belong to a different RDF (RA) group.
- You cannot have one mirror in synchronous and the other in semi-synchronous mode.

Remote Data Copy

All SRDF operations that emanate outward from the R1 device can be performed on concurrent SRDF configurations. Failback, restore, and R1 update operations cannot be performed concurrently, as data cannot be copied from two R2 devices to a single R1 device. To resolve this problem, you must use the **Remote Data Copy** option. Use this option when you want to restore data to the R1 device and to any other concurrent R2 devices. (This implies that only a single R2 device has the correct data.) The data is first copied from the specified R2 device to the R1 device; then, when the concurrent link is ready, data will also be copied to the concurrent SRDF R2 mirror(s). This option is available with the failback, restore, and update operations.

The **Remote Data Copy** option sets the state of the concurrent link to Write Disabled or Not Ready.

Device groups and RA groups

When concurrent SRDF is enabled in the Symmetrix system, a device group can contain up to two RA groups. BCV, RBCV, and BRBCV devices can be added from either RA group in the device group, but not from both. For example, you can create a standard SRDF1 device group and add a device from SRDF group 1 to it, followed by a device from SRDF group 2, followed by a concurrent SRDF device from SRDF groups 1 and 2. If you add a third RA group, a failure is returned.

To create a device group for the concurrent SRDF devices and initially synchronize (establish) the devices across the concurrent SRDF:

1. Create an R1/R2 device group by selecting the SRDF folder within a Symmetrix folder
2. Add all devices to the group
3. Establish the concurrent group

Related topics

- Adaptive Copy Disk Mode
- Adaptive Copy Write Mode
- Consistency groups
- Device group operations

SRDF: Device group operations

ControlCenter allows you to set up groups of devices on which to monitor status, change SRDF mode of operation, or perform SRDF operations. For example, you might set up a group of all devices used by a particular host. Another group might be all devices used in a particular database.

After you set up a device group, it is always accessible from the tree panel.

Refer to Device group operations for a description of how to create a device group.

After creating your R1 or R2 device group, select the devices that you want associated with the device group, and drag them to the new group folder.

SRDF device group operation notes

- SRDF device group operations on devices outside of a device group can only be performed when none of the selected R1 or R2 devices are currently in a device group.
- These are SYMCLI device groups and will be accessible through SYMCLI when created in ControlCenter, as well as ControlCenter displaying device groups created by SYMCLI.
- You can add a device to a device group, even if it has already been paired with another device. You should avoid doing this, as this situation requires the use of the **Force** option during establish operations, and can produce many warning messages when adding devices in large drag-and-drop operations.

  To avoid this problem, associate the paired SRDF device with this group, thereby eliminating the need for the **Force** option. You may want to use the TimeFinder, SRDF or Device properties tables to determine if a device is already a member of a device group.

Related topics

- General device group operations
- Device properties table
- TimeFinder properties table
- SRDF properties table
- TimeFinder device group operations
- Consistency groups

SRDF: Splitting SRDF pairs

Splitting is an SRDF control operation that suspends SRDF link traffic and read/write enables the R2 device to its local host. The split causes the R2 device to provide an additional copy to the local host.

A *differential split* is the splitting of an SRDF pair that archives only changed (differential) data from the first mirror to the remaining mirror set when the SRDF split is complete.

Before splitting an SRDF pair, the pair must be in one of the following states:

- SYNCHRONIZED
- SUSPENDED
- R1UPDATED
- SYNCINPROG (and Force is specified)

Splitting SRDF pairs

1. Click **Data Protection**.
2. Select the appropriate Symmetrix system in the tree panel or the target panel.
3. Select one or more SRDF devices or SRDF device groups from the tree panel.
4. Select **SRDF** from the menu bar.
5. Select **Split** from the **SRDF** menu. The SRDF Split dialog box appears. You can also use the right-click menu to reach this command.

   The following options are available:

Option	Description
Force	Overrides some of the normal checking for SRDF operations. For the split operation, this option ignores a synchronization in progress and proceeds to split the Symmetrix units. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
Sym Force	Forces the Symmetrix system to split the pair even though it may be in the SYNC_IN_PROG or RESTORE_IN_PROG state. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
BCV	Specifies that the SRDF control operation is intended for one or more R1 BCV devices in the SRDF hop 1 link that are associated with the group.
BCV Remote BCV	Specifies that the SRDF control operation is intended for remotely associated BCV devices (connected through the local BCV device) that are defined as BCV devices in the SRDF hop 2 link. The Symmetrix unit must have a minimum mircocode level of 5x66.
Bypass Lock	Bypasses Symmetrix exclusive locks for the local and/or remote units during SRDF operations. Use this only if you are sure that no other SRDF operation is in progress to the local and/or remote Symmetrix units.
All	Specifies that the SRDF control operation is for concurrent SRDF and is intended for all SRDF devices (both BCV and STD) that are associated with the group.
Remote BCV	Specifies that the SRDF control operation is intended for remotely associated BCV devices (connected through the local STD device) that are configured as BCV devices in the SRDF hop 2 link. The Symmetrix unit must have a minimum mircocode level of 5x66.

6. Select the appropriate option and then click **OK**.

Note: After the split operation is complete, the Pair State column of the SRDF table can display two different values. If the device was unmapped, FAILED_OVER is displayed. If the device was mapped, SPLIT is displayed.

Device group operations

Note: SRDF device group operations on devices outside of a device group can only be performed when none of the selected R1 or R2 devices are currently in a device group.

Related topics

- Failover (target takeover)
- Displaying table data

SRDF: Establishing SRDF pairs

Establishing (or Copy Source to Target) resumes links and copies data between source (R1) devices and target (R2) devices. Establish will propagate any updates made to the R1devices while the links were suspended, bringing the R2 devices up to date and completely overwriting the content of the R2 devices with the source device content.

This operation occurs after you have suspended the SRDF links so that you can read and write data on both the R1and R2 devices concurrently. This suspension would have enabled you, for example, to run backups on the R2 devices while production processing continued on the R1devices (a business continuance practice).

Before establishing an SRDF pair, the pair must be in one of the following states:

- SPLIT
- SUSPENDED (and write-disabled or not ready at the source)

To establish an SRDF pair:

1. Click **Data Protection**.
2. Select the appropriate Symmetrix system in the tree panel or the target panel.
3. Select one or more SRDF devices or SRDF device groups from the tree panel.
4. Select **SRDF** from the menu bar.
5. Select **Establish** from the **SRDF** menu. The SRDF Establish dialog box appears. You can also use the right-click menu to reach this command.

The following options are available:

Option	Description
Incremental	Resumes SRDF operation between the R1 and R2 Symmetrix units. Any new data on the R1 unit is immediately copied to the R2 unit. Any new data on the R2 unit is discarded.
Force	Overrides some of the normal checking for SRDF operations. For the establish operation, an STD device will not be processed if an appropriate R2 device cannot be found. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
All	Specifies that the SRDF control operation is for concurrent SRDF and is intended for all SRDF devices (both BCV and STD) that are associated with the group.
Remote BCV	Specifies that the SRDF control operation is intended for remotely associated BCV devices (connected through the local STD device) that are configured as BCV devices in the SRDF hop 2 link. The Symmetrix unit must have a minimum mircocode level of 5x66.
Bypass lock	Bypasses Symmetrix exclusive locks for the local and/or remote units during SRDF operations. Use this only if you are sure that no other SRDF operation is in progress to the local and/or remote Symmetrix units.
Sym force	Forces the Symmetrix system to perform the current operation even though it may be in the SYNC_IN_PROG or RESTORE_IN_PROG state. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
BCV	Specifies that the SRDF control operation is intended for one or more R1 BCV devices in the SRDF hop 1 link that are associated with the group.
BCV Remote BCV	Specifies that the SRDF control operation is intended for remotely associated BCV devices (connected through the local BCV device) that are defined as BCV devices in the SRDF hop 2 link. The Symmetrix unit must have a minimum mircocode level of 5x66.

Device group operations

Note: SRDF device group operations on devices outside of a device group can only be performed when none of the selected R1 or R2 devices are currently in a device group.

SRDF: Restoring from target

Restore operations copy data from target (R2) to source (R1). This operation is useful if, for example, you performed application testing on the R2 devices, production processing was halted on the R1 devices, the testing was successful, and you want to keep the updates.

Before restoring an SRDF pair, the pair must be in one of the following states:

- SPLIT
- SUSPENDED (and write-disabled or Not Ready at the source)

You can perform a full or incremental restore. A full restore copies the full R2 device back to the R1 device in the pair, and reassigns the R2 device as the next available mirror to the R1 device.

To restore an SRDF pair:

1. Click **Data Protection**.
2. Select the appropriate Symmetrix system in the tree panel or the target panel.
3. Select one or more SRDF devices or device groups from the tree panel.
4. Select **SRDF** from the menu bar.
5. Select **Restore** from the **SRDF** menu. The SRDF Restore dialog box appears. You can also use the right-click menu to reach this command.

The following options are available:

Option	Description
Incremental	Copies to the R1 device only that data on the R2 device that was changed since the split. Data on the R1 device that is new since the split is discarded.
Bypass Lock	Bypasses Symmetrix exclusive locks for the local and/or remote units during SRDF operations. Use this only if you are sure that no other SRDF operation is in progress to the local and/or remote Symmetrix units.
Sym force	Forces the Symmetrix system to perform the current operation even though it may be in the SYNC_IN_PROG or RESTORE_IN_PROG state. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
BCV	Specifies that the SRDF control operation is intended for one or more R1 BCV devices in the SRDF hop 1 link that are associated with the group.
BCV Remote BCV	Specifies that the SRDF control operation is intended for remotely associated BCV devices (connected through the local BCV device) that are defined as BCV devices in the SRDF hop 2 link. The Symmetrix unit must have a minimum mircocode level of 5x66.
Force	Overrides some of the normal checking for SRDF operations. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
Remote Data Copy	Use this option when you want to restore data to the R1 device and to any other concurrent R2 devices. (This implies that only a single R2 device has the correct data.) The data is first copied from the specified R2 device to the R1 device, then, when the concurrent link is ready, data will also be copied to the concurrent SRDF R2 mirror(s). This option is available with the failback, restore, and update commands.
All	Specifies that the SRDF control operation is for concurrent SRDF and is intended for all SRDF devices (both BCV and STD) that are associated with the group.
Remote BCV	Specifies that the SRDF control operation is intended for remotely associated BCV devices (connected through the local STD device) that are configured as BCV devices in the SRDF hop 2 link. The Symmetrix unit must have a minimum mircocode level of 5x66.

6. Select the appropriate option, and then click **OK**.

Device group operations

Note: SRDF device group operations on devices outside of a device group can only be performed when none of the selected R1 or R2 devices are currently in a device group.

SRDF: Suspending links

Suspending a link breaks all link paths between the selected source (R1) and target (R2) devices, preventing data transfer to R2 volumes. The Suspend Link operation is directed to the Symmetrix unit containing the R1 devices. The link can be suspended only if there are no invalid tracks for the source (R1) volumes, and no invalid tracks for the R2 volumes seen on either the source or target volumes.

To suspend a link, the SRDF pair(s) must already be in one of the following states:

- Synchronized
- R1 Updated
- SYNC_IN_PROG (requires use of the Sym Force option)
- RESTORE_IN_PROG (requires use of the Sym Force option)

Suspending an SRDF link

To suspend links:

1. Click **Data Protection**.
2. Select the appropriate Symmetrix system in the tree panel or the target panel.
3. Select one or more SRDF devices or device groups from the tree panel.
4. Select **SRDF** from the menu bar.
5. Select **Suspend Link** from the **SRDF** menu. The Suspend Link dialog box appears. You can also use the right-click menu to reach this command.

   The following options are available:

Option	Description
Force	Overrides some of the normal checking for SRDF operations. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
Bypass Lock	Bypass Symmetrix exclusive locks for the local and/or remote units during SRDF operations. Use this only if you are sure that no other SRDF operation is in progress to the local and/or remote Symmetrix units.
Sym Force	Forces the Symmetrix system to suspend the link between the pair even though it may be in the SYNC_IN_PROG or RESTORE_IN_PROG state. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.

6. Select the appropriate option, and then click **OK**.

When the suspend has completed successfully, the devices will be suspended on the SRDF links and their link status set to Not Ready (NR).

Device group operations

Note: SRDF device group operations on devices outside of a device group can only be performed when none of the selected R1 or R2 devices are currently in a device group.

SRDF: Resuming links

Resuming links resumes data transfers between the selected source (R1) and target (R2) devices, allowing data transfer to R2 devices. The Resume Link operation is run against the Symmetrix unit containing the R1devices. The link can be resumed only if the R2 device is write-enabled and there are no invalid tracks for the R1 devices on the R2 devices.

Note: To resume links, the SRDF pair(s) must already be in the Suspended state.

To resume a link:

1. Click **Data Protection**.
2. Select the appropriate Symmetrix system in the tree panel or the target panel.
3. Select one or more SRDF devices or device groups from the tree panel.
4. Select **SRDF** from the menu bar.
5. Select **Resume Link** from the **SRDF** menu. The SRDF Resume Link dialog box appears. You can also use the right-click menu to reach this command.

   The following options are available:

Option	Description
Force	Overrides some of the normal checking for SRDF operations. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
Sym force	Forces the Symmetrix system to perform the current operation even though it may be in the SYNC_IN_PROG or RESTORE_IN_PROG state. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
BCV	Specifies that the SRDF control operation is intended for one or more R1 BCV devices in the SRDF hop 1 link that are associated with the group.
BCV Remote BCV	Specifies that the SRDF control operation is intended for remotely associated BCV devices (connected through the local BCV device) that are defined as BCV devices in the SRDF hop 2 link. The Symmetrix unit must have a minimum mircocode level of 5x66.
Bypass Lock	Bypasses Symmetrix exclusive locks for the local and/or remote units during SRDF operations. Use this only if you are sure that no other SRDF operation is in progress to the local and/or remote Symmetrix units.
All	Specifies that the SRDF control operation is for concurrent SRDF and is intended for all SRDF devices (both BCV and STD) that are associated with the group.
Remote BCV	Specifies that the SRDF control operation is intended for remotely associated BCV devices (connected through the local STD device) that are configured as BCV devices in the SRDF hop 2 link. The Symmetrix unit must have a minimum mircocode level of 5x66.

6. Select the appropriate option and then click **OK**.

Device group operations

Note: SRDF device group operations on devices outside of a device group can only be performed when none of the selected R1 or R2 devices are currently in a device group.

SRDF: Failover (target takeover)

The Failover operation causes the target (R2) devices to take over read/write operations for source (R1) devices. This operation halts all I/O activity to the Symmetrix unit containing the R1 devices; this will write-disable the R1 devices. This operation is typically performed when you need to transfer I/O operation from the R1 devices to the R2 devices.

To invoke a failover, the SRDF pair(s) must already be in one of the following states:

- SYNCHRONIZED
- SUSPENDED
- R1 UPDATED
- Partitioned while invoking this operation at target side
- SYNC_IN_PROG (requires use of the Sym Force option)
- SPLIT (requires use of the Sym Force option)
- R1_UPDATE_IN_PROG (requires use of the Sym Force option)
- INVALID (requires use of the Sym Force option)

The target takeover operation assumes the following:

- If the links are functional at the time the takeover begins, and the option to check for the Adaptive Copy mode is enabled, the target takeover operation attempts to disable the Adaptive Copy mode. If it cannot disable this mode, the error condition is reported, but the failover operation continues. If the Adaptive Copy mode can be disabled, the operation issues the Disable Adaptive Copy mode command to all Symmetrix devices, regardless of whether the Adaptive Copy mode is configured for those volumes. You must manually set the Adaptive Copy mode after performing a source takeover operation to restore that mode of operation on the desired volumes.

  Note: This action is non-destructive to your data and does not affect the failover operation.
- Once a failover occurs from host A to host B, all read/write activity is performed with the R2 volumes in the Symmetrix unit attached to host B. No activity with host A takes place with the corresponding source (R1) volumes in the Symmetrix unit attached to host A.
- Once activity resumes with host A, all read/write activity is performed with the R1 volumes on the Symmetrix unit attached to host A, and host B no longer performs read/write operations with the R2 volumes in the Symmetrix unit to which it is attached.
- Failover can occur at the volume level and is not restricted to the entire site.

To start a failover operation

1. Click **Data Protection**.
2. Select the appropriate Symmetrix system in the tree panel or the target panel.
3. Select one or more SRDF devices or device groups from the tree panel.
4. Select **SRDF** from the menu bar.
5. Select **Failover** from the **SRDF** menu. The SRDF Fail Over dialog box appears. You can also use the right-click menu to reach this command.

The following options are available:

Option	Description
Force	Overrides some of the normal checking for SRDF operations. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
Sym force	Forces the Symmetrix system to failover the pair even though it may be in the SYNC_IN_PROG or RESTORE_IN_PROG state. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
BCV	Specifies that the SRDF control operation is intended for one or more R1 BCV devices in the SRDF hop 1 link that are associated with the group.
BCV Remote BCV	Specifies that the SRDF control operation is intended for remotely associated BCV devices (connected through the local BCV device) that are defined as BCV devices in the SRDF hop 2 link. The Symmetrix unit must have a minimum mircocode level of 5x66.
Bypass Lock	Bypasses Symmetrix exclusive locks for the local and/or remote units during SRDF operations. Use this only if you are sure that no other SRDF operation is in progress to the local and/or remote Symmetrix units.
All	Specifies that the SRDF control operation is for concurrent SRDF and is intended for all SRDF devices (both BCV and STD) that are associated with the group.
Remote BCV	Specifies that the SRDF control operation is intended for remotely associated BCV devices (connected through the local STD device) that are configured as BCV devices in the SRDF hop 2 link. The Symmetrix unit must have a minimum mircocode level of 5x66.

Device group operations

Note: SRDF device group operations on devices outside of a device group can only be performed when none of the selected R1 or R2 devices are currently in a device group.

Related topics

- Update source volumes

SRDF: Failback (source takeover)

This topic describes the steps to execute a source takeover (failback) on devices in the Symmetrix system to which the host is attached.

To invoke a failback, the SRDF pair(s) must already be in one of the following states:

- Split
- Suspended
- Failed over
- Partitioned
- R1 Updated
- R1 UpdInProg

Note: Performing a failover when the SRDF Link is down, leaves the SRDF pair in a split state. You cannot perform a source takeover when the SRDF pairs are in the split state. To recover from the failover when the SRDF Link is down you must run the Restore command in place of the failback.

To perform a failback operation on an SRDF source volume:

1. Click **Data Protection**.
2. Select the appropriate Symmetrix system in the tree panel or the target panel.
3. Select one or more SRDF devices from the tree panel.
4. Select **SRDF** from the menu bar.
5. Select **Failback** from the **SRDF** menu. The Fail Back dialog box appears. You can also use the right-click menu to reach this command.

The following options are available:

Option	Description
Force	Overrides some of the normal checking for SRDF operations. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
Remote Data Copy	Restores data to the R1 device and to any other concurrent R2 devices. (This implies that only a single R2 device has the correct data.) The data is first copied from the specified R2 device to the R1 device; then, when the concurrent link is ready, data will also be copied to the concurrent SRDF R2 mirror(s). This option is available with the Failback, Restore, and Update commands.
All	Specifies that the SRDF control operation is for concurrent SRDF and is intended for all SRDF devices (both BCV and STD) that are associated with the group.
Remote BCV	Specifies that the SRDF control operation is intended for remotely associated BCV devices (connected through the local STD device) that are configured as BCV devices in the SRDF hop 2 link. The Symmetrix unit must have a minimum mircocode level of 5x66.
Bypass Lock	Bypasses Symmetrix exclusive locks for the local and/or remote units during SRDF operations. Use this only if you are sure that no other SRDF operation is in progress to the local and/or remote Symmetrix units.
Sym force	Forces the Symmetrix system to perform the current operation even though it may be in the SYNC_IN_PROG or RESTORE_IN_PROG state. **Note:** Exercise extreme caution when using this option as it may result in data loss if used improperly.
BCV	Specifies that the SRDF control operation is intended for one or more R1 BCV devices in the SRDF hop 1 link that are associated with the group.
BCV Remote BCV	Specifies that the SRDF control operation is intended for remotely associated BCV devices (connected through the local BCV device) that are defined as BCV devices in the SRDF hop 2 link. The Symmetrix unit must have a minimum mircocode level of 5x66.

Device group operations

Note: SRDF device group operations on devices outside of a device group can only be performed when none of the selected R1 or R2 devices are currently in a device group.

SRDF: Update source devices

Update Source (R1) operations update the source device with the changes from the target (R2) device while the target device is still operational with its local host(s).

This operation is required if you have previously performed a failover operation from the R1 volume to the R2 volume.

To update a source volume, the SRDF pair(s) must already be in one of the following states:

- R1 Updated
- FailedOver
- Suspended or Write Disabled or Not Ready at source

Updating an SRDF source volume

To update an SRDF source volume:

1. Click **Data Protection**.
2. Select the appropriate Symmetrix system in the tree panel or the target panel.
3. Select one or more SRDF devices from the tree panel.
4. Select **SRDF** from the menu bar.
5. Select **Update Source** from the **SRDF** menu. The SRDF Update Source dialog box appears. You can also use the right-click menu to reach this command.

   The following options are available:

Option	Description
Force	Overrides some of the normal checking for SRDF operations. **Note:** Exercise extreme caution when using this flag as it may result in data loss if used improperly.
Remote Data Copy	Restores data to the R1 device and to any other concurrent R2 devices. (This implies that only a single R2 device has the correct data.) The data is first copied from the specified R2 device to the R1 device; then, when the concurrent link is ready, data will also be copied to the concurrent SRDF R2 mirror(s). This option is available with the Failback, Restore, and Update commands.
Bypass Lock	Bypasses Symmetrix exclusive locks for the local and/or remote units during SRDF operations. Use this only if you are sure that no other SRDF operation is in progress to the local and/or remote Symmetrix units.

6. Select the appropriate option, and then click **OK**.

Device group operations

Note: SRDF device group operations on devices outside of a device group can only be performed when none of the selected R1 or R2 devices are currently in a device group.

Related topics

- SRDF: Failover

SRDF: Changing mode of operation

ControlCenter allows you to change the SRDF mode of operation and attributes for selected R1 and R2 devices. These configuration operations are also known as *setting the logical volume attributes*.

To set the mode of operation:

1. Select an SRDF group from the tree panel.
2. Select **Mode Control** from the **SRDF** menu. The SRDF Mode Control dialog box appears. You can also use the right-click menu to reach this command.

The following options are available:

Option	Description
Force	Overrides some of the normal checking for SRDF operations. **Note:** Exercise extreme caution when using this flag as it may result in data loss if used improperly.
Bypass lock	Bypasses Symmetrix exclusive locks for the local and/or remote units during SRDF operations. Use this only if you are sure that no other SRDF operation is in progress to the local and/or remote Symmetrix units.
Mode: Sync	Notifies host of successful I/O only after target (R2) device signals success.
Mode: SemiSync	Notifies host of successful I/O after source (R1) device signals success.
Domino Effect	Causes an R1 device to become not ready to its host, and all I/O activity ceases with that device if the R2 volume fails or a link failure occurs. When the fault condition is corrected, you must manually make the master device ready. This feature ensures that a remotely mirrored pair is always synchronized.
Adaptive Copy: Disk	Transfers data from the R1 device to the R2 device and does not wait for confirmation. This mode is intended to be a temporary SRDF operating state and is designed for situations requiring the transfer of large amounts of data without loss of performance.
Adaptive Copy: Change Skew	Modifies the Adaptive Copy skew threshold. When the skew threshold is exceeded, the remotely mirrored pair operates in the pre-determined SRDF state (synchronous or semi-synchronous). As soon as the number of invalid tracks drop below this value, the remotely mirrored pair reverts back to the Adaptive Copy Write Pending mode. The skew value is configured at the device level and may be set to a value between 0 and 65,534 tracks. For devices larger than a 2 GB capacity drive, a value of 65,535 can be specified to target all the tracks of any given drive.
Adaptive Copy: Write Pending	Transfers data from the R1 device to the R2 device and does not wait for confirmation. This mode is ideal for situations when a large amount of data must be transferred to remote devices and performance must not be compromised at the local site.

The following table describes which attributes can be set simultaneously.

Synchronous	Semi-Synchronous	Adapt Copy - Write Pending	Adapt Copy - Disk	Domino Effect
X				
X		X		
X			X	
X				X
	X			
	X	X		
	X		X	

SRDF: Synchronous mode

Synchronous mode is used primarily in SRDF campus solutions. In this operational mode, Symmetrix maintains a real-time mirror image of the data on remotely mirrored devices. Data on the source (R1) and target (R2) devices are always fully synchronized at the completion of an I/O sequence.

In normal operation, this mode has an impact on write performance to R1 devices. This performance impact is due to overhead associated with remote data transfer, fiber latency, and acknowledgment of the synchronous operation.

The Symmetrix unit containing the R1 device informs the host that an I/O sequence has successfully completed only after the Symmetrix unit containing the R2 device acknowledges that it has received and checked the data.

The Symmetrix unit containing the R1 device handles each I/O command separately and informs the host of successful completion when the Symmetrix unit containing the R2 device acknowledges and checks receipt of the data.

When the Symmetrix unit containing the R1 device has valid data in cache destined for a R2 device, the Remote Link Director (RLD) transfers data to the cache in the Symmetrix unit housing the R2 device through its link path. This data transfer occurs while the Symmetrix unit containing the R1 device continues to process I/O commands. If the Symmetrix unit containing the R1 device does not receive acknowledgment of a successful transfer from the other Symmetrix unit within its time-out period or another failure occurs that prevents the data transfer, the Symmetrix unit containing the R1 device notifies the host of the error condition.

Related topics

- SRDF Mode Control dialog box
- Semi-synchronous mode

SRDF: Semi-synchronous mode

Semi-synchronous mode is used primarily in SRDF Extended Distance Solutions. In this mode, the Symmetrix unit containing the source (R1) device maintains a semi-synchronous mirror image of its data in the Symmetrix unit containing the target (R2) device. Data on remotely mirrored devices are always synchronized between the R1 and the R2 prior to initiating the next write operation to these devices.

This mode supports situations where high performance is needed at the R1, and can tolerate a gap of up to one I/O (worst case) in data synchronization.

The R1 informs the host of successful completion after each write operation. When the R1 has valid data in cache destined for a R2 device, the Remote Link Director (RLD) transfers data to the cache in the R2 through an available link path. This data transfer occurs while the R1 continues to perform additional commands.

If the host issues a new write operation for a R1 device with a write pending status, the R1 disconnects from the host channel. The R1 then starts another I/O operation on another channel. When the write pending status is cleared (write completed, acknowledged, and checked from the R2 volume), the R1 reconnects to the channel and continues processing the write operation on the channel from which it disconnected. This mode keeps the data in the R2, at most, one I/O behind the data in the R1, while minimizing the impact on local application performance.

Note: Although write operations can be held up due to synchronization between R1 and R2 volumes, read operations continue uninterrupted.

If the R1 does not get acknowledgment of a successful transfer from the R2 within its time-out period or another failure occurs that prevents the data transfer, the R1 marks that data as invalid for the R2 device. Symmetrix copies that data to the R2 device as a background operation to re-establish synchronization of the remotely mirrored pair.

Related topics

- SRDF Mode Control dialog box
- Synchronous mode

SRDF: Domino Effect

This attribute, when set along with the SYNC attribute, ensures that the data on the source (R1) and target (R2) devices are fully synchronized. When this attribute is enabled, Symmetrix forces the other SRDF (R1 or R2) device to the Not Ready state, and notifies the host whenever it detects that one device in a remotely mirrored pair is unavailable or a link failure has occurred. After the problem has been corrected, the not ready device must be made ready again to the host using the SRDF utilities. If the failed device or link is still not available when the SRDF device is made ready, the device remains not ready.

Under normal operating conditions (Domino Effect not enabled), a remotely mirrored device continues processing I/Os with its host even when an SRDF device or link failure occurs. New data written to the R1 or R2 device, while its pair is unavailable or link paths are out of service, are marked for later transfer. When a link path is re-established or the device becomes available, resynchronization begins between the R1 and R2 devices. Each R1 device notifies the host when synchronization completes on that device.

Note: This attribute cannot be set to On for any R1 devices to be involved in a DSS/Backup preprocessing operation. This attribute will cause both the R1 and R2 devices to go Not Ready when the DSS/Backup pre-processing operation suspends the links between the Symmetrix units.

Related topics

- SRDF Mode Control dialog box

SRDF: Adaptive Copy Disk Mode

This SRDF mode of operation stores new data for a remotely mirrored pair on the source (R1) device of that pair as invalid tracks. This operation continues until the data can be successfully transferred to the target (R2) device. A skew parameter associated with this mode indicates the maximum number of tracks that can be out of synchronization between the two devices at any given time.

This mode instructs the Symmetrix unit to acknowledge all writes to source (R1) devices as if they were local devices. New data accumulates as invalid tracks on the R1 device for subsequent transfer to the target (R2) device. The Remote Link Director transfers each write to the R2 device whenever a link path becomes available. This mode also has a user-configurable skew (maximum number of invalid tracks threshold) that, when exceeded, causes the remotely mirrored volume to operate in the pre-determined SRDF state (Synchronous or Semi-synchronous) when this mode is in effect. As soon as the number of invalid tracks drops for a device below this value, the remotely mirrored pair reverts back to the Adaptive Copy Disk mode. The skew is configured at the device level and may be set to a value between 0 and 65,535 (decimal).

Related topics

- SRDF Mode Control dialog box
- Adaptive Copy - Write mode
- Synchronous mode
- Semi-synchronous mode

SRDF: Adaptive Copy Write Pending

This SRDF mode of operation stores new data destined for a remotely mirrored pair in the cache of the local Symmetrix unit until it can be successfully written to both the source (R1) and target (R2) devices. A *skew* parameter associated with this mode determines the maximum number of write pendings that can exist for a remotely mirrored pair.

When this mode is enabled, Symmetrix acknowledges all writes to the R1 device as if it was a local device. The new data accumulates in cache until it is successfully written to the R1 device and the Remote Link Director has transferred the write to the R2 device.

When the skew rate is exceeded, the remotely mirrored pair starts to operate in the pre-determined SRDF state (Synchronous or Semi-synchronous). As soon as the number of write pendings drops below the skew rate, the remotely mirrored pair reverts back to the Adaptive Copy - Write Pending mode. The skew is configured at the device level and may be set to a value between 0 and 65,535.

Notes

- If the Adaptive Copy - Disk mode is also enabled, the Adaptive Copy - Write Pending mode takes precedence.
- When all Adaptive Copy modes are disabled, the SRDF volumes begin operating in their base configured state (Synchronous or Semi-synchronous). Otherwise, if the Adaptive Copy - Disk mode is on, it is in effect.

Related topics

- Adaptive Copy - Disk mode
- Synchronous mode
- Semi-Synchronous mode
- SRDF Mode Control dialog box

ECC Administration

ECC administration involves tasks that the ControlCenter administrator can perform in order to do the following:

- Install and configure agents
- Create and configure data collection policies
- Monitor data retention in the repository
- Review reports to monitor system performance and activity
- Set up schedules for when you want ControlCenter events to occur, such as alerts and data collection
- Manage ControlCenter security
- Learn about the physical and logical configuration (topology) of your storage environment

To learn about each of the administrative tasks above, select from the following:

- AgentsOverview of agent administration, including configuring, starting, and stopping agents.
- Data collection policiesOverview of ControlCenter data collection policies.
- Data retentionIntroduction to data retention in the ECC repository.
- InstallAgent installation procedure.
- ReportsOverview of ControlCenter reports.
- SchedulesOverview of ControlCenter schedules.
- Security ManagementOverview of managing ControlCenter security.
- TopologyOverview of the topology of your storage environment configuration.

Related topics

- Introducing EMC ControlCenter
- Control Center agents overview
- ControlCenter architecture

Data collection policies overview

Collecting data is one of the functions performed by ControlCenter agents. Agent data collection is performed differently for each agent. Some agents:

- Start data collection automatically upon startup
- Require manual configuration to collect data
- Require that data collection policies are defined, assigned, and enabled to manage how and when the data is collected

Data collection policies

Data collection policies are a formal set of statements used to manage the data collected by ControlCenter agents. The policies specify the data to collect and the frequency of collection. Each agent has associated predefined collection policies and collection policy templates, which can be managed through ControlCenter Administration.

Data collection policy templates

Collection policy templates provide default values for the creation of new collection policies. ControlCenter provides one or more template for each agent. You can define your own policies by modifying the collection policy templates.

Predefined data collection policies

Predefined collection policies are provided automatically with each agent. Predefined collection policies can be edited, copied, or deleted.

Related topics

- ControlCenter agents overview
- Installing and configuring agents
- Defining and assigning data collection policies
- Data collection policy descriptions

Data collection concepts

Data collection policy descriptions

Collecting data is one of the functions performed by ControlCenter Agents. Agent data collection is performed differently for each agent. Some agents:

- Start data collection automatically upon startup
- Require manual configuration to collect data
- Require that data collection policies are defined, assigned, and enabled to manage how and when the data is collected

The following tables list the agents that use data collection policies to manage data collection. If an agent is not listed it means that data collection is managed using another process. See the agent overview topic for more details.

Please note, that this topic assumes that the agents are installed and started.

The following agents are provided with different data collection policies. Some data collection policies are enabled by default. If the policy is enabled by default, data collection begins automatically, and requires no user assistance.

Backup Agent for	Data collection policies
TSM	• TSMMissedException • TSMServerSnapshot • TSMServerStatistics • TSMSessionException

Common Agents	Data collection policies
WLA Archiver	• Data Retention

Connectivity Agents for	Data collection policies
SDM	• Discover
SNMP	• SNMPAgentChangedRequest • SNMPDiscoverRequest • SMMPPingRequest • SNMPPortConfigRequest • SNMPRescanRequest • SNMPStatusRequest
Switches	• Switch Agent Fabric Validation • Switch Agent Topology Validation

Database Agents for	Data collection policies
Oracle	• WLA Daily • WLA Revolving • WLA Analyst

Host Agent for	Data collection policies
AIX	• Discovery • WLA Daily • WLA Revolving • WLA Analyst
HP-UX	• Discovery • WLA Daily • WLA Revolving • WLA Analyst
Solaris	• Discovery • WLA Daily • WLA Revolving • WLA Analyst
Windows	• Discovery • WLA Daily • WLA Revolving • WLA Analyst

Physical Agent for	Data collection policy
MVS	• MMP data collection

Storage Agents for	Data collection policies
Celerra	• Discovery Request • Status Request
CLARiiON	• Discovery
Compaq StorageWorks	• Discovery
HDS	• HDS Storage Array • HDS Storage Device
IBM ESS	• IBM ESS Data Collection
Symmetrix	• Alert Polling • Configuration • Local Discovery • Performance Statistics • Proxy Discovery • WLA Daily • WLA Revolving • WLA Analyst

Related topics

- Agent overview
- Installing and configuring agents
- Defining and Assigning data collection policies
- Enabling data collection policies

Data collection policy descriptions

Backup Agent for TSM data collection policies

Data collection policies allow the Backup Agent for TSM to collect the following information about Tivoli Storage Manager servers:

- TSMMissedException - Log of missed scheduled sessions (backups or archives).
- TSMServerSnapshot - Instance log of TSM Server storage utilization status information.
- TSMServerStatistics - Interval log of TSM Server statistics such as backup, throughput, and media wait statistics.
- TSMSessionException - Exception log of statistical information on the backup that encountered problems.

By default, these collection policies runs once per day at 1:00 AM. To change how often the collection policy runs or at what time of day, edit the attached to the policy.

Related topics

- Data collection policies overview
- Assigning and defining data collection policies
- Backup Agent for TSM overview
- Installing and configuring agents

Connectivity Agent for SDM data collection policy

The Connectivity Agent for Storage Device Masking (SDM Agent) has one data collection policy that monitors volume-access control in Symmetrix systems.

SDM Agent Discover data collection policy

The SDM Agent Discover policy causes the SDM Agent to:

- Monitor the VCM databases in Symmetrix FAs in the SAN for storage access control configuration changes
- Update the Console with configuration changes

Enabled by default

Yes

Configuration requirements

The following information is defined in the SDM Agent *Discover* policy:

- Polling interval

Monitored resources

The Discover policy monitors volume-access control configuration changes in the VCM databases in Symmetrix system FAs.

Default settings

The SDM Agent *Discover* policy has the following default settings:

- Polling interval 15 minutes.

Related topics

- Connectivity Agent for SDM overview
- Connectivity Agent for SDM administration
- Installing agents
- Assigning data collection policies
- Editing data collection policies
- Discovery and monitoring requirements

Connectivity Agent for SNMP data collection policies

The Connectivity Agent for SNMP data collection policies tell the agent which data to collect and the frequency of collection. The policies target specific connectivity devices, ports, and links for discovery. The policies then direct the agent to monitor these connectivity devices for configuration changes and health status.

The Connectivity Agent for SNMP collects data from the SNMP agents associated with the connectivity devices targeted in the policies and then sends that data to the Repository where it is accessed by ControlCenter and displayed in the Console. One SNMP agent can manage multiple remote devices in addition to the local device on which it is installed.

Data collection policies

The following six data collection policies are associated with the Connectivity Agent for SNMP:

- SNMP Dscover Request runs discovery once
- SNMP Rescan Request runs cyclic discovery
- SNMP Agent Changed Request monitors configuration changes to connectivity devices
- SNMP Ping Request pings connectivity devices continually
- SNMP Port Config Request monitors port configuration changes
- SNMP Status Request monitors health of connectivity devices

All six Connectivity Agent for SNMP policies appear enabled in the ControlCenter tree after installation of the SNMP Connectivity Agent. However, you must define an IP address, range or subnet in the SNMP Discover Request policy to start the SNMP Connectivity Agent monitoring the SNMP agents at these IP addresses. No additional configuration is required, because by default, four of the remaining policies target the SNMP agents, devices, and ports that are discovered by the SNMP Connectivity Agent. The sixth policy, SNMP Rescan Request, is generally used for monitoring specific instances, such as the startup of a new hub or switch.

You can keep the default policies; or you can copy a default policy, edit it, save it, and then assign it.

Notes

1. In addition to monitoring the IP addresses entered into its data collection policies, the Connectivity Agent for SNMP monitors the IP addresses entered into the Search for connectivity devices dialog box during user-initiated discovery.
2. The default IP setting (*) in each of the following policies targets the devices discovered by the Connectivity Agent for SNMP. Typically, you do not need to change the default setting. When monitored events occur, alerts are generated to the Console and changes appear in the device properties. You can access the device properties in the Console tree panel.
   - SNMP Agent Changed Request
   - SNMP Ping Request
   - SNMP Port Config Request
   - SNMP Status Request

   Note: Replacing the default indicator (*) with a specified IP setting, restricts a policy to the IP address(es) entered. To safeguard SAN monitoring, retain the default policies, and edit copies of them. Do not rename copies of policies. ControlCenter distinguishes distinct IP settings in like-named policies. For more information, see Creating new policies from a template.

Related topics

- Connectivity Agent for SNMP overview
- Connectivity Agent for SNMP administration
- Connectivity Agent for SNMP alerts
- Data collection policy overview
- Assigning data collection policies
- Installing agents
- Discovery and monitoring requirements

Connectivity Agent for Switches data collection policies

The Connectivity Agent for Switches (Switch Agent) data collection policies:

- Monitor the connection settings and topology information of Fibre Channel switches and fabrics in the SAN
- Update the Repository with new and changed information
- Check for broken links

Data collection policies

There two Switch Agent data collection policies are:

- Switch Agent Fabric Validation monitors fabrics
- Switch Agent Topology Validation monitors Fibre Channel switch topology

The ControlCenter administrator must assign each of these policies before the Switch Agent will function. You can assign the default policies; or you can edit them and then assign them. See Assigning data collection policies.

Related topics

- Connectivity Agent for Switches overview
- Connectivity Agent for Switches administration
- Assigning data collection policies
- Installing agents
- Discovery and monitoring requirements

Database Agent for Oracle data collection policies

The ControlCenter data collection policies and templates are used to manage the data collected by the Oracle Agent.

The Oracle Agent has three data collection policies associated to it:

- WLA Daily - Daily collections manage the historical performance data collected for the Oracle database. The daily data is collected in intervals. At each interval the statistical data for that time period is processed and saved as performance archives.
- WLA Analyst - Analyst collections manage the performance data collected for the Oracle database for a specific time period. Analyst collections are created on demand. Each Analyst collection is based upon unique settings defined in the policy.
- WLA Revolving - Revolving collections manage the continuous performance data collected for the Oracle database. The amount of data contained in a Revolving collection is determined by the defined window size. Once the duration is reached, the oldest interval is removed and the most recent data is appended to the collection.

Related topics

- Database Agent for Oracle overview
- Database Agent for Oracle administration
- Database Agent for Oracle Space alerts
- Database Agent for Oracle Environment alerts

Host Agents for AIX, HP-UX, and Solaris data collection policies

ControlCenter provides several data collection policies to allow you to collect statistics on AIX, HP-UX and Solaris hosts for activities like consolidated reporting and capacity planning.

The UNIX data collection policies include:

- **Discovery**Collects statistics on file systems, logical volumes, physical volumes, storage devices, partitions, VERITAS storage objects (Solaris only), and volume groups (AIX and HP-UX only). By default the policy initiates collection once per day.
- **WLA Daily**, **Revolving**, and **Analyst**Collect CPU and disk performance statistics.
  - DailyManages the historical performance data collected for the host. The daily data is collected in intervals. At each interval the statistical data for that time period is processed and saved as performance archives.
  - RevolvingManages the continuous performance data collected for the host. The amount of data contained in a Revolving collection is determined by the defined window size. Once the duration is reached, the oldest interval is removed and the most recent data is appended to the collection.
  - AnalystCollects a single set of statistics on demand. Each Analyst collection is based upon unique settings defined in the policy.

To see the collected statistics, you can:

- View the latest statistics by exploring host properties in the Console main window
- View how a resource relates to other resources in your network, such as which host logical volumes map to which physical disks
- Run one of ControlCenter's pre-defined reports
- Create a custom report

Tip

- You can have only one Discovery, WLA Daily, and WLA Revolving policy per ControlCenter UNIX agent type. For example, you can have only one Discovery policy, one WLA Daily policy, and one WLA Revolving policy for all of your Host Agents for AIX.
- You can also collect UNIX performance statistics using the AIX, HP-UX, and Solaris Storage Agents' reporting features.

Related topics

- Assigning data collection policies
- Performance monitoring guidelines
- UNIX: Troubleshooting the UNIX Host Agents
- Host Agents for AIX, HP-UX, and Solaris administration
- Host Agents for AIX, HP-UX, and Solaris overview

Host Agent for Windows data collection policies

ControlCenter provides several data collection policies to allow you to collect statistics on Windows systems. You can use these statistics for activities such as consolidated reporting and capacity planning.

The Host Agent for Windows data collection policies include:

- **Discovery**Collects statistics on file systems, logical volumes, storage devices, partitions, and volume groups. By default the policy initiates collection once per day.
- **WLA Daily**, **Revolving**, and **Analyst**Collect CPU and disk performance statistics.
  - DailyCollects statistics at regular intervals you define. Use this policy to collect trending data.
  - RevolvingCollects statistics continuously and retains the statistics for a number of minutes that you specify. By default, this policy retains statistics for 120 minutes; after 120 minutes, the newest records overwrite the oldest records.
  - AnalystCollects a single set of statistics on demand.

To see the collected statistics, you can:

- View the latest statistics by exploring host properties in the Console main window
- View how a resource relates to other resources in your network, such as which host logical volumes map to which physical disks
- Run one of ControlCenter's predefined reports
- Create a custom report

Tip

- You can also collect Windows performance statistics using the Host Agent for Windows recording feature.

Related topics

- Windows: Monitoring performance
- Windows: Monitoring disk performance
- Assigning and defining data collection policies
- Data collection policies overview
- Host Agent for Windows overview
- Installing and configuring agents

IBM ESS Data Collection policy

The IBM ESS Data Collection policy allows the Storage Agent for IBM ESS to collect statistics about the following IBM ESS components:

- MVS volumesunit address, number of volumes, serial numbers, and track format
- SubsystemsIDs and serial numbers
- IBM ESS devicesnames, serial numbers for the IBM ESS and each device, types, status, size (in KB), and track size (block size)
- Cache size

Purpose

This policy collects IBM ESS statistics to create an inventory of the storage resources on the host. ControlCenter uses the statistics to populate reports, property views, and topology views.

To see the collected statistics, you can:

- View the latest statistics by exploring host properties in the Console main window.
- View cache summary information by viewing the cache summary reports.

Enabled by default

Yes

Configuration requirements

The agent collects the statistics according to the schedule you specify and for the host(s) you select.

Default settings

By default, this collection policy runs once per day at 1:00 AM. To change the frequency with which the collection policy runs or the time of day, edit the schedule attached to the policy.

Monitored resources

The IBM Data Collection policy collects statistics for IBM ESS hosts.

Related topics

- Data collection policies overview
- Editing data collection policies
- Creating new policies from a template
- Assigning and defining data collection policies
- Installing and configuring agents
- Storage Agent for IBM ESS administration
- Storage Agent for IBM ESS overview

Storage Agent for Celerra data collection policies

The ControlCenter data collection policies and templates are used to manage the data collected by the Storage Agent for Celerra.

The Storage Agent for Celerra has two data collection policies associated to it:

- Discovery Request data collection policy
- Status Request data collection policy

Related topics

- Storage Agent for Celerra overview
- Storage Agent for Celerra administration
- Storage Agent for Celerra alert
- Responding to the Storage Agent for Celerra alert

Storage Agent for CLARiiON data collection policy

The Storage Agent for CLARiiON is provided with the Discovery data collection policy.

Purpose

The Discovery policy is used to discover the system resources. This policy manages the collection of data that will not change very often, such as configuration information.

Enabled by default

Yes

Configuration requirements

This data collection starts once the agent is installed. Optionally, you can edit the policy settings.

Monitored resources

The Storage Agent for CLARiiON collects data about CLARiiON FC 4700 Storage Array and the Storage Devices in the array.

Related topics

- Data collection policies overview
- Enabling or disabling data collection policies
- Editing data collection policies
- Creating a new data collection policy from a template
- Storage Agent for CLARiiON overview
- Storage Agent for CLARiiON Installation and Configuration

Storage Agent for Compaq StorageWorks data collection policies

ControlCenter provides the Discovery data collection policy to allow you to collect statistics for Compaq StorageWorks subsystems for activities like consolidated reporting and capacity planning.

The Discovery policy collects statistics on the StorageWorks subsystem configuration. The statistics include the device types and sizes. By default the policy initiates collection once per day.

For more information, see Storage Agent for Compaq StorageWorks: Discovery data collection policy.

To see the collected statistics, you can:

- View the latest statistics by exploring host properties in the Console main window
- View how a resource relates to other resources in your network, such as which units map to which physical disks (you must also have the Host Agent for Windows installed to view these mappings)
- Run one of the ControlCenter predefined reports
- Create a custom report

Related Topics

- Data collection policies overview
- Storage Agent for Compaq StorageWorks overview
- Storage Agent for Compaq StorageWorks administration

Storage Agent for HDS data collection policies

The Storage Agent for HDS collects the HDS storage array status information and logs it to the central database. The policies define what data is collected and the schedule on which the data is collected.

- Storage Agent for HDS Storage Array data collection policy
- Storage Agent for HDS Storage Array Storage Device data collection policy

Related topics

- Data collection policies overview
- Assigning and defining data collection policies
- Storage Agent for HDS overview
- Storage Agent for HDS installation and configuration

Storage Agent for Symmetrix: data collection policies

The ControlCenter data collection policies and templates are used to manage the data collected by the Storage Agent for Symmetrix.

The Symmetrix Agent has the following data collection policies associated with it:

- Local Discovery Discovers which Symmetrix systems are visible on the local host.
- Proxy Discovery Discovers which Symmetrix systems are visible on proxied hosts.
- Configuration Checks for configuration changes on previously discovered Symmetrix.
- Performance Statistics Collects Symmetrix performance statistics.
- Alert Polling Polls for Symmetrix alarms.
- WLA Daily Manages the historical performance data collected for Symmetrix systems. The daily data is collected in intervals. At each interval the statistical data for that time period is processed and saved as performance archives.
- WLA Revolving Manages the continuous performance data collection for Symmetrix systems. The amount of data contained in a revolving collection is determined by the defined window size. Once the duration is reached, the oldest interval is removed and the most recent data is appended to the collection.
- WLA Analyst Manages the performance data collected for Symmetrix statistics for a specific time period. Analyst collections are created on demand. Each analyst collection is based upon unique settings defined in the policy.

These policies can be edited, copied, or deleted after navigating to Administration, Data Collection Policies, Symmetrix Agent V500, right-clicking, and selecting the appropriate command.

Related topics

- Data collection policies overview
- Storage Agent for Symmetrix overview
- Storage Agent for Symmetrix administration
- Assigning data collection policies
- Copying data collection policies
- Editing data collection policies
- Deleting data collection policies
- Viewing data collection policies

WLA Retention data collection policy

WLA (Workload Analyzer) Retention is the only data collection policy or template associated with the WLA Archiver. Data collection policies and templates are used to manage the data collected by ControlCenter Agents and products.

Purpose

WLA Retention is used to

- Define how many days, weeks, or months worth of the performance archives, revolving collections, analyst collections, and WLA Automation reports to retain on the host running the WLA Archiver .
- Define a schedule for when and how often the WLA Retention policy is activated.
- Select the WLA Archiver to which the policy will be assigned.

Enabled by default

Yes

Configuration requirements

The WLA Archiver must be installed and started.

Monitored resources

The WLA Retention policy monitors how many of the performance archives, revolving collections, analyst collections and automation reports are stored on the WLA Archiver host.

Default settings

By default the WLA Retention policy is set to save:

WLA Data Collection	Number of files to save*
Revolving	30
Analyst	20
Interval	7
Daily archives	60
Weekly archives	104
Monthly archives	60
Daily Reports	30
Weekly Reports	24
Monthly Reports	12

*All data collections and automation reports are saved starting with the most recent.

You can keep or edit and save the default policy settings or you can assign a new WLA Retention policy.

Related Topics

- Data collection policy overview
- Editing data collection policies
- WLA Archiver overview

Defining and assigning data collection policies

Each agent is assigned a set of predefined policies and a set of policy templates. You can define new data collection policies from a predefined policy or from a policy template. Once you have defined the settings, you can choose the agent to which the policy is assigned.

To assign and define a data collection policy:

1. Select the type of agent to which you are assigning the policy. From the tree, expand **Administration**, **Data Collection Policies**, **Policies**, and the agent folder. If the agent folder in the Policies folder does not contain the policy you want to assign, expand the **Policy Templates** folder, and then the agent folder. If the policy template is not listed under the agent folder, then the policy does not exist for the type of agent you selected.
2. Right-click the policy you are assigning.
3. If you are assigning from an existing policy, select **Edit Policy** or **Copy Policy** (select **Copy Policy**, if you are only slightly modifying the policy). **Note:** If you do not get the **Copy Policy** option, it means only one instance of the policy can be run for each type of agent. Refer to the specific policy description for more information. If you are assigning from a policy template, select **New Policy**. The **Policy Definition and Assignment** dialog box opens.
4. Select the **Policy Enabled?**checkbox, for the policy to start once the assignment and definition is completed.
5. Enter a unique name in **Document** (this step is mandatory if you are copying a policy). This information will appear in parenthesis next to the default policy name in the tree.
6. In the **Source** tab, select the data that will be collected for this policy. The **Source** tab has different selections for each type of agent.
7. Open the **Properties** tab, and enter a **Description**, or leave the default description.
8. Open the **Actions** tab.
9. Assign a schedule for the policy. To assign a schedule, you can select an existing one from the list box, **Edit** an existing schedule or create a **New** schedule. Once you assign the schedule, the schedule information appears under **Interval** (how often the data is collected), **Days** (which days of the week the data is collected), and **Range** (the range of hours each day that the data is collected).
10. Open the **Assign to** tab.
11. Select the **Apply These Policies to All Applicable Hosts/MOs?** checkbox to assign this policy to all agents or managed objects eligible for this policy. To select specific agents or managed objects, select the host items to which you are assigning the policy from the **Available** list and **Move** them to the **Selected** list.
12. Click **OK** once you have finished assigning and defining the data collection policies.

Related topics

- Data collection policy descriptions
- Creating a policy from a template
- Editing a schedule
- Creating a new schedule

Editing data collection policies

You can edit all settings for an existing data collection policies, however you can only edit the schedule and properties defined by the data collection policy templates.

To edit a data collection policy:

1. Select the policy or template you are editing. From the tree panel, expand **Administration**, **Data Collection Policies**, **Policies**, and the agent folder.
2. Right-click the policy you are editing, and select **Edit Policy**
3. Make any changes to the policy settings, and click **OK** when you are done. The changes to the policy take effect immediately.

Related Topics

- Editing data collection policy templates
- Defining and assigning data collection policies
- Deleting data collection policies

Copying data collection policies

Use the copy policy function when you want to have more than one data collection policy with similar settings.

Note: There are some policies that cannot be copied. These policies can only have one assignment per type of agent. For example, there can only be one Discovery policy assigned to all of the Host Agents for AIX, not each Host Agent for AIX. For more information, see your specific data collection policy description.

To copy a data collection policy:

Note: This procedure assumes that the policy you are copying already exists. See Defining and assigning data collection policies for instructions to create a new policy.

1. Select the type of agent to which you are copying the policy. From the tree, expand **Administration**, **Data Collection Policies**, **Policies**, and the agent folder. If the agent folder in the Policies folder does not contain the policy you want to copy, you cannot copy the policy and must create a new one from the policy templates. If the policy template is not listed under the agent folder, then the policy does not exist for the type of agent you selected.
2. Right-click the policy you are copying.
3. Select **Copy Policy**. The Policy Definition and Assignment dialog box opens.
4. Add a title or description in the **Document** field. This is the only mandatory change you must make when copying a policy.
5. Make any other changes to the policy. For example, you may want to define a different schedule, or assign the policy to different agents from the **Assign to** tab.
6. Click **OK** when you are done.

Related Topics

- Data collection policy descriptions
- Defining and assigning data collection policies
- Creating a new policy from a template

Deleting data collection policies

You can delete data collection policies only in the **Policies** branch of the Administration tree. Data collection policy templates, located in the **Policy Templates** branch of the Administration tree, cannot be deleted.

If you want to stop a data collection temporarily, do not delete the policy. Instead, disable the data collection policy.

To delete a data collection policy:

1. Select the type of agent from which you are deleting the policy. From the tree, expand **Administration**, **Data Collection Policies**, **Policies**, and the agent folder.
2. Right-click the policy you are deleting, and click **Delete Policy**. The policy is removed from the tree.

Related Topics

- Data collection policy descriptions
- Editing data collection policies
- Enabling and disabling data collection policies

Viewing data collection policy properties

You can create a tabular view of specific data collection policies and template settings.

1. Select **Properties** from the task menu.
2. From the tree panel, expand **Administration**, **Data Collection Policies**, **Policies**, or **Templates**.
3. Expand the agent folder that contains the policy or template you want to view.
4. Select the checkbox(es) in the tree to the left of the policy, or drag and drop the policy into the Target panel. A table opens with the policy information.

Data collection policies property table

Field Name	Description
Agent Name	The data collection policy or template listed in the **Element** field, can only be assigned to the type of agent listed in the **Agent Name** field.
Element	The policy or template name to which the settings displayed in this column are being applied.
MO Type	The type of object from which the data is being collected.
Schedule	The schedule assigned to the data collection policy or template.
Key Labels	The categories you can use to filter the collection. The key labels vary for each data collection policy and template. The key labels are provided from the **Source** tab of the Policy Definition and Assignment dialog box.
Key Values	The value that defines what or how much data to collect from the source. The key values vary for each data collection policy and template. The key values are provided from the **Source** tab of Policy Definition and Assignment dialog box.
Document (not in template view)	The unique title provided to the data collection policy by the user.
Date Modified	The last date that the policy or template was modified.
Who Modified	The ECC user who last modified the policy or template. `Installation` means that the policy was supplied with installation and has not been edited since.

Related topics

- Data collection policies
- Defining and assigning data collection policies

Data Retention overview

Data retention policies define how long and how much historical ALERT, ALLOCATION, LOG, and SNAP data to save in the Repository.

Data Type	Description
Alert	Alerts that have already been fired.
Allocation	This is information that grows or changes, for example filesystem size.
Log	Files that contain logs about ControlCenter installation or when the Repository has been reset.
SNAP	Container that holds snapshots of configuration information. A new snapshot is created each time there is a configuration change.

Related Topics

- Defining data retention policies

Defining data retention policies

Data retention policies define how long and how much historical ALERT, ALLOCATION, LOG, and SNAP data to save in the Repository.

To define a data retention policy:

1. Select the type of data to which you are assigning the retention policy. From the tree panel, expand **Administration**, **Data Retention Policies**, and select the data type.
2. Right-click the data type and select **Edit Retention**.
3. Enter the number of days, weeks, or months worth of historical data to retain, and then select **Days**, **Weeks**, or **Months**.
4. Select how often the data retention policy will run: **Weekly**, **Monthly**, or **Daily**.
5. Enter the date and time when the data retention policy will start.
6. **Enable** the policy and click **OK**. The data retention policy will begin to retain the data from the date entered in the **Starting** field.

Related Topic

- Introduction to data retention policies

Agent administration overview

Agent administration involves different tasks and procedures that an administrator performs in order to install, configure, and start and stop agents. Administration tasks and procedures are unique to each agent, whether it is an MVS, Windows, or Solaris agent, for example. Each agent requires specific installation prerequisites and post-installation configurations, if any, that enable the administrator to install the agent and get it up and running correctly. Once set up, the agent can monitor and collect information about your storage environment that is most important to you.

A time might arise when you need to stop or restart an agent, possibly for maintenance purposes, or you may need to update its configuration to reflect changes in your storage environment. Choose one of the following for more information:

- Starting and stopping agentsExplains how to start and stop agents.
- Updating agent configurationsExplains why and how to update or change an agent's configuration.
- Updating MVS agent configurationsProvides configuration procedures specific to MVS agents. You can still use the link above for general agent configurations.

To learn more about the administration tasks that are specific to your agent, select from the following:

Common Agents	Storage Agents	Host Agents	Connectivity Agents	Database Agents	Backup Agent	Tape Agent
Master Agent	Storage Agent for Celerra	Host Agent for Windows	Connectivity Agent for SDM	Database Agent for Oracle	Backup Agent for TSM	Tape Agent for MVS
Integration Gateway	Storage Agent for CLARiiON	Host Agent for HSM	Connectivity Agent for Switches	Database Agent for DB2		
WLA Archiver	Storage Agent for Compaq StorageWorks	Host Agent for SMS	Connectivity Agent for SNMP			
	Storage Agent for HDS	Host Agent for Solaris				
	Storage Agent for IBM ESS	Host Agent for Novell				
	Storage Agent for Symmetrix	Host Agent for AIX				
	Storage Agent for RVA/SVA	Logical Agent for MVS				
		Physical Agent for MVS				
		Host Agent for HP-UX				

Related topics

- Installing and configuring agents
- Updating agent configurations
- Updating MVS agent configurations
- Starting and stopping agents
- ControlCenter agents overview

Installing and configuring agents

Important: MVS agents do not install through the Console. Refer to the *EMC ControlCenter Installation and Configuration Guide* for MVS agent installation procedures.

Installing agents requires that you complete the following tasks:

1. Preparing the agent host.
   Important! If you do not complete this step, the agent installation may install improperly or not at all.
2. Collecting system information requested during the agent installation.
3. Installing the agent.
4. Configuring the agent.

Note: See ControlCenter Agent Overview for agents overview information.

Preparing the Agent Host

Before attempting to install an agent on an agent host machine, verify that agent-specific host conditions are met:

Common Agents	Storage Agents	Host Agents	Connectivity Agents	Database Agents	Backup Agent	Tape Agent
Master Agent	Storage Agent for Celerra	Host Agent for Windows	Connectivity Agent for SDM	Database Agent for Oracle	Backup Agent for TSM	Tape Agent for MVS
Integration Gateway	Storage Agent for CLARiiON	Host Agent for HSM	Connectivity Agent for Switches	Database Agent for DB2		
WLA Archiver	Storage Agent for Compaq StorageWorks	Host Agent for SMS	Connectivity Agent for SNMP			
	Storage Agent for HDS	Host Agent for Solaris				
	Storage Agent for IBM ESS	Host Agent for Novell				
	Storage Agent for Symmetrix	Host Agent for AIX				
	Storage Agent for RVA/SVA	Logical Agent for MVS				
		Physical Agent for MVS				
		Host Agent for HP-UX				

Collecting Agent-Specific System Information

During the agent installation procedure, ControlCenter system information is requested. To view the system information required by an agent, click the agent from the list that follows then note the information to use during the installation process.

Common Agents	Storage Agents	Host Agents	Connectivity Agents	Database Agents	Backup Agent
Master Agent	Storage Agent for Celerra	Host Agent for Windows	Connectivity Agent for SDM Agent	Database Agent for Oracle	Backup Agent for TSM
Integration Gateway	Storage Agent for CLARiiON	Host Agent for Solaris	Connectivity Agent for Switches		
WLA Archiver	Storage Agent for Compaq StorageWorks	Host Agent for Novell	Connectiivity Agent for SNMP		
	Storage Agent for HDS Agent	Host Agent for AIX			
	Storage Agent for Symmetrix	Host Agent for HP-UX			

Installing Agents

There are two methods to install open systems agents on a host (refer to the *EMC ControlCenter Installation and Configuration Guide* for MVS agent installation procedures):

- Remote install through the Console
- Local install through the Installation Utility (Connectivity Agent for SNMP, Storage Agent for Celerra)

The agent type determines the installation method. The majority of agents install through the Console.

Configuring the agent

The following table lists the agents that have configurable parameters. Click an agent to view its configurable parameters.

Common Agents	Storage Agents	Host Agents	Connectivity Agents	Database Agents	Backup Agent	Tape Agent
Master Agent	Storage Agent for Celerra	Host Agent for Windows	Connectivity Agent for SDM	Database Agent for Oracle	Backup Agent for TSM	Tape Agent for MVS
Integration Gateway	Storage Agent for CLARiiON	Host Agent for HSM	Connectivity Agent for Switches	Database Agent for DB2		
WLA Archiver	Storage Agent for Compaq StorageWorks	Host Agent for SMS	Connectivity Agent for SNMP			
	Storage Agent for HDS	Host Agent for Solaris				
	Storage Agent for IBM ESS	Host Agent for Novell				
	Storage Agent for Symmetrix	Host Agent for AIX				
	Storage Agent for RVA/SVA	Logical Agent for MVS				
		Physical Agent for MVS				
		Host Agent for HP-UX				

Related topics

- Starting and stopping agents
- ControlCenter agent overview
- Viewing agent install log files
- Viewing a list of installed agents

Starting and stopping agents

How you start an agent can vary depending on the type of agent and the operating system that agent runs on. Most agents start or stop through the Console.

Important! For MVS agents, make sure that you have specified a fully-qualified host name when defining the Symmetrix remote discovery policy. Otherwise, when you start the Master Agent, the store will no longer recognize the host.

- Starting an agent from the Console
- Stopping an agent from the Console

Before attempting to start or stop an agent through the Console, verify that your agent does not have agent-specific start requirements or stop requirements. This information, if it exists, is included in the agent-specific administration topics:

Common Agents	Storage Agents	Host Agents	Connectivity Agents	Database Agents	Backup Agent	Tape Agent
Master Agent	Storage Agent for Celerra	Host Agent for Windows	Connectivity Agent for SDM	Database Agent for Oracle	Backup Agent for TSM	Tape Agent for MVS
Integration Gateway	Storage Agent for CLARiiON	Host Agent for HSM	Connectivity Agent for Switches	Database Agent for DB2		
WLA Archiver	Storage Agent for Compaq StorageWorks	Host Agent for SMS	Connectivity Agent for SNMP			
	Storage Agent for HDS	Host Agent for Solaris				
	Storage Agent for IBM ESS	Host Agent for Novell				
	Storage Agent for Symmetrix	Host Agent for AIX				
	Storage Agent for RVA/SVA	Logical Agent for MVS				
		Physical Agent for MVS				
		Host Agent for HP-UX				

Starting an agent from the Console

To start an agent from the Console:

1. Click **ECC Administration** for the ECC Administration View.
2. Open Start Agent dialog box using either of the following methods:
   From the **Agents** menu, click **Start**.
   or
   Expand the **Administration, Install, Hosts** folders, and then right-click the host where you want the agent to start and select **Agents**, **Start**.
3. On the Start Agent dialog box, select the agent you want to start and the method you want to use to start the agent, then click **OK**.
4. To verify the agent start status, select the **Hosts** checkbox to view all hosts then; select the host. Expand **System Information, ECC Agents** then right-click and select **Properites.** The Properties-Agents information displays in the target panel, and if the status indicates Active, the agent is running.

Stopping an agent from the Console

To stop an agent from the Console:

1. Click **ECC Administration** for the ECC Administration View.
2. Open the Stop Agent dialog box using either of the following methods:
   From the **Agents** menu, click **Stop**.
   or
   Expand the **Administration, Install, Hosts** folders, and then right-click the host where you want the agent to stop running and select **Agents**, **Stop**.
3. On the Stop Agent dialog box, select the agent you want to stop and the method you want to use to stop the agent, then click **OK**.
4. A confirmation dialog box appears. Click **Yes** to confirm that you want the selected agent(s) to stop running.
5. To verify the agent stop status, click the **Hosts** checkbox to view all hosts then select the host and expand **System Information, ECC Agents** the right-click and select **Properties**. The Properties-Agents information displays in the target panel, and if the status indicates Not Active, the agent is not running.

Related topics

- Installing and configuring agents
- Updating agent configurations
- Updating MVS agent configurations
- ControlCenter agents overview

Updating agent configurations

You may need to update the configuration of one or more of your agents. For example, if you have finished installing an agent and accidentally made a mistake during the installation, you can update the agent's configuration with the correct information. Or, if you need to change an ECC server's IP address, you need to update the agents on that server with the new IP address number, which you can do for multiple agents simultaneously.

Use the Edit Agent Configuration dialog box to change or update an agent's configuration from the host that is running the ControlCenter console.

Important! The Edit Agent Configuration dialog box does not support MVS agents. It also does not support the Storage Agent for Celerra or the Connectivity Agent for SNMP. You must manually edit the agent's initialization (.ini) file, the file that contains the agent's configuration parameters and settings.

Also, as a ControlCenter user, make sure that you have read and/or edit permissions in order to view and edit each agent's configuration.

To display the Edit Agent Configuration dialog box:

1. Locate and select the host, object, Symmetrix, device, or folder, etc. that contains the agent you want to update. To select more than one item, either hold down Shift and drag over the items, or hold down the Control key while selecting.
2. With the item, or items, still selected, right-click it and select **Agents**, **Update Configuration...**. The Edit Agent Configuration dialog box appears displaying a list of all agents you selected in the Agents table.

Related topics

- Using the Edit Agent Configuration dialog box
- Installing and configuring agents
- Updating MVS agent configurations
- ControlCenter agents overview

See the *EMC ControlCenter Installation and Configuration Guide*, also available in PDF format on the Documentation CD.

Updating MVS agent configurations

During or after installation, you may need to change the configuration of MVS agents to correct errors or omissions or to reflect changes to your environment. Use the instructions in this section to assist you.

Note: This configuration procedure applies only to MVS agent parameters that cannot be edited in the Console. Before you use this procedure, see topics on general administration and agent-specific administration.

This procedure requires you to run a job on an MVS system and to restart the agents you modify.

To change configuration parameters for ControlCenter agents on MVS:

1. Start the installation ISPF panels. To access the ISPF panels, execute the following command from ISPF option 6:
   ex '*codehlq*.**install(SETUP)**'

   where *codehlq* is the high-level qualifier of the installation partitioned data set.

2. In the primary menu, select option **3**. The Configuration panel displays.
3. In the Configuration panel, select with **S** the system profile you want to edit and press **Enter**. The Configuration Options panel displays.
4. In the Configuration Options panel, choose the option of the configuration you want to edit. You can change startup settings, agent parameters, and user ID mappings.
5. Enter changes as desired; then press **Enter** to verify. Press **PF3**.
6. Continue making changes by selecting the agent configuration option you want.
7. When you have completed all changes, press **PF3** until you reach the Configuration Options panel.
8. Select option **4**, **Tailor and Submit Batch Jobs**.
9. In the Job Creation Tasks menu, select option **1** to edit the job card as needed. Press **PF3** when complete.
10. Select option **3**, **Create, Edit, and Submit Jobs**.
11. Type **Sub** and press **Enter** to submit the job.
12. Review the job output to make sure the job ran correctly.
13. At the MVS operator console issue the command:
    F CSMAGENT,env r *xxxxxxxx*

    where *xxxxxxxx* is the eight-character agent code.

See the *EMC ControlCenter Installation and Configuration Guide*, also available in PDF format on the Documentation CD.

Agent codes

- MMNSERVR - NetServer (infrastructure)

  This component handles communications between MVS agents and the ECC Server. Always start MMNSERVR after the Master Agent and before any other agents.
- MM2AGENT - Database Agent for DB2
- MM3AGENT - Console Framework Agent (infrastructure)
- MMCAGENT - Storage Agent for IBM ESS
- MMHAGENT - Host Agent for HSM
- MMIAGENT - Storage Agent for RVA/SVA
- MMLAGENT - Logical Agent for MVS
- MMPAGENT - Physical Agent for MVS
- MMSAGENT - Host Agent for SMS
- MMTAGENT - Tape Agent for MVS
- MMYAGENT - Backup Agent for TSM

You can also change automatic startup values and mappings from ControlCenter user IDs to MVS user IDs.

Related topics

- Installing and configuring agents
- Updating agent configurations
- ControlCenter agents overview

Administering agents

Backup Agent for TSM administration

The following contains supporting information necessary during the installation and configuration procedure for the Backup Agent for TSM. It provides detailed information about what you must do before and after the installation. First ensure that the host to which you are installing the agent meets the specified requirements listed. Once your host is ready for the agent installation, you can install the agent. After installing the agent, see if there are additional configurations you must perform.

- Preparing the host
- Configuring the agent
- Updating agent configuration on open systems
- Updating agent configuration on MVS

Preparing the host

Before you install Tivoli Storage Manager Agent, ensure the following:

- Tivoli Storage Manager 3.7 or 4.1 is installed.
- The TSM administrative client is installed and configured.
- All TSM servers on a single host are the same version (if you want ControlCenter to manage them).
- All TSM servers on a host have unique names.

Complete the following procedure: Determining required TSM server names This procedure also describes how to ensure unique names.

To install on a Windows, AIX, HP-UX, or Solaris host, return to Installing and configuring agents.

To install on an MVS host, perform the pre-installation, installation, and post-installation procedures in the *EMC ControlCenter Installation and Configuration Guide*.

Configuring the Tivoli Storage Manager Agent

After installing and starting the agent, perform the following configurations to complete the installation and ensure that the agent runs properly:

- Configuring repository logging for TSM data
- Configuring additional TSM servers on a host

Also, verify the configuration of data collection policies.

- Backup Agent for TSM: data collection policies

Updating agent configuration on open systems

If you need to change the ECC server, port number, or store, see Updating the agent configuration.

Updating agent configuration on MVS

To change the ECC server, port number, or store, see Updating MVS agent configuration. To make other changes, continue reading.

Server configuration

You can update any of the following for a TSM server:

- Server name
- TCP/IP port number
- Administrator user ID
- Administrator password

If you defined a TSM server through the Console, use the Console to update the configuration of the Backup Agent for TSM. See Configuring additional TSM servers on a host.

If you defined a TSM server as part of the initial installation of the agent through ISPF, use the ISPF setup program to edit its configuration. See Updating MVS agent configuration.

Tivoli Storage Manager product configuration

To update any of the following, see Updating MVS agent configuration:

- TSM load library data set name
- TSM admin client messages data set
- TSM admin client options data set
- Error log HLQ

Related topics

- Installing and configuring agents
- Starting and stopping agents
- Backup Agent for TSM data collection policies
- Updating agent configurations
- ControlCenter agents overview

Connectivity Agent for SDM administration

The Connectivity Agent for Storage Device Masking (SDM Agent) monitors volume-access control in Symmetrix systems in the SAN and updates the Repository when configuration changes occur. The information monitored is stored in the VCM database in each Symmetrix Fibre Channel adapter.

Preparing the host

The SDM Agent must be installed through the Console onto all hosts used to monitor volume-access control in Symmetrix systems. Before installing the SDM Agent, the host must be configured as follows:

- Master agent installed
- Fibre Channel connection
- Connection to a VCM-enabled Symmetric system

Configuring the SDM Agent

It is not necessary to configure the SDM Agent. However, if you wish to change the default configuration, see Updating agent configurations.

Data collection policies

The SDM Agent has one data collection policy that causes it to poll Symmetrix systems in the SAN every 15 minutes. This policy is enabled by default upon installation of the agent. For more information on the SDM Agent collection policy, see Connectivity Agent for SDM data collection policy.

Related topics

- Connectivity Agent for SDM overview
- Connectivity Agent for SDM data collection policy
- Installing and configuring agents
- Starting and stopping agents
- Updating agent configurations
- ControlCenter agents overview
- Topology discovery
- Discovery and monitoring requirements

Connectivity Agent for SNMP administration

Installed as part of the ControlCenter infrastructure, the Connectivity Agent for SNMP discovers and monitors connectivity devices in the SAN through the SNMP protocol. It communicates with connectivity devices through the SNMP agents that manage them. One SNMP agent can manage multiple remote devices in addition to the local device on which it is installed. The Connectivity Agent for SNMP sends the data it collects from the SNMP agents to the Repository, where it is accessed by ControlCenter and displayed in the Console.

Preparing the host

No special host preparation is required before installing the Connectivity Agent for SNMP. However, it is recommended to install the Connectivity Agent for SNMP on the same host as the ECC Server.

Configuring the Connectivity Agent for SNMP

It is not necessary to configure the Connectivity Agent for SNMP.

If you wish to change the current configuration on this agent, edit the Connectivity Agent for SNMP `.INI` file (`EGA.ini`) by hand on the host where it resides.

Note: By default, `EGA.ini` resides in: `<INSTALL_ROOT>\exec\EGA500\`, where `INSTALL_ROOT` is `C:\ecc`.

Data collection policies

The six data collection policies associated with the SNMP Connectivity Agent are used to discover and monitor the SAN. Only the SNMP Discover Request policy has to be assigned. Four of the policies are enabled upon installation of the agent and, by default, target all of the devices discovered by the Connectivity Agent for SNMP. The sixth policy, SNMP Rescan Request, is typically used to monitor specific instances, such as the startup of a new hub or switch, and must be assigned before it becomes active.

Note: There can only be one SNMP Discover Request policy assigned.

For more information, see Connectivity Agent for SNMP data collection policies.

Notes

- In addition to monitoring the IP addresses entered into its data collection policies, the Connectivity Agent for SNMP monitors the IP addresses entered into the Search for Connectivity Devices dialog box during a user-initiated discovery.
- The Connectivity Agent for SNMP finds connectivity devices, including switches, in the SAN. However, to further discover the topology information for switches found, it is necessary to perform switch discovery through the Search for Connectivity Devices dialog box. See Topology discovery.

Related topics

- Connectivity Agent for SNMP overview
- Connectivity Agent for SNMP data collection policies
- Connectivity Agent for SNMP alerts
- Installing and configuring agents
- Starting and stopping agents
- ControlCenter agents overview
- Topology discovery
- Discovery and monitoring requirements

Connectivity Agent for Switches administration

The Connectivity Agent for Switches (Switch Agent) discovers and monitors connection settings and topology information associated with Fibre Channel switches and fabrics in the SAN. It sends the data it discovers to the Repository, where it is accessed by ControlCenter and displayed in the Console. One Switch Agent installation services all users accessing the ECC Server.

Preparing the host

One instance of the Switch Agent is required to be installed per ECC Server for all users. However, multiple instances of the Switch Agent in the SAN are harmless. The Switch Agent is installed through the Console.

Before installing the Switch Agent on a host, it must have the following:

- Master agent installed
- IP connection to the switches that the Switch Agent will manage

Configuring the Switch Agent

It is not necessary to configure the Switch Agent. If you wish to change the current configuration, see Updating agent configurations.

Data collection policies

The Switch Agent has two data collection policies that poll Fibre Channel switches and fabrics every 15 minutes. These policies must be assigned from the Policy Templates directory in the tree panel before the Switch Agent can function. See Connectivity Agent for Switches data collection policies.

Related topics

- Connectivity Agent for Switches overview
- Connectivity Agent for Switches data collection policies
- Installing and configuring agents
- Starting and stopping agents
- Updating agent configurations
- ControlCenter agents overview
- Topology discovery
- Discovery and monitoring requirements

Database Agent for DB2 administration

The following contains supporting information necessary during the installation and configuration procedure for the Database Agent for DB2. It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the agent meets the specified requirements. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring the Database Agent for DB2 to see if there are additional configurations you must perform.

- Preparing the host
- Configuring the Database Agent for DB2
- Updating agent configuration

Preparing the host

The Database Agent for DB2 has the following requirements for MVS and OS/390 systems:

- OS/390 1.3 or later
- IBM DB2 5 or 6

Configuring the Database Agent for DB2

After installing the Database Agent for DB2, perform the following configurations to complete the installation and ensure that the agent runs properly:

- Configuring data collection for DB2 alerts and reports
- Configuring collection of DB2 summary data

Updating agent configuration

- To change the server or store to which the agent is connected, see Updating agent configurations.
- To edit an existing DB2 subsystem definition or to add a new DB2 subsystem to ControlCenter, see Updating MVS agent configuration.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- ControlCenter agents overview

Database Agent for Oracle administration

The following contains supporting information necessary during the installation and configuration procedure for the Database Agent for Oracle. It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the agent meets the specified requirements listed. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring, to see if there are additional configurations you must perform.

- Preparing the host
- Configuring the Database Agent for Oracle

Preparing the host

Before installing the Database Agent for Oracle ensure that::

- you have installed the Repository, Store, and Console
- you have installed the Master Agent on the host on which you are installing the Database Agent for Oracle

Configuring the Database Agent for Oracle

After installing the Database Agent for Oracle you must execute the following SQL scripts.

- Logged in as Oracle user "sys," execute the SQL script sys8.sql. This script creates the Oracle user "oraagent."
- As oracle user "oraagent," execute the SQL script oraagent8.sql. This script creates the views that the Oracle agent uses.

If you wish to change the current configuration, see Updating the agent configuration.

Return to Installing and configuring agents to install the agent.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- Database Agent for Oracle data collection policy
- Updating agent configurations
- ControlCenter agents overview

Host Agents for AIX, HP-UX, and Solaris administration

The following contains supporting information necessary during the installation and configuration procedure for the AIX, HP-UX, and Host Agent for Solariss. It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the agent meets the specified requirements listed. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring the Host Agents for AIX, HP-UX, and Solaris , to see if there are additional configurations you must perform.

- Preparing the host
- Configuring the Host Agents for AIX, HP-UX, and Solaris

Preparing the host

Before installing the Host Agent for AIX, HP-UX, or Solaris, ensure that the following are true:

AIX

- AIX 4.3 is installed.

HP-UX

- HP-UX 11.0 is installed.

Solaris

- Solaris 2.6, 2.7 or 2.8 is the installed operating system.
- VERITAS Volume Manager is optional but is required for all VERITAS functionality. If VERITAS Volume Manager is installed, it must be Volume Manager 3.1 with VERITAS File System 3.3.3.
- If VERITAS Volume Manager is installed on the host, the *PATH* environment variable for the superuser account used by the agent must point to the VERITAS-installed commands.

Return to Installing and configuring agents to install the agent.

Configuring the Host Agents for AIX, HP-UX, and Solaris

After installing the Host Agents for AIX, HP-UX, and Solaris, no further configuration is necessary unless a Symmetrix system is attached to the host. In this situation, Symmetrix API (SymAPI) shared libraries must be installed, and the host agents must know where to find them. To inform the agents of the location of the SymAPI libraries you need to:

AIX

- Define or update the LIBPATH to include the path to the shared library. If the library is installed (or a link to it) in /usr/lib then there is no need to define LIBPATH.

HP-UX

- Define or update the SHLIB_PATH to include the path to the shared library. If the library is installed (or a link to it) in /usr/lib then there is no need to define SHLIB_PATH.

Solaris

- Define or update the LD_LIBRARY_PATH to include the path to the shared library. If the library is installed (or a link to it) in /usr/lib then there is no need to define LD_LIBRARY_PATH.

Usually, when the SymAPI is installed in a host, /usr/lib has a link to the actual installed directory.

Updating agent configuration

- To change the server or store to which the agent is connected, see Updating agent configurations.

Note

- You can test if VERITAS Volume Manager is installed on a Solaris host by using the command `pkginfo`. If VERITAS information is returned by the command, Volume Manager is installed. The agent uses the command `pkginfo VRTSvxvm` to detect VERITAS on the host. If you cannot detect VERITAS using this method, the agent may have trouble doing so as well.

Related topics

- How the UNIX Host Agents operate
- Checking the status of UNIX Host Agents
- Installing and configuring agents
- Starting and stopping agents
- Host Agents for AIX, HP-UX, and Solaris policies
- Host Agents for AIX, HP-UX, and Solaris overview
- ControlCenter agents overview

Host Agent for MVS HSM administration

The following contains supporting information necessary during the installation and configuration procedure for the Host Agent for MVS HSM. It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the agent meets the specified requirements. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring, to see if there are additional configurations you must perform.

Preparing the host

Configuring the Host Agent for MVS HSM

Updating agent configuration

Preparing the host

The Host Agent for MVS HSM has the following requirements for MVS and OS/390 systems:

- MVS/ESA 5.1 or later, OS/390, or z/OS for full function support
- MVS/ESA 4.2.2 for support without console messaging
- TCP/IP 3.1 or later
- TSO/E 2.4 or later
- DFSMShsm 2.6 or later

To collect all possible data, MVS HSM must be installed on all images where HSM is running.

Configuring the Host Agent for MVS HSM

After installing the agent, perform the following configurations to complete the installation and ensure that the agent runs properly:

- MVS HSM: Configuring automation setup rules
- MVS HSM: Configuring backup automation rules

Updating agent configuration

- To change the CDSs that the agent monitors, see Pointing MVS HSM to new CDSs.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- Updating MVS agent configuration
- ControlCenter agents overview

Host Agent for MVS SMS administration

The following contains supporting information necessary during the installation and configuration procedure for the Host Agent for MVS SMS. It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the agent meets the specified requirements. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring, to see if there are additional configurations you must perform.

- Preparing the host
- Configuring the MVS Host Agent for MVS SMS
- Updating agent configuration

Preparing the host

The MVS Host Agent for MVS SMS has the following requirements for MVS and OS/390 systems:

- MVS/ESA 5.1 or later, OS/390, or z/OS for full function support
- MVS/ESA 4.2.2 for support without console messaging
- TCP/IP 3.1 or later
- TSO/E 2.4 or later
- MVS/DFP 3.2 or later or DFSMS
- The IBM maintenance fix: DFSMSdfp PTF UW31734

Configuring the Host Agent for MVS SMS

After installing the agent, perform the following configurations to complete the installation and ensure that the agent runs properly:

- Configuring storage monitoring rules
- Configuring fragmentation monitoring rules

Updating agent configuration

- To change the DFSMSdss load library dataset name, see Updating MVS agent configurations.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- Updating and configuring MVS agents
- ControlCenter agents overview

Host Agent for Novell administration

The following contains supporting information necessary during the installation and configuration procedure for the Novell Storage Agent. It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the agent meets the specified requirements listed. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring the Novell Storage Agent, to see if there are additional configurations you must perform.

- Preparing the host
- Configuring the Host Agent for Novell

Preparing the host

Before installing the Host Agent for Novell, ensure that the following are true:

- Windows NT or Windows 2000 is running the NetWare client on which the agent will be installed.
- The client workstation on which the agent is installed must be dedicated to running the agent. In Novell, only one active, licensed login can be maintained to an NDS tree for a given machine. Secondary logins by users on the workstation will interfere with the agent's ability to operate.
- The servers to be administered and monitored are running NetWare 4.x or 5.x.
- If NetWare 4.x is being used, IPX/SPX must be enabled on the client machine. NetWare 5.x systems use TCP/IP.
- The Novell client machine on which the agent will be installed is on the same network as the NetWare server(s) to be administered and monitored. A good test is to ensure that you can you ping the NetWare server(s).

Return to Installing and configuring agents to install the agent.

Configuring the Novell Storage Agent

There are no additional configurations necessary for running this agent.

Updating agent configuration

- To change the server or store to which the agent is connected, see Updating agent configurations.

Related topics

- How the Host Agent for Novell operates
- Checking the status of the Host Agent for Novell
- Installing and configuring agents
- Starting and stopping agents
- Host Agent for Novell overview
- ControlCenter agents overview

Host Agent for Windows administration

This topic contains information needed to install and configure the Host Agent for Windows. Before you install, refer to Preparing the host to ensure that the host to which you are installing the agent meets the specified requirements. After you prepare the host, install the agent. Upon completion, see Configuring the Host Agent for Windows to determine whether you must perform additional configuration steps.

- Preparing the host
- Configuring the Host Agent for Windows

Preparing the host

Before installing the Host Agent for Windows, ensure that:

- You have installed the ECC Server, Repository, Store, and Console
- You have installed the Master Agent on the host on which you are installing the Host Agent for Windows

The host to which you are installing the agent must have:

- Windows NT 4.0 Workstation, Server, or Enterprise Edition or Windows 2000 Professional or Server
- Pentium-class processor or equivalent
- 64 MB RAM
- TCP/IP
- Internet Explorer 4.0 or later with Active Desktop component (Active Desktop does not have to be active) for Recycle Bin functionality
- Logical and physical disk counters enabled for performance monitoring functionality.
- The Microsoft's Windows Management Instrumentation (WMI) interface. The WMI core components (including `MOFComp.exe`) are a standard part of the Microsoft Windows 2000 operating system, but not the Windows NT 4.0 operating systems. You can download the WMI core components for Windows NT 4.0 from the Microsoft site (http://www.microsoft.com). Search for "WMI core".
- Approximately 4 MB for the agent files and 4.5 MB for files that are shared with other agents on the same system. In addition, you should allocate a minimum of 20 MB for the agent's log files and up to 300 MB if you enable the highest level of tracing.

Return to Installing and configuring agents to install the agent.

Configuring the Host Agent for Windows

After you install the Host Agent for Windows, perform the following additional tasks before using the agent.

Ensure the agent has the required user rights

- Ensuring the Host Agent for Windows has required rightsThe user that the Host Agent for Windows runs as must have the "Act as part of the operating system" and "Back up files and directories" user rights.

Configure agent features

Certain Host Agent for Windows features require additional setup steps. Perform these optional steps after you start the agent:

- Enabling I/O monitoringYou can monitor the I/O events that occur against a file or folder. See this topic for steps on specifying the files to monitor.
- Enabling or disabling event log monitoringThe agent allows you to receive alerts when specific messages are written to the Windows event logs. Although this monitoring is set up by default, this topic explains how to change the extent of the agent's monitoring.
- Enabling disk countersTo use the agent's disk performance monitoring features, you must ensure that counters for Windows disk performance object are enabled. See how in this topic.

Edit agent defaults

Read the following topics for instructions on changing some of the agent's defaults:

- Changing the evaluation frequency for performance alerts
- Changing the folder for event log backups
- Changing restart attempts for Service Failure alert

Note that you cannot change these settings through the Edit Agent Configuration dialog box. You must restart the agent after changing any of these defaults.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- Updating agent configurations
- ControlCenter agents overview
- Host Agent for Windows data collection policies
- Host Agent for Windows overview

Integration Gateway administration

The following contains supporting information necessary during the installation and configuration procedure for the Integration Gateway. It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the agent meets the specified requirements listed. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring the Integration Gateway, to see if there are additional configurations you must perform.

- Preparing the host
- Configuring the Integration Gateway

Preparing the host

Before installing the Integration Gateway ensure that:

- the Installation Utility resides on the current host
- the ECC Server and Store have been installed and are currently running

Configuring the Integration Gateway

The ECC Server and Store must be running before starting the Integration Gateway.

If you wish to change the current configuration, see Updating the agent configuration.

Return to Installing and configuring agents to install the agent.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- Updating agent configurations
- ControlCenter agents overview

Master Agent administration

The following contains supporting information necessary during the installation and configuration procedure for the Master Agent. It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the agent meets the specified requirements listed. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring, to see if there are additional configurations you must perform.

- Preparing the host
- Configuring the Master Agent

Preparing the host

Before installing the Master Agent ensure that:

- the Installation Utility resides on the current host
- the Repository has been installed and is currently running
- The Repository is selected on this host

Return to Installing and configuring agents to install the agent.

Configuring the Master Agent

There are no additional configurations necessary for running this agent. If you wish to change the current configuration, see Updating the agent configuration.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- Updating agent configurations
- ControlCenter agents overview

Logical Agent for MVS administration

The following contains supporting information necessary during the installation and configuration procedure for the Logical Agent for MVS. It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the agent meets the specified requirements. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring, to see if there are additional configurations you must perform.

Preparing the host

Configuring the Logical Agent for MVS

Updating agent configuration

Preparing the host

The Logical Agent for MVS has the following requirements for MVS and OS/390 systems:

- MVS/ESA 5.1 or later, OS/390, or z/OS for full function support
- MVS/ESA 4.2.2 for support without console messaging
- TCP/IP 3.1 or later
- TSO/E 2.4 or later

Configuring the Logical Agent for MVS

After installing the agent, perform the following configuration procedures to complete the installation and to ensure that the agent runs properly:

- Basic Setup
- Application IDs
- CSL Dump configuration

Updating agent configuration

- If you change your SORT utility or need to change the data set you use for DCOLLECT activity, go to the Basic Setup menu.
- If you change your DUMP utility data set name, refer to the CSL Dump menu.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- Updating MVS agent configurations
- ControlCenter agents overview

Physical Agent for MVS administration

The following contains supporting information necessary during the installation and configuration procedure for the Physical Agent for MVS. It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the agent meets the specified requirements. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring, to see if there are additional configurations you must perform.

Preparing the host

Configuring the Physical Agent for MVS

Updating agent configuration

Preparing the host

The Physical Agent for MVS has the following requirements for MVS and OS/390 systems:

- MVS/ESA 5.1 or later, OS/390, or z/OS for full function support
- MVS/ESA 4.2.2 for support without console messaging
- TCP/IP 3.1 or later
- TSO/E 2.4 or later

Configuring the Physical Agent for MVS

After installing the Physical Agent for MVS, no further configuration is required. You may want to configure certain alerts, but the agent has no standard configuration to work.

Updating agent configuration

The agent does not require any updates to its configuration.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- Updating MVS agent configurations
- ControlCenter agents overview

Storage Agent for Celerra administration

The following contains supporting information necessary during the installation and configuration procedure for the Storage Agent for Celerra . It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the agent meets the specified requirements listed. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring, to see if there are additional configurations you must perform.

- Preparing the host
- Configuring the Storage Agent for Celerra

Preparing the host

Before installing the Storage Agent for Celerra ensure that:

- the Installation Utility resides on the current host
- the ECC Server and Store have been installed and are running

Configuring the Storage Agent for Celerra

After installing the Storage Agent for Celerra ensure that:

- the ECC Server and Store are running before starting the Storage Agent for Celerra
- the Storage Agent for Celerra is running on the same host as the ECC Server

Discovering and removing Celerras

If you want the Storage Agent for Celerra to discover additional Celerras after the initial agent installation you must manually edit the CNC.ini file in C:\ECC\ecc_inf\data\<machine_name>\data.

Under the heading [[Celerra Agent]] add the additional Celerra IP and port information.

Delete the Celerra IP and port information to remove that Celerra from the Console.

Note: The Storage Agent for Celerra polls the CNC.ini file every 5 minutes. Added or deleted entries are updated in the Console each polling cycle.

For more information about changing the current configuration, see Updating the agent configuration.

Return to Installing and configuring agents to install the agent.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- Updating agent configurations
- ControlCenter agents overview

Storage Agent for CLARiiON administration

The following contains supporting information necessary during the installation and configuration procedure for the CLARiiON Agent. It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the agent meets the specified requirements listed. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring the CLARiiON Agent, to see if there are additional configurations you must perform.

- Preparing the host
- Configuring the Storage Agent for CLARiiON

Preparing the host

- Make sure the host on which you are installing the agent meets these requirements:
  - Navisphere SP Agent must be installed and running on the FC4700 SP Hosts.
  - Access Logix software must be installed and enabled on FC4700 SP Hosts.
  - Navisphere Agent and Navisphere CLI software must be installed on the Windows NT or Windows 2000 server where the CLARiiON agent is running.
  - User must update the `MxL.ini file` in the [`DiskArrayHosts`] section with the names of the SPA and SPB hosts.
  - Optional - for SnapView support, SnapView must be installed.
  - Check ECC_HOME to make sure it is set correctly.

Return to Installing and configuring agents to install the agent.

Configuring the Storage Agent for CLARiiON

The user will be asked during install to specify the path.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- Updating agent configurations
- ControlCenter agents overview

Storage Agent for Compaq StorageWorks administration

This topic contains information needed to install and configure the Storage Agent for Compaq StorageWorks. Before you install, refer to Preparing the host to ensure that the host on which you are installing the agent meets the specified requirements. After you prepare the host, install the agent. Upon completion, see Configuring to determine whether you must perform additional configuration steps.

- Preparing the host
- Configuring the Storage Agent for Compaq StorageWorks

Preparing the host

Before installing the Storage Agent for Compaq StorageWorks, ensure that:

- You have installed the ECC Server, Repository, Store, and Console
- You have installed the Master Agent on the host on which you are installing the Storage Agent for Compaq StorageWorks

The host on which you are installing the agent must have:

- Windows NT 4.0 Workstation, Server, or Enterprise Edition or Windows 2000 Professional or Server.
- Pentium-class processor or equivalent.
- 64 MB RAM.
- TCP/IP.
- Approximately 4 MB for the agent files and 4.5 MB for files that are shared with other agents on the same system. In addition, you should allocate a minimum of 20 MB for the agent's log files and up to 300 MB if you enable the highest level of tracing.

Connecting to StorageWorks subsystems

You have two options for connecting to Compaq StorageWorks subsystems. During installation, you can create one of each type of connection. You can add three more connections by updating the agent configuration file manually. For more information on this process, refer to the *EMC ControlCenter Installation and Configuration Guide*. The connection options are:

- Connecting through a physical connection
- Connecting through a Compaq StorageWorks Enterprise Array Manager (STEAM) Agent

Connecting through a physical connection

In this method, you create a physical connection to the StorageWorks subsystem through a maintenance-port connection, in which a serial cable connects a communications port (COM1, COM2, and so on) on the Windows system to a maintenance port on either of the subsystem's two controllers, or the appropriate controller if the subsystem is so configured. For this method, the installation process prompts you for:

- Connection type (specify SERIAL)
- Serial port name (specify COM1, COM2, and so on)
- Baud rate
- Parity
- Stopbit
- Bits

Connecting through a Compaq StorageWorks Enterprise Array Manager (STEAM) Agent

By connecting to a STEAM Agent, you establish connections to all the StorageWorks subsystems to which the STEAM Agent is connected. Additionally, the Storage Agent for Compaq StorageWorks does not have to run on a system that has a physical connection to a Compaq array. To connect to subsystems through a STEAM Agent, the installation process prompts you for:

- Connection type (specify STEAM)
- Host (specify the hostname or IP Address of the host where the STEAM agent is running)
- TCP_PORT (specify the TCP port through which the Storage Agent for Compaq StorageWorks will communicate with the STEAM Agentleave this field as zero unless the STEAM Agent has been configured to use a port other than the default set by Compaq)
- Password (specify a password the Storage Agent for Compaq StorageWorks will use to authenticate itself with the STEAM Agent)
- Timeout (optional)
- Debug (optional)

In addition to specifying these parameters during installation, you must:

1. Run the Agent Configuration Utility (a utility provided by Compaq) on the host running the STEAM Agent.
2. In the utility, add the name of the host running the Storage Agent for Compaq StorageWorks to the list of hosts allowed to access the STEAM Agent over the network. You *must* specify at least **Detailed Status** as the **Access Privilege** for the newly added host.

Return to Installing and configuring agents to install the agent.

Configuring the Storage Agent for Compaq StorageWorks

There are no additional configuration requirements to run this agent. If you want to change the current configuration, see Updating agent configurations. Do not manually update the configuration (.ini) file for the Storage Agent for Compaq StorageWorks. You may corrupt the connection, requiring you to reinstall the agent.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- Updating agent configurations
- ControlCenter agents overview
- Storage Agent for Compaq StorageWorks data collection policies
- Storage Agent for Compaq StorageWorks overview

Storage Agent for HDS administration

The following contains supporting information necessary during the installation and configuration procedure for the agent. It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the agent meets the specified requirements listed. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring, to see if there are additional configurations you must perform.

- Preparing the host
- Configuring the HDS Agent

Preparing the host

The RAID Manager program must to be installed and configured.

Set the env variables to support BC.

Successfully start up RAID Manager program.

Create the HDSPATH file (text file) which contains the RAID Manager installation path and the primary configuration file full path. Copy this file to the HDS agent directory.

Return to Install and configuring agents to install the agent.

Configuring the HDS Agent

There are no additional configurations necessary for running this agent. If you wish to change the current configuration, see Updating agent configurations.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- HDS: Storage Array data collection policy
- HDS: Storage Device data collection policy
- Updating agent configurations
- ControlCenter agents overview

Storage Agent for IBM ESS administration

Before starting this agent, ensure that the Master Agent is running.

There are no requirements for installing the Storage Agent for IBM ESS. See the *EMC ControlCenter Installation and Configuration Guide* for installing agents on MVS systems.

To update the configuration for the Storage Agent for IBM ESS, see Updating MVS agent configurations.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- Storage Agent for IBM ESS data collection policy
- Updating MVS agent configurations
- Storage Agent for IBM ESS overview
- ControlCenter agents overview

Storage Agent for RVA/SVA administration

The following contains supporting information necessary during the installation and configuration procedure for the Storage Agent for RVA/SVA. It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the agent meets the specified requirements listed. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring, to see if there are additional configurations you must perform.

- Preparing the host
- Configuring the Storage Agent for RVA/SVA
- Updating agent configuration
- Managing agent communication with the subsystem

Preparing the host

The Storage Agent for RVA/SVA supports IXFP version 2.1. To use Deleted Data Space Release functionality, including related alerts, each applicable image must be actively running IXFP version 2.1 at the time you want the functions to run.

Configuring the Storage Agent for RVA/SVA

There is no additional configuration required for this agent.

Updating agent configuration

- To change the server or store to which the agent is connected, see Updating the agent configuration.
- To change any of the following parameters, see Updating MVS agent configurations:
  - IXFP load library data set name
  - IXFP CLIST names
  - Primary and secondary allocations for Net Capacity Load data

Managing agent communication with the subsystem

The Storage Agent for RVA/SVA requires access to an ECAM, an MVS device needed to communicate with the RVA or SVA subsystem.

It is recommended that the MVS device used as an ECAM have no other users.

If agent performance seems poor, you can make a new device into the ECAM by adding an ECAM and dropping the old one.

- Exploring ECAM devices
- Available command in the ECAM devices display
- Executing ECAM device commands

Related topics

- Updating MVS agent configurations
- Starting and stopping agents
- Storage Agent for RVA/SVA overview
- ControlCenter agents overview

Storage Agent for Symmetrix administration

The following topic contains information necessary during the installation and configuration procedure for the Storage Agent for Symmetrix. It provides detailed information about what you must do before and after the installation. Under *Preparing the host,* ensure that the host to which you are installing the agent meets the specified requirements listed. Once your host is ready for the agent installation, you can install the agent. After installing the agent, look under Configuring the agent, to see if there are additional configurations you must perform.

Preparing the host

Installing the Storage Agent for Symmetrix

Configuring the agent

Starting and stopping the Storage Agent for Symmetrix

Preparing the host

Before installing the agent, ensure that you have installed:

- One of:
  - Windows NT or Windows 2000 Advanced Server
  - Solaris 2.6 - 2.8
- 4.3.2 GA release of Solutions Enabler
- Symmetrix Version 4.8, 5.0, or 5.5
- Minimum microcode level 5x65, 5x66, 5267.22.x, or 5567.29.x
- To run Optimizer, the service processor must be upgraded to run Symmetrix Optimizer 4.3.1. Contact your EMC Customer Support Engineer.

Configuring the Storage Agent for Symmetrix

Navigate down through the tree panel in the console to the Symmetrix agent, and then right-click and select **Update Configuration**.

The Edit Agent Configuration dialog box appears.

If you wish to change the current configuration, see Updating the agent configuration.

Starting and stopping the Storage Agent for Symmetrix

You can start and stop the agent from the right click menu commands available from the Symmetrix node in the ECC Agents folder.

Related topics

- Storage Agent for Symmetrix overview
- Storage Agent for Symmetrix data collection policies
- WLA Archiver overview
- Viewing real-time performance statistics

Configuring Symmetrix alerts

- Symmetrix alarm alerts
- Symmetrix device alerts
- Symmetrix director alerts
- Symmetrix disk alerts
- Symmetrix general alerts
- Symmetrix port alerts

Responding to Symmetrix alerts

- Responding to Symmetrix alarm alerts
- Responding to Symmetrix device alerts
- Responding to Symmetrix director alerts
- Responding to Symmetrix disk alerts
- Responding to Symmetrix port alerts
- Responding to Symmetrix general alerts

Tape Agent for MVS administration

The following contains supporting information necessary to install and configure the Tape Agent for MVS. It provides detailed information about what you must do before and after the installation. Ensure that the host to which you are installing the agent meets the specified requirements listed.

- Preparing the host
- Configuring the Tape Agent for MVS

Preparing the host

The Tape Agent for MVS has the following requirements.

Hardware

The agent supports the IBM Virtual Tape Server, IBM 3494/3495, and the StorageTek library.

Software

- For StorageTek Tape Library functionality, the host must be running HSC 2.0.1 or higher.
- For VTS and 3494/3495 functionality, the library must be SMS-managed. Any level of DFSMS that supports the hardware is acceptable.
- The agent's CA-1functionality requires CA-1 5.1.
- The agent's DFSMSrmm functionality requires DFSMS 1.5 or higher.

Return to Installing and configuring agents to install the agent.

Configuring the Tape Agent for MVS

There are no additional configuration steps necessary to run this agent.

Updating agent configuration

- To change the Server or Store to which the agent is connected, see Updating agent configurations.
- To change the load library data set name of the StorageTek Host Software Component (HSC), see Updating MVS agent configuration.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- ControlCenter agents overview
- Checking the status of the Tape Agent for MVS

WLA Archiver administering

The following contains supporting information necessary to install and configure the WLA Archiver. It provides detailed information about what you must do before and after the installation. Under Preparing the host, ensure that the host to which you are installing the WLA Archiver meets the specified requirements listed. Once your host is ready you can install the WLA Archiver.

- Preparing the host
- Configuring the agent

Preparing the host for installation of WLA Archiver

WLA Archiver can only be installed on a host running Windows 2000 or Windows NT.

Before installing the WLA Archiver ensure that you have:

- Installed and started the Master Agent
- Installed and started the NobleNet Portmapper (installed with the Master Agent)

Note: Both the Master Agent and NobleNet Portmapper are installed from the host on which you are installing the WLA Archiver, therefore, you should install and start both products at the same time.

Configuring WLA Archiver

There are no required post-installation, configuration steps.

Related topics

- Installing and configuring agents
- Starting and stopping agents
- WLA Archiver: data collection policy
- Updating agent configurations
- ControlCenter agents overview

Schedules

Introduction to alert and data collection policy schedules

Alert or data collection policy schedules define when ControlCenter should evaluate alerts and collect statistics through a data collection policy. In a schedule, you can define the interval at which an event occurs (every 10 seconds, minutes, hours, and so on), the days of the week, and the days of the year. ControlCenter provides several pre-defined schedules, and you can define additional ones. ControlCenter provides a different type of schedule for reports.

Related topics

- Creating a schedule for an alert or data collection policy
- Copying an alert or data collection policy schedule
- Deleting an alert or data collection policy schedule
- Editing an alert or data collection policy schedule
- Assigning a schedule to multiple alerts
- Alert concepts and procedures
- Data collection policies overview

Copying an alert or data collection policy schedule

You can create schedules by copying existing ones. You use schedules to specify when ControlCenter should evaluate alerts and run data collection policies to collect statistics. You can use one schedule with multiple alerts or data collection policies.

Reports use a different type of schedule. For more information on report schedules, see Edit/Create a Schedule.

To copy a schedule:

1. In the selection tree, expand **Administration** and **Schedules**.
2. Right-click the schedule you want to copy and select **Copy Schedule**. The Copy Schedule dialog box appears.
3. In the **Name** box, type a descriptive name. Choose a name that gives some indication of the frequency of the schedule.
4. Specify the schedule parameters:
   - Select a numeric value and unit of time for the interval, such as **10** and **Min** for every 10 minutes.
   - Select the days of the week the schedule should cause events to occur.
   - Specify the times of the day and days of the year the schedule should apply.

Tip

- Schedules generally display alphabetically in the Console. Use a naming scheme, such as consistent prefixes, that logically groups the schedules when they display alphabetically. This allows you to find a specific schedule more quickly.

Related topics

- Editing an alert or data collection policy schedule
- Assigning a schedule to multiple alerts
- Deleting an alert or data collection policy schedule
- Introduction to alert and data collection policy schedules
- Alert concepts and procedures
- Data collection policies overview

Creating a schedule for an alert or data collection policy

Use schedules to specify when ControlCenter should evaluate alerts and run data collection policies to collect statistics. You can use one schedule with multiple alerts or data collection policies.

Reports use a different type of schedule. For more information on report schedules, see Edit/Create a Schedule.

To create a schedule for an alert or data collection policy:

1. In the selection tree, expand **Administration.**
2. Right-click **Schedules** and select **New Schedule**. The New Schedule dialog box appears.
3. In the **Name** box, type a descriptive name. The name cannot contain spaces. Choose a name that gives some indication of the schedule's frequency.
4. Specify the schedule parameters:
   - Select a numeric value and unit of time for the interval, such as **10** and **Min** for every 10 minutes.
   - Select the days of the week the schedule should cause events to occur.
   - Specify the times of the day and days of the year the schedule should apply.

Tip

- Schedules generally display alphabetically in the Console. Use a naming scheme, such as consistent prefixes, that logically groups the schedules when they display alphabetically. This allows you to find a specific schedule more quickly.

Related topics

- Copying an alert or data collection policy schedule
- Editing an alert or data collection policy schedule
- Assigning a schedule to multiple alerts
- Deleting an alert or data collection policy schedule
- Introduction to alert and data collection policy schedules
- Alert concepts and procedures
- Data collection policies overview

Deleting an alert or data collection policy schedule

Deleting a schedule completely removes it from ControlCenter. The schedule is no longer available to any ControlCenter users.

Reports use a different type of schedule. For more information on report schedules, see Edit/Create a Schedule.

To delete a schedule:

1. In the selection tree, expand **Administration** and **Schedules**.
2. Right-click the schedule and select **Delete Schedule**. If the schedule is attached to alerts or collection policies, the Delete Schedule dialog box appears, listing the alerts and collection policies to which the schedule is attached.
3. To change the schedule for an alert or collection policy, right-click it and select **Edit**.
4. Select a new schedule from the **Schedule** box on the **Actions** tab of the Edit Alert dialog box, then click **OK**.
5. After changing the schedules for the listed alerts and collection policies, click **OK**.

Note

- If you delete a schedule that is still attached to an alert or collection policy, the alert or collection policy no longer has a schedule. You must assign a new schedule for ControlCenter to evaluate the alert or perform the data collection.

Related topics

- Creating a schedule for an alert or data collection policy
- Editing an alert or data collection policy schedule
- Copying an alert or data collection policy schedule
- Introduction to alert and data collection policy schedules
- Alert concepts and procedures
- Data collection policies overview

Editing an alert or data collection policy schedule

Edit a schedule to change the frequency with which events that use the schedule occur, such as the evaluation of an alert or the collection of a set of statistics.

Reports use a different type of schedule. For more information on report schedules, see Edit/Create a Schedule.

To edit a schedule:

1. In the selection tree, expand **Administration** and **Schedules**.
2. Right-click the schedule you want to edit and click **Edit Schedule**. The Edit Schedule dialog box appears.
3. Change the schedule parameters as desired:
   - Select a numeric value and unit of time for the interval, such as **10** and **Min** for every 10 minutes.
   - Select the days of the week the schedule should cause events to occur.
   - Specify the times of the day and days of the year the schedule should apply.

Notes

- You cannot edit the schedule name.
- A schedule might be used by several alerts and data collection policies. If you change a schedule, make sure your changes are appropriate for all the elements to which it is attached.

Related topics

- Creating a schedule for an alert or data collection policy
- Copying an alert or data collection policy schedule
- Assigning a schedule to multiple alerts
- Introduction to alert and data collection policy schedules
- Alert concepts and procedures
- Data collection policies overview

Assigning a schedule to multiple alerts

You can assign schedules to groups of alerts. For example, you might want to change how frequently ControlCenter evaluates a group of alerts.

To assign a schedule to multiple alerts:

1. In the selection tree, expand **Administration** and **Alert Management**.
2. Right-click **Alert Templates** or **Alerts**, or any folder beneath those folders, and click **Assign Schedule**. The Assign Schedule dialog box appears.
3. Select a schedule from the list and click **OK**. ControlCenter applies the schedule to all the alerts in the selected folder and all sub-folders.

Notes

- To assign a schedule to an individual alert or alert template, right-click the alert or template and click **Edit Alert**. Select the schedule on the Actions tab.
- You cannot assign a schedule to multiple data collection policies or reports at one time.
- Be careful when changing the schedules attached to multiple alerts. You cannot undo the assignment to multiple alerts. You must reassign the schedules in groups or individually.

Related topics

- Creating a schedule for an alert or data collection policy
- Understanding spike controlling and evaluation frequency
- Introduction to alerts
- Alerts concepts and procedures

ControlCenter security management overview

The security management system controls the authorization for performing ControlCenter actions. The system manages permissions based on authorization rules, which grant specific users, or groups of user, permission to perform actions on specific objects, or groups of objects.

For example, the TimeFinder rule could grant the backup manager (user) permission to use the TimeFinder application (action) on a named Symmetrix (object).

A ControlCenter administrator, a member of the ECCAdministrators group, creates each authorization rule and manages the users and the objects named in each rule. The following restrictions apply to authorization rules:

- There can be only one rule for each user or user group.
- A user or user group named in one rule cannot be named in any other rule until an administrator removes it from the first one. However, a user can belong to more than one user group.
- If a user is named in one rule and is also part of a user group, the rules for that user group also apply to the user along with its initial rule.

If users attempt to perform a command for which they are not authorized, ControlCenter issues a message and prevents the command from executing.

Default user groups, object groups, and rules

When the ECC Server starts for the first time, the program creates:

- A default rule called ECCAdministrators Rule
- A default user group called ECCAdministrators
- An initial user that the installer of the ECC Server defines

The initial user is included in the ECCAdministrators group, and the ECCAdministrators Rule grants all permissions on all objects to the ECCAdministrators group. This allows the initial user to create users and groups and grant permissions on ControlCenter objects. You cannot delete the ECCAdministrators group or remove all its permissions.

ControlCenter creates several additional user groups, object groups, and rules to facilitate security management setup. See Initial ControlCenter user groups and rules for more information.

Getting started

After installing ControlCenter, the security administrator should:

- Create user groups based on similar responsibilities, such as UNIX administrators or Symmetrix performance administrators.
- Optionally create object groups, such as a UNIX Systems Group that includes all your UNIX systems, or a Finance Group that includes all the hosts and subsystems used by your Finance department.
- Create authorization rules for each user group, granting permissions to ControlCenter actions based on responsibility. For example, grant the UNIX Administrators user group full permissions for the UNIX Systems object group.
- Create users and include them in the appropriate user groups. By including a user in a group, the user inherits the permissions of the group.

Related topics

- Creating an authorization rule
- Creating a ControlCenter user group
- Creating a ControlCenter user
- Creating ControlCenter object groups
- ControlCenter permissions
- Managing a ControlCenter user's permissions
- Managing ControlCenter authorization rules
- Monitoring ControlCenter status and security
- Understanding inheritance of ControlCenter permissions

Security management concepts

Initial ControlCenter user groups and rules

To facilitate setting up ControlCenter security, the product provides some initial user groups and rules.

Initial user groups and rules

ControlCenter creates several default user groups and rules when you first start the ECC Server. After you create your users, add them to these user groups to grant them sets of permissions.

The user groups and rules are organized according to typical job responsibilities. The rules grant permissions based on object types, such as Symmetrix devices or hosts. For example, users included in the Symmetrix Configuration Manager group gain a set of permissions for all Symmetrix systems in ControlCenter.

Following are the default user groups and rules.

User group and rule name	Group members permissions
ECCAdministrators	All objects. You cannot delete the group or rule or remove all its permissions. It is provided to ensure you can create users and groups and assign permissions.
ESN Manager	Networking actions, such as actions for managing fabrics, switches, zones, and zone sets.
Symmetrix Configuration Manager	Configuring Symmetrix subsystems, such as defining device types and configuring logical devices and ports.
Symmetrix Data Protection Manager	Managing Symmetrix backup and recovery functions, such as using the SRDF and TimeFinder applications.
Symmetrix Performance Manager	Using Symmetrix tuning functions, such as Optimizer, QoS-LRU, Mirror QoS, and TimeFinder SRDF/QoS.

To see which permissions a rule grants for which object types, click **Properties** in the toolbar and double-click the rule in the tree panel. For definitions of the permissions, see ControlCenter permissions.

You can also modify the default rules to meet your requirements.

Related topics

- Managing ControlCenter object groups
- Managing a ControlCenter user's permissions
- Managing ControlCenter authorization rules
- Using ControlCenter groups effectively
- Understanding inheritance of ControlCenter permissions
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Understanding inheritance of ControlCenter permissions

Users inherit permissions from the groups in which they are included. User groups inherit permissions from the other groups in which they are included.

If you include an object group in an authorization rule and then nest another object group within the first object group, the authorization rule now also grants permissions on the second object group.

The inheritance rules for the ChangeMembership permission differ from those of other rules.

Related topics

- Viewing a ControlCenter user's permissions
- ControlCenter permissions
- ControlCenter security management overview

Understanding the ChangeMembership permission

ControlCenter allows you to create object groups to logically group hosts, Symmetrix systems, and other objects that ControlCenter manages. You can assign permissions based on your object groups. For example, you might assign a UNIX administrator full permissions for the UNIX Hosts object group. The ChangeMembership permission enables you to maintain strict control over which members are included in the UNIX Hosts group by restricting who can add members to or delete members from an object group. Without the ChangeMembership permission, the UNIX administrator could gain permissions on a Windows NT or OS/390 host by dragging that host into the UNIX Hosts group. You can, however, allow users to affect the membership of a group by granting the user the ChangeMembership permission for that group.

The group home property

Each group has a home, which is the location in which the group was created or to which it has been moved. When users create groups, they must have the ChangeMembership permission on the group's home. In turn, once the users create those groups, the users have ChangeMembership permission on those groups, which the user inherits through the group's home.

Inheritance of the ChangeMembership permission

All other ControlCenter permissions follow a strict inheritance. For example:

- When you include a user in a user group, the user inherits the permissions of the user group.
- When you include an object in an object group, users with permissions on the object group gain permission for the object.

The ChangeMembership permission does not confer in the same way. The ChangeMembership permission always remains with the group's home. For example:

- Assume there are two object groups: GroupA and GroupB.
- You have the ChangeMembership permission for GroupA but not GroupB.
- You link GroupB into GroupA by pressing the Control and Shift keys and dragging GroupB on top of GroupA.
- Users who have permissions for the objects in GroupA now also have the same permissions for the objects in GroupB.
- You do not gain the ChangeMembership permission for GroupB. In other words, you cannot add objects to GroupB.

Implications of the ChangeMembership permission

The inheritance behavior of the ChangeMembership permission has the following implications.

Action	Implications
Deleting a group	You must have ChangeMembership permissions for a group's home to delete a group.
Renaming a group	You must have ChangeMembership permissions for a group's home to rename a group.
Creating a group	If you have ChangeMembership for GroupA, you can create a GroupB within GroupA, and you inherit the ChangeMembership permission for GroupB because you have ChangeMembership for GroupA. GroupB's home is GroupA.
Adding existing groups to a group	If you have ChangeMembership for GroupA, you can copy or link existing GroupB to GroupA. GroupB's home does not become GroupA. When you link GroupB to GroupA, users in GroupB receive GroupA's permissions. Any modifications to GroupA also affect GroupB, because the groups are linked together. When you copy GroupB to GroupA you are actually making a new, different group, called GroupB, which contains the same objects and settings as the original GroupB. You have ChangeMembership permissions on the copy, which means that you can modify the copy of GroupB, but your modifications to not affect the original GroupB. You must have ChangeMembership for GroupA and GroupB's home to *move* GroupB to GroupA. GroupA becomes GroupB's new home.
Removing members from a group	Removing a member from a group does not mean deleting a group entirely; these are two separate actions. If you have ChangeMembership for GroupA, you can remove members (objects or other object groups) from GroupA.
Deleting members from a group	Deleting a member means completing removing it from ControlCenter. You must have ChangeMembership on a group's home to delete a group. To delete GroupB, which is linked to or copied in GroupA, you must have ChangeMembership for GroupA and GroupB.

Related topics

- Managing ControlCenter object groups
- Initial ControlCenter groups and rules
- Managing a ControlCenter user's permissions
- Viewing a ControlCenter user's permissions
- ControlCenter security management overview

Viewing security management information

There are two ways to view security management information:

- View the basic properties of users, groups, and authorization rules, such as names and descriptions for users and groups and the permissions granted by a rule.
- View which rules apply to which users, groups, and objects.

To view basic properties:

1. Click **Properties** on the toolbar.
2. In the tree panel, double-click the **Security Management** folder to see the basic properties of users, groups, and rules. Or, double-click any of the individual folders, users, groups, or rules to view a subset of the Security Management folder.

To view which rules apply to which users, groups, and objects:

1. Click **ECC Administration** in the main window and select **Authorization**.
2. In the tree panel, double-click the **Security Management** folder to see the rules for users and groups. Or, double-click any of the individual folders, users, or groups to view a subset of the Security Management folder. To view the rules that apply to an object or object group, double-click the object in the tree panel.

For more specific procedures, see:

- Viewing a ControlCenter user's permissions
- Viewing authorization rules for hosts and subsystems
- Viewing the groups a ControlCenter user belongs to

Tip

- Clear or split the target panel to view the authorization rules in their own panel.

Related topics

- Managing a ControlCenter user's permissions
- Managing ControlCenter authorization rules
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Working with users

Creating a ControlCenter user

Before creating a ControlCenter user, the user must already exist as a user of the machine on which the ECC Server is running. The user will use the same user ID and password to log in to ControlCenter.

After you create the user account on the ECC Server host, do the following to create the ControlCenter user:

1. In the tree panel, expand **Administration** and **Security Management**.
2. Right-click **ECC Users** and select **New User**. The Create a User dialog box appears.
3. Type the server user ID of the new user in Login ID.
4. Type a meaningful description of the user in Description.
5. Click **OK** to save the new user and close the dialog box. The new user now appears in the list of ECC Users.

Notes

- You can use ControlCenter to create user accounts on UNIX hosts. ..
- You cannot create user accounts for Windows hosts using ControlCenter. Consult the Windows documentation for instructions on how to create user accounts.

Tips

- To define the user permissions, right-click the user and select **Authorization**, **New Rule**. ..
- Create user groups to manage user permissions more easily. When you include a user in a user group, the user inherits all the permissions of the group.

Related topics

- Editing a ControlCenter user
- Deleting a ControlCenter user
- Creating a ControlCenter user group
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Editing a ControlCenter user

There are occasions when you will need to edit a ControlCenter user; for example, when the login ID for a user changes or when you need to update a user's description.

To edit a user:

1. In the tree panel, expand **Administration, Security Management**, and **ECC Users**.
2. Right-click the user whose information you want to change, and select **Edit User**. The Edit User dialog box appears.
3. Make your changes to the login ID and description.
4. Click **OK** to save the changes and close the dialog box. If you edited the Login ID field, the updated user ID now appears in the ECC Users list.

Related topics

- Creating a ControlCenter user
- Deleting a ControlCenter user
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Deleting a ControlCenter user

To remove a user's access to ControlCenter, delete the user. If you only want to change a user's permissions, or temporarily disable the user's access to ControlCenter, you can remove the user from any groups to which it belongs and remove any authorization rules applied to the user.

To delete a ControlCenter user:

1. In the tree panel, expand **Administration, Security Management**, and **ECC Users**.
2. Right-click the user you want to delete, and select **Delete User**. A message appears, prompting you to confirm removing the user.
3. Click **Yes**. The dialog box closes and the user is removed from the list of ECC Users.

Related topics

- Creating a ControlCenter user
- Deleting a ControlCenter object group
- Editing a ControlCenter user
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Managing a ControlCenter user's permissions

A ControlCenter user's permissions are controlled by:

- An authorization rule applied directly to the user
- Permissions the user inherits from the user groups to which it belongs

You can apply an authorization rule to a user, even if the user belongs to one or more groups. Such a user would inherit permissions from the groups to which it belongs and the individual authorization rule applied to it.

Applying permissions

To apply a set of permissions to a user, choose from the following:

- Create an authorization rule for the userallows the greatest customization of the user's permissions but also requires the most maintenance.
- Assign the user to one or more groupsmakes managing user permissions easier; you can change the permissions for multiple users by changing the authorization rules of the groups to which they belong. Note that you can still apply rules to individual users, even if they belong to groups.

Changing permissions

To change a user's permissions, choose from the following:

- First view the user's permissions to see whether they come from an authorization rule, are inherited from user group memberships, or both.
- If the user has an authorization rule, edit the authorization rule.
- If the user belongs to one or more groups, remove the user from the groups or edit the authorization rules for those groups. If you edit the rules for a group, ensure that your changes are appropriate for all members of the group. See: Removing a user from a group, Managing ControlCenter authorization rules (editing)

Removing permissions

To remove a user's permissions, choose from the following:

- To completely remove the user from ControlCenter, delete the user.
- To temporarily disable a user from using ControlCenter or to delete a user's permissions in order to reapply them, first view the user's permissions.
  - Then remove the user from any groups to which it belongs.
  - And remove the user from any authorization rule to which it is assigned.

Related topics

- ControlCenter security management overview
- Monitoring ControlCenter status and security

Removing an authorization rule from a ControlCenter user

Remove an authorization rule from a user to temporarily or permanently remove or change the user's permissions. Note that some users may only inherit permissions from the groups to which they belong and may not have individual authorization rules.

To remove an authorization rule from a user:

1. If necessary, view the user properties to determine the authorization rule name.
2. In the tree panel, expand **Administration, Security Management**, and **Authorization Rules**.
3. Right-click the user's authorization rule and select **Edit Rule**. The Edit Rule *rule_name* dialog box displays.
4. Select the user in the Selected users/groups panel of the dialog box.
5. Click the back arrow button (<) next to the Selected users/groups panel.
6. Click **OK** to close the dialog box and save your changes.

Related topics

- Deleting an authorization rule
- Renaming an authorization rule
- Managing a ControlCenter user's permissions
- Managing ControlCenter authorization rules
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Removing a ControlCenter user from a group

Remove a ControlCenter user from a user group to change or remove the user's permissions.

To remove a ControlCenter user from a user group:

1. If necessary, view the user properties to determine the names of the groups to which the user belongs.
2. In the tree panel, expand **Administration, Security Management**, and **ECC User Groups**.
3. Expand the folder for the group the user belongs to. If the group is a subgroup, first expand any parent groups.
4. In the user group folder, right-click the user and select **Remove From Group** *group_name*.

Related topics

- Managing a ControlCenter user's permissions
- Managing ControlCenter authorization rules
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Viewing a ControlCenter user's permissions

It is occasionally helpful to review all the permissions granted to a user. This is especially important when a user's role or duties change and the administrator must adjust the permissions accordingly.

To view a user's permissions:

1. On the toolbar, click **Properties**.
2. In the tree panel, double-click the folder for the user. The permissions assigned to the user display in the target panel. Note that the user receives permissions from any authentication rule applied to it and inherits permissions from any groups to which it belongs.

Note

- If necessary, clear the target panel by right-clicking anywhere in the tree panel and selecting **Clear Target** before performing this procedure.

Related topics

- Creating a ControlCenter user
- Editing a ControlCenter user
- Deleting a ControlCenter user
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Viewing the groups a ControlCenter user belongs to

ControlCenter users can belong to one or more user groups. To modify user permissions or change the groups a user belongs to, first identify the groups to which a user belongs.

To view the groups a user belongs to:

1. On the toolbar, click **Properties**.
2. In the tree panel, double-click the folder for the user. Detailed user properties appear in the target panel, including a list of the groups to which the user belongs.

Note

- If necessary, clear the target panel by right-clicking anywhere in the tree panel and selecting **Clear Target** before performing this procedure.

Tip

- When you select a user in the tree panel, the folders for the user in the groups to which it belongs also highlight, with a light gray background.

Related topics

- Viewing a ControlCenter user's permissions
- Managing a ControlCenter user's permissions
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Working with users and user groups

Creating a ControlCenter user group

To help manage ControlCenter users, create logical user groups and then apply authorization rules at the group level. Users in a group inherit the permissions of the group.

To create a ControlCenter group:

1. In the tree panel, expand **Administration** and **Security Management**.
2. Right-click **ECC User Groups** and select **New User Group**. The Create a Group dialog box appears.
3. Type a descriptive name for the group in Group Name.
4. Type a meaningful description of the group in Description.
5. Click **OK** to save the new group and close the dialog box. The new group now appears in the list of ECC User Groups.

Note

- The users in a subgroup inherit the permissions of the parent group.

Tip

- To nest a group within another group, drag the group you want to nest on top of the desired parent group. You can create an unlimited number of subgroups.

Related topics

- Creating a ControlCenter user
- Creating an authorization rule
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Editing a ControlCenter user group

There are occasions when you will need to edit a user group; for example, you may need to rename a user group or update its description.

To edit a user group:

1. In the tree panel, expand **Administration, Security Management**, and **ECC User Groups**.
2. Right-click the user group whose information you want to change and select **Edit User**. The Edit Group dialog box displays.
3. Make your changes to the group name and description.
4. Click **OK** to save the changes and close the dialog box. If you edited the Group Name field, the new name now appears in the ECC User Groups list.

Related topics

- Creating a ControlCenter user group
- Deleting a ControlCenter user group
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Deleting a ControlCenter user group

To delete a ControlCenter user group:

1. In the tree panel, expand **Administration, Security Management**, and **ECC User Groups**.
2. Right-click the user you want to delete and select **Delete User Group**. A message displays, confirming that you want to remove the user group.
3. Click **Yes**. The user group is removed from the list of ECC User Groups.

Related topics

- Creating a ControlCenter user group
- Editing a ControlCenter user group
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Using ControlCenter groups effectively

ControlCenter allows you to create user and object groups to simplify the management of ControlCenter users, permissions, and objects. You can grant ControlCenter permissions to a user by including the user in a group. The user inherits the permissions of a group in which it is included. You can also include users in multiple groups, thereby granting the permissions of those groups. Similarly, you can create a rule that grants permissions on a group of objects. Whey you assign the rule to a user group, members of the user group gain permissions on the objects in the group.

Nesting groups

You can nest user and object groups within other groups of the same kind. Theoretically, the levels of nesting are unlimited. A group that is included within another group inherits the permissions of the parent group.

To include user groups within other groups, drag the user groups on top of each other. Do the same to nest object groups.

Note: You must have the proper object group permissions to move it. The ChangeMembership permission controls group permissions. See Understanding the ChangeMembership permission for more information.

Initial groups and rules

To facilitate setting up ControlCenter security, the ECC Server creates several groups and rules when it first starts. These groups are based on typical job responsibilities. You can drag users to the groups to grant them sets of permissions. For example, grant a network administrator permissions on fabrics and switches by dragging the user into the ESN Manager group.

For more information on these initial groups, see Initial ControlCenter groups and rules.

Related topics

- Creating a ControlCenter user group
- Understanding inheritance of ControlCenter permissions
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Working with ControlCenter object groups

Creating ControlCenter object groups

Object groups allow you to group similar ControlCenter objects, such as hosts and Symmetrix systems. For example, you can create a group for all your UNIX hosts or a Finance Group that includes all of the hosts and devices used by your Finance department. Object groups make setting up ControlCenter permissions easier.

To create a ControlCenter object group:

1. Right-click any open space in the tree panel of the Console (in other words, do not click any part of the tree) and select **New**, **Group**. A new folder appears in the tree panel. The folder name is New Group.
2. Type a new name for the object group and press Enter.

Tip

- To add an object to the new group, drag the object on top of the group in the tree panel. The group appears below the new group in the tree.

Related topics

- Creating a ControlCenter user
- Deleting a ControlCenter object group
- Creating a ControlCenter user group
- Creating an authorization rule
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Managing ControlCenter object groups

Object groups allow you to logically group hosts, Symmetrix systems, and other objects that ControlCenter manages. Creating object groups simplifies how you manage permissions for the objects. For example, you can create an object group that includes all your UNIX hosts and then grant your UNIX administrators permissions to perform actions on those hosts.

Nesting object groups

You can nest object groups. For example, you might create a Symmetrix group that grants Symmetrix administrators a set of basic permissions. You could then nest more specific object groups within the Symmetrix group to grant more specific permissions to administrators of certain subsystems or devices.

ChangeMembership permission

The ChangeMembership permission restricts users from altering the hosts and subsystems that are included in an object group. For more detailed information, see Understanding the ChangeMembership permission.

The group home property

Each group has a home, which is the folder in which the group was created or to which it has been moved. The user who creates a group has the ChangeMembership permission for the group's home. You must have to ChangeMembership permission for a group's home to rename or delete a group or delete objects from a group.

Moving, copying, and linking object groups

To organize your object groups, you can move, copy, or link object groups. However, you must have the proper permissions to do so. The following table explains the procedures for moving, copying, and linking and the type of permissions you need.

Operation	Procedure (from the tree panel)	Permissions required
Move	Drag the group on to another group. This changes a group's home.	ChangeMembership permission for both the old and new home.
Copy	Select the group, press the control key, and drag the group on to another group. The new group has the same members as the original, but there is no other connection between the groups.	ChangeMembership permission for the destination group.
Link	Select the group, press the control and shift keys, and drag the group to another group. This creates a link for the group in the new folder. Any additions to or deletions from the original group are reflected in the linked group.	ChangeMembership permission for the destination group.

Related topics

- Creating an authorization rule
- Creating a ControlCenter user group
- Creating a ControlCenter user
- Creating ControlCenter object groups
- ControlCenter permissions
- Managing a ControlCenter user's permissions
- Managing ControlCenter authorization rules
- Monitoring ControlCenter status and security
- Understanding inheritance of ControlCenter permissions

Working with authorization rules and permissions

ControlCenter permissions

See the following sections for descriptions of the ControlCenter permissions:

- Agent INI permissionsfor editing agent initialization (`.ini`) files, which contain agent configuration information.
- Symmetrix permissionsfor Symmetrix devices and ports.
- Storage network (ESN) permissionsfor managing fabrics, switches, zone sets, and zones.
- Object Group permissionsfor managing user-defined ControlCenter object groups.
- SST Server Commands permissionfor managing commands executed by ControlCenter's host agents.
- Host permissionsfor creating and modifying device groups.
- Authorization Data permissionsfor managing access to ControlCenter's authorization rules.
- User Account Manager Data permissionsfor creating and modifying users and user groups.

Related topics

- Viewing a ControlCenter user's permissions
- Understanding the ChangeMembership permission
- Understanding inheritance of ControlCenter permissions
- ControlCenter security management overview

Creating an authorization rule

An authorization rule contains three elements:

- a user or user group
- an object or group of objects
- an action

You combine these elements in a variety of ways to create authorization rules. You can expand Administration and Security Management to access current rules, users, and user groups. You can then right-click either authorization rules or an individual user to create a new rule.

You can do the following to create authorization rules:

- Creating a rule by right-clicking authorization rules
- Creating a rule by right-clicking an ECC user group
- Creating a rule by right-clicking a user

Creating a rule by right-clicking authorization rules

To create an authorization rule:

1. In the tree panel, expand **Administration** and **Security Management**.
2. Right-click **Authorization Rules** and select **New Rule**. The Create Rule dialog box appears.
3. Enter a name for the new rule in **Rule Group Name**. This is a required field.
4. Select a user or user group from the list in the Choose users/groups and Create new users/groups pane on the left. Note that users and user groups for which rules currently exist are disabled. You must select a user or a group that does not have an existing rule. To make this rule apply to all users, select **ECC Users**. You may right-click **ECC User Groups** or **ECC Users** to create a new user group or a new user without returning to the Console.
5. Click **>**. The selection displays in the Selected users/groups panel on the right.
6. Under **Choose Objects** select either **Groups/Instances** or **Types**.
   - **Groups/Instances**The rule you are creating applies only to the groups or instances of the objects selected in the Object groups/instances panel.
   - **Types**The rule you are creating applies to all objects of the type selected.

   The permissions that pertain to your choice display in the Available actions panel.
7. Click one or more Available actions, then click **>** to display the actions in the Selected actions panel.
8. Click **OK** to save the new rule and exit the dialog box.

Creating a rule by right-clicking an ECC user group

To create a new authorization rule:

1. In the tree panel, expand **Administration** and **Security Management**.
2. Right-click any user group and select **Authorization**, **New Rule**. The Create Rule for User Group dialog box displays.
3. Enter a name for the new rule in **Rule Group Name**. This is a required field.
4. Under **Choose Objects**, select either **Groups/Instances** or **Types**.
   - **Groups/Instances**The rule you are creating applies only to the groups or instances of the objects selected in the Object groups/instances panel.
   - **Types**The rule you are creating applies to all objects of the type selected.

   The permissions that pertain to your choice display in the Available actions panel.
5. Click one or more Available actions and click **>** to display the actions in the Selected actions panel.
6. Click **OK** to save the new rule and exit the dialog box.

Creating a rule by right-clicking a user

To create an authorization rule:

1. In the tree panel, expand **Administration** and **Security Management**.
2. Right-click a user and select **Authorization**, **New Rule**. The Create Rule for User dialog box displays.
3. Enter a name for the new rule in **Rule Group Name**. This is a required field.
4. Under **Choose Objects**, select either **Groups/Instances** or **Types**.
   - **Groups/Instances**The rule you are creating applies only to the groups or instances of the objects selected in the Object groups/instances panel.
   - **Types**The rule you are creating applies to all objects of the type selected.

   The permissions that pertain to your choice display in the Available actions panel.
5. Click one or more Available actions, then click **>** to display the actions in the Selected actions panel.
6. Click **OK** to save the new rule and exit the dialog box.

Related topics

- Renaming an authorization rule
- Removing an authorization rule from a ControlCenter user
- Managing ControlCenter authorization rules
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Creating an authorization rule that applies to all users

You can create an authorization rule that applies to all ControlCenter users. By creating such a rule, you can more easily manage permissions that apply to the entire ControlCenter community.

To create a rule that applies to all ControlCenter users:

1. In the tree panel, expand **Administration** and **Security Management**.
2. Right-click **Authorization Rules** and select **New Rule**. The Create Rule dialog box displays.
3. Enter a name in **Rule Name**. Use a name that indicates this rule applies to all ControlCenter users.
4. In the Choose users/groups and create new users/groups list, select the **ECC Users** folder. If this folder is grayed out, then a rule has already been created for all users.
5. Click **>** next to the list. A user group called Any User appears in the Selected users/groups list.
6. Select the objects and object types and actions for which you want to grant all users permissions.

Related topics

- Creating an authorization rule
- Renaming an authorization rule
- Removing an authorization rule from a ControlCenter user
- Managing ControlCenter authorization rules
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Deleting an authorization rule

To delete an authorization rule:

1. Expand **Administration**, **Security Management**, **Authorization Rules**. A list of the current authorization rules appears.
2. Locate the rule you want to delete.
3. Right-click the rule and select **Delete Rule**. The Delete Rule message appears prompting you to confirm the rule deletion.
4. Click **Yes**. The rule disappears from the list.

Note

- When you delete an authorization rule, all users, user groups, objects, or object groups are no longer affected by that rule.

Related topics

- Removing an authorization rule from a ControlCenter user
- Renaming an authorization rule
- Managing a ControlCenter user's permissions
- Managing ControlCenter authorization rules
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Renaming an authorization rule

To rename any authorization rule:

1. Click once on the name of the authorization rule, next to the icon. The name changes to a field that can be edited.
2. Type the new name for the rule and press Enter. The new name appears in place of the previous name.

Related topics

- Creating an authorization rule
- Managing ControlCenter authorization rules
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Managing ControlCenter authorization rules

ControlCenter provides authorization rules to allow you to control user access to hosts, Symmetrix systems, and the ControlCenter security management system. You create authorization rules for users or user groups. Although you can only create one authorization rule per user or user group, the security management system provides endless flexibility by allowing you to include users in multiple groups and to nest groups within other groups. Users inherit the authorization rules of the groups to which they belong and, similarly, groups inherit the authorization rules of the groups in which they are nested.

To create an authorization rule, see Creating an authorization rule.

To copy an authorization rule, right-click the rule and select **Copy Rule**.

To edit an authorization rule, right-click the rule and select **Edit Rule**.

To delete an authorization rule, right-click the rule and select **Delete Rule**.

Related topics

- Creating a ControlCenter user
- Creating a ControlCenter user group
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Viewing authorization rules for hosts and subsystems

You can view which users have which permissions for each host, Symmetrix system, or other object managed by ControlCenter.

To view the permissions users have for the hosts, subsystems, and other objects managed by ControlCenter:

1. In the main Console window, click **ECC Administration** and select **Authorization** from the menu provided.
2. In the tree panel, select the objects (hosts or subsystems, etc.) for which you want to view authorization rules. Select the objects by double-clicking them or by placing a checkmark next to them in the tree panel. The rules for the selected objects display in the target panel. See Object Rules view for column heading descriptions.

Tip

- Clear or split the tree panel to view the authorization rules in their own panel.

Related topics

- Creating a ControlCenter user
- Renaming an authorization rule
- Managing a ControlCenter user's permissions
- Managing ControlCenter authorization rules
- Monitoring ControlCenter status and security
- ControlCenter security management overview

Alerts

ControlCenter provides numerous alerts to help monitor various aspects of your distributed storage environment, such as:

- Space availability of volumes or disks
- Size of files
- Performance of hosts and storage subsystems
- Status of backup operations
- Availability and status of ControlCenter components

Notification options

You have great flexibility in how ControlCenter notifies you about alerts. Notification options include:

- Displaying color-coded messages in the ControlCenter Console
- Sending e-mail messages
- Sending messages to a third-party framework like HP OpenView Network Node Manager or Tivoli NetView

See also Creating a management policy

Automated responses

To help streamline your storage management activities, ControlCenter provides automatic responses, called *autofixes*, that you can attach to alerts. For example, ControlCenter provides an alert that triggers when a Windows event log reaches a certain size. You can attach to this alert an autofix that automatically backs up and clears the event log.

ControlCenter allows you to create your own autofixes as well. To create your own autofix, specify the name of a shell or perl script or an executable that should run when an alert triggers.

See also Creating an autofix, Autofix syntax

Creating alerts

You can create alerts from the templates ControlCenter provides or by copying existing alerts. You control:

- Which resources are monitored
- The values that cause an alert to trigger
- How often ControlCenter evaluates the alert
- What happens when the alert triggers

The online Help provides detailed configuration descriptions for each alert.

See also Overview of creating alerts

Viewing alerts

ControlCenter provides several options for viewing alerts. You can view:

- A series of bar charts showing the total alerts for each host or storage subsystem
- All the defined alerts for a host or subsystem
- All triggered alerts in a color-coded, sortable table

If a Console object (such as a subsystem or host) has an active alert, an icon indicating the severity of the condition displays next to the object. In the tree panel, a small downward arrow on a folder indicates that an object within the folder has an active alert.

See also Overview of viewing alerts

Responding to alerts

In addition to the automated responses, you can respond to a triggered alert by right-clicking it and selecting from a list of commands. The online Help provides recommendations for how to respond to each alert.

See also Overview of responding to alerts

Related topics

- Understanding alert terminology
- Alert concepts and procedures

Alert concepts

Alert concepts and procedures

For information about managing alerts and associated elements like autofixes, schedules, and management policies, select from the following topics:

- Alert concepts
- Creating alerts
- Editing and deleting alerts
- Viewing alerts
- Responding to alerts
- Working with autofixes
- Working with schedules
- Working with management policies
- Troubleshooting

Alert concepts

- Introduction to alerts
- Understanding alert severity and escalation
- Understanding alert terminology
- Understanding alert types
- Understanding spike controlling and evaluation frequency
- Understanding trigger values and alert severity levels

Creating alerts

- Overview of creating alerts
- Creating an alert from a template
- Copying an alert
- Monitoring multiple hosts or subsystems with the same alert

Editing and deleting alerts

- Changing the severity of an alert
- Deleting an alert
- Editing an alert
- Editing an alert template
- Enabling or disabling an alert
- Enabling or disabling multiple alerts
- Setting how often an alert is evaluated

Viewing alerts

- Overview of viewing alerts
- Viewing triggered alerts
- Viewing all triggered alerts for a host or subsystem
- Viewing an overview of all triggered alerts
- Viewing all alert definitions
- Viewing alert templates
- Finding out about alerts that trigger outside your work hours

Responding to alerts

- Overview of responding to alerts
- Automatically notifying staff members by e-mail or page
- Automatically responding to alerts with commands and scripts
- Preventing exceptional conditions from triggering alerts (controlling spikes)
- Reducing the number of alerts that display
- Removing unneeded alerts from your Console
- Resetting an alert whose condition has been resolved

Working with autofixes

- Attaching an autofix to an alert
- Autofix syntax
- Creating an autofix
- Editing an autofix
- Deleting an autofix

Working with schedules

- Introduction to alert and data collection policy schedules
- Creating a schedule for an alert or data collection policy
- Copying an alert or data collection policy schedule
- Deleting an alert or data collection policy schedule
- Editing an alert or data collection policy schedule
- Assigning a schedule to multiple alerts

Working with management policies

- Creating a management policy
- Copying a management policy
- Editing a management policy
- Assigning a management policy to multiple alerts

Troubleshooting

- Troubleshooting alerts and autofixes

Understanding alert severity and escalation

ControlCenter provides five severity levels for each alert. You can assign different trigger values for each severity level. You do not see a new alert in the Active Alerts view each time the alert changes severity, rather the icon and color of the alert changes. Associated management policies and autofixes do run each time an alert moves from one severity to the next, whether it increases or decreases in severity.

Example

Consider the following alert:

- Monitors the percent of free space on a Windows volume
- Trigger values: Warning at less than 20% free, Critical at less than 10%, and Fatal at less than 5%
- Has an hourly schedule
- Management policy sends alert to user JSMITH's Console and sends e-mail to jsmith@bigcompany.com

The following events occur as the alert moves from one severity to another:

1. At 1:00 P.M., ControlCenter sees that the volume space is at 15% free. A Warning alert appears in JSMITH's Active Alerts view, and ControlCenter sends an e-mail.
2. At 2:00 P.M., ControlCenter sees that the volume space is at 8% free. In JSMITH's Active Alerts view, the Warning alert changes to a Critical alert, and ControlCenter sends an e-mail.
3. JSMITH deletes some temp files on the volume.
4. At 3:00 P.M., ControlCenter sees that the volume space is at 40% free. ControlCenter removes the alert from JSMITH's Active Alerts view and does not send an e-mail.

Related topics

- Changing the severity of an alert
- Creating an alert from a template
- Creating a management policy
- Understanding alert terminology
- Introduction to alerts
- Alert concepts and procedures

Understanding alert terminology

Refer to the following table for definitions of alert terminology.

Term	Definition
Active alert (also triggered alert)	An alert for which one or more trigger values have been met. Active alerts display in the Active Alerts view in the Console. Respond to an active alert by right-clicking it and selecting from a list of available commands. An active alert displays until you remove or reset it or the conditions that caused the alert to trigger are alleviated. See also: Overview of responding to alerts
AgentControlled	Some alerts have an AgentControlled schedule, which means that you cannot change how often ControlCenter evaluates the alert. Alerts with AgentControlled schedules usually monitor: • The state of a system or piece of software, such as the performance of a disk subsystem reaching a critical threshold • The result of an event, such as a critical backup not occurring ControlCenter continuously monitors for these types of events and immediately reports them so you can react quickly.
Alert definition	An alert for which keys, trigger values, and a schedule have been defined, and optionally autofixes and a management policy. You create alert definitions using the alert templates or by copying existing alerts. See also: Overview of creating alerts
Alert template	Provides default values for the creation of new alerts. ControlCenter provides templates for every alert. You can specify your own default settings by modifying the alert templates. See also: Editing alert templates, Creating an alert from a template
Alert type	Determines how ControlCenter evaluates an alert and what type of trigger value you should specify. There are four alert types: count, interval, rate, and state. See also: Understanding alert types
Autofix	An action that ControlCenter can perform automatically when an alert triggers, such as backing up or clearing a log file. ControlCenter provides System autofixes that you can use with specific alerts. You can also create your own autofixes to use with any alert. Create these User autofixes using existing scripts, batch files, and executables or by writing new ones. See also: Creating an autofix, Autofix syntax
Generic Agent Alert	Each ControlCenter component generates messages as it runs. The components write these messages to a log file. However, you can also receive these messages in the Console as alerts. Each component provides a Generic Agent Alert that allows you to determine: • Whether the messages generated by the component display as alerts • Which ControlCenter users receive the alerts See also: Generic Agent Alerts
Sources	The specific resources that an alert monitors, for example the name of a file, volume, or database table. Some alerts have multiple sourcesfor example, an alert that monitors tablespace use in a database may require you to specify both the database and tablespace names. Other alerts do not require any sources, such as an alert that looks for a specific message number or an alert that monitors a specific log file. You can often use wild cards when specifying alert sources. See an alert's online Help topic to determine whether wild cards are supported.
Management policy	Defines the users that ControlCenter should notify when an alert triggers and how those users should be notified. Notification options include: a message through the Console, an e-mail, and a message to a management framework like HP OpenView Network Node Manager. See also: Creating a management policy, Automatically notifying staff members by e-mail or page

Schedule	Defines at what times ControlCenter should evaluate an alert. In a schedule, you can define the interval at which the evaluation occurs (every 10 seconds, minutes, hours, and so on), the days of the week, and the days of the year. ControlCenter provides several pre-defined schedules, and you can define additional ones. See also: Creating a schedule for an alert or data collection policy, Understanding spike controlling and evaluation frequency
Server alerts	Alerts that help the ControlCenter administrator monitor ControlCenter status and security. You should attach a management policy to these alerts to ensure that only the ControlCenter administrator receives them. See also: Monitoring ControlCenter status and security
Severity	The relative importance of an alert to you. You can specify different trigger values for each severity level: Fatal, Critical, Warning, Minor, and Harmless. For example, you could enable three severity levels for an alert that evaluates file system free space: • Warning when the free space is less than 30 percent • Critical when the free space is less than 15 percent • Fatal when the free space is less than 5 percent See also: Understanding trigger values and alert severity levels
Spike	A situation in which a monitored resource temporarily exceeds a trigger value, and then quickly returns to an acceptable level (for example, a volume exceeding 90 percent occupancy when a user creates a large file, and then falling back below 70 when the user deletes the file). ControlCenter provides a way to prevent alerts from triggering when these temporary conditions occur. See also: Understanding spike controlling and evaluation frequency
SNMP notification	When an alert triggers, ControlCenter allows you to send notification to framework products like HP OpenView Network Node Manager or Computer Associates Unicenter TNG. You use a management policy to specify that you want this notification sent. SNMP notification also requires additional configuration steps. See also: Automatically notifying staff members by e-mail or page
Trigger value	The value at which an alert triggers (or becomes active). You can specify a different trigger value for each alert severity level. Trigger values can be numeric or true/false values, depending on the alert type. See also: Understanding trigger values and alert severity levels, Understanding alert types

Related topics

- Introduction to alerts
- Alert concepts and procedures

Understanding alert types

An alert's type determines how ControlCenter evaluates the alert and what type of trigger value you should specify. There are four alert types.

Alert type	Description	Specify this type of trigger value
Count	Monitors values that can be calculated, such as the percentage of free space in a file system or the size of a file. Specify numeric values for the triggers.	Numeric values
Interval	Monitors the number of times an event occurs within a specified time range. For example, if you specify 15 minutes as the schedule for the alert and 10 as the trigger value, then the condition must occur 10 times within 15 minutes for the alert to trigger.	Numeric values
Rate	Monitors the number of times a condition occurs every second. For example, if you specify 100 as the trigger value, the condition must occur 100 times per second for the alert to trigger.	Numeric values
State	Evaluates whether a condition is true or false, such as whether a subsystem or database is active or whether an important file was backed up.	TRUE or FALSE **Note:** For most state alerts, you should specify TRUE.

Related topics

- Introduction to alerts
- Overview of creating alerts
- Alert concepts and procedures
- Understanding alert terminology

Understanding spike controlling and evaluation frequency

Alert spikes occur when system conditions temporarily cause an alert to trigger, but then quickly return to an acceptable level. Or, conversely, system conditions momentarily return to an acceptable level before reaching dangerous levels again.

Consider the following scenario, for example:

1. You create a Fatal alert that triggers when the free space on a volume drops to five percent.
2. A user creates a large file that causes the free space to drop below five percent.
3. The user immediately deletes the file, and free space returns to 20 percent.

In this case, you would probably not want to know that free space temporarily dropped below your threshold. However, you would want to know if the free space remained below the threshold for an hour or a day, or whatever timeframe you consider critical.

You can control alert spikes using the **Before** and **After** fields on the **Conditions** tab of the alert definition dialog boxes.

- **Before** fieldSpecify how many times an alert must evaluate to true before the product triggers the alert.
- **After** fieldSpecify how many times, after an alert has triggered, that the alert must evaluate to false before ControlCenter removes the alert.

You define how often ControlCenter evaluates an alert through theschedule that is attached to the alert. You can define different before and after values for each severity level.

Returning to the earlier example, we can use the **Before** field to ensure an alert does not trigger when the volume free space temporarily drops to, or below, five percent.

Schedule:	Evaluates alert hourly			
Before field:	3			
Time:	**12:30**	**1:30**	**2:30**	**Alert triggers**
Free space percent:	20	5	20	No
	5	4	5	Yes

Related topics

- Introduction to alerts
- Alerts concepts and procedures

Understanding trigger values and alert severity levels

For each ControlCenter alert, you can specify unique trigger values for each of five different severity levels. Create standards in your data center for the types of conditions that correspond to the different severity levels. The following table provides recommendations.

Severity level	Possible meaning	Examples
Fatal	A resource critical to the daily operation of your organization has failed or cannot perform at an acceptable level. The alert requires immediate attention.	A critical volume or file system is out of space. A critical process has failed.
Critical	A critical resource is failing or its performance is severely degrading. The alert requires immediate attention to ensure the resource can continue to perform or does not fail.	A high disk queue is affecting the performance of a critical application. The memory performance of a critical server is poor.
Warning	The performance or availability of a resource is nearing an unacceptable range. Monitor the resource carefully and possibly take action.	The free space in a database tablespace is below an acceptable threshold. A Symmetrix subsystem raised an environmental alarm.
Minor	An abnormal event occurred. The event may indicate current or future problems.	The daily backup of a nonessential file system did not occur. A Symmetrix subsystem issued an error message.
Information	Use this severity level for informational messages.	The backup of a critical resource completed successfully. A device mapping changed.

Alert escalation example

Assume you created a file size alert with the following settings.

Severity	Comparison operator	Trigger value
Fatal	>=	1 GB
Critical	>=	750 MB
Warning	>=	500 MB
Minor (not selected)		
Information (not selected)		

The following sequence would occur as the file size changes:

- A Warning alert appears in the Active Alerts view in the Console when the file size exceeds 500 MB.
- In the Active Alerts view, the alert changes to Critical when the file size reaches 750 MB.
- When the file size returns below 500 MB, ControlCenter removes the alert from the Active Alerts view.

Note

- Many ControlCenter alerts are pre-configured on installation. Adjust the severity levels of these alerts to meet the requirements of your data center.

Related Topics

- Understanding spike controlling and evaluation frequency
- Understanding alert terminology
- Introduction to alerts
- Alert concepts and procedures

Creating and editing alerts

Overview of viewing alerts

ControlCenter provides several methods for viewing alerts. You can view:

- The alert templates for one or more agents
- All of the alerts that have been created
- The triggered (or active) alerts for a host
- All triggered alerts
- A collection of graphs showing how many alerts of each severity level have triggered on hosts and subsystems

In addition, the Console provides visual clues, through a button in the upper-right corner of the main window, about the number of triggered alerts and the triggered alert with the highest severity. You can access the Active Alerts view by clicking this button.

Related topics

- Introduction to alerts
- Overview of creating alerts
- Overview of responding to alerts
- Alert concepts and procedures

Overview of creating alerts

ControlCenter provides numerous alerts to help monitor your storage environment, such as free space on a volume or performance levels of a server or subsystem. For each alert, ControlCenter provides a template that defines default values for the alert. You can create new alerts either from the template or by copying and modifying existing alerts.

The general steps for creating an alert include:

1. **Create the alert**either from a template or by copying an existing alert. This step includes defining the resources (such as files, volumes, databases, and so on) an alert applies to, and the trigger values.
2. **Attach a management policy**to the alert to define who will be notified when the alert triggers and how the notification will occur, whether through the Console, by e-mail, by page, or by another method.
3. **Define a schedule**that determines how often the agent evaluates the alert.
4. **Attach an autofix**which is a script that an agent provides or that you write. The autofix runs when the alert triggers.
5. **Specify the hosts or storage systems to monitor**do this by applying the alert to specific hosts or storage systems or to all available systems.

For specific procedures on creating an alert, see:

- Creating an alert from a template
- Copying an existing alert

Note

- The online Help provides detailed descriptions of each alert. In the alert dialog boxes, click **Help** to access detailed Help on the alert you are editing. In the Active Alerts view, right-click an alert and select **View alert Help** to view suggestions for responding to the alert you selected.

Related topics

- Introduction to alerts
- Viewing all alerts for a host
- Alert concepts and procedures

Creating an alert from a template

For every alert, ControlCenter provides templates that define an alert's default values. You can create new alerts from these templates.

To create an alert from a template:

1. In the selection tree, expand **Administration**, **Alert Management**, and **Alert Templates**.
2. Expand the folder for the agent for which you want to create the alert.
3. Locate the alert template by expanding the sub-folders.
4. Right-click the template and select **New Alert**. The New Alert dialog box appears.
5. Click **Sources** and specify the objects (for example: files, volumes, databases, and so on) you want the alert to monitor. Most alerts support wildcards for specifying multiple objects. Click **Help** for information on the proper syntax for specifying the objects and for using supported wild cards.
6. Click **Conditions** and specify the trigger values for the various alert severity levels.
7. Click **Actions** and assign a schedule, management policy, and optionally any autofixes.
8. Click **Apply To** and select the hosts or storage systems to which the alert applies.

Notes

- If you do not select a management policy, the alert appears in all ControlCenter users' Consoles when it triggers.
- You cannot delete the alert templates.

Tips

- In addition to right-clicking alert templates in the selection tree, you can create new alerts by right-clicking templates in the various Console views or by clicking a template and selecting from the Alerts menu on the menu bar.
- To specify your own default values for new alerts, edit the alert template.

Related topics

- Copying an existing alert
- Introduction to alerts
- Understanding alert terminology
- Troubleshooting alerts and autofixes
- Overview of creating alerts

Copying an alert

You can create alerts by copying existing alerts. The new alert has the exact settings as the existing alert. Modify the alert definition to set up the monitoring you want to perform.

To create an alert by copying an existing alert:

1. In the selection tree, expand **Administration**, **Alert Management**, and **Alerts**.
2. Expand the folder for the agent for which you want to create the alert.
3. Locate the alert you want to copy by expanding the sub-folders.
4. Right-click the alert and select **Copy Alert**. The Copy Alert dialog box appears.
5. Ensure the **Alert Enabled** checkbox in the upper-right corner of the dialog box is selected.
6. Click **Sources** and specify the resources (for example: files, volumes, databases, and so on) you want the alert to monitor. Most alerts support wildcards for specifying multiple objects. Click **Help** for information on the proper syntax for specifying the objects and for using supported wild cards.
7. Click **Conditions** and specify the trigger values for the various alert severity levels.
8. Click **Actions** and assign a schedule, management policy, and optionally any autofixes.
9. Click **Apply To** and select the hosts or storage systems to which the alert applies.

Note

- If you do not select a management policy, the alert appears in all ControlCenter users' Consoles when it triggers.

Tip

- You can also create alerts from the alert templates.
- In addition to right-clicking alerts in the selection tree, you can perform alert commands by right-clicking the alerts in the various Console views or by clicking an alert and selecting from the Alerts menu on the menu bar.

Related topics

- Introduction to alerts
- Understanding alert terminology
- Troubleshooting alerts and autofixes
- Alerts concepts and procedures

Changing the severity of an alert

ControlCenter provides five severity levels that allow you to classify alerts by importance to you. Change the severity of an alert to indicate how critical that alert is to your environment. Many ControlCenter alerts are pre-configured when you install the product. Determine whether the severity levels of these alerts are appropriate for your environment and alter the severity levels if necessary.

To change the severity of an alert:

1. In the selection tree, expand **Administration**, **Alert Management**, and **Alerts**.
2. Expand the folder for the agent for which you want to change an alert severity.
3. Locate the alert by expanding the sub-folders.
4. Right-click the alert and select **Edit Alert**. The Edit Alert dialog box appears.
5. Click **Conditions**.
6. In the **Enabled** column, select one or more severity levels for the alert. The appearance of an alert changes as it moves from one severity to another.
7. In the **Operator** column, select comparison operatorsfor example, greater than (>) or less than (<)for each severity level you selected.
8. In the **Value** column, type or select trigger values for the severity levels you selected. Most alerts have default trigger values. If necessary, modify the defaults to meet your data center's needs.

Tips

- For specific information on setting up an alert, click **Help** in the alert dialog boxes.
- To modify the severity levels for all future alerts of this type, edit the alert template.

Related topics

- Understanding alert severity and escalation
- Understanding alert terminology
- Introduction to alerts
- Troubleshooting alerts and autofixes
- Alerts concepts and procedures

Deleting an alert

Deleting an alert completely removes it from ControlCenter. The alert is no longer available to any ControlCenter users.

To delete an alert:

1. In the selection tree, expand **Administration**, **Alert Management**, and **Alerts**.
2. Expand the folder for the agent to which the alert you want to delete belongs.
3. Locate the alert by expanding the sub-folders.
4. Right-click the alert and select **Delete Alert**.

Note

- Deleting an alert does not remove the template from which the alert was created.

Tips

- You can disable an alert without deleting it.
- To remove a triggered alert without deleting the alert, right-click the triggered alert and select **Reset this alert for all users**. The alert does not appear until it triggers again.
- You can re-create an alert either from the alert templates or by copying an existing alert.

Related topics

- Introduction to alerts
- Understanding alert terminology
- Alerts concepts and procedures

Editing an alert

Edit an alert to change:

- The resources an alert monitors
- The frequency at which ControlCenter evaluates the alert
- The values at which the alert triggers
- Any notification or automatic actions that occur when the alert triggers
- The hosts or subsystems to which an alert applies

To edit an alert:

1. In the selection tree, expand the **Administration**, **Alert Management**, and **Alerts**.
2. Expand the folder for the agent to which the alert you want to edit belongs.
3. Expand the sub-folders to locate the alert.
4. Right-click the alert and select **Edit**. The Edit Alert dialog box appears. See the dialog box topic for information on specific fields.

Tips

- For more information on the appropriate values for the specific alert you are editing, click **Help** in the Edit Alert dialog box.
- After an alert triggers, you can edit it by right-clicking it and selecting **Edit alert**.

Related topics

- Enabling or disabling an alert
- Changing the severity of an alert
- Deleting an alert
- Introduction to alerts
- Understanding alert terminology
- Alerts concepts and procedures

Editing an alert template

Alert templates provide default values for the creation of alerts. Upon installation, ControlCenter provides a template for each alert. Edit a template to change the default values for an alert.

To edit an alert template:

1. In the selection tree, expand **Administration**, **Alert Management**, and **Alert Templates**.
2. Expand the folder for the agent or component that contains the template you want to modify.
3. Expand the sub-folders to locate the template.
4. Right-click the template and select **Edit Template**. The Edit Alert Template dialog box appears. See the dialog box topic for specific field descriptions.
5. Click **Conditions**.
6. Specify default severity levels and trigger values.
7. Click **Actions**.
8. Edit the default schedule and management policy, and select default autofixes.

Tip

- In addition to right-clicking an alert template in the selection tree, you can edit a template by right-clicking it in the various Console views or by clicking a template and selecting from the Alerts menu on the menu bar.

Related topics

- Creating an alert from a template
- Editing an alert
- Introduction to alerts
- Alert concepts and procedures

Enabling or disabling an alert

When you disable an alert, ControlCenter no longer evaluates the alert, but it does preserve the alert settings.

To enable or disable an alert:

1. In the selection tree, expand **Administration** and **Alert Management**.
2. Expand the folder for the agent that provides the alert you want to enable or disable.
3. Expand the sub-folders to locate the alert.
4. Right-click the alert and select **Edit Alert**. The Edit Alert dialog box displays.
5. Click the **Alert Enabled** checkbox to enable or disable the alert.

Note

- When you enable or disable alerts, the changes apply for all ControlCenter users.

Tip

- You can also enable or disable multiple alerts at one time.
- In addition to right-clicking an alert in the selection tree, you can enable or disable an alert by right-clicking it in the various Console views or by clicking an alert and selecting from the Alerts menu on the menu bar.

Related topics

- Creating an alert from a template
- Copying an alert
- Introduction to alerts
- Alerts concepts and procedures

Enabling or disabling multiple alerts

You can enable or disable groups of alerts. When you disable an alert, ControlCenter no longer evaluates the alert, but it does preserve the alert settings.

To enable or disable multiple alerts:

1. In the selection tree, expand **Administration** and **Alert Management**.
2. Right-click the Alerts folder, or any folder beneath it, and select **Enable** or **Disable**. ControlCenter enables or disables all alerts in the selected folder and all sub-folders.

Note

- When you enable or disable alerts, the changes apply for all ControlCenter users.

Tip

- To enable or disable an individual alert, right-click the alert and select **Edit Alert**. Select or clear **Enabled** at the top of the dialog box.

Related topics

- Enabling or disabling an alert
- Creating an alert from a template
- Copying an alert
- Introduction to alerts
- Alerts concepts and procedures

Monitoring multiple hosts or subsystems with the same alert

If one or more of your hosts or subsystems has similar configurations and performance characteristics, you may want to monitor them with the same alert. Using a single alert can simplify the management of a group of systems:

- It reduces the total number of alerts you have to manage.
- If you decide to modify the settings for an alert, you only have to do it in one place.

When the alert triggers, the host or storage system for which the alert trigger is identified in the Active Alerts view.

To monitor multiple systems with the same alert:

1. Create the alert (see more) or edit an existing alert (see more).
2. On the **Apply To** tab of the Alert dialog box, select the hosts or storage systems to which you want to apply the alert. To apply the alert to all hosts or storage systems for which the alert is valid, select **Apply this alert to all applicable hosts**.

Related topics

- Creating an alert from a template
- Copying an alert
- Introduction to alerts
- Alerts concepts and procedures

Preventing exceptional conditions from triggering alerts (controlling spikes)

ControlCenter provides a way for you to prevent alerts from triggering when a resource temporarily exceeds a threshold, called an *alert spike*. For example, if a user creates a temporary file that causes the free space on a volume to drop below a threshold, you may want to know about the condition only if the free space remains low for several hours and not when it temporarily dips. You can control these spikes using the **Before** and **After** fields in the alert definition dialog boxes and the schedule attached to the alert.

To prevent an alert from triggering when spikes occur:

1. In the selection tree, expand **Administration**, **Alert Management**, and **Alerts**.
2. Expand the folder for the agent to which the alert you want to edit belongs.
3. Expand the sub-folders to locate the alert.
4. Right-click the alert and select **Edit**. The Edit Alert dialog box appears.
5. Click **Conditions**.
6. In the **Before** boxes, specify the number of times that the alert conditions must exist before ControlCenter triggers the alert.
7. In the **After** boxes, specify the number of times the alert conditions must be acceptable before ControlCenter removes the alert.
8. Click **Actions**.
9. From the **Schedule** list box, select a schedule to indicate how often ControlCenter should evaluate the alert.

Related topics

- Understanding spike controlling and evaluation frequency
- Setting how often an alert is evaluated
- Introduction to alerts
- Alerts concepts and procedures

Setting how often an alert is evaluated

The schedule that is attached to an alert determines how often ControlCenter evaluates the alert. When ControlCenter evaluates an alert, it compares the trigger values you have specified against the state of the resource being monitored.

To set how often an alert is evaluated:

1. In the selection tree, expand **Administration**, **Alert Management**, and **Alerts**.
2. Expand the folder for the agent to which the alert you want to edit belongs.
3. Expand the sub-folders to locate the alert.
4. Right-click the alert and select **Edit**. The Edit Alert dialog box appears.
5. Click **Actions**.
6. From the **Schedule** list box, select an appropriate schedule. Or, click **New** to create a schedule. Click **Edit** to view or modify the schedule properties.

Notes

- Evaluation frequency affects the processing resources ControlCenter consumes. Only use very high frequency schedules (for example, a schedule with an interval of one second) for short periods for diagnostic purposes.
- You can use schedules with more than one alert or collection policy. If you edit a schedule, make sure your edits are appropriate for all the alerts and collection policies that use it.

Tip

- You can also assign schedules to multiple alerts at one time.

Related topics

- Creating a schedule for an alert or data collection policy
- Copying an alert or data collection policy schedule
- Editing an alert or data collection policy schedule
- Deleting an alert or data collection policy schedule
- Introduction to alerts
- Understanding alert terminology
- Alert concepts and procedures

Alert descriptions

All agents

Generic Agent Alerts

Responding to this alert Alert dialog box Help

Each ControlCenter agent, or software component, generates messages as it runs. The components write these messages to a log file. However, you can also receive these messages in the Console as alerts by enabling the Generic Agent Alert for a component.

Enabled by default

Yes

Monitored resource (source)

The monitored resource is the agent. You do not specify a source for these alerts.

Trigger values

You cannot modify the trigger values for these alerts. The ControlCenter components trigger the alerts based on the severity of the error condition they encounter.

Evaluation frequency (schedule)

The evaluation frequency is controlled by the ControlCenter component.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or to the users responsible for maintaining the individual ControlCenter components. If you do not attach management policies to these alerts, all ControlCenter users receive them.

Possible uses of this alert

- Monitoring ControlCenter status and security

Related topics

- Introduction to alerts
- Alert concepts and procedures

ControlCenter infrastructure

Agent Inactive alert

Responding to this alert Alert dialog box Help

Use this alert to monitor the status of the ControlCenter components and to ensure ControlCenter availability. The alert triggers when a ControlCenter agent becomes inactive.

Enabled by default

Yes

Monitored resource (source)

You do not specify a source for this alert.

Trigger values
Always specify **TRUE** as the trigger value for this alert. Select an appropriate severity.

Evaluation frequency (schedule)
The evaluation frequency is controlled by ControlCenter.

Notification policies (management policies)
Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for ControlCenter security. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert
- Monitoring ControlCenter status and security

Related alerts
- MO Has Been Added/Removed by User alert
- Repository alert
- Server Message Logged alert
- Server Shutdown alert
- Primary/Secondary Assignment alert
- Store Message Logged alert

Related topics
- Introduction to alerts
- Alert concepts and procedures

MO Has Been Added/Removed by User alert

Responding to this alert Alert dialog box Help

This alert triggers when a user adds to or removes from ControlCenter a monitored host or subsystem. Use this alert to monitor the status of the ControlCenter components.

Enabled by default
Yes

Monitored resource (source)
You do not specify a source for this alert.

Trigger values
Always specify **TRUE** as the trigger value for this alert. Select an appropriate severity.

Evaluation frequency (schedule)
The evaluation frequency is controlled by ControlCenter.

Notification policies (management policies)
Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for ControlCenter security. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert
- Monitoring ControlCenter status and security

Related alerts
- Agent Inactive alert
- Repository alert
- Server Message Logged alert
- Server Shutdown alert
- Primary/Secondary Assignment alert
- Store Message Logged alert

Related topics

- Introduction to alerts
- Alert concepts and procedures

Primary/Secondary Assignment alert

Responding to this alert Alert dialog box Help

This alert triggers when a ControlCenter component that was serving as a data source fails, and ControlCenter automatically changes to the secondary data source. Use this alert to monitor the status of the ControlCenter components.

Enabled by default

Yes

Monitored resource (source)

You do not specify a source for this alert.

Trigger values

Always specify **TRUE** as the trigger value for this alert. Select an appropriate severity.

Evaluation frequency (schedule)

The evaluation frequency is controlled by ControlCenter.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for ControlCenter security. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

- Monitoring ControlCenter status and security

Related alerts

- Agent Inactive alert
- MO Has Been Added/Removed by User alert
- Repository alert
- Server Message Logged alert
- Server Shutdown alert
- Store Message Logged alert

Related topics

- Introduction to alerts
- Alert concepts and procedures

Respository alert

Responding to this alert Alert dialog box Help

This alert triggers when the ECC Server receives an alert regarding the ControlCenter Repository database. Use this alert to monitor the status of the ControlCenter components.

Enabled by default

Yes

Monitored resource (source)

You do not specify a source for this alert.

Trigger values

Always specify **TRUE** as the trigger value for this alert. Select an appropriate severity.

Evaluation frequency (schedule)

The evaluation frequency is controlled by ControlCenter.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for ControlCenter security. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

- Monitoring ControlCenter status and security

Related alerts

- Agent Inactive alert
- MO Has Been Added/Removed by User alert
- Server Message Logged alert
- Server Shutdown alert
- Primary/Secondary Assignment alert
- Store Message Logged alert

Related topics

- Responding to this alert
- Introduction to alerts
- Alert concepts and procedures

Server Message Logged alert

Responding to this alert Alert dialog box Help

This alert triggers when a message about the ECC Server is written to the log file. Use this alert to monitor the status of the ControlCenter components.

Enabled by default

Yes

Monitored resource (source)

You do not specify a source for this alert.

Trigger values

Always specify **TRUE** as the trigger value for this alert. Select an appropriate severity.

Evaluation frequency (schedule)

The evaluation frequency is controlled by ControlCenter.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for ControlCenter security. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

- Monitoring ControlCenter status and security

Related alerts

- Agent Inactive alert
- MO Has Been Added/Removed by User alert
- Repository alert
- Server Shutdown alert
- Primary/Secondary Assignment alert
- Store Message Logged alert

Related topics

- Introduction to alerts
- Alert concepts and procedures

Server Shutdown alert

Responding to this alert Alert dialog box Help

This alert triggers when the ECC Server is shut down under normal conditions. Use this alert to monitor the status of the ControlCenter components.

Enabled by default

Yes

Monitored resource (source)

You do not specify a source for this alert.

Trigger values

Always specify **TRUE** as the trigger value for this alert. Select an appropriate severity.

Evaluation frequency (schedule)

The evaluation frequency is controlled by ControlCenter.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for ControlCenter security. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

- Monitoring ControlCenter status and security

Related alerts

- Agent Inactive alert
- MO Has Been Added/Removed by User alert
- Repository alert
- Server Message Logged alert
- Primary/Secondary Assignment alert
- Store Message Logged alert

Related topics

- Introduction to alerts
- Alert concepts and procedures

Store Message Logged alert

Responding to this alert Alert dialog box Help

This alert triggers when a message about the Store is written to the log file. Use this alert to monitor the status of the ControlCenter components.

Enabled by default

Yes

Monitored resource (source)

You do not specify a source for this alert.

Trigger values

Always specify **TRUE** as the trigger value for this alert. Select an appropriate severity.

Evaluation frequency (schedule)

The evaluation frequency is controlled by ControlCenter.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for ControlCenter security. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

- Monitoring ControlCenter status and security

Related alerts

- Agent Inactive alert
- MO Has Been Added/Removed by User alert
- Repository alert
- Server Message Logged alert
- Server Shutdown alert
- Primary/Secondary Assignment alert

Related topics

- Introduction to alerts
- Alert concepts and procedures

ControlCenter security

User Change alert

Responding to this alert Alert dialog box Help

This alert triggers when users are added to or removed from ControlCenter or when any change is made to a user's profile. The ControlCenter security administrator can use this alert to track user histories and detect security breaches.

Enabled by default

Yes

Monitored resource (source)

You do not specify a source for this alert.

Trigger values

Always specify **TRUE** as the trigger value for this alert. Select an appropriate severity.

Evaluation frequency (schedule)

The evaluation frequency is controlled by ControlCenter.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or to individual responsible for ControlCenter security. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

- Monitoring ControlCenter status and security

Related alerts

- User Change alert
- User Group Change alert
- User Logged On/Off alert
- User Logon Failure alert

Related topics

- Introduction to alerts
- Alert concepts and procedures

User Group Change alert

Responding to this alert Alert dialog box Help

This alert triggers when a user group is added to or removed from ControlCenter or when any change is made to the user group properties. The ControlCenter security administrator can use this alert to monitor the use of user groups and detect security breaches.

Enabled by default

Yes

Monitored resource (source)

You do not specify a source for this alert.

Trigger values

Always specify **TRUE** as the trigger value for this alert. Select an appropriate severity.

Evaluation frequency (schedule)

The evaluation frequency is controlled by ControlCenter.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for ControlCenter security. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

- Monitoring ControlCenter status and security

Related topics

- User Change alert
- User Logged On/Off alert
- User Logon Failure alert

Related topics

- Introduction to alerts
- Alert concepts and procedures

User Logged On/Off alert

Responding to this alert Alert dialog box Help

This alert triggers when a user successfully logs on or off ControlCenter. The ControlCenter security administrator can use this alert to monitor user activity and detect security breaches.

Enabled by default

Yes

Monitored resource (source)

You do not specify a key for this alert.

Trigger values

Always specify **TRUE** as the trigger value for this alert. Select an appropriate severity.

Evaluation frequency (schedule)

The evaluation frequency is controlled by ControlCenter.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for ControlCenter security. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

- Monitoring ControlCenter status and security

Related alerts

- User Change alert
- User Group Change alert
- User Logon Failure alert

Related topics

- Introduction to alerts
- Alert concepts and procedures

User Logon Failure alert

Responding to this alert Alert dialog box Help

This alert triggers when a user fails to log on to ControlCenter. Repeated logon failures could indicate an attempted security breach.

Enabled by default

Yes

Monitored resource (source)

You do not specify a source for this alert.

Trigger values

Always specify **TRUE** as the trigger value for this alert. Select an appropriate severity.

Evaluation frequency (schedule)

The evaluation frequency is controlled by ControlCenter.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for ControlCenter security. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

- Monitoring ControlCenter status and security

Related alerts

- User Change alert
- User Group Change alert
- User Logged On/Off alert

Related topics

- Introduction to alerts
- Alert concepts and procedures

Backup Agent for TSM

TSM: Activity Log Failure Count alert

Responding to this alert Alert dialog box Help

The alert triggers when the number of failed events for a node exceeds a threshold.

Enabled by default

Yes

Monitored resources (source)

Server Name	The name of the TSM server whose activity log you want to monitor. Specify * to monitor all servers.
Node Name	The name of the nodes whose events you want to monitor with this alert. Specify * to monitor all nodes.

Trigger values

The trigger value is the number of failed events for a single node (client), as listed in the activity log. By default, a single failure triggers a Harmless alert, with increasing severity for additional failures on a node.

Evaluation frequency (schedule)

Once per day at 6 a.m. by default.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring nodes for failed, missed, and severed events

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Activity Log Search alert

Responding to this alert Alert dialog box Help

The alert triggers when a user-defined string appears in the activity log. You can use this alert to inform you when a certain file name, message number, or other string occurs in the activity log. If you want instant notification, choose a more frequent schedule than the default of every day at 6 a.m.

Enabled by default

Yes

Monitored resources (source)

Server Name	The name of the TSM server whose activity log you want to monitor. Specify * to monitor all servers.
Search String	The string that should cause the alert to trigger when it appears in the activity log.

Trigger values

The trigger value is the presence of the search string defined in the monitored resources in the activity log of servers defined in the monitored resources. Do not change the Value field. Check and clear checkboxes for the severity you want associated with the appearance of the string.

Evaluation frequency (schedule)

Once per day at 6 a.m. by default.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring nodes for failed, missed, and severed events

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Client Licenses alert

Responding to this alert Alert dialog box Help

The alert triggers when the number of available client licenses falls below a threshold. If the alert triggers, add more client licenses to ensure you can add the TSM backup client to new machines without running out of licenses.

This alert is available for TSM 3.7 only.

Enabled by default

No

Monitored resource (source)

Server Name	The name of the TSM server (version 3.7 only) whose license count you want to monitor. Specify * to monitor all servers.

Trigger values

The trigger value is the number of available client licenses. This is the number of new clients (nodes) on which you can install TSM software and begin conducting backups.

Evaluation frequency (schedule)

Once per day at 6 a.m. by default.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Managing backup nodes

Related topics

- Alert concepts and procedures

TSM: Database Cache Hit Percentage alert

Responding to this alert Alert dialog box Help

The alert triggers when cache performance for the TSM database is poor.

Enabled by default

Yes

Monitored resource (source)

Server Name	The name of the TSM server whose database performance you want to monitor. Specify * to monitor all servers.

Trigger values

The trigger value is the percentage of requests that accessed a buffer page on the databases for the monitored TSM servers.

Evaluation frequency (schedule)

Once per hour, by default.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring TSM database performance

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Database Cache Wait Percent alert

Responding to this alert Alert dialog box Help

The alert triggers when cache performance for the TSM database is poor. A wait percent greater than zero (0) normally means that improvements to the database configuration are required.

Enabled by default

Yes

Monitored resource (source)

Server Name	The name of the TSM server whose database performance you want to monitor. Specify * to monitor all servers.

Trigger values

The trigger value is the percentage of cache requests that had to wait for a buffer page on the databases for the monitored TSM servers.

Evaluation frequency (schedule)

Once per hour by default.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring TSM database performance

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Database Utilization alert

Responding to this alert Alert dialog box Help

The alert triggers when the size of the database has exceeded a certain percentage of the preconfigured database allocation. The TSM database has a preconfigured size allocation. The alert warns you when the database is approaching the limit of the size allocation. In response to the alert, you can add database volumes and extend the database.

Enabled by default

Yes

Monitored resource (source)

Server Name	The name of the TSM server whose database performance you want to monitor. Specify * to monitor all servers.

Trigger values

The trigger value is the actual size of the database.

Evaluation frequency (schedule)

Once per hour by default.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring TSM databases and logs for space problems

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Database Volume Percent alert

Responding to this alert Alert dialog box Help

The alert triggers when the utilization of a database volume exceeds a threshold.

Enabled by default

No

Monitored resource (source)

Server Name	The name of the TSM server whose database volumes you want to monitor. Specify * to monitor all servers.
Database Volume	The database volumes you want to monitor. Specify * to monitor all database volumes.

Trigger values

The percentage of the database volume that is utilized.

Evaluation frequency (schedule)

Once per hour, by default.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring TSM databases and logs for space problems

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Event Log Failed Events alert

Responding to this alert Alert dialog box Help

The alert triggers for failed events on any of the monitored servers and nodes. If multiple events fail, the alert appears multiple times, showing the affected server and node. The alert is configured to run once per day at 6 a.m., primarily to inform you of problems on the previous night's backups when you arrive in the morning. If you are monitoring backups at time of execution, you can change the schedule or use on-demand exploring and reporting.

Enabled by default

Yes

Monitored resources (source)

Server Name	The name of the TSM server whose event log you want to monitor. Specify * to monitor all servers.
Node Name	The name of the nodes whose events you want to monitor with this alert. Specify * to monitor all nodes.

Trigger values

The alert triggers for any failed event on the monitored servers and nodes. Check the severity level you want for the servers and nodes that this alert monitors (as specified in the keys). For example, one alert may monitor nodes that are production systems; check Warning or Critical for this alert. A different alert may monitor events for desktop nodes; check Harmless, Minor, or whatever severity you consider appropriate for a desktop.

Do not change the value of TRUE in this alert. To disable the alert, clear the checkbox that enables the entire alert (at the top of the dialog box) or clear the checkbox for the severity you want to turn off.

Evaluation frequency (schedule)

Once per day at 6 a.m. by default. Keep this daily schedule (a ControlCenter schedule, not a TSM schedule) if you want the alert to show you problems with the previous night's backups each day. Use a more frequent schedule if you are monitoring the actual execution of events during the backup window. In addition to the alert, use on-demand exploring and reporting of the event log.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring nodes for failed, missed, and severed events

Related topics

- Alert concepts and procedures
- Event Log Failed Events alert
- Activity Log Failure Count alert
- Use of quotes, blanks, and wildcards

TSM: Event Log Missed Events alert

Responding to this alert Alert dialog box Help

The alert triggers for missed events on any of the monitored servers and nodes. If multiple events are missed, the alert appears multiple times, showing the affected server and node. The alert is configured to run once per day at 6 a.m., primarily to inform you of problems on the previous night's backups when you arrive in the morning. If you are monitoring backups at time of execution, you can change the schedule or use on-demand exploring and reporting.

Enabled by default

Yes

Monitored resources (source)

Server Name	The name of the TSM server whose event log you want to monitor. Specify * to monitor all servers.
Node Name	The name of the nodes whose events you want to monitor with this alert. Specify * to monitor all nodes.

Trigger values

The alert triggers for any missed event on the monitored servers and nodes. Check the severity level you want for the servers and nodes that this alert monitors (as specified in the keys). For example, one alert may monitor nodes that are production systems; check Warning or Critical for this alert. A different alert may monitor events for desktop nodes; check Harmless, Minor, or whatever severity you consider appropriate for a desktop.

Do not change the value of TRUE in this alert. To disable the alert, clear the checkbox that enables the entire alert (at the top of the dialog box) or clear the checkbox for the severity you want to turn off.

Evaluation frequency (schedule)

Once per day at 6 a.m. by default. Keep this daily schedule (a ControlCenter schedule, not a TSM schedule) if you want the alert to show you problems with the previous night's backups each day. Use a more frequent schedule if you are monitoring the actual execution of events during the backup window. In addition to the alert, use on-demand exploring and reporting of the event log.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring nodes for failed, missed, and severed events

Related topics

- Alert concepts and procedures
- Event Log Failed Events alert
- Event Log Severed Events alert
- Activity Log Failure Count alert
- Use of quotes, blanks, and wildcards

TSM: Log Volume Utilization alert

Responding to this alert Alert dialog box Help

The alert triggers when the utilization of a log volume exceeds a percentage.

Enabled by default

No

Monitored resources (source)

Server Name	The name of the TSM server whose log pools you want to monitor. Specify * to monitor all servers.

Trigger values

The percentage of the log volume that is utilized.

Evaluation frequency (schedule)

Once per hour, by default.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring TSM databases and logs for space problems

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Invalid Sign On Count alert

Responding to this alert Alert dialog box Help

The alert monitors the number of invalid sign-on attempts occuring on a node in the previous 24-hour period. (You can change the period.) A triggered alert of warning, critical, or fatal severity could represent an attempted security breach and should be investigated quickly and carefully. It could also simply represent a forgotten password.

Enabled by default

No

Monitored resources (source)

Server Name	The name of the TSM server whose nodes you want to monitor. Specify * to monitor all servers.
Node Name	The name of the nodes whose sign-on count you want to monitor with this alert. Specify * to monitor all nodes.

Trigger values

The trigger value is the number of sign-ons that occur unsuccessfully in the scheduled interval.

Evaluation frequency (schedule)

Once per day at 6 a.m. by default. With this default, the alert may not trigger for many hours after the repeated sign-on attempts.

If you want more immediate notification, choose a schedule with a more frequent interval (such as hourly). Note, however, that the alert only monitors the number of sign-ons in that shorter interval. Also, the alert may trigger in the hour when the sign-ons occur, then reset (cancel itself) in the next hour if no invalid attempts occur. In this case, it would no longer appear in the Active Alerts table and you would have to search an EMC ControlCenter log to find whether and when the alert triggered.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Managing backup nodes

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Log Logpool Percent alert

Responding to this alert Alert dialog box Help

The alert triggers when the utilization of a log pool exceeds a percentage. TSM uses buffer pages to hold data to be written to the recovery log. If the buffer pages fill up, then data may be lost. These buffer pages are called log pools.

Enabled by default

Yes

Monitored resources (source)

Server Name	The name of the TSM server whose log pools you want to monitor. Specify * to monitor all servers.

Trigger values

The percentage of the buffer page (log pool) that is utilized.

Evaluation frequency

Once per hour, by default.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring TSM databases and logs for space problems

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Log Utilization alert

Responding to this alert Alert dialog box Help

The alert triggers when the percentage utilization of the recovery log exceeds a threshold. The recovery log may be critical to quickly restoring TSM to operation if it crashes or if its operations are affected by other system problems.

The activity and event logs are part of the TSM database. The Database Utilization alert monitors their space use.

Enabled by default

Yes

Monitored resource (source)

Server Name	The name of the TSM server whose log you want to monitor. Specify * to monitor all servers.

Trigger values

The percent of the log that is full.

Evaluation frequency

Once per hour, by default.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring TSM databases and logs for space problems

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Log Volume Utilization alert

Responding to this alert Alert dialog box Help

The alert triggers when the utilization of a log volume exceeds a percentage.

Enabled by default

No

Monitored resources (source)

Server Name	The name of the TSM server whose log pools you want to monitor. Specify * to monitor all servers.

Trigger values

The percentage of the log volume that is utilized.

Evaluation frequency (schedule)

Once per hour, by default.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring TSM databases and logs for space problems

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Size Archive Storage Size alert

Responding to this alert Alert dialog box Help

The alert triggers when the size of archived data (in KB) has exceeded a threshold for a node.

Enabled by default

No

Monitored resources (source)

Server Name	The name of the TSM server whose nodes you want to monitor. Specify * to monitor all servers.
Node Name	The name of the nodes whose backup sizes you want to monitor with this alert. Specify * to monitor all nodes.

Trigger values

The trigger value is the size of archived data for a node (client).

Evaluation frequency (schedule)

Once per day at 6:00 am, by default.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring client backup and archive size in TSM

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Size Backup Storage Size alert

Responding to this alert Alert dialog box Help

The alert triggers when the size of backed-up data in KB has exceeded a threshold for a node.

Enabled by default

No

Monitored resources (source)

Server Name	The name of the TSM server whose nodes you want to monitor. Specify * to monitor all servers.
Node Name	The name of the nodes whose backup sizes you want to monitor with this alert. Specify * to monitor all nodes.

Trigger values

The trigger value is the size of backed-up data for a node (client).

Evaluation frequency (schedule)

Once per day at 6:00 am, by default.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring client backup and archive size in TSM

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Size Space Managed Storage Size alert

Responding to this alert Alert dialog box Help

The alert triggers when the size of space-managed storage data (in KB) has exceeded a threshold for a node.

Enabled by default

No

Monitored resources (source)

Server Name	The name of the TSM server whose nodes you want to monitor. Specify * to monitor all servers.
Node Name	The name of the nodes whose space managed storage sizes you want to monitor with this alert. Specify * to monitor all nodes.

Trigger values

The trigger value is the size of space managed storage data for a node (client).

Evaluation frequency (schedule)

Once per day at 6:00 am.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring client backup and archive size in TSM

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Status Filling alert

Responding to this alert Alert dialog box Help

The alert triggers when a storage pool is neither empty nor completely full.

Enabled by default

No

Monitored resources (source)

Server Name	The name of the TSM server whose volumes you want to monitor. Specify * to monitor all servers.
Volume Name	The volumes storing TSM backups and archives whose status you want to monitor. Specify * to monitor all volumes.

Trigger values

The alert triggers when the TSM Query Volume command returns a volume status of Filling. ControlCenter issues the Query Volume command according to the schedule defined for the alert.

Evaluation frequency (schedule)

Once per day at 6:00 a.m.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring availability of TSM backup volumes
- Monitoring volumes and storage pools for space problems

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Status Offline alert

Responding to this alert Alert dialog box Help

The alert triggers when a backup volume is offline. Neither the server nor client nodes can store data to the volume as of the time the alert triggered.

Enabled by default

No.

Monitored resources (source)

Server Name	The name of the TSM server whose volumes you want to monitor. Specify * to monitor all servers.
Volume Name	The volumes storing TSM backups and archives whose status you want to monitor. Specify * to monitor all volumes.

Trigger values

The alert triggers when the TSM Query Volume command returns a status of "Offline" for the volume. ControlCenter issues the Query Volume command according to the schedule defined for the alert.

Evaluation frequency (schedule)

Every three hours.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring availability of TSM backup volumes

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Status Unavailable alert

Responding to this alert Alert dialog box Help

The alert triggers when a backup volume is unavailable. Neither the server nor client nodes can store data to the volume as of the time the alert triggered.

Enabled by default

No

Monitored resources (source)

Server Name	The name of the TSM server whose volumes you want to monitor. Specify * to monitor all servers.
Volume Name	The volumes storing TSM backups and archives whose status you want to monitor. Specify * to monitor all volumes.

Trigger values

The alert triggers when the TSM Query Volume command returns a volume status of Unavailable. ControlCenter issues the Query Volume command according to the schedule defined for the alert.

Evaluation frequency (schedule)

Every three hours.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring availability of TSM backup volumes

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Storage Pool Utilization alert

Responding to this alert Alert dialog box Help

The alert triggers when the utilization of a storage pool exceeds a threshold. If the alert triggers, you may need to add volumes to a storage pool.

Enabled by default

No

Monitored resources (source)

Server Name	The name of the TSM server whose storage pools you want to monitor. Specify * to monitor all servers.
Storage Pool Name	The storage pools whose utilization you want to monitor. Specify * to monitor all storage pools.

Trigger values

The percent of the buffer page (log pool) that is full.

Evaluation frequency (schedule)

Once per hour.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring volumes and storage pools for space problems

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Volume Read Errors Count alert

Responding to this alert Alert dialog box Help

The alert triggers when a volume encounters excessive read errors in a 24-hour period (or the period you define in the schedule).

Enabled by default

No

Monitored resources (source)

Server Name	The name of the TSM server whose volumes you want to monitor. Specify * to monitor all servers.
Volume Name	The volumes you want to monitor. Specify * to monitor all volumes.

Trigger values

The percentage of the volume that is filled.

Evaluation frequency (schedule)

Once per day at 6:00 a.m.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring availability of TSM backup volumes

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Volume Utilization alert

Responding to this alert Alert dialog box Help

The alert triggers when the utilization of a backup (or archive) volume exceeds a threshold.

Enabled by default

No

Monitored resources (source)

Server Name	The name of the TSM server whose volumes you want to monitor. Specify * to monitor all servers.
Volume Name	The volumes storing TSM backups and archives whose utilization you want to monitor. Specify * to monitor all volumes.

Trigger values

The percentage of the volume that is filled.

Evaluation frequency (schedule)

Once per hour.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring volumes and storage pools for space problems

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

TSM: Volume Write Errors Count alert

Responding to this alert Alert dialog box Help

The alert triggers when a volume encounters excessive write errors in a 24-hour period (or the period you define in the schedule).

Enabled by default

No

Monitored resources (source)

Server Name	The name of the TSM server whose volumes you want to monitor. Specify * to monitor all servers.
Volume Name	The volumes you want to monitor. Specify * to monitor all volumes.

Trigger values

The number of write errors that occur for a volume in the period defined by the schedule.

Evaluation frequency (schedule)

Once per day at 6:00 a.m.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring availability of TSM backup volumes

Related topics

- Alert concepts and procedures
- Use of quotes, blanks, and wildcards

Connectivity Agent for SNMP

Connectivity Agent for SNMP alerts

The Connectivity Agent for SNMP generates four alerts in conjunction with its monitoring of connectivity devices. These alerts are triggered automatically and do not have to be configured.

When an alert is triggered on a connectivity device or port, a severity designation appears on its icon in the tree panel and in topology map, and the alert description appears in the Active Alerts panel.

To view the alerts on a connectivity device or a port:

1. Select one or more connectivity devices or ports in the Connectivity folder in the tree panel.
2. Click the **Monitoring** task and select **Alerts** drop-down menu. The Active Alerts panel appears displaying the alerts for the selected devices or ports.

Notes

- No severity designation on an icon in the tree panel signifies that there are no alerts for that device or port.
- Selecting the folder for a particular device type displays the alerts for all the devices in the folder.

Alerts

The following alerts are associated with the Connectivity Agent for SNMP:

- SNMP Agent Configuration Change
- SNMP Agent Unreachable
- SNMP Agent Unit Status Change
- SNMP Agent Port Status Change

Related topics

- Connectivity Agent for SNMP administration
- Connectivity Agent for SNMP data collection policies

SNMP Agent Configuration Change alert

Responding to this alert

This alert does not have to be configured. It is triggered when the following configuration changes occur in the topology:

- A connectivity device is added
- A connectivity device is removed
- Connectivity devices are swapped

When this alert is triggered on a connectivity device, a designation appears on the device's icon in the tree panel and in topology map, and the alert description appears in the Active Alerts panel. See Connectivity Agent for SNMP alerts for information on viewing alerts generated by this agent.

Enabled by default

Yes.

Monitored resource

The Connectivity Agent for SNMP monitors the SNMP agents running on devices whose IP addresses are defined in the Connectivity Agent for SNMP data collection policies. When a configuration change is recorded in the SNMP agent, the Connectivity Agent for SNMP detects the change and generates this alert.

Trigger values

This alert triggers when configuration changes occur to devices located at the IP addresses defined in the following data collection policies:

- SNMP Agent Change Request
- SNMP Rescan Request
- SNMP Discover Request

Evaluation frequency

The frequency of device monitoring in the SAN is driven by the Connectivity Agent for SNMP data collection policies. The following default collection policy polling intervals apply to this alert:

- SNMP Agent Changed Request 10 minutes
- SNMP Rescan Request 30 minutes
- SNMP Discover Request 5 minutes Although a default polling time is set, the SNMP Discover Request policy runs only once, when it is manually invoked.

Possible uses of this alert

This alert can be applied to all devices, to a subset of devices, or to a single device in the SAN, by creating and editing instances of the SNMP Agent Change Request data collection policy. Do not rename this alert when creating multiple instances of it.

Related alerts

- SNMP Agent Port Status Change
- SNMP Agent Unit Status Change
- SNMP Agent Unreachable

Related topics

- Connectivity Agent for SNMP alerts
- Responding to Connectivity Agent for SNMP alerts
- Connectivity Agent for SNMP Data collection policies

SNMP Agent Port Status Change alert

Responding to this alert

This alert does not have to be configured. It is triggered when the status of a port changes.

Examples of status changes include equipment failure and power problems. Status messages are as follows:

- `Fatal` (value = 5)
- `Warning` (4)
- `Minor` (1)
- `Informational` (0)

When this alert is triggered on a port, a designation appears on the port's icon in the tree panel and in topology map, and the alert description appears in the Active Alerts panel. See Connectivity Agent for SNMP alerts for information on viewing alerts generated by this agent.

Enabled by default

Yes

Monitored resource

The Connectivity Agent for SNMP monitors the SNMP agents running on devices whose IP addresses are defined in the Connectivity Agent for SNMP data collection policies. When a change of port status is recorded in the SNMP agent, the Connectivity Agent for SNMP detects the change and generates this alert.

Trigger values

There are two trigger sources for this alert:

- The Connectivity Agent for SNMP generates this alert in real time whenever port status changes occur.
- Connectivity Agent for SNMP polls the SNMP agents according to the polling interval set in the SNMP Port Config policy and generates this alert when a port status change is detected.

Evaluation frequency

This alert is generated both in real time and according to the polling intervals defined in the SNMP Port Config Request policy. The following default collection policy polling interval applies to this alert:

- SNMP Port Config Request 5 minutes

Possible uses of this alert

This alert can be applied to all devices, to a subset of devices, or to a single device in the SAN, by creating and editing instances of the SNMP Port Config Request data collection policy. Do not rename this alert when creating multiple instances of it.

Related alerts

- SNMP Agent Configuration Change
- SNMP Agent Unit Status Change
- SNMP Agent Unreachable

Related topics

- Connectivity Agent for SNMP alerts
- Responding to Connectivity Agent for SNMP alerts
- SNMP Port Config Request data collection policy
- SNMP Collector data collection policies

SNMP Agent Unit Status Change alert

Responding to this alert

This alert does not have to be configured. It is triggered when the status of a device changes.

Examples of status changes include equipment failure and power problems. Status messages are as follows:

- `Fatal` (value = 5)
- `Warning` (4)
- `Minor` (1)
- `Informational` (0)

When this alert is triggered on a connectivity device, a designation appears on the device's icon in the tree panel and in topology map, and the alert description appears in the Active Alerts panel. See Connectivity Agent for SNMP alerts for information on viewing alerts generated by this agent.

Enabled by default

Yes

Monitored resource

The Connectivity Agent for SNMP monitors the SNMP agents running on devices whose IP addresses are defined in the Connectivity Agent for SNMP data collection policies. When a change of unit status is recorded in the SNMP agent, the Connectivity Agent for SNMP detects the change and generates this alert.

Trigger values

There are multiple trigger sources for this alert:

- The Connectivity Agent for SNMP generates this alert in real time whenever unit status changes occur.
- The Connectivity Agent for SNMP polls SNMP agents in the SAN according to the polling intervals set in the following data collection policies and generates this alert when a status change is detected:
  - SNMP Status Request
  - SNMP Rescan Request
  - SNMP Discover Request

Evaluation frequency

This alert is generated both in real time and according to the polling intervals defined in the following data collection policies (See Trigger values):

- SNMP Status Request 10 minutes
- SNMP Rescan Request 30 minutes
- SNMP Discover Request 5 minutes Although a default polling time is set, the SNMP Discover Request policy runs only once, when it is manually invoked.

Possible uses of this alert

This alert can be applied to all devices, to a subset of devices, or to a single device in the SAN, by creating and editing instances of the SNMP Status Request data collection policy. Do not rename this alert when creating multiple instances of it.

Related alerts

- SNMP Agent Configuration Change
- SNMP Agent Port Status Change
- SNMP Agent Unreachable

Related topics

- Connectivity Agent for SNMP alerts
- Responding to Connectivity Agent for SNMP alerts
- Connectivity Agent for SNMP data collection policies

SNMP Agent Unreachable alert

Responding to this alert

This alert does not have to be configured. It is triggered when a device becomes unreachable.

When this alert is triggered on a connectivity device, a designation appears on the device's icon in the tree panel and in topology map, and the alert description appears in the Active Alerts panel. See Connectivity Agent for SNMP alerts for information on viewing alerts generated by this agent.

Enabled by default

Yes

Monitored resource

The Connectivity Agent for SNMP monitors the SNMP agents running on devices whose IP addresses are defined in the Connectivity Agent for SNMP data collection policies. When the Connectivity Agent for SNMP cannot detect a defined SNMP agent, it generates this alert.

Trigger values

This alert triggers when status changes occur to devices located at the IP addresses defined in the following data collection policies:

- SNMP Ping Request
- SNMP Rescan Request
- SNMP Discover Request

Evaluation frequency

The frequency of device monitoring in the SAN is driven by the Connectivity Agent for SNMP data collection policies. The following default collection policy polling intervals apply to this alert:

- SNMP Ping Request 1 minute
- SNMP Rescan Request 30 minutes
- SNMP Discover Request 5 minutes Although a default polling time is set, the SNMP Discover Request policy runs only once, when it is manually invoked.

Possible uses of this alert

This alert can be applied to all devices, to a subset of devices, or to a single device in the SAN, by creating and editing instances of the SNMP Status Request data collection policy. Do not rename this alert when creating multiple instances of it.

Related alerts

- SNMP Agent Configuration Change
- SNMP Agent Port Status Change
- SNMP Agent Unit Status Change

Related topics

- Connectivity Agent for SNMP alerts
- Responding to Connectivity Agent for SNMP alerts
- Connectivity Agent for SNMP data collection policies

Database Agent for DB2

DB2 Index Check Index Return Code alert

Responding to this alert Alert dialog box Help

This alert monitors the return code for Check Index and by default triggers a fatal alert for a return code of 8 or higher. If you want to be informed of successful Check Index operations (so you can view the output messages), then edit the alert trigger values (conditions).

Enabled by default

Yes.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use * to specify all subsystems.
Owner	The owner of the indexes you want to monitor. Use * to monitor all owners.
Index	The index or indexes you want to monitor. Use * to monitor all indexes.

Trigger values

This alert monitors the return code for Check Index, and by default triggers a fatal alert for a return code of 8 or higher. If you want to be informed of successful Check Index operations (so you can view the output messages), then edit the alert and check the Warning and Harmless severities to activate them.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring DB2 database integrity and consistency

Related topics

- Alert concepts and procedures

DB2 Index Partition Percent Rows Far From Optimal alert

Responding to this alert Alert dialog box Help

This alert monitors the percentage of rows far from their original position in a partition. The alert helps you identify candidates for reorganization. Widely distributed rows take longer to access and can slow index performance.

Because the current alert uses percentages, this alert may be easier to use than the DB2 Index Partition Rows Far From Original alert, which uses absolute numbers.

Enabled by default

Yes.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use * to specify all subsystems.
Owner	The owner of the indexes you want to monitor. Use * to monitor all owners.
Index	The index or indexes you want to monitor. Use * to monitor all indexes.
Partition	The name of the partition you want to monitor. A partition typically maps to an index data set. Use * to specify all partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

The trigger value is the percentage of rows far from their original position in a partition.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring for reorganization candidates

Related topics

- Alert concepts and procedures

DB2 Index Partition Percent Rows Near Optimal alert

Responding to this alert Alert dialog box Help

This alert monitors the percentage of modified rows written to a page near their original positions. If this percentage is too low, then performance may suffer and the index may need to be reorganized.

Enabled by default

Yes.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use * to specify all subsystems.
Owner	The owner of the indexes you want to monitor. Use * to monitor all owners.
Index	The index or indexes you want to monitor. Use * to monitor all indexes.
Partition	The name of the partition you want to monitor. A partition typically maps to an index data set. Use * to specify all partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

Specify the percentage of modified rows.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring for reorganization candidates

Related topics

- Alert concepts and procedures

DB2 Index Partition Rows alert

Responding to this alert Alert dialog box Help

This alert monitors the number of rows in individual index partitions.

Enabled by default

Yes.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use * to specify all subsystems.
Owner	The owner of the indexes you want to monitor. Use * to monitor all owners.
Index	The index or indexes you want to monitor. Use * to monitor all indexes.
Partition	The name of the partition you want to monitor. A partition typically maps to an index data set. Use * to specify all partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

Specify the number of rows in the index partition.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring database space utilization and trends

Related topics

- Alert concepts and procedures

DB2 Index Partition Rows Far From Optimal alert

Responding to this alert Alert dialog box Help

This alert monitors the number of rows far from their original position in a partition. The alert helps you identify candidates for reorganization. Widely distributed rows take longer to access and can slow index performance.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use * to specify all subsystems.
Owner	The owner of the indexes you want to monitor. Use * to monitor all owners.
Index	The index or indexes you want to monitor. Use * to monitor all indexes.
Partition	The name of the partition you want to monitor. A partition typically maps to an index data set. Use * to specify all partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

Specify the number of rows in a partition far from their original position for the alert to trigger.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring for reorganization candidates

Related topics

- Alert concepts and procedures

DB2 Index Partition Rows Near Optimal alert

Responding to this alert Alert dialog box Help

This alert monitors the number of rows near their original position.

Enabled by default

Yes.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use * to specify all subsystems.
Owner	The owner of the indexes you want to monitor. Use * to monitor all owners.
Index	The index or indexes you want to monitor. Use * to monitor all indexes.
Partition	The name of the partition you want to monitor. A partition typically maps to an index data set. Use * to specify all partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

The alert triggers when the number of rows near their optimal position exceeds a threshold.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring for reorganization candidates

Related topics

- Alert concepts and procedures

DB2 Index Partition Space alert

Responding to this alert Alert dialog box Help

This alert monitors the allocated space for index partitions.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use * to specify all subsystems.
Owner	The owner of the indexes you want to monitor. Use * to monitor all owners.
Index	The index or indexes you want to monitor. Use * to monitor all indexes.
Partition	The name of the partition you want to monitor. A partition typically maps to an index data set. Use * to specify all partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

Specify the number of kilobytes that an index partition should exceed to trigger an alert of a given severity. To convert default values in kilobytes to megabytes or gigabytes, see the conversion table.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring DB2 space utilization and trends
- Monitoring for reorganization candidates

Related topics

- Alert concepts and procedures

DB2 Index Space Usage alert

Responding to this alert Alert dialog box Help

This alert monitors the allocated space for individual indexes.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use * to specify all subsystems.
Owner	The owner of the indexes you want to monitor. Use * to monitor all owners.
Index	The index or indexes you want to monitor. Use * to monitor all indexes.

Trigger values

Specify the number of kilobytes that an index should reach before triggering an alert of a given severity. To convert default values in kilobytes to megabytes or gigabytes, see the conversion table.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring DB2 space utilization and trends

Related topics

- Alert concepts and procedures

DB2 Subsystem Database Share alert

Alert dialog box Help

This alert monitors DB2 databases to see if they are shared by more than one subsystem. This alert is available for DB2 version 5 only. The information is not available to the agent for DB2 version 6.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.

Trigger values

The alert triggers when a subsystem and database are shared.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Related topics

- Alert concepts and procedures

DB2 Subsystem Database Space alert

Responding to this alert Alert dialog box Help

This alert monitors the allocated space of individual DB2 databases.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.

Trigger values

Specify the size of the database in kilobytes (KB) that should trigger various alert levels. Increasing database size should trigger alerts of increasing severity. To convert default values in kilobytes to megabytes or gigabytes, see the conversion table.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring DB2 space utilization and trends

Related topics

- Alert concepts and procedures

DB2 Subsystem Database Trend alert

Responding to this alert Alert dialog box Help

This alert monitors the percentage growth of individual DB2 databases.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.

Trigger values

The alert compares the size of the object in the most recent set of detector statistics with the size in the previous set. If the percentage growth exceeds the trigger value, the alert triggers. Set the trigger value (percentage growth) to account for the interval between detector statistics collection. Learning how often DB2 detector statistics are collected

Evaluation frequency (schedule)

The alert continuously monitors the trigger values, but new data is only available when the detector statistics are updated. In practical terms, the evaluation frequency is determined by the frequency of detector statistics collection. Learning how often DB2 detector statistics are collected

There is no user-configurable schedule for this alert.

Possible uses of this alert

- Monitoring DB2 space utilization and trends

Related topics

- Alert concepts and procedures

DB2 Subsystem Index Trend alert

Responding to this alert Alert dialog box Help

The alert triggers when the growth of an index exceeds a certain percentage.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

The alert compares the size of the object in the most recent set of detector statistics with the size in the previous set. If the percentage growth exceeds the trigger value, the alert triggers. Set the trigger value (percentage growth) to account for the interval between detector statistics collection. Learning how often DB2 detector statistics are collected

Evaluation frequency (schedule)

The alert continuously monitors the trigger values, but new data is only available when the detector statistics are updated. In practical terms, the evaluation frequency is determined by the frequency of detector statistics collection. Learning how often DB2 detector statistics are collected

There is no user-configurable schedule for this alert.

Possible uses of this alert

- Monitoring DB2 space utilization and trends

Related topics

- Alert concepts and procedures

DB2 subsystem stogroup space alert

Responding to this alert Alert dialog box Help

This alert monitors the allocated space for DB2 stogroups and subsystems.

Enabled by default

No. While the alert is technically enabled by default, you must check (enable) one or more severity levels in the Conditions tab of the Edit Alert dialog box.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Stogroup	The name of the stogroup you want to monitor. Use wildcards to specify multiple stogroups.

Trigger values

Specify the space in kilobytes that should trigger alerts of various severities. To convert default values in kilobytes to megabytes or gigabytes, see the conversion table.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring DB2 space utilization and trends

Related topics

- Alert concepts and procedures

DB2 subsystem stogroup trend alert

Responding to this alert Alert dialog box Help

This alert monitors growth trends in stogroup space utilization.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

The alert triggers when the growth of a stogroup exceeds a certain percentage.The alert compares the size of the object in the most recent set of detector statistics with the size in the previous set. If the percentage growth exceeds the trigger value, the alert triggers. Set the trigger value (percentage growth) to account for the interval between detector statistics collection. Learning how often DB2 detector statistics are collected

Evaluation frequency (schedule)

The alert continuously monitors the trigger values, but new data is only available when the detector statistics are updated. In practical terms, the evaluation frequency is determined by the frequency of detector statistics collection. Learning how often DB2 detector statistics are collected

There is no user-configurable schedule for this alert.

Possible uses of this alert

- Monitoring DB2 space utilization and trends

Related topics

- Alert concepts and procedures

DB2 Subsystem Table Trend alert

Responding to this alert Alert dialog box Help

This alert monitors the growth trends of database tables.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

The alert triggers when the growth of a table exceeds a certain percentage. The alert compares the size of the object in the most recent set of detector statistics with the size in the previous set. If the percentage growth exceeds the trigger value, the alert triggers. Set the trigger value (percentage growth) to account for the interval between detector statistics collection. Learning how often DB2 detector statistics are collected

Evaluation frequency (schedule)

The alert continuously monitors the trigger values, but new data is only available when the detector statistics are updated. In practical terms, the evaluation frequency is determined by the frequency of detector statistics collection. Learning how often DB2 detector statistics are collected

There is no user-configurable schedule for this alert.

Possible uses of this alert

- Monitoring DB2 space utilization and trends

Related topics

- Alert concepts and procedures

DB2 Subsystem Tablespace Trend alert

Responding to this alert Alert dialog box Help

This alert monitors the recent percentage growth of tablespace allocated size.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

The alert triggers when the growth of a tablespace exceeds a certain percentage. The alert compares the size of the object in the most recent set of detector statistics with the size in the previous set. If the percentage growth exceeds the trigger value, the alert triggers. Set the trigger value (percentage growth) to account for the interval between detector statistics collection. Learning how often DB2 detector statistics are collected

Evaluation frequency (schedule)

The alert continuously monitors the trigger values, but new data is only available when the detector statistics are updated. In practical terms, the evaluation frequency is determined by the frequency of detector statistics collection. Learning how often DB2 detector statistics are collected

There is no user-configurable schedule for this alert.

Possible uses of this alert

- Monitoring DB2 space utilization and trends

Related topics

- Alert concepts and procedures

DB2 Table Check Pending Status alert

Responding to this alert Alert dialog box Help

This alert monitors tables for Check Pending status.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

The alert triggers when the agent finds a table is in Check Pending status.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert. You can change the frequency of detector processing to control the evaluation frequency.

Possible uses of this alert

- Monitoring DB2 database integrity and consistency

Related topics

- Alert concepts and procedures

DB2 Table Definition Incomplete alert

Responding to this alert Alert dialog box Help

This alert monitors DB2 tables to ensure they are completely defined. The alert triggers for any of the following reasons. The table may lack:

- a primary index
- a required index on a row ID
- a required index on a unique key
- an auxiliary table or auxiliary index for an LOB column

Note: This alert is renamed in this version. In the former DB2 Agent, this alert was called DB2 Table No Primary Key Index Status alert.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

You do not need to change the trigger values except for the severity you desire for this alert. The alert triggers when the agent finds a flag in the Status field of the SYSIBM.SYSTABLES table.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring DB2 database integrity and consistency

Related topics

- Alert concepts and procedures

DB2 Table Rows Usage alert

Responding to this alert Alert dialog box Help

This alert monitors tables for the number of rows.

Enabled by default
Yes. All DB2 alerts are enabled by default.

Monitored resources (source)
The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Owner	The owners of the tables you want to monitor.
Table	The tables you want to monitor.

Trigger values
The number of rows in a table.

Evaluation frequency (schedule)
The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert
- Monitoring DB2 space utilization and trends

Related topics
- Alert concepts and procedures

DB2 Tablespace Check Data Return Code alert

Responding to this alert Alert dialog box Help

This alert monitors detector-initiated Check Data execution.

Enabled by default
Yes. All DB2 alerts are enabled by default.

Monitored resources (source)
The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.

Trigger values
The alert triggers when Check Data fails during the course of detector processing.

Evaluation frequency (schedule)
The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert
- Monitoring DB2 database integrity and consistency

Related topics
- Responding to this alert
- Alert concepts and procedures

DB2 Tablespace Check Pending Scope alert

Responding to this alert Alert dialog box Help

This alert monitors table spaces for Check Pending status at a level other than the entire table space.

Enabled by default
Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.

Trigger values

The alert triggers when the agent finds a table space in Check Pending status for a set of resources less than the entire table space.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert. You can change the detector frequency to control evaluation frequency.

Possible uses of this alert

- Monitoring DB2 database integrity and consistency

Related topics

- Alert concepts and procedures

DB2 Tablespace Check Pending Status alert

Responding to this alert Alert dialog box Help

This alert monitors table spaces in Check Pending status.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Owner	The owners of tables you want to monitor.
Table	The tables you want to monitor.

Trigger values

The alert triggers when the agent finds a table space in Check Pending status.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring DB2 database integrity and consistency

Related topics

- Alert concepts and procedures

DB2 Tablespace Lack Partitioned Index Status alert

Responding to this alert Alert dialog box Help

This alert monitors partitioned table spaces to ensure they have partitioned indexes.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.

Trigger values

The alert triggers when the agent finds a partitioned table space without a partitioned index.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring DB2 database integrity and consistency

Related topics

- Alert concepts and procedures

DB2 Tablespace No Table Status alert

Responding to this alert Alert dialog box Help

This alert monitors table spaces for No Table Status.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.

Trigger values

The alert triggers when the agent finds a table space in No Table Status.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring DB2 database integrity and consistency

Related topics

- Alert concepts and procedures

DB2 Tablespace Partition Check Pending alert

Responding to this alert Alert dialog box Help

This alert monitors table space partitions for Check Pending status.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

The alert triggers when the agent finds a table space partition in Check Pending status.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring DB2 database integrity and consistency

Related topics

- Alert concepts and procedures

DB2 Tablespace Partition Percent Active Table alert

Responding to this alert Alert dialog box Help

This alert monitors the percentage of tables in a table space partition that are active (rather than dropped). A low percentage indicates a problem.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

The alert triggers when a partitioned table space has a low percentage of space occupied by active tables rather than dropped tables whose space has not been recovered.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring databases for dropped tables

Related topics

- Alert concepts and procedures

DB2 Tablespace Partition Percent Dropped Table alert

Responding to this alert Alert dialog box Help

This alert monitors the space in a table space partition belonging to tables that are dropped.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

The alert triggers when the percentage of space used by dropped tables exceeds a threshold.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring databases for dropped tables

Related topics

- Alert concepts and procedures

DB2 Tablespace Partition Percent Rows Far From Original alert

Responding to this alert Alert dialog box Help

This alert monitors table spaces that may require reorganization.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

The alert triggers for a percentage of rows relocated far from their original position.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring for reorganization candidates

Related topics

- Alert concepts and procedures

DB2 Tablespace Partition Percent Rows Near Original alert

Responding to this alert Alert dialog box Help

This alert monitors table spaces that may need reorganization.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

The alert triggers when a percentage of rows have been relocated near their original position.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring for reorganization candidates

Related topics

- Alert concepts and procedures

DB2 Tablespace Partition Rows alert

Responding to this alert Alert dialog box Help

This alert monitors the number of rows in individual DB2 tablespace partitions.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values
Specify the number of rows that should trigger various alert levels. Increasing number of rows should trigger alerts of increasing severity.

Evaluation frequency (schedule)
The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert
- Monitoring DB2 space utilization and trends

Related topics
- Alert concepts and procedures

DB2 Tablespace Partition Rows Far From Original alert

Responding to this alert Alert dialog box Help

This alert monitors for reorganization candidates.

Enabled by default
Yes. All DB2 alerts are enabled by default.

Monitored resources (source)
The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values
The alert triggers when the number of rows relocated far from their original position exceeds a threshold.

Evaluation frequency (schedule)
The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert
- Monitoring for reorganization candidates

Related topics
- Alert concepts and procedures

DB2 Tablespace Partition Rows Near Original alert

Responding to this alert Alert dialog box Help

This alert monitors for possible reorganization candidates.

Enabled by default
Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

The alert triggers when the number of rows relocated near their original position exceeds a threshold.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring for reorganization candidates

Related topics

- Alert concepts and procedures

DB2 Tablespace Partition Space alert

Responding to this alert Alert dialog box Help

This alert monitors the allocated space for individual DB2 table space partitions.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the table space you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a table space data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

Specify the size of the table space in kilobytes (KB) that should trigger various alert levels. Increasing partition size should trigger alerts of increasing severity.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Monitoring DB2 space utilization and trends

Related topics

- Alert concepts and procedures

DB2 Tablespace RUNSTATS Return Code alert

Responding to this alert Alert dialog box Help

This alert monitors RUNSTATS execution during scheduled detector processing.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.
Partition	The name of the partition you want to monitor. A partition typically maps to a tablespace data set. Use wildcards to specify multiple partitions. (Note that these partitions are for DB2 running on MVS. Partitions are conceptually different in UDB, the open-systems version of DB2.)

Trigger values

The alert triggers when a detector-initiated RUNSTATS has a non-zero return code.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- DB2: Monitoring DB2 RUNSTATS execution

Related topics

- Alert concepts and procedures

DB2 Tablespace Space Usage alert

Responding to this alert Alert dialog box Help

This alert monitors the allocated space for individual DB2 tablespaces.

Enabled by default

Yes. All DB2 alerts are enabled by default.

Monitored resources (source)

The alert monitors the following resources.

Subsystem	The name of the DB2 subsystem you want to monitor. Use wildcards to specify multiple subsystems.
Database	The name of the DB2 database you want to monitor. Use wildcards to specify multiple databases.
Tablespace	The name of the tablespace you want to monitor. Use wildcards to specify multiple tablespaces.

Trigger values

Specify the size of the tablespace in kilobytes (KB) that should trigger various alert levels. Increasing tablespace size should trigger alerts of increasing severity. To convert default values in kilobytes to megabytes or gigabytes, see the conversion table.

Evaluation frequency (schedule)

The alert continuously monitors the trigger values. You cannot change the schedule of this alert.

Actual evaluation frequency depends on how often the detector statistics are collected. The more frequently you run detector statistics, the more often the alert will check up-to-date data.

Possible uses of this alert

- Monitoring DB2 space utilization and trends

Related topics

- Alert concepts and procedures

Storage Agent for Celerra alert

Responding to Celerra alerts Alert dialog box Help

The Storage Agent for Celerra alert triggers when the status of the Celerra has changed.

The alert message is displayed in the Active Alerts panel, is formatted with variables, and may contain additional text not described in this topic. The alert name is the formal name of the alert and can be viewed by navigating to *Administration, Alert Management, Alert Templates, <AgentName>, <AlertType>*.

Alert name	Alert message	Alert type	Default frequency	Default conditions	Descriptions	Agents issued for	Enable by default
Celerra Agent Unit Status Changes	The status of the Celerra is *state*	State	Every three minutes	Triggered by TRUE for all levels.	The status of the Celerra has changed.	Storage Agent for Celerra for Windows Storage Agent for Celerra for Solaris	No.

Related topics

- Storage Agent for Celerra overview
- Storage Agent for Celerra administration
- Responding to the Storage Agent for Celerra alert
- Storage Agent for Celerra data collection policies

Database Agent for Oracle alerts

Database Agent for Oracle Space alerts

The Oracle Space alerts trigger when the size of one of the following managed objects reaches or exceeds a value that you set.

The alert message is displayed in the Active Alerts panel, is formatted with variables, and may contain additional text not described in this topic. The alert name is the formal name of the alert and can be viewed by navigating to *Administration, Alert Management, Alert Templates, <AgentName>, <AlertType>*.

Alert name	Alert message	Alert type	Default frequency	Default conditions	Descriptions	Agents issued For	Enable by default
Table Size % Used	Table Used percent for sid table : value	Count	Every Hour	Fatal = 75 Critical = 50 Warning = 40 Minor = 30 Harmless = 25	Table Percentage Used.	Database Agent for Oracle for Windows Database Agent for Oracle for Solaris	No.
Table Blocks % Free	Table Blocks Free(%) for sid table : value	Count	Every Hour	Fatal = 10 Critical = 15 Warning = 30 Minor = 80 Harmless = 100	Percentage of free table blocks.	Database Agent for Oracle for Windows Database Agent for Oracle for Solaris	No.
Index Extents % Used	Index extents Used percent for sid index: value	Count	Every Hour	Fatal = 75 Critical = 50 Warning = 40 Minor = 30 Harmless = 25	Percentage of the index extents that are used.	Database Agent for Oracle for Windows Database Agent for Oracle for Solaris	No.
Used Megs	Tablespace used Megabytes for sid tablespace: value	Count	Every Hour	Fatal = 2000 Critical = 1000 Warning = 500 Minor = 100 Harmless = 50	Space used in a tablespace (in MB).	Database Agent for Oracle for Windows Database Agent for Oracle for Solaris	No.
Used % of Tablespace	Tablespace used Percent for sid tablespace: value	Count	Every Hour	Fatal = 75 Critical = 50 Warning = 40 Minor = 30 Harmless = 25	Percentage of space in the tablespace that is used.	Database Agent for Oracle for Windows Database Agent for Oracle for Solaris	No.
Free Megs in Tablespace	Tablespace Megabytes free for sid tablespace: value	Count	Every 6 Hours	Fatal = 20 Critical = 40 Warning = 100 Minor = 500 Harmless = 600	Free space in a tablespace (in MB).	Database Agent for Oracle for Windows Database Agent for Oracle for Solaris	No.

Free % of Tablespace	Tablespace Free % for sid tablespace: value	Count	Every Hour	Fatal = 10 Critical = 15 Warning = 30 Minor = 80 Harmless = 100	Free Space in a tablespace as a percentage of the tablespace.	Database Agent for Oracle for Windows Database Agent for Oracle for Solaris	No.
Used % of total SID datafiles space	Total Tablespace percent of SID sid tablespace: value	Count	Every Hour	Fatal = 75 Critical = 50 Warning = 40 Minor = 30 Harmless = 25	Total Space allocated to a tablespace as a percentage of the space used by SID data files space.	Database Agent for Oracle for Windows Database Agent for Oracle for Solaris	No.

Related topics

- Database Agent for Oracle overview
- Database Agent for Oracle administration
- Database Agent for Oracle data collection policies
- Responding to Database Agent for Oracle Space alerts
- Database Agent for Oracle Environment alerts
- Responding to Database Agent for Oracle Environment alerts

Database Agent for Oracle Environment alert

Responding to Oracle environment alerts Alert dialog box Help

The Oracle Environment alerts trigger when an Oracle component reaches or exceeds a value that you set or the state of the managed object changes.

The alert message is displayed in the Active Alerts panel, is formatted with variables, and may contain additional text not described in this topic. The alert name is the formal name of the alert and can be viewed by navigating to *Administration, Alert Management, Alert Templates, <AgentName>, <AlertType>*.

Alert name	Alert message	Alert type	Default frequency	Default conditions	Descriptions	Agents issued for	Enable by default
Oracle SID Up	Oracle SID is up for *sid*	State	Every Hour	Triggered by TRUE for all levels.	The Oracle database has come up.	Database Agent for Oracle for Windows Database Agent for Oracle for Solaris	No.
Oracle SID Down	Oracle SID is down for *sid*	State	Every Hour	Triggered by TRUE for all levels.	The Oracle database has gone down.	Database Agent for Oracle for Windows Database Agent for Oracle for Solaris	No.

Oracle Error	Oracle Error error found in SID sid	State	Every Hour	Triggered by TRUE for all levels.	For local SIDs only. The SID has experienced the specified Oracle error.	Database Agent for Oracle for Windows Database Agent for Oracle for Solaris	No.
Count of Oracle Errors	Oracle Error error in SID sid occurs value times	Count	Every Hour	Fatal = 21 Critical = 11 Warning = 5 Minor = 4 Harmless = 0	Count of the Oracle errors encountered .	Database Agent for Oracle for Windows Database Agent for Oracle for Solaris	No.
Num Chained Rows	Chained Rows for sid table: value	Count	Every Hour	Fatal = 55 Critical = 30 Warning = 20 Minor = 10 Harmless = 5	Number of Chained rows within the table.	Database Agent for Oracle for Windows Database Agent for Oracle for Solaris	No.
User Connected to Oracle	User Connected SID sid oracleid osid	State	Every Hour	Triggered by TRUE for all levels.	Oracle user/OS user has connected to system.	Database Agent for Oracle for Windows Database Agent for Oracle for Solaris	No.

Related topics

- Database Agent for Oracle overview
- Database Agent for Oracle administration
- Database Agent for Oracle data collection policies
- Database Agent for Oracle Space alerts
- Responding to Database Agent for Oracle Space alerts
- Responding to Database Agent for Oracle Environment alerts

Host Agents for AIX, HP-UX, and Solaris

UNIX: Disk Space Free on a File System alert

Responding to this alert Alert dialog box Help

The Disk Space Free on a File System alert triggers when the megabytes of free disk space on a file system on a UNIX host fall below a value that you set.

Enabled by default

Yes.

Monitored resource (source)

The alert monitors the following resource.

File system name	The file system that will be monitored.

Trigger values

Trigger values are specified in megabytes. The alert triggers if the size of the free space on the specified file system is less than a pre-defined trigger value at the time the agent checks for the alert condition.

Evaluation frequency (schedule)

By default, the agent is set up to check the size every 15 minutes.

Possible uses of this alert

- Monitoring available storage space on a file system or host
- Predictive analysis of when new storage space will be needed on the host

Related topics

- Responding to storage space-related alerts
- Alert concepts and procedures
- Monitoring AIX, HP-UX, and Solaris hosts
- Host Agents for AIX, HP-UX, and Solaris overview

UNIX: Disk Space Percent Free on the File System alert

Responding to this alert Alert dialog box Help

The Disk Space Percent Free on the File System alert triggers when the percentage of free disk space on a file system on a UNIX host fall below a value that you set.

Enabled by default

Yes.

Monitored resource (source)

The alert monitors the following resource.

File system name	The file system that will be monitored.

Trigger values

Trigger values for the alert are specified as percentages. The alert triggers if the percentage of free space on the specified file system is less than a pre-defined trigger value at the time the agent checks for the alert condition.

Evaluation frequency (schedule)

By default, the agent is set up to check the size every 15 minutes.

Possible uses of this alert

- Monitoring available storage space on a file system or host
- Predictive analysis of when new storage space will be needed on the host

Related topics

- Responding to storage space-related alerts
- Alert concepts and procedures
- Monitoring AIX, HP-UX, and Solaris hosts
- Host Agents for AIX, HP-UX, and Solaris overview

UNIX: File and Directory Size alert

Responding to this alert Alert dialog box Help

The File and Directory Size alert triggers when a monitored file or directory reaches a specified size in kilobytes.

Enabled by default

No.

Monitored resource (source)

The alert monitors the following resource.

File or directory name	The file or directory that you want to monitor.

Trigger values

The trigger values are specified in kilobytes. The alert triggers if the size of the file or directory specified is greater than the pre-defined trigger value(s) at the time the agent checks for the alert condition.

Evaluation frequency (schedule)

By default, the agent is set up to check the size at 10 pm.

Possible uses of this alert

- Monitoring files and directories on UNIX hosts
- Preventing system log files from growing too large
- Monitoring the size of a flat file database
- Monitoring the amount of storage space consumed by a user or application

Related topics

- Responding to storage space-related alerts
- Monitoring files and directories on UNIX hosts
- Alert concepts and procedures
- Monitoring AIX, HP-UX, and Solaris hosts
- Host Agents for AIX, HP-UX, and Solaris overview

UNIX: Hard Quotas: Free Disk Space or Files alerts

Responding to this alert Alert dialog box Help

This topic covers the alerts:

Free Hard Quota of Disk Space

Percentage of Free Hard Quota of Disk Space

Free Hard Quota of Files

Percentage of Free Hard Quota of Files

The hard quota alerts trigger when a user's hard quota of free disk space or files, or percentage thereof, reaches a specific percent or size in megabytes on a specified file system.

Enabled by default

No.

Monitored resource (source)

The alerts monitor the following resources.

File system name	The file system name that will be monitored.
User name	The user name that will be monitored.

Trigger values

The trigger values are specified in megabytes (MGR.Quota.DiskSpace.Hard and MGR.Quota.File.Hard) or percentages (MGR.Quota.DiskSpace.PctHard and MGR.Quota.File.PctHard) depending on the alert. Individual alerts trigger if the storage space consumed by the user reaches or surpasses the set trigger values of a preset hard quota on the file system.

Evaluation frequency (schedule)

By default, the agent is set up to check these alerts every three hours.

Possible uses of this alert

- Managing users and groups on UNIX hosts
- Monitoring the amount of storage space consumed by a user

Related alerts

- Soft Quotas: Free Disk Space or Files alerts

Related topics

- Responding to storage space-related alerts
- Managing users and groups on UNIX hosts
- Alert concepts and procedures
- Monitoring AIX, HP-UX, and Solaris hosts
- Host Agents for AIX, HP-UX, and Solaris overview

UNIX: Soft Quotas: Free Disk Space or Files alerts

Responding to this alert Alert dialog box Help

This topic covers the alerts:

Free Soft Quota of Disk Space

Percentage of Free Soft Quota of Disk Space

Free Soft Quota of Files

Percentage of Free Soft Quota of Files

These alerts trigger when a user's soft quota of free disk space or files, or percentage thereof, reaches a specific percent or size in megabytes on a specified file system.

Enabled by default

No.

Monitored resource (source)

The alerts monitor the following resources.

File system name	The file system name that will be monitored.
User name	The user name that will be monitored.

Trigger values

The trigger values are specified in megabytes (MGR.Quota.DiskSpace.Soft and MGR.Quota.File.Soft) or percentages (MGR.Quota.DiskSpace.PctSoft and MGR.Quota.File.PctSoft) depending on the alert. Individual alerts trigger if the storage space consumed by the user reaches the set trigger values of a preset soft quota limit on the file system.

Evaluation frequency (schedule)

By default, the agent is set up to check these alerts every three hours.

Possible uses of this alert

- Managing users and groups on UNIX hosts
- Monitoring the amount of storage space consumed by a user

Related alerts

- Hard Quotas: Free Disk Space or Files alerts

Related topics

- Responding to storage space-related alerts
- Alert concepts and procedures
- Monitoring AIX, HP-UX, and Solaris hosts
- Host Agents for AIX, HP-UX, and Solaris overview

UNIX: Inodes (files) Free on the File System alert

Responding to this alert Alert dialog box Help

This alert monitors the number of free inodes (files) available to a specified file system.

Enabled by default

Yes.

Monitored resource (source)

The alert monitors the following resource.

File system name	The file system that will be monitored.

Trigger values

The alert triggers if the number of free inodes on the specified file system is less than the trigger value at the time the agent checks for the alert condition. The trigger values are specified as whole numbers.

Evaluation frequency (schedule)

By default, the agent is set up to check the available inodes every 15 minutes.

Possible uses of this alert

- Managing file systems on UNIX hosts
- Monitoring the amount of inodes available to end users and applications

Related topics

- Responding to storage space-related alerts
- Managing file systems on UNIX hosts
- Alert concepts and procedures
- Monitoring AIX, HP-UX, and Solaris hosts
- Host Agents for AIX, HP-UX, and Solaris overview

UNIX: Swap Space Megabytes Free alert

Responding to this alert Alert dialog box Help

The Swap Space Megabytes Free alert triggers when the megabytes of swap space available on a UNIX host fall below a value that you set.

Enabled by default

Yes.

Monitored resource (source)

The alert monitors the following resource.

Swap space name	The swap space that will be monitored. A value of asterisk (*) monitors all swap spaces. Individual swap spaces can be monitored by entering the swap space device name into this field. See the Note below to learn more about identifying swap space devices.

Trigger values

The alert triggers if the megabytes of available swap space are less than a specified trigger value at the time the agent checks for the alert condition. The trigger values are specified in megabytes.

Evaluation frequency (schedule)

By default, the agent is set up to check the available swap space every 15 minutes.

Possible uses of this alert

- Monitoring host system performance and health

Note

- To find the swap spaces that you can monitor, see Exploring page spaces on UNIX hosts or use ControlCenter to execute one of the following commands using a superuser account:
  - Solaris: `/usr/sbin/swap -l` The name of the device is listed under "swapfile."
  - HP-UX: `/usr/sbin/swapinfo -m` The name of the device is listed under "NAME."
  - AIX: `/usr/sbin/lsps -a` The name of the device is listed under "Page Space"

Related topics

- Responding to swap space related performance alerts
- Alert concepts and procedures
- Monitoring AIX, HP-UX, and Solaris hosts
- Host Agents for AIX, HP-UX, and Solaris overview

UNIX: Swap Space Percent Free alert

Responding to this alert Alert dialog box Help

The Swap Space Percent Free alert triggers when the percentage of available swap space on a UNIX host fall below a value that you set.

Enabled by default

Yes.

Monitored resource (source)

The alert monitors the following resource.

Swap space name	The swap space that will be monitored. A value of * monitors all swap spaces. Individual swap spaces can be monitored by entering the swap space device name into this field. See the Note below to learn more about identifying swap space devices.

Trigger values

The alert triggers if the percentage of megabytes of available swap space are less than a specified trigger value at the time the agent checks for the alert condition. The trigger values are specified as percentages.

Evaluation frequency (schedule)

By default, the agent is set up to check the percentage of available swap space every 15 minutes.

Possible uses of this alert

- Monitoring host system performance and health

Note

- To find the swap spaces that you can monitor, see Exploring page spaces on UNIX hosts or use ControlCenter to execute one of the following commands using a superuser account:
  - Solaris: `/usr/sbin/swap -l` The name of the device is listed under "swapfile."
  - HP-UX: `/usr/sbin/swapinfo -m` The name of the device is listed under "NAME."
  - AIX: `/usr/sbin/lsps -a` The name of the device is listed under "Page Space"

Related topics

- Responding to swap space related performance alerts
- Alert concepts and procedures
- Monitoring AIX, HP-UX, and Solaris hosts
- Host Agents for AIX, HP-UX, and Solaris overview

Solaris: VERITAS Disk Group Free Space alerts

Responding to this alert Alert dialog box Help

This topic covers the alerts:

MB Free VERITAS Disk Group Disk Space

Percent Free VERITAS Disk Group Space

The VERITAS Disk Group Free Space alerts monitor the megabytes or percentage of free disk space available on a VERITAS disk group.

Enabled by default

Yes.

Monitored resource (source)

The alert monitors the following resource.

VERITAS disk group name	The VERITAS disk group that will be monitored.

Trigger values

These alerts trigger if the megabytes or percentage of free disk space available on a VERITAS disk group are less than a specified trigger value at the time the agent checks for the alert condition. The trigger values are specified in megabytes (MGR.VXDiskGroup.Space.FreeSpace) or as percentages (MGR.VXDiskGroup.Space.PctFreeSpace).

Evaluation frequency (schedule)

By default, the agent is set up to check the megabytes or percentage of free disk space available on a VERITAS disk group every 15 minutes.

Possible uses of this alert

- Monitoring available storage space on a VERITAS disk group
- Predictive analysis of when new storage space will be needed on the host

Related topics

- Responding to storage space-related alerts
- Alert concepts and procedures
- Monitoring AIX, HP-UX, and Solaris hosts
- Host Agents for AIX, HP-UX, and Solaris overview

UNIX: Volume Group Megabytes of Disk Space Free alert

Responding to this alert Alert dialog box Help

This topic covers the alerts:

MB Free Volume Group Disk Space (MGR.VolumeGroup.Space.FreeSpace)

Percent Free Volume Group Space (MGR.VolumeGroup.Space.PctFreeSpace)

The Volume Group Free Space alerts monitor the megabytes or percentage of free disk space available on a volume group.

Enabled by default

Yes.

Monitored resource (source)

The alert monitors the following resource.

Volume group name	The name of the volume group that will be monitored.

Trigger values

These alerts trigger if the megabytes or percentage of free disk space available on a volume group are less than a specified trigger value at the time the agent checks for the alert condition. The trigger values are specified in megabytes (MGR.VolumeGroup.Space.FreeSpace) or as percentages (MGR.VolumeGroup.Space.PctFreeSpace).

Evaluation frequency (schedule)

By default, the agent is set up to check the megabytes or percentage of free disk space available on a volume group every 15 minutes.

Possible uses of this alert

- Monitoring available storage space on a volume group
- Predictive analysis of when new storage space will be needed on a host or to a volume group

Related topics

- Responding to storage space-related alerts
- Alert concepts and procedures
- Monitoring AIX, HP-UX, and Solaris hosts
- Host Agents for AIX, HP-UX, and Solaris overview

Host Agent for MVS HSM

MVS HSM: ARC0003I Task Abended alert

Responding to this alert Alert dialog box Help

This alert indicates that a task ended abnormally. Unless this alert appears repeatedly, it is probably nothing to be concerned about. If it appears repeatedly, then you have a condition in HSM triggering abends.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the HSM host ID on which the agent is installed.

Trigger values
This alert triggers when an abend is detected in HSM.

Evaluation frequency (schedule)
The agent checks for this condition based on an internal schedule that you cannot adjust.

Possible uses for this alert
- Monitoring for unusual conditions that cause repeated abends. Typically one particular task or job will be causing the abends when you see several in a short span of time.

Related topics
- Alert concepts and procedures

MVS HSM: ARC0004I User Exit Abended alert

Responding to this alert Alert dialog box Help

This alert notifies you that a user exit caused an abnormal end. Check the user exit for errors.

Enabled by default
Yes

Monitored resource (source)
This alert monitors the HSM host ID designated when the agent was installed.

Trigger values
This alert triggers when this condition is detected on a host for the agent.

Evaluation frequency (schedule)
The agent checks for this condition based on its internal settings, which cannot be adjusted.

Possible uses for this alert
- Monitoring for user exit abends

Related topics
Alert concepts and procedures

MVS HSM: ARC0007I General Volume Pool alert

Responding to this alert Alert dialog box Help

This alert issues when HSM Agent detects no volumes in the HSM JES3 general pool.

Enabled by default
Yes

Monitored resource (source)
This alert monitors the HSM host ID on which the agent is installed.

Trigger values
When this message is detected, the alert triggers.

Evaluation frequency (schedule)
This alert is monitored by the agent based on internal settings and cannot be adjusted.

Possible uses for this alert
- Monitoring for lack of volumes in the HSM JES3 general pool

Related topics
- Alert concepts and procedures

MVS HSM: ARC0011I JES3 Volume Pool Failure alert

Responding to this alert Alert dialog box Help

This alert issues when the JES3 volume pool in HSM has too many volumes in it.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the HSM host ID for this message to appear.

Trigger values

This alert triggers when HSM issues the message.

Evaluation frequency (schedule)

This alert checks for this condition based on internal settings, and cannot be adjusted.

Possible uses for this alert

- Notifying the HSM administrator when a JES3 volume pool failure occurs

Related topics

- Alert concepts and procedures

MVS HSM: ARC0014I VTOC Interface Abend alert

Responding to this alert Alert dialog box Help

This alert issues when there is a problem between the VTOC interface and HSM.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the HSM host ID for this message to appear.

Trigger values

This alert triggers when this message is detected.

Evaluation frequency (schedule)

This alert is agent-controlled, and its frequency cannot be adjusted.

Possible uses for this alert

- Receiving notification of VTOC interface to HSM failures

Related topics

- Alert concepts and procedures

MVS HSM: ARC0015I DFDSS Load Failure alert

Responding to this alert Alert dialog box Help

This alert issues when HSM fails to load DFDSS.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the HSM host ID for the host on which its agent is installed.

Trigger values
This alert triggers when this message is detected in the JES2 log.

Evaluation frequency (schedule)
The frequency with which the agent checks for this message is regulated by the agent and cannot be adjusted.

Possible uses for this alert
- Detecting HSM failures to load the DFDSS

Related topics
- Alert concepts and procedures

MVS HSM: ARC0023I Journal Control Read Failed alert

Responding to this alert Alert dialog box Help

This alert issues when a read error occurs in one of the HSM journal data sets.

Enabled by default
Yes

Monitored resource (source)
This alert monitors the HSM host ID on which the agent is installed.

Trigger values
When HSM Agent detects this message, it issues the alert.

Evaluation frequency (schedule)
This alert runs based on internal agent settings and cannot be adjusted.

Possible uses for this alert
- Tracking this HSM message, so the HSM administrator can correct the problem

Related topics
- Alert concepts and procedures

MVS HSM: ARC0026I Journaling Disabled alert

Responding to this alert Alert dialog box Help

This alert issues when an HSM's journal is disabled. When this happens, you must take immediate action. HSM will not carry out another task until it is able to record entries to the journal again.

Enabled by default
Yes

Monitored resource (source)
This alert monitors the HSM host ID for this message to appear.

Trigger values
If this message is detected, the agent issues the alert.

Evaluation frequency (schedule)
This alert is agent-controlled and runs based on the agent's internal scheduling.

Possible uses for this alert
- Keeping your HSM journal healthy; HSM cannot process jobs if its journal is disabled and will generate a backlog of work until the administrator takes action.

Related topics

- Alert concepts and procedures

MVS HSM: ARC0133I OCDS Open Failure alert

Responding to this alert Alert dialog box Help

This alert issues when the offline control data set (OCDS) fails to open.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the HSM host ID for this message to appear.

Trigger values

This alert triggers when the corresponding message appears in the JES2 log.

Evaluation frequency (schedule)

This alert is agent-controlled, and its schedule cannot be adjusted.

Possible uses for this alert

- Notifying the HSM administrator when an OCDS does not open

Related topics

- Alert concepts and procedures

MVS HSM: ARC0134I BCDS Open Failure alert

Responding to this alert Alert dialog box Help

This alert issues when the backup control data set (BCDS) fails to open.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the HSM host ID for this message to appear.

Trigger values

This alert triggers when the corresponding message appears in the JES2 log.

Evaluation frequency (schedule)

This alert is agent-controlled, and its schedule cannot be adjusted.

Possible uses for this alert

- Notifying the HSM administrator when a BCDS does not open

Related topics

- Alert concepts and procedures

MVS HSM: ARC0187I CDS IO Error alert

Responding to this alert Alert dialog box Help

This alert triggers in response to a detected I/O error occurring in an HSM control data set (CDS).

Enabled by default

Yes

Monitored resource (source)

There are no settings to edit with this alert. You can modify the severity of the alert.

Trigger values

This alert issues when the agent detects this message has been issued.

Evaluation frequency (schedule)

This condition is checked for based on the agent's internal settings, and cannot be adjusted.

Possible uses for this alert

- Determining when I/O errors occur in an HSM CDS

Related topics

- Alert concepts and procedures

MVS HSM: ARC0188I Error Deleting CDS Record alert

Responding to this alert Alert dialog box Help

This alert indicates that HSM attempted to delete a record from one of its control data sets (CDSs), and an error occurred when it tried deleting the record.

Enabled by default

Yes

Monitored resource (source)

There are no settings to edit for this alert. You can change the severity of the alert.

Trigger values

When this message is detected in the HSM log, the agent issues an alert.

Evaluation frequency (schedule)

This alert condition is checked for based on the agent's internal settings.

Possible uses for this alert

- Monitoring for ARC0188I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0298I Volume Processing Halted alert

Responding to this alert Alert dialog box Help

This alert indicates that there are problems with a volume that HSM attempted to process, leading to an abend. The HSM administrator should check the volume for problems.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but the severity of the alert can be changed.

Trigger values

This alert triggers when an ARC0298I message is detected in the HSM logs.

Evaluation frequency (schedule)

The agent checks for this alert based on internal settings.

Possible uses for this alert

- Notifying the HSM administrator of volumes that are causing problems during HSM processing. Since a volume that abends probably will not have its data migrated or backed up, the administrator should inspect the volume in question to determine the root cause.

Related topics

- Alert concepts and procedures

MVS HSM: ARC0299I Volume Not Processed alert

Responding to this alert Alert dialog box Help

This alert indicates a volume was not processed by HSM because of earlier abends (abnormal ends) caused by that volume.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but the severity of the alert can be changed.

Trigger values

This alert triggers when the ARC0299I message is detected in the HSM log files.

Evaluation frequency (schedule)

This alert is agent-controlled, and the agent monitors for this alert based on internal settings.

Possible uses for this alert

- Monitoring for ARC0299I messages. This alert indicates that a particular volume has problems that are preventing HSM processing from taking place on that volume.

Related topics

- Alert concepts and procedures

MVS HSM: ARC0315I OCDS Not Defined alert

Responding to this alert Alert dialog box Help

This alert issues in response to the absence of an offline control data set (OCDS) for HSM to record its activity.

Enabled by default

Yes

Monitored resource (source)

There are no settings to edit with this alert, but the severity of the alert can be changed.

Trigger values

This alert triggers in response to the agent detecting an ARC0315I message in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled and checked for based on the agent's internal settings.

Possible uses for this alert

- Monitoring for ARC0315I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0316I Recall Exit Failed alert

Responding to this alert Alert dialog box Help

This alert issues when the RECALL installation exit reports a bad value.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can change the severity level of the alert.

Trigger values

This alert triggers in response to ARC0316I messages appearing in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert

- Monitoring for ARC0316I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0317I Recall Exit Abended alert

Responding to this alert Alert dialog box Help

This alert issues when an installation RECALL exit abnormally ends (abends).

Enabled by default

Yes

Monitored resource (source)

This agent does not have any settings to configure, but you can adjust the severity of the alert.

Trigger values

This alert triggers in response to ARC0317I messages appearing in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be modified.

Possible uses for this alert

- Monitoring for ARC0317I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0331I SDSP In Use alert

Responding to this alert Alert dialog box Help

This alert issues when HSM does not dump data sets to a migration level 1 (ML1) volume because the SDSP on the volume is in use by the migration.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can adjust the severity level of the alert.

Trigger values
This alert triggers in response to ARC0331I messages appearing in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert
- Monitoring for ARC0331I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0335I Volume Not Unpinned alert

Responding to this alert Alert dialog box Help

This alert issues in response to HSM finding a volume it cannot unpin.

Enabled by default
Yes

Monitored resource (source)
There are no settings to configure in this alert. You can modify the severity level of the alert.

Trigger values
This alert triggers when HSM Agent detects ARC0335I in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and the agent determines when to check for the alert. You cannot modify the scheduling.

Possible uses for this alert
- Detecting ARC0335I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0355I CDS IO Error alert

Responding to this alert Alert dialog box Help

This alert triggers when an I/O error occurs in one of the HSM control data sets (CDSs).

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to configure, but you can adjust the severity level of the alert.

Trigger values
This alert triggers when it detects ARC0355I messages in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert
- Monitoring for ARC0355I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0359I RACF TapVol Error alert

Responding to this alert Alert dialog box Help

This alert issues in response to HSM finding an error when attempting to update the RACF tape volume set for HSM volumes.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can adjust the severity level of the alert.

Trigger values

This alert triggers in response to detection of ARC0359I messages in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert

- Monitoring for ARC0359I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0367I Recall Task Disabled alert

Responding to this alert Alert dialog box Help

This alert issues when a recall task has been disabled because of an error unallocating a data set.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to modify, but you can change the severity level of the alert.

Trigger values

This alert triggers when ARC0367I messages are detected.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be modified.

Possible uses for this alert

- Detecting ARC0367I messages.

Related topics

- Alert concepts and procedures

MVS HSM: ARC0378I Tape Inconsistency alert

Responding to this alert Alert dialog box Help

This alert issues in response to an inconsistency between a tape volume and the HSM tape table of contents (TTOC) record.

Enabled by default

Yes

Monitored resource (source)
This alert has no settings to modify, but you can adjust the severity of the alert.

Trigger values
This alert triggers in response to ARC0378I messages being detected in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert
- Monitoring for ARC0378I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0379I Tape Invalid Block Count alert

Responding to this alert Alert dialog box Help

This alert issues in response to an inconsistency being found between the HSM Tape Table of Contents (TTOC) and the tape volume based on an invalid block count.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to modify, but you can adjust the severity of the alert.

Trigger values
This alert issues in response to ARC0379I messages being found in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert
- Monitoring the HSM logs for ARC0379I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0382I RACF Profile Error alert

Responding to this alert Alert dialog box Help

This alert issues when a RACF profile update fails.

Enabled by default
Yes

Monitored resource (source)
There are no settings to adjust in this alert, but you can alter the severity level of the alert.

Trigger values
This alert triggers when it detects ARC0382I messages in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and internal settings control when it checks for this condition.

Possible uses for this alert

- Monitoring for ARC0382I messages on your HSM hosts

Related topics

- Alert concepts and procedures

MVS HSM: ARC0383I Dataset Recovered Without RACF alert

Responding to this alert Alert dialog box Help

This alert issues when a RACF-associated data set is recovered without its RACF profile.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can modify the severity level of the alert.

Trigger values

This alert triggers in response to ARC0383I messages in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be modified.

Possible uses for this alert

- Monitoring for ARC0383I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0385I Fail To Set RACF alert

Responding to this alert Alert dialog box Help

This alert issues when HSM fails to set the catalog RACF indicator for a discretely protected VSAM data set.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to modify, but you can change the severity level of the alert.

Trigger values

This alert triggers when ARC0385I messages are detected in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert

- Monitoring for ARC0385I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0404I VTOC Access Failure alert

Responding to this alert Alert dialog box Help

This alert triggers in response to a VTOC access failure by HSM.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings that you can adjust, but you can change the severity level of the alert.

Trigger values
This alert triggers when ARC0404I messages are detected in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling is regulated by the agent.

Possible uses for this alert
- Monitoring for ARC0404I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0409I VTOC Read Failure alert

Responding to this alert Alert dialog box Help

This alert issues in response to VTOC read errors and failures being found in the HSM logs.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to adjust, but you can modify the severity of the alert.

Trigger values
This alert appears when ARC0409I messages are found in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and this condition is checked for based on the agent's internal settings.

Possible uses for this alert
- Detecting ARC0409I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0424I Failed alert

Responding to this alert Alert dialog box Help

This alert issues when the copy of a tape volume fails.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to edit, but you can adjust the severity level of the alerts.

Trigger values
This alert triggers in response to ARC0424I messages appearing in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert
- Monitoring for ARC0424I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0425I Alternate Failure alert

Responding to this alert Alert dialog box Help
This alert issues if the creation of a copy of a tape volume failed.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to configure, but you can adjust the severity of the alert.

Trigger values
This alert triggers in response to ARC0425I messages appearing in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert
- Monitoring for ARC0425I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0431I TTOC Chain Failure alert

Responding to this alert Alert dialog box Help
This alert issues when the agent detects chaining errors in tape table of contents (TTOC) records.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to adjust, but you can change the severity level of the alert.

Trigger values
This alert triggers when it detects ARC0431I messages in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert
- Monitoring for ARC0431I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0432I TTOC Update Failure alert

Responding to this alert Alert dialog box Help

This alert issues when a tape table of contents (TTOC) update failure occurs during an HSM TAPEREPLACE operation.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings that you can modify, but the severity level of the alert can be changed.

Trigger values

This alert triggers when the agent finds ARC0432I messages in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert

- Monitoring the HSM logs for ARC0432I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0440I TapeVol Bad Data alert

Responding to this alert Alert dialog box Help

This alert issues when a tape has been positioned incorrectly.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings that you can modify, but its severity level can be adjusted.

Trigger values

This alert triggers in response to ARC0440I messages that appear in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert

- Detecting ARC044OI messages in the log files

Related topics

- Alert concepts and procedures

MVS HSM: ARC0450I Invalid Tape DSN alert

Responding to this alert Alert dialog box Help

This alert issues when an invalid CDD is found during HSM RECYCLE processing.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to adjust, but you can modify the level of severity.

Trigger values
This alert triggers in response to ARC0450I messages appearing in the HSM logs.

Evaluation frequency (schedule)
The scheduling of this alert is agent-controlled and cannot be modified.

Possible uses for this alert
- Detecting ARC0450I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0501I IO Error on VTOC alert

Responding to this alert Alert dialog box Help

This alert issues when an I/O error occurs during processing of a volume table of contents (VTOC).

Enabled by default
Yes

Monitored resource (source)
This alert has no settings for you to adjust, but you can change the severity level of the alert.

Trigger values
This alert triggers when ARC0501 messages are detected in the HSM logs.

Evaluation frequency (schedule)
This alert's scheduling is agent-controlled,

Possible uses for this alert
- Monitoring for ARC0501 messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0502I User Exit Abend alert

Responding to this alert Alert dialog box Help

This alert issues when an abnormal end (ABEND) occurs in an installation exit.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to modify, but you can change the severity level of the alert.

Trigger values
This alert triggers in response to ARC0502I messages appearing in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be modified.

Possible uses for this alert
- Monitor for ARC0502I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0514I CDS Error During Migration alert

Responding to this alert Alert dialog box Help

This alert issues if HSM fails to update a control data set during migration.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can adjust the severity level of the alerts.

Trigger values

This alert triggers when ARC0514I messages are detected in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its settings cannot be adjusted.

Possible uses for this alert

- Monitoring for ARC0514I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0532I Migration Terminated alert

Responding to this alert Alert dialog box Help

This alert indicates that HSM terminated migration to tape because of an error accessing the control data set.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can adjust the severity level of the alert.

Trigger values

This alert triggers in response to ARC0532I messages appearing in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert

- Monitoring for ARC0532I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0534I Migration Held alert

Responding to this alert Alert dialog box Help

This alert indicates HSM is holding the migration function.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to change, but you can alter the severity level of the alert.

Trigger values
This alert triggers in response to ARC0534I messages appearing in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert
- Monitoring for ARC0534I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0539I Migration Held SDSP Error alert

Responding to this alert Alert dialog box Help

This alert issues when HSM holds the migration function because of excessive I/O errors attempting to determine whether recall needs an SDSP.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to adjust, but you can modify the severity level of the alert.

Trigger values
This alert triggers in response to ARC0539I messages appearing in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its settings cannot be adjusted.

Possible uses for this alert
- Monitoring for ARC0539I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0541I SDSP Errors alert

Responding to this alert Alert dialog box Help

This alert issues when HSM is unable to process an SDSP data set.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to configure, but you can adjust the severity level of the alert.

Trigger values
This alert triggers in response to ARC0541I messages appearing in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert
- Monitoring for ARC0541I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0543I Volume Not Processed alert

Responding to this alert Alert dialog box Help

This alert issues when a volume is not processed because of an error reading the migration control data set (MCDS) volume record.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to adjust, but you can modify the severity level of the alert.

Trigger values

This alert triggers when ARC0543I messages are detected in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert

- Monitoring for ARC0543I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0547I TapeVol failed DELVOL alert

Responding to this alert Alert dialog box Help

This alert issues when HSM is unable to indicate that a data set migration made a tape volume ineligible for DELVOL processing.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can adjust the severity level of its alerts.

Trigger values

This alert triggers in response to ARC0547I messages appearing in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert

- Monitoring for ARC0547I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0554I VTOC Opened Failed alert

Responding to this alert Alert dialog box Help

This alert issues if HSM cannot open a volume table of contents (VTOC).

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to adjust, but you can modify the severity level of the alert.

Trigger values

This alert triggers when ARC0554I messages are found in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert

- Detecting ARC0554I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0560E Migration Limited alert

Responding to this alert Alert dialog box Help

This alert indicates that HSM has limited migration.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to modify, but you can adjust the severity of the alert.

Trigger values

This alert triggers when ARC0560E messages are found in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be modified.

Possible uses for this alert

- Detecting ACR0560E messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0570I Process Terminated alert

Responding to this alert Alert dialog box Help

This alert indicates that an HSM function has terminated because of an error.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings that you can modify, but the severity level of the alert can be changed.

Trigger values

This alert triggers in response to ARC0570I messages appearing in the HSM logs.

Evaluation frequency (schedule)

The scheduling of this alert is agent-controlled and cannot be altered.

Possible uses for this alert

- Monitoring for ARC0570I messages.

Related topics

- Alert concepts and procedures

MVS HSM: ARC0584I SDSP IO Failed alert

Responding to this alert Alert dialog box Help

This alert indicates that an error occurred when HSM accessed a record in an SDSP data set.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can adjust the severity level of the alert.

Trigger values

This alert triggers in response to ARC0584I messages appearing in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling is not configurable.

Possible uses for this alert

- Detecting ARC0584I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0624I Volume Halted alert

Responding to this alert Alert dialog box Help

This alert issues when HSM terminates processing of a volume.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can adjust the severity level.

Trigger values

This alert triggers when ARC0624I messages are detected in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert

- Monitoring for ARC0624I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0625I Auto Dump Halted alert

Responding to this alert Alert dialog box Help

This alert issues when HSM terminates the automatic dump function before it has completed.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to adjust, but the severity level of the alert can be adjusted.

Trigger values
This alert triggers when ARC0625I messages are detected in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert
- Monitoring for ARC0625I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0626I Process Failed alert

Responding to this alert Alert dialog box Help

This alert issues if HSM terminates the dump or restore of a volume because of an error accessing a control data set record.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to configure, but you can adjust the severity level of the alert.

Trigger values
This alert triggers when ARC0626I messages are detected.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert
- Detecting ARC0626I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0627I System Timer INOP alert

Responding to this alert Alert dialog box Help

This alert issues when HSM cannot perform the automatic dump function because the system timer is not operating.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to configure, but you can adjust the severity of the alert.

Trigger values
This alert triggers in response to ARC0627I messages appearing in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert
- Monitoring for ARC0627I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0634I Failed Restart alert

Responding to this alert Alert dialog box Help

This alert issues when HSM cannot restart its automatic dump function because the current time is not in the automatic dump window.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can adjust the severity of the alert.

Trigger values

This alert triggers when the agent detects ARC0634I messages in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled and its scheduling cannot be adjusted.

Possible uses for this alert

- Monitoring for ARC0634I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0647I Held alert

Responding to this alert Alert dialog box Help

This alert issues when HSM holds automatic dumps because no more space is available on migration level 1 (ML1) volumes for the VTOC copy data sets.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can adjust the severity of the alert.

Trigger values

This alert triggers when ARC0647I messages are detected in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert

- Monitoring for ARC0647I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0682I Expirebv Terminated alert

Responding to this alert Alert dialog box Help

This alert indicates that the HSM EXPIREBV function has terminated early.

Enabled by default

Yes

Monitored resource (source)
This alert has no settings to configure, but you can adjust the severity level of the alert.

Trigger values
This alert triggers when ARC0628I messages are detected in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert
- Detecting ARC0682I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0702I Spill Terminated alert

Responding to this alert Alert dialog box Help

This alert indicates that BACKUP or SPILL processing of a volume terminated early.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to configure, but you can adjust the severity level of the alert.

Trigger values
This alert triggers when ARC0702I messages are detected in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert
- Monitoring for ARC0702I messages

Related alerts
- ARC703I Spill Terminated alert

Related topics
- Alert concepts and procedures

MVS HSM: ARC0703I Spill Terminated alert

Responding to this alert Alert dialog box Help

This alert issues when BACKUP or SPILL processing terminates early because of an allocation failure.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to configure, but you can adjust the severity level of the alert.

Trigger values
This alert triggers when ARC0703I messages are found in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its schedule cannot be altered.

Possible uses for this alert

- Monitoring for ARC0703I messages

Related alerts

- ARC0702I Spill Terminated alert

Related topics

- Alert concepts and procedures

MVS HSM: ARC0704I Process Terminated alert

Responding to this alert Alert dialog box Help

This alert issues when HSM terminates processing of a volume because of a volume table of contents (VTOC) copy-related error.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can alter the severity level of the alert.

Trigger values

This alert triggers in response to ARC0704I messages appearing in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert

- Monitoring for ARC0704I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0705I Process Terminated ML1VTOC alert

Responding to this alert Alert dialog box Help

This alert issues when HSM terminates backup or dump of a volume because there is no migration level 1 (ML1) space for the volume table of contents (VTOC) copy data set.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can alter the severity level of the alert.

Trigger values

This alert triggers in response to ARC0705I messages appearing in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert

- Monitoring for ARC0705I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0706I Process Term TgtVol alert

Responding to this alert Alert dialog box Help

This alert issues when backup of a volume terminates because no backup volume is available.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can alter the severity level of the alert.

Trigger values

This alert triggers in response to ARC0706I messages appearing in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert

- Monitoring for ARC0706I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0708I Process Terminated Storage alert

Responding to this alert Alert dialog box Help

This alert issues when processing of a volume is terminated because of a GETMAIN or FREEMAIN error.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can alter the severity level of the alert.

Trigger values

This alert triggers in response to ARC0708I messages appearing in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert

- Monitoring for ARC0708I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0710I MIG2BACK Process Terminated alert

Responding to this alert Alert dialog box Help

This alert issues when HSM terminates backup of migrated data sets or movement of backup versions because of allocation failures.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to configure, but you can alter the severity level of the alert.

Trigger values
This alert triggers in response to ARC0710I messages appearing in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert
- Monitoring for ARC0710I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0711I MIG2BACK Process Terminated alert

Responding to this alert Alert dialog box Help

This alert issues when HSM terminates backup of migrated data sets or movement of backup versions because of an error accessing a control data set.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to configure, but you can alter the severity level of the alert.

Trigger values
This alert triggers in response to ARC0711I messages appearing in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert
- Monitoring for ARC0711I messages

Related topics
- Alert concepts and procedures

MVS HSM: ARC0730I Volume Process Terminated alert

Responding to this alert Alert dialog box Help

This alert issues when HSM terminates processing of a volume because of an error accessing a control data set.

Enabled by default
Yes

Monitored resource (source)
This alert has no settings to configure, but you can alter the severity level of the alert.

Trigger values
This alert triggers in response to ARC0730I messages appearing in the HSM logs.

Evaluation frequency (schedule)
This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert

- Monitoring for ARC0730I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0733I Volume Process Terminated alert

Responding to this alert Alert dialog box Help

This alert indicates that HSM ended a backup of migrated data sets or movement of backup versions because of an error accessing a control data set.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can alter the severity level of the alert.

Trigger values

This alert triggers in response to ARC0733I messages appearing in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert

- Monitoring for ARC0733I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0738I Task Failed Backup Held alert

Responding to this alert Alert dialog box Help

This alert indicates that HSM has disabled backups due to an error in a control task.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can alter the severity level of the alert.

Trigger values

This alert triggers in response to ARC0738I messages appearing in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert

- Monitoring for ARC0738I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0739I Volume Process Terminated alert

Responding to this alert Alert dialog box Help

This alert issues when HSM terminates processing of a volume because of an error reading a JFCB.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can alter the severity level of the alert.

Trigger values

This alert triggers in response to ARC0739I messages appearing in the HSM logs.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert

- Monitoring for ARC0739I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0744I All Functions Held alert

Responding to this alert Alert dialog box Help

This alert issues when the HSM Agent notices a CDS backup failure and all functions being held.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the HSM host on which it is installed. You do not have to specify a source for the alert to monitor.

Trigger values

This alert triggers when the ARC0744I message appears. Setting the alert to True activates it, and setting the alert to False deactivates it. You can also adjust the severity level of the alert.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses for this alert

- Detecting ARC0744I messages

Related topics

- Alert concepts and procedures

MVS HSM: ARC0747I alert

Responding to this alert Alert dialog box Help

HSM backed up a CDS, but when it attempted to write that CDS to disk, a problem was encountered, such as a data set name with the same name or a problem with the catalog on that disk.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the HSM host ID assigned when you installed the agent.

Trigger values

This alert triggers when this condition is found on an HSM host.

Evaluation frequency (schedule)

This alert is agent-controlled, and checks based on internal settings in the agent.

Possible uses for this alert

- Notifying you when there is a problem with HSM handling a CDS

Related topics

- Alert concepts and procedures

MVS HSM: Automatic Backup Failed alert

Responding to this alert Alert dialog box Help

This alert issues when an automatic backup on an HSM host either fails to run as scheduled or fails to complete.

Enabled by default

Yes

Monitored resource (source)

This alert monitors all hosts running HSM.

Trigger values

When this condition is detected on an HSM host, an alert is issued to notify the administrator.

Evaluation frequency (schedule)

This alert runs every Sunday at 4 a.m., but you can adjust the time when this condition is checked.

Possible uses for this alert

- Preventing backlogs of backup jobs and backup jobs that run into production time.

Related alerts

- MVS HSM: Automatic Dump Failed alert

Related topics

- General alert concepts and procedures

MVS HSM: Automatic Dump Failed alert

Responding to this alert Alert dialog box Help

Use this alert to notify you when an automatic dump on a host running HSM fails to run when scheduled or fails to complete successfully.

Enabled by default

Yes

Monitored resource (source)

This alert monitors HSM hosts for an automatic dump failure condition.

Trigger values

When this condition is found on a host, the alert triggers.

Evaluation frequency (schedule)

This alert runs every Sunday at 4 a.m. You can change the time and how often this alert condition is checked.

Possible uses for this alert

- Preventing automatic dump failures from going unnoticed. It helps protect against job backlogs.

Related alerts

- MVS HSM: Automatic Backup Failed alert

Related topics

- General alert concepts and procedures

MVS HSM: CDS Backup Failed alert

Responding to this alert Alert dialog box Help

This alert notifies you that the control data sets (CDSs) backup did not complete successfully, or the number of records moved during backup decreased more than you specified in the HSM Agent setup dialogs.

CDSs consist of three types of data sets: backup CDSs, migration CDSs, and offline CDSs. Backup CDSs record all HSM-related activity.

Enabled by default

Yes

Monitored resource (source)

This agent monitors the one-character Host ID assigned to the host when HSM Agent was installed.

Trigger values

When this condition is detected on an HSM host, the alert triggers.

Evaluation frequency (schedule)

The default is to check every day at 4 a.m., but you can modify the frequency in the alert.

Possible uses for this alert

- Correcting backup failures of CDSs. CDSs are critical to the successful operation of HSM, especially since HSM cannot operate without these data sets functioning properly.

Related alerts

- MVS HSM: CDS Alerts Setup

Related topics

- General alert concepts and procedures

MVS HSM: HSM Address Space Inactive alert

Responding to this alert Alert dialog box Help

This alert issues when the HSM address space is inactive. Because of the journaling activity in HSM, it needs to remain active at all times to prevent loss of data and jobs not being carried out such as data migrations and expirations.

Enabled by default

Yes

Monitored resource (source)

This alert monitors hosts you designate that their HSM address space remains active. If the agent detects the address space is inactive, it issues an alert.

Trigger values

This alert triggers when an HSM address space on a designated host is inactive.

Evaluation frequency (schedule)

By default the HSM Agent checks every five minutes to verify the address space is active. You can adjust the frequency with which it checks this condition.

Possible uses for this alert

- Keeping HSM address spaces active and to prevent work backlogs and missed batch processing.

Related topics

- General alert concepts and procedures

MVS HSM: User-Defined Alert

Responding to this alert Alert dialog box Help

This alert allows you to detect HSM ARC messages not already defined in alerts within the Host Agent for MVS HSM. You can also use this alert to detect other message IDs, too.

Enabled by default

No

Monitored resource (source)

This alert monitors the HSM host on which it is installed. You do not have to specify a source for this alert.

Trigger values

This alert triggers in response to ARC messages you define as needing monitoring. This alert has no settings to configure, but you can alter the severity level of the alert. Setting the alert to True turns it on, and setting it to False turns it off.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be changed.

Possible uses for this alert

- Monitoring for any ARC messages not already defined in alerts within the agent

Related alerts

- MVS HSM: User Specified alert

Related topics

- General alert concepts and procedures

MVS HSM: ML1/ML2 Space Usage alert

Responding to this alert Alert dialog box Help

This alert automates the extracting of HSM control data set MCV records that are summarized in history file records.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the HSM host on which it is installed. You do not have to specify a source for this alert.

Trigger values

This alert triggers when the following return codes appear:

- 1
- 4
- 8
- 12

This alert works on a True/False mechanism. Setting an alert condition to False deactivates the alert.

Evaluation frequency (schedule)

This alert's default scheduling is to run daily at midnight. You can adjust the scheduling.

Possible uses for this alert

Use this alert to automate the extraction of HSM control data set MCV records.

Related topics

- General alert concepts and procedures

MVS HSM: Primary Space Management Failed alert

Responding to this alert Alert dialog box Help

This alert monitors primary space management failures and issues an alert when primary space management failures are detected or when primary space management fails to complete.

Enabled by default

Yes

Monitored resource (source)

This alert monitors all hosts running HSM.

Trigger values

This alert triggers when primary space management on a host running HSM fails.

Evaluation frequency (schedule)

This alert checks every Sunday at 4 a.m. for primary space management failures. You can modify this alert to occur more or less frequently.

Possible uses for this alert

- Monitoring for primary space management failures

Related alerts

- MVS HSM: Secondary Space Management Failed alert

Related topics

- General alert concepts and procedures

MVS HSM: Secondary Space Management Failed alert

Responding to this alert Alert dialog box Help

This alert issues when secondary space management in HSM either fails to run on schedule or runs but does not complete successfully.

Enabled by default

Yes

Monitored resource (source)

This alert monitors all hosts running HSM and issues an alert when this condition is found.

Trigger values

This alert triggers when this failure is detected on a host running HSM.

Evaluation frequency (schedule)

This alert runs every Sunday at 4 a.m., but you can adjust the alert to run less or more frequently.

Possible uses for this alert

- Verifying that secondary space management is carried out successfully

Related alerts

- MVS HSM: Primary Space Management Failed alert

Related topics

- General alert concepts and procedures

MVS HSM: User-Specified alert

Responding to this alert Alert dialog box Help

This alert allows you to issue an alert when a specific HSM message appears in the JES2 log. HSM Agent reports on several alerts, so check the list before using this feature. The message you want an alert issued in response to may already have a predefined alert available for it.

Enabled by default

No

Monitored resource (source)

This alert monitors for the HSM message that you designate, and issues an alert when it is detected.

Trigger values

This alert triggers when the condition, in this case the issuing of an HSM message, is true.

Evaluation frequency (schedule)

This alert is agent controlled, so the agent will check as often as internal settings designate.

Possible uses for this alert

- Monitoring for an HSM condition for which an alert does not already exist

Related alerts

- MVS HSM: User Defined alert

Related topics

- General alert concepts and procedures

Host Agent for MVS SMS

MVS SMS: DASD Init alert

Responding to this alert Alert dialog box Help

This alert issues if DASD volumes are initialized. This alert is informational only.

Enabled by default

No

Monitored resource (source)

This alert monitors the SMS agent on which it is installed. You do not have to specify a source for this alert.

Trigger values

This alert triggers when DASD volumes are initialized. Setting the alert to True activates it, and False deactivates it.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Receive notifications when DASD volumes are initialized

Related topics

- Alert concepts and procedures

MVS SMS: IGD011I alert

Responding to this alert Alert dialog box Help

This alert issues if an IGD011I message appears in the JES2 log, indicating that an SMS parameter record with a certain member name contains ACDS or command names that conflict with current commands.

Enabled by default

Yes

Monitored resource (source)

This alert monitors an OS/390 host running SMS. It has no settings to configure, but you can adjust the severity level of the alert. This alert monitors the host on which it is installed without requiring configuration.

Trigger value

This alert triggers when an IGD011I message is detected. You can deactivate the alert by setting its value to False. It is set to True by default.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Monitoring for IGD011I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD008I alert

Responding to this alert Alert dialog box Help

This alert issues when message IGD008I appears in the JES2 log. This alert indicates that a new configuration has been activated from an SMS control dataset (SCDS). The dataset name of the SCDS is specified in the actual error message.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to configure, but you can adjust the severity level of the alert.

Trigger value

When enabled, this alert triggers if IGD008I messages are found in the JES2 log.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Monitoring for IGD008I messages indicating that a new SCDS dataset has been activated

Related topics

- Alert concepts and procedures

MVS SMS: IGD022I alert

Responding to this alert Alert dialog box Help

This alert indicates that message IGD022I has been found in the JES2 log. This indicates that the SMS address space failed and is restarting.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host it is installed on and requires no configuration. You can adjust the severity level of the alert.

Trigger value

This alert triggers when IGD022I messages are detected. Setting the alert to True activates it, and setting it to False deactivates it.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Detecting IGD022I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD023I alert

Responding to this alert Alert dialog box Help

This alert issues if an IGD023I message appears in the JES2 log. This message indicates that one or more errors have been detected in the SMS address space with a return and reason code being provided in the message itself.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. It has no settings to configure, but you can adjust the severity level of the alert.

Trigger value

This alert triggers when an IGD023I message is detected. Setting the alert to True activates it, and the JES2 log is monitored for this message, and setting it to False deactivates it.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Detecting IGD023I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD013I alert

Responding to this alert Alert dialog box Help

This alert issues if an IGD013I message is detected in the JES2 log. This message indicates that an abend occurred during the processing of a command

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed and requires no configuration to run. You can adjust the severity level of the alert.

Trigger value

This alert triggers when an IGD013I message is found. Specifying True activates the alert, and specifying False deactivates it.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Detecting IGD013I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD058I alert

Responding to this alert Alert dialog box Help

This alert issues if an IGD058I message is detected in the JES2 log. This message indicates that an unexpected error occurred with an SCDS, ACDS, or COMMDS.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert triggers when it detects an IGD058I message. Setting the alert to True activates the alert, and setting it to False deactivates it. You can adjust the severity level of the alert.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Detecting IGD058I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD049I alert

Responding to this alert Alert dialog box Help

This alert issues if an IGD049I message appears in the JES2 log. This message indicates that an activate failed because an SCDS or ACDS contains an invalid configuration.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert trigges when an IGD049I message appears. It works on a True/False mechanism. Setting the alert to True activates it, and setting it to False deactivates it. You can adjust the severity level of the alert.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Detecting IGD049I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD044I alert

Responding to this alert Alert dialog box Help

This alert indicates that an IGD044I message has been generated. This message indicates that a SCDS, ACDS, or COMMDS dataset supports more than eight systems and cannot be accessed on this system.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert. You can adjust the severity level of the alert.

Trigger value

This alert triggers when an IGD044I message appears in the JES2 log. Setting the alert to True activates it, and setting the alert to False deactivates it.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Monitoring for IGD044I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD045I alert

Responding to this alert Alert dialog box Help

This alert issues if an IGD045I message is detected in the JES2 log. This alert indicates that an activate failed. Either a system has been defined as a system group, or a system group has been defined as a system in the configuration.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert triggers when message IGD045I appears. Setting the alert to True activates it, and setting it to False deactivates it. You can also adjust the severity level of the alert.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Detecting IGD045I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD041I alert

Responding to this alert Alert dialog box Help

This alert issues if an IGD041I message appears in the JES2 log. It indicates that an I/O error for an SCDS, ACDS, or COMMDS dataset has occurred.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source. You can adjust the severity level of the alert.

Trigger value

This alert triggers in response to detecting IGD041I messages. Setting the alert to True activates it, and setting it to False deactivates it.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Detecting IGD041I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD059I alert

Responding to this alert Alert dialog box Help

This alert issues if an IGD059I message appears in the JES2 log. This message indicates that DFSMS was unable to allocate any storage for SMS Trace table.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert issues when message IGD059I is detected. Setting the alert to True activates it, and setting it to False deactivates it. You can adjust the severity level of the alert.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Detecting IGD059I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD025I alert

Responding to this alert Alert dialog box Help

This alert issues if an IGD025I message is detected, meaning that SMS failed to start because of an unexpected error in initialization processing.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert. You can adjust the severity level of this alert.

Trigger value

This alert triggers when an IGD025I message appears in the JES2 log. Setting the alert to True activates it, and setting the alert to False deactivates it.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling is not adjustable.

Possible uses of this alert

- Monitoring for IGD025I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD072A alert

Responding to this alert Alert dialog box Help

This alert issues if an IGD072A message appears in the JES2 log. This message indicates that a previously active COMMDS could not be updated with a new COMMDS.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert triggers when message IGD072A is detected. Setting the alert to True activates it, and setting the alert to False deactivates it.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling is not adjustable.

Possible uses of this alert

- Detecting IGD072A messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD021I alert

Responding to this alert Alert dialog box Help

This alert issues when an IGD021I message appears in the JES2 log. This alert indicates that SMS failed to start. The message in the JES2 log will include the return code and reason code for the failure.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. It has no settings to configure, but you can adjust the severity level of the alert.

Trigger value

This alert triggers when IGD021I messages are detected. Setting the alert to True activates it, and setting it to False deactivates it.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Monitoring for IGD021I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD042I alert

Responding to this alert Alert dialog box Help

This alert issues if an IGD042I message appears in the JES2 log. It indicates that a COMMDS dataset name was successfully repaired. This is an informational message.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert to monitor. You can also adjust the severity level of the alert.

Trigger value

This alert triggers when the agent detects an IGD042I message in the log. Setting the alert to True activates it, and setting the alert to False deactivates it.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be modified.

Possible uses of this alert

- Monitoring for IGD042I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD07001I alert

Responding to this alert Alert dialog box Help

This alert issues if IGD07001I appears in the JES2 log. This alert indicates that a GDG Roll In error occurred.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert triggers when an IGD07001I message is detected. Setting the alert to True activates it, and setting the alert to False deactivates it. You can adjust the severity level of the alert.

Evaluation frequency (schedule)

This alert is agent-controlled, and its settings cannot be adjusted.

Possible uses of this alert

- Detecting IGD07001I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD060I alert

Responding to this alert Alert dialog box Help

This alert issues if message IGD060I appears in the JES2 log. It indicates that DFSMS was unable to allocate the SMS Trace table.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert triggers when it detects messages IGD060I. Setting the alert to True activates it, and setting the alert to False deactivates it.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Detecting IGD060I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD051I alert

Responding to this alert Alert dialog box Help

This alert issues if message IGD051I appears in the JES2 log. This message indicates that a failed installation exit is now deactivated.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert triggers in response to finding IGD051I messages. Setting the alert to True activates it, and setting it to False deactivates it. You can adjust the severity level of this alert.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Detecting IGD051I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD306I alert

Responding to this alert Alert dialog box Help

This alert issues if message IGD306I appears in the JES2 log. This message indicates an unexpected error occurred during processing.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert triggers when IGD306I is detected. Setting the alert to True activates it, and setting it to False deactivates it. You can adjust the severity level of this alert.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Detecting IGD306I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD307I alert

Responding to this alert Alert dialog box Help

This alert issues if message IGD307I appears in the JES2 log. This alert indicates that a dataset allocation request failed, meaning that there was an error in the installation exit.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert triggers when IG307I is detected. Setting the alert to True activates it, and setting it to False deactivates it. You can change the severity level of the alert.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

Use this alert to detect IGD307I messages.

Related topics

Alert concepts and procedures

MVS SMS: IGD17100I alert

Responding to this alert Alert dialog box Help

This alert indicates that IGD17100I message was detected in the JES2 log. This means that an unexpected catalog error for a particular dataset occurred.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert triggers when IGD17100I is found. Setting the alert to True activates it, and setting it to False deactivates it. You can adjust the severity level of this alert.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Detecting IGD17100I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD312I alert

Responding to this alert Alert dialog box Help

This alert issues if message IGD312I appears in the JES2 log. This alert indicates that an abend occurred during SMS processing because no SDWA was available.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert triggers when IGD312I messages are detected. Setting the alert to True activates it, and setting it to False deactivates it. You can adjust the severity level of the alert.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Detecting IGD312I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD300I alert

Responding to this alert Alert dialog box Help

This alert issues if message IGD300I appears in the JES2 log. This message indicates that an abend occurred during SMS processing. If you receive multiple abends, it generally indicates that a specific job is generating the abends.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert triggers when message IGD300I is found. Setting the alert to True activates it, and setting it to False deactivates it. You can also adjust the severity level of the alert.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling is not adjustable.

Possible uses of this alert

- Detecting IGD300I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD073I alert

Responding to this alert Alert dialog box Help

This alert issues if message IGD073I appears in the JES2 log. This message indicates that an anomaly was detected in COMMDS. The reason code is listed in the actual message.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert triggers when message IGD073I is detected. Setting the alert to True activates it, and setting it to False deactivates it.

Evaluation frequency (schedule)

This alert is agent-controlled, and its settings are not adjustable.

Possible uses of this alert

- Detecting IGD073I messages

Related topics

- Alert concepts and procedures

MVS SMS: IGD311I alert

Responding to this alert Alert dialog box Help

This alert issues if message IGD311I appears in the JES2 log. This message indicates an unexpected error occurred during processing.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert.

Trigger value

This alert triggers when IGD311I is detected. Setting the alert to True activates it, and setting it to False deactivates it. You can adjust the severity level of this alert.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling cannot be adjusted.

Possible uses of this alert

- Detecting IGD311I messages

Related topics

- Alert concepts and procedures

MVS SMS: Occupancy alert

Responding to this alert Alert dialog box Help

This alert issues when a storage group reaches a certain occupancy percentage.

Enabled by default

Yes

Monitored resource (source)

This alert monitors all storage groups on the SMS host on which it is active, and issues alerts when storage groups begin running out of space.

Trigger value

This alert triggers when storage space is approaching a user-defined threshold. Setting the alert to True activates it, and setting it to False deactivates it.

Evaluation frequency (schedule)

This alert by default checks for this condition on its SMS host hourly. You can adjust the frequency of this inspection.

Possible uses of this alert

- Monitoring storage groups for declining space conditions

Related topics

- Alert concepts and procedures

MVS SMS: Quiesce alert

Responding to this alert Alert dialog box Help

This alert issues notifications as the amount of free space in a storage group of quiesced volumes declines.

Enabled by default

Yes

Monitored resource (source)

This alert monitors the SMS host on which it is installed and issues alerts when storage group space reaches certain thresholds. You do not need to specify a source for this alert to monitor.

Trigger value

This alert triggers when the percentage of space declines beyond certain predefined amounts. This alert acts based on a True/False mechanism. Specifying True for a trigger value turns that trigger on. Specifying False deactivates that trigger. You can also modify the severity level that you want assigned to a particular alert in addition to the value of the trigger.

Evaluation frequency (schedule)

This alert's scheduling can be changed. Its default setting is to run hourly. The default percentages for alert severity are 80 percent for harmless, 65 percent for minor, 50 percent for warning, 35 percent for critical, and 20 percent for fatal. The 65 and 80 percent conditions do not trigger alerts unless you set the alert to trigger at those levels.

Possible uses of this alert

- Monitoring for diminishing storage space on quieseced automatic storage groups

Related topics

- Alert concepts and procedures

MVS SMS: SCDS Activate alert

Responding to this alert Alert dialog box Help

This alert issues if an SMS source control dataset (SCDS) configuration is activated. This indicates that any SMS-related displays may now be inaccurate because of the update.

Enabled by default

No

Monitored resource (source)

This alert monitors the SMS host on which it is installed. You do not have to specify a source for this alert to monitor.

Trigger value

This alert triggers if an SCDS configuration is activated. Setting the alert to True activates it, and setting it to False deactivates it.

Evaluation frequency (schedule)

This alert is agent-controlled, and its scheduling is not adjustable.

Possible uses of this alert

- Detecting SCDS activations that would invalidate an existing SMS display

Related topics

- Alert concepts and procedures

MVS SMS: SCDS Update alert

Responding to this alert Alert dialog box Help

This alert issues when the SMS source control dataset (SCDS) has been updated. This is an informational message.

Enabled by default

Yes

Monitored resource (source)

This alert has no settings to modify, but you can change the frequency with which the condition is monitored.

Trigger value

This alert triggers when this condition is found to be true.

Evaluation frequency (schedule)

This alert's scheduling can be modified. The default monitoring schedule is hourly.

Possible uses of this alert

- Receiving notification of updates to the SMS source control dataset (SCDS)

Related topics

- Alert concepts and procedures

Host Agent for Novell

Novell: Deleted File Space Threshold alert

Responding to this alert Alert dialog box Help

This alert triggers when the percentage of disk space used by all deleted files on a NetWare server volume exceeds a value that you specify. You can use this alert to periodically remind yourself to purge a volume's deleted files or to identify when the deleted files on a volume take up an unacceptable amount of space.

Enabled by default

Yes.

Monitored resource (source)

The alert monitors the following resources:

Server Name	The NetWare server on which the volume resides.
Volume Name	The name of the volume to be monitored.

Trigger values

This is a count alert. The alert triggers when percent of space occupied by deleted files on the specified volume reaches a value you specify. Specify the percent as a whole number less than 100 and greater than 0. Do not use percent signs or decimal points. (In other words, specify 50, not 50% or .50.)

Evaluation frequency (schedule)

By default, the agent uses a control group that checks free space percentage once per day. However, ControlCenter allows you to use whatever control group provides the level of monitoring that you want to achieve.

Possible uses of this alert

- Monitoring volumes for excessive deleted file space that can be purged and re-used for other purposes

Related topics

- Responding to the Deleted File Space Threshold alert
- Monitoring NetWare servers and file systems
- Alert concepts and procedures
- Host Agent for Novell overview

Novell: Large File alert

Responding to this alert Alert dialog box Help

This alert triggers when the size of a specified file exceeds a value that you set.

Enabled by default

No.

Monitored resource (source)

The alert monitors the following resource:

File Name	The filename and path of the file to monitor. Example: `ServerName\VolumeName\DirectoryName\FileName`

Trigger values

This is a count alert. The alert triggers when the size of a specified file reaches a value that you set. Specify the file size value as a whole number in bytes.

Evaluation frequency (schedule)

By default, the agent uses a control group that checks file size every minute. However, ControlCenter allows you to use whatever control group provides the level of monitoring that you need.

Possible uses of this alert

- Monitoring file and database sizes to prevent wasted storage space
- Creating reminders to backup or delete important log files at pre-defined file sizes

Related topics

- Compressing files on NetWare servers
- Comparing compressed and uncompressed file size on NetWare servers
- Monitoring NetWare servers and file systems
- Alert concepts and procedures
- Host Agent for Novell overview

Novell: Space Usage alert

Responding to this alert Alert dialog box Help

This alert triggers when the space that a user consumes on a specified volume meets the conditions set for the alert trigger and comparison values. For example, use this alert to monitor, but not limit, the storage space used by important users for whom a set size limit should not be applied.

Enabled by default

Yes.

Monitored resource (source)

The alert monitors the following resources:

Server Name	The NetWare server on which the volume resides.
Volume Name	The name of the volume to be monitored.
User Name	The full typeless username of the user to be monitored.

Trigger values

This is a count alert. The alert triggers when the space consumed by a user on a specified volume reaches or exceeds a value that you specify. Specify the space-used value as a whole number in megabytes (MB).

Evaluation frequency (schedule)

By default, the agent uses a control group that checks space usage once per day. However, ControlCenter allows you to use whatever control group provides the level of monitoring that you need.

Possible uses of this alert

- Monitoring the space usage of important users. You may want to use this alert to track how much space is being used by important users such as the administrator (admin) or a CEO or company president without limiting the space available to them.

You may also want to create an autofix for these alerts. See General alert topics for more information.

Related topics

- Exploring and administering user space restrictions on NetWare volumes
- Monitoring NetWare servers and file systems
- Alert concepts and procedures
- Host Agent for Novell overview

Novell: User Quota alert

Responding to this alert Alert dialog box Help

This alert triggers when a user reaches a specified percentage of quota free space remaining. You can use this alert to identify and respond to users that will soon require more storage space than their quotas allow on a volume .

Enabled by default

Yes.

Monitored resource (source)

The alert monitors the following resources:

Server Name	The NetWare server on which the volume resides.
Volume Name	The name of the volume to be monitored.
User Name	The user ID of the user to be monitored.

Trigger values

This is a count alert. The alert triggers when percentage of quota free space remaining for a user on a volume reaches a value you specify. Specify the percent as a whole number less than 100 and greater than 0. Do not use percent signs or decimal points. (In other words, specify 50, not 50% or .50.)

Evaluation frequency (schedule)

By default, the agent uses a control group that checks user quota space usage once per day. However, ControlCenter allows you to use whatever control group provides the level of monitoring that you need.

Possible uses of this alert

- Identifying users who will soon reach their quota limit
- Monitoring the space usage of key or benchmark users

Related topics

- Monitoring NetWare servers and file systems
- Alert concepts and procedures
- Host Agent for Novell overview

Novell: Volume % Free Space alert

Responding to this alert Alert dialog box Help

This alert monitors the percentage of free space on a Novell NetWare volume.

Enabled by default

Yes.

Monitored resource (source)

The alert monitors the following resources:

Server Name	The NetWare server on which the volume resides.
Volume Name	The name of the volume to be monitored.

Trigger values

This is a count alert. The alert triggers when percent of free space on the specified volume reaches a value you specify. Specify the percent as a whole number less than 100 and greater than 0. Do not use percent signs or decimal points. (In other words, specify 50, not 50% or .50.)

Evaluation frequency (schedule)

By default, the agent uses a control group that checks free space percentage every hour. Use a control group that provides the level of monitoring that you want to achieve.

Possible uses of this alert

- Monitoring volumes

Related topics

- Monitoring NetWare servers and file systems
- Alert concepts and procedures
- Host Agent for Novell overview

Novell: Volume Free Space alert

Responding to this alert Alert dialog box Help

This alert triggers when the free space on a specified volume on a NetWare server matches or drops below a value that you set. For example, you can use this alert to receive notification when the free space on critical volumes drops to dangerous or disruptive levels.

Enabled by default

Yes.

Monitored resource (source)

The alert monitors the following resources:

Server Name	The NetWare server on which the volume resides.
Volume Name	The name of the volume to be monitored.

Trigger values

This is a count alert. The alert triggers when the free space on the specified volume reaches a value you specify. Specify the free space value as a whole number in megabytes (MB).

Evaluation frequency (schedule)

By default, the agent uses a control group that checks free space every hour. However, ControlCenter allows you to use whatever control group provides the level of monitoring that you need.

Possible uses of this alert

- Monitoring volumes

Related topics

- Monitoring NetWare servers and file systems
- Alert concepts and procedures
- Host Agent for Novell overview

Host Agent for Windows

Windows: Agent-initiated event log alerts

Responding to these alerts Alert dialog box Help

These alerts trigger after the Host Agent for Windows attempts to back up or clear the system, application, or security event log. Use these alerts to receive notification on the success or failure of these operations. All of the agent-initiated alerts are enabled by default. You may want to disable the success alerts and only receive notification when the agent could not back up or clear a log.

The alerts include:

- Application Event Log Backup Completed
- Application Event Log Backup Failed
- Application Event Log Clear Completed
- Application Event Log Clear Failed
- Security Event Log Backup Completed
- Security Event Log Backup Failed
- Security Event Log Clear Completed
- Security Event Log Clear Failed
- System Event Log Backup Completed
- System Event Log Backup Failed
- System Event Log Clear Completed
- System Event Log Clear Failed

Note that these alerts only trigger when the agent is used to back up or clear an event log. You will not receive notification when other tools, such as Windows native tools, back up or clear a log.

Enabled by default

Yes

Monitored resource (source)

You do not have to specify a resource for these alerts.

Trigger values

Always set the trigger values to TRUE for these alert.

Evaluation frequency (schedule)

The agent evaluates the alerts after backing up or clearing an event log. You cannot change the schedule for these alerts.

Related alerts

- Windows: Event log size alerts

Related topics

- Windows: Monitoring event logs
- Alert concepts and procedures

Windows: Agent-initiated performance alerts

You can set up the Host Agent for Windows to periodically record various system statistics, allowing you to collect the trending information necessary for capacity planning and system tuning. The agent-initiated performance alerts trigger after the agent makes the final recording each day for the performance objects for which you have set up recordings.

The alerts include:

- Cache Recorder Complete
- Logical Storage Recorder Complete
- Memory Recorder Complete
- Page File Recorder Complete
- Physical Storage Recorder Complete
- Process Recorder Complete
- Server Recorder Complete
- Operating System Recorder Complete

Enabled by default

Yes

Monitored resource (source)

You do not have to specify a resource for these alerts.

Trigger values

Always set the trigger values to TRUE for these alert.

Evaluation frequency (schedule)

The agent triggers the alerts after completing the final performance recordings for the day. You cannot change the schedule for these alerts.

Related topics

- Windows: Recording performance statistics
- Windows: Creating baseline performance statistics
- Alert concepts and procedures

Windows: Agent-initiated service alerts

Responding to these alerts Alert dialog box Help

These alerts trigger after the agent attempts to restart a service as the result of the Execute Restart Service autofix, which is attached to the Service Failure alert. The alerts include:

- Service Restart completed
- Service Restart failed

Enabled by default

Yes

Monitored resource (source)

You do not have to specify a resource for these alerts.

Trigger values

Always set the trigger values to TRUE for these alert.

Evaluation frequency (schedule)

The agent evaluates the alerts after attempting to restart a service. You cannot change the schedule for these alerts.

Related alerts

- Windows: Service Active alert
- Windows: Service Inactive and Service Failure alerts

Related topics

- Windows: Monitoring event logs
- Alert concepts and procedures

Windows: Event logged alerts

Responding to this alert Alert dialog box Help

These alerts trigger when a specific event is written to one of the Windows event logs. The Host Agent for Windows provides alerts for the system, application, and security event logs. The agent further categorizes the alerts by event type:

- Application log: error event logged
- Application log: warning event logged
- Application log: information event logged
- System log: error event logged
- System log: warning event logged
- System log: information event logged
- Security log: audit failure event logged
- Security log: audit success event logged

You might use these alerts to receive notification of system and application errors or to help detect security breaches.

Enabled by default

No

Monitored resource (source)

The alert monitors the following resource.

Event Text	The text of the event that is posted to the log. You can use wildcards here to apply the alert to multiple events. For example, you could specify `*YourProduct*` to monitor for all events containing the string YourProduct.

Special requirements

The settings on the Event Log Monitoring dialog box affect the processing of these alerts. The dialog box allows you to specify which event types (Information, Warning, and so on) and how many hours worth of messages the agent should monitor. By default, the agent is set up to monitor the last 24 hours worth of messages for all three logs and all event types.

Trigger values

Always set the trigger value to TRUE for this alert.

Evaluation frequency (schedule)

By default, the agent is set up to check the event logs every minute.

Specify schedules in conjunction with the retention times on the Event Log Monitoring dialog box.

Possible uses of this alert

- Windows: Monitoring Windows security
- Windows: Monitoring event logs

Related alerts

- Windows: Event log size alerts

Related topics

- Alert concepts and procedures

Windows: Event log size alerts

Responding to this alert Alert dialog box Help

The Host Agent for Windows event log size alerts trigger when the size of an event log exceeds a threshold. The alerts include:

- Application Event Log Size (KB) Limit
- Security Event Log Size (KB) Limit
- System Event Log Size (KB) Limit

Use these alerts to help keep your event logs at a manageable size and to ensure you have a complete audit trail of the events occurring on your Windows server. In addition, you can attach autofixes to these alerts to automatically back up and clear the logs.

Enabled by default

Alert: Yes

Autofix: No

Monitored resource (source)

You do not have to specify a source for this alert. The event log is the source.

Trigger values

Specify trigger values in kilobytes. The alert triggers if the size of the specified log is greater than the trigger value at the time the agent checks for the alert condition.

Evaluation frequency (schedule)

By default, the agent is set up to check the size every hour. Select a schedule that provides the level of monitoring you want to achieve.

Autofixes

The agent provides two predefined autofixes for these alerts:

- Execute Clear the Event Logautomatically clears the event log when the alert is triggered.
- Execute Backup and Clear the Event Logfirst backs up the log, and then clears it.

If you select the Execute Backup and Clear the Event Log autofix, the agent saves the backup file in the agent's working directory in a folder named `\EventLogBk\`*logname*, where *logname* is the name of the log the agent is backing up. The agent uses the following format in naming the backup file: *yyyydddhhmm*`.log`, where *yyyy* is the year, *ddd* is the julian day, *hh* is the hour in 24-hour format, and *mm* is the minutes. The ControlCenter administrator can change the folder to which the agent saves the backup files.

After the agent attempts to back up or clear an event log, it triggers an alert indicating the result. See Windows: Agent-initiated event log alerts.

Use ControlCenter's security management features to restrict access to these autofixes.

Possible uses of this alert

- Windows: Monitoring event logs
- Windows: Monitoring Windows security

Related alerts

- Windows: Event logged alerts

Related topics

- Alert concepts and procedures

Windows: File Count alert

Responding to this alert Alert dialog box Help

The Host Agent for Windows File Count alert monitors the number of files in a folder. Use this alert to ensure the existence of critical application files or to help estimate user requirements.

Enabled by default

No

Monitored resource (source)

The alert monitors the following resource.

Directory Name	The name of the folder you want to monitor. You must include the full path when specifying this value, for example: `C:\Winnt\System32`. Use wild cards to monitor multiple folders.

Trigger values

Specify a numeric value. The alert triggers when the number of files in the monitored folder reaches a specific number.

Evaluation frequency (schedule)

By default, the agent checks file count every hour. Use a schedule that provides the level of monitoring that you want to achieve.

Possible uses of this alert

- Windows: Monitoring files and folders

Related alerts

- Windows: File Count alert
- Windows: File Count Change Percent alert
- Windows: File and Directory Change alerts
- Windows: File and Directory Size alerts
- Windows: File and Directory Size Change alerts
- Windows: File and Directory Size Change Percent alerts

Related topics

- Alert concepts and procedures

Windows: File Count Change alert

Responding to this alert Alert dialog box Help

The Host Agent for Windows File Count Change alert monitors how much the number of files in a folder changes. Use this alert to receive notification when the number of files drops or rises significantly.

Enabled by default

No

Monitored resource (key)

The alert monitors the following resource, also called the alert key.

Directory Name	The name of the folder you want to monitor. You must include the full path when specifying this value, for example: `C:\Winnt\System32`. Use wildcards to monitor multiple folders.

Trigger values

Specify a numeric value. The alert triggers when the number of files in the monitored folder changes by a specific number.

Evaluation frequency (schedule)

By default, the agent checks file count **every hour**. Use a schedule that provides the level of monitoring that you want to achieve.

Possible uses of this alert

- Windows: Monitoring files and folders

Related Alerts

- Windows: File Count alert
- Windows: File Count Change Percent alert
- Windows: File and Directory Changed alerts
- Windows: File and Directory Size alerts
- Windows: File and Directory Size Change alerts
- Windows: File and Directory Size Change Percent alerts

Related topics

- Alert concepts and procedures

Windows: File Count Change Percent alert

Responding to this alert Alert dialog box Help

The Host Agent for Windows File Count Change Percent alert monitors how much the number of files in a folder changes. For example, use this alert to receive notification when the number of files drops or rises by a significant percent.

Enabled by default

No

Monitored resource (source)

The alert monitors the following resource.

Directory Name	The name of the folder you want to monitor. You must include the full path when specifying this value, for example: `C:\Winnt\System32`. Use wildcards to monitor multiple folders.

Trigger values

Specify a percent (for example: 30, 40, 50). Do not use a percent sign or decimal point.

The alert triggers when the number of files in the monitored folder changes by a percent.

Evaluation frequency (schedule)

By default, the agent checks file count every hour. Use a schedule that provides the level of monitoring that you want to achieve.

Possible uses of this alert

- Windows: Monitoring files and folders

Related alerts

- Windows: File Count alert
- Windows: File Count Change alert
- Windows: File and Directory Changed alerts
- Windows: File and Directory Size alerts
- Windows: File and Directory Size Change alerts
- Windows: File and Directory Size Change Percent alerts

Related topics

- Alert concepts and procedures

Windows: File and Directory Changed alerts

Responding to this alert Alert dialog box Help

The Host Agent for Windows File and Directory Changed alerts monitor changes to files and folders. The alerts include:

- File Changed alert
- Directory Changed alert

The alerts trigger when any of the following events occurs against the file or folder you are monitoring: rename, create, delete, or an attribute change.

Do not use these alerts for files or folders that change very frequently, such as Windows' system folder. Doing so can create heavy system overhead.

Enabled by default

No

Monitored resource (source)

The following table describes the source for the Directory Changed alert.

Directory	The name of the folder you want to monitor. You must include the full path when specifying this value, for example: `C:\MyFolder\Temp\`. Use wildcards to monitor multiple folders.

The following table describes the source for the File Changed alert.

Path and File Name	The name and full path of the file you want to monitor, for example: `C:\MyFolder\myfile.txt`. Use wildcards to monitor multiple files.

Trigger values

The trigger value should always be TRUE.

Evaluation frequency (schedule)

The agent continuously monitors for file and folder changes. You cannot change the evaluation frequency.

Possible uses of this alert

- Windows: Monitoring files and folders

Related alerts

- Windows: File and Directory Size alerts
- Windows: File and Directory Size Change alerts
- Windows: File and Directory Size Change Percent alerts
- Windows: File Count alert
- Windows: File Count Change alert
- Windows: File Count Change Percent alert

Related topics

- Alert concepts and procedures

Windows: File and Directory Size alerts

Responding to this alert Alert dialog box Help

The Host Agent for Windows File and Directory Size alerts trigger when a monitored file or folder reaches a specific size. The alerts include:

- Directory Size alert
- File Size alert

Enabled by default

No

Monitored resource (source)

The following table describes the source for the Directory Size alert.

Directory Name	The name of the folder you want to monitor. You must include the full path when specifying this value, for example: `C:\Winnt\System32`. Use wildcards to monitor multiple folders.

The following table describes the source for the File Size alert.

Path and File Name	The name and full path of the file you want to monitor, for example: `C:\Winnt\System32\myfile.txt`. Use wildcards to monitor multiple files.

Trigger values

Specify the trigger values in bytes. The alerts trigger when the monitored file or folder reaches a specific size.

Evaluation frequency (schedule)

By default, the agent checks file or folder size every hour. Use a schedule that provides the level of monitoring that you want to achieve.

Possible uses of this alert

- Windows: Monitoring files and folders

Related alerts

- Windows: File and Directory Size Change alerts
- Windows: File and Directory Size Change Percent alerts
- Windows: File and Directory Change alerts
- Windows: File Count alert
- Windows: File Count Change alert
- Windows: File Count Change Percent alert

Related topics

- Alert concepts and procedures

Windows: File and Directory Size Change alerts

Responding to this alert Alert dialog box Help

The Host Agent for Windows File and Directory Size Change alerts monitor how much the size of a file or folder changes over time. Use these alerts to detect rapid growth that can impact the availability of a volume or application.

The alerts include:

- Directory Size Change
- File Size Change

Enabled by default

No

Monitored resource (source)

The following table describes the source for the Directory Size Change alert.

Directory Name	The name of the folder you want to monitor. You must include the full path when specifying this value, for example: `C:\Winnt\System32`. Use wildcards to monitor multiple folders.

The following table describes the source for the File Size Change alert.

Path and File Name	The name and full path of the file you want to monitor, for example: `C:\Winnt\System32\myfile.txt`. Use wildcards to monitor multiple file.

Trigger values

Specify the trigger values in bytes. The alerts trigger when the size of the monitored file or folder changes by a specified amount during the time interval indicated by the schedule.

Evaluation frequency (schedule)

By default, the agent checks file or folder size every six hours. Use a schedule that provides the level of monitoring that you want to achieve.

Possible uses of this alert

- Windows: Monitoring files and folders

Related alerts

- Windows: File and Directory Size alerts
- Windows: File and Directory Size Change Percent alerts
- Windows: File and Directory Change alerts
- Windows: File Count alert
- Windows: File Count Change alert
- Windows: File Count Change Percent alert

Related topics

- Alert concepts and procedures

Windows: File and Directory Size Change Percent alerts

Responding to this alert Alert dialog box Help

The Host Agent for Windows File and Directory Size Change Percent alerts monitor how much the size of a file or folder changes over time. Use these alerts to detect rapid growth that can impact the availability of a volume or application.

The alerts include:

- File Size Change Percent alert
- Directory Size Change Percent alert

Enabled by default

No

Monitored resource (source)

The following table describes the source for the Directory Size Change Percent alert.

Directory Name	The name of the folder you want to monitor. You must include the full path when specifying this value, for example: `C:\Winnt\System32`. Use wildcards to monitor multiple folders.

The following table describes the source for the File Size Change Percent alert.

Path and File Name	The name and full path of the file you want to monitor, for example: `C:\Winnt\System32\myfile.txt`. Use wildcards to monitor multiple files.

Trigger values

Specify the trigger values as percentages. The alerts trigger when the size of the monitored file or folder changes by a specified percent during the time interval indicated by the schedule.

Evaluation frequency (schedule)

By default, the agent checks file or folder size every hour. Use a schedule that provides the level of monitoring that you want to achieve.

Possible uses of this alert

- Windows: Monitoring files and folders

Related alerts

- Windows: File and Directory Size alerts
- Windows: File and Directory Size Change alerts
- Windows: File and Directory Change alerts
- Windows: File Count alert
- Windows: File Count Change alert
- Windows: File Count Change Percent alert

Related topics

- Alert concepts and procedures

Windows: Logical Volume Percent Free alert

Responding to this alert Alert dialog box Help

The Host Agent for Windows Logical Volume Percent Free alert monitors the percentage of free space on a Windows volume. Use this alert to prevent application or system outages due to insufficient disk space.

Enabled by default

No

Monitored resource (source)

The alert monitors the following resource.

Logical Volume (Drive)	The name of the volume that you want to monitor, for example, `C:` or `D:`. Use wildcards to specify multiple volumes.

Trigger values

Specify the percentage as a whole number less than or equal to 100, and greater than or equal to 0. The alert triggers when the percentage of free space on the specified volume reaches the trigger value. Do not use percent signs or decimal points. (In other words, specify 50, not 50% or .50.)

Evaluation frequency (schedule)

By default, the agent checks free space percentage every hour. Use a schedule that provides the level of monitoring that you want to achieve.

Possible uses of this alert

- Windows: Monitoring volumes

Related alerts

- Windows: Logical Volume Size Free alert
- Windows: File and Directory Size alerts
- Windows: File and Directory Size Change alerts
- Windows: File and Directory Size Change Percent alerts

Related topics

- Alert concepts and procedures

Windows: Logical Volume Size Free alert

Responding to this alert Alert dialog box Help

The Host Agent for Windows Logical Volume Size Free alert monitors the amount of free space (in megabytes) on a Windows volume.

Enabled by default

No

Monitored resource (source)

The alert monitors the following resource.

Logical Volume (Drive)	The name of the logical volume, or drive, that you want to monitor, for example `C:` or `D:`. Use wildcards to specify multiple volumes.

Trigger values

Specify the free space level, in megabytes, at which you want to be notified. For example, specify 50 if you want to be notified when there are only 50 megabytes free on the volume.

Evaluation frequency (control group)

By default, the agent checks amount of free space every hour. Select a control group that provides the level of monitoring that you want to achieve.

Possible uses of this alert

- Windows: Monitoring volumes

Related alerts

- Windows: Logical Volume Percent Free alert
- Windows: File and Directory Size alerts
- Windows: File and Directory Size Change alerts
- Windows: File and Directory Size Change Percent alerts

Related topics

- Alert concepts and procedures

Windows: Pagefile Capacity alert

Responding to this alert Alert dialog box Help

The Host Agent for Windows Pagefile Capacity alert monitors the number of times allocations from the paged pool have failed. A high number of failures can indicate that your system does not have enough physical memory or that the paging file is too small. When Windows has to expand the paging file on its own, application performance suffers drastically because the processor is devoting time to expanding the paging file.

Although this alert has default settings based on recommendations in the Microsoft documentation, you should determine acceptable performance levels at your data center and adjust the settings appropriately.

Enabled by default

No

Monitored resource (source)

The alert monitors paging file capacity. You do not have to specify a source for this alert.

Trigger values

This alert triggers when the paged pool failures exceeds a threshold you define. Set the alert's advanced settings to prevent the alert from triggering when the number of paged pool failures temporarily spikes but does not remain high.

Evaluation frequency (schedule)

ControlCenter checks the monitored counter every 10 seconds by default. Only the ControlCenter administrator can change the frequency (see more).

Possible uses of this alert

- Windows: Monitoring memory performance

Related alerts

- Windows: Memory Usage Bottleneck (Percent of I/O) alert
- Windows: Memory Usage Bottleneck (Pages Per Second) alert

Related topics

- Windows: Understanding memory management
- Windows: Performance monitoring terminology
- Windows: Creating performance baselines
- Alert concepts and procedures

Windows: Memory Usage Bottleneck (Pages Per Second) alert

Responding to this alert Alert dialog box Help

The Host Agent for Windows Memory Usage Bottleneck (Pages Per Second) alert monitors the number of pages per second occurring on the server. If the server has to devote a large amount of time to paging, the performance of services and applications suffers.

Although this alert has default settings based on recommendations in the Microsoft documentation, you should determine acceptable performance levels at your data center and adjust the settings appropriately.

Enabled by default

No

Monitored resource (source)

The alert monitors the memory object's Pages/sec counter. You do not have to specify a source.

Trigger values

This alert triggers when the memory performance object's Pages/sec counter exceeds a threshold you define. Set the alert's advanced settings to prevent the alert from triggering when paging activity temporarily spikes but does not remain high.

Evaluation frequency (schedule)

ControlCenter checks the monitored counter every 10 seconds by default. Only the ControlCenter administrator can change the frequency (see more).

Possible uses of this alert

- Windows: Monitoring memory performance

Related alerts

- Windows: Memory Usage Bottleneck (Percent of I/O) alert
- Windows: Pagefile Capacity alert

Related topics

- Windows: Understanding memory management
- Windows: Performance monitoring terminology
- Windows: Creating performance baselines
- Alert concepts and procedures

Windows: Memory Usage Bottleneck (Percent of I/O) alert

Responding to this alert Alert dialog box Help

The Host Agent for Windows Memory Usage Bottleneck (Percent of I/O) alert monitors the percentage of server I/O activity devoted to paging. When the server devotes significant time to reading from and writing to the paging file, application performance suffers because there is a smaller percentage of I/O time available.

Although this alert has default settings based on recommendations in the Microsoft documentation, you should determine acceptable performance levels at your data center and adjust the settings appropriately.

Enabled by default

No

Monitored resource (source)

The agent monitors the percent of server I/O activity devoted to paging. You do not have to specify an alert source.

Trigger values

This alert triggers when the percentage of I/O activity devoted to paging exceeds a threshold you define. The agent determines the percentage of I/O by dividing the pages per second by the rate of I/O activity to the logical disk that contains the paging file.

Use the Before and After fields on the alert definition dialog box to prevent the alert from triggering when paging activity temporarily spikes but does not remain high.

Evaluation frequency (schedule)

ControlCenter checks the monitored counter every 10 seconds by default. Only the ControlCenter administrator can change the frequency.

Possible uses of this alert

- Windows: Monitoring memory performance

Related alerts

- Windows: Memory Usage Bottleneck (Pages Per Second) alert
- Windows: Pagefile Capacity alert

Related topics

- Windows: Understanding memory management
- Windows: Performance monitoring terminology
- Windows: Creating performance baselines
- Alert concepts and procedures

Windows: Physical Disk Bottleneck (Average Transfer Rate) alert

Responding to this alert Alert Definition dialog box Help

This Host Agent for Windows alert monitors how long it takes the operating system to read from or write to a physical disk. If you create a baseline for this statistic, you can set this alert to trigger when disk performance is poor compared with the baseline.

Although this alert has default settings based on recommendations in the Microsoft documentation, you should determine acceptable performance levels at your data center and adjust the settings appropriately.

Enabled by default

No

Monitored resource (source)

The alert monitors the following resource, also referred to as the alert source.

Device Number	The index number of the physical disk you want to monitor. The base index is 0, which is also the default. Use the asterisk wildcard (*) to monitor all disks.

Special requirements

Windows NT or Windows 2000 disk performance counters must be enabled for this alert to work.

Trigger value

The alert triggers when the disk transfer rate exceeds a threshold you define. To determine the transfer rate, the agent monitors the physical disk object's Avg. Disk sec/Transfer counter.

Use the Before and After fields on the alert definition dialog box to prevent the alert from triggering when the transfer rate temporarily spikes but does not remain high.

Evaluation frequency (schedule)

The alert checks the monitored devices every 10 seconds by default. You cannot change the schedule attached to this alert. Only the ControlCenter administrator can change the frequency of the alert.

Possible uses of this alert

- Windows: Monitoring disk performance

Related alerts

- Windows: Physical Disk Bottleneck (Queue Length) alert

Related topics

- Windows: Creating baseline performance statistics
- Windows: Performance monitoring terminology
- Windows: Performance monitoring alerts
- Alert concepts and procedures

Windows: Physical Disk Bottleneck (Queue Length) alert

Responding to this alert Alert dialog box Help

This Host Agent for Windows alert monitors physical disk queues on Windows systems. A lengthy disk queue is a key indicator that a disk is not handling I/O requests sufficiently. When a disk has a long queue, system performance suffers as services and programs wait for the disk subsystem to satisfy their I/O requests.

Although this alert has default settings based on recommendations in the Microsoft documentation, determine acceptable performance levels at your data center and adjust the settings appropriately.

Enabled by default

No

Monitored resource (source)

The alert monitors the following resource, also referred to as the alert source.

Device Number	The index number of the physical disk you want to monitor. The base index is 0, which is also the default. Use the asterisk wildcard (*) to monitor multiple disks.

Special requirements

Windows NT or Windows 2000 disk performance counters must be enabled for this alert to work.

Trigger value

This alert triggers when the Avg. Disk Queue Length counter for Windows physical-disk performance object exceeds a threshold.

Use the Before and After fields on the alert definition dialog box to prevent the alert from triggering when disk activity temporarily spikes but does not remain high.

Evaluation frequency (schedule)

The alert checks the monitored devices every 10 seconds by default. You cannot change the schedule attached to this alert. Only the ControlCenter administrator can change the frequency of the alert.

Possible uses of this alert

- Windows: Monitoring disk performance

Related alerts

- Windows: Physical Disk Bottleneck (Average Transfer Rate) alert

Related topics

- Windows: Creating baseline performance statistics
- Windows: Performance monitoring terminology
- Windows: Performance monitoring alerts
- Alert concepts and procedures

Windows: Printer Changed alert

Responding to this alert Alert dialog box Help

The Host Agent for Windows Printer Changed alert triggers when a local printer is added to or deleted from the monitored Windows system. You cannot monitor network printers using this alert. Once you enable the alert, ControlCenter continuously monitors for printer changes.

Enabled by default

No

Monitored resource (source)

The alert monitors the following resource.

Printer name	The name of the local printer you want to monitor (for example: `\\myserver\myprinter`). Use wildcards to monitor multiple printers. **Note:** If the driver of a monitored printer changes, Windows changes the name of the printer to the driver name, by default. Any alerts that monitor that printer by name will no longer work. You must update the alerts.

Trigger value
Always set the trigger values to TRUE for this alert.

Evaluation frequency (schedule)
ControlCenter monitors continuously for printer changes when you enable this alert. You cannot change the evaluation frequency of this alert.

Possible uses of this alert
- Windows: Monitoring printers

Related alerts
- Windows: Printer Driver Changed alert
- Windows: Printer Job Changed alert
- Windows: Printer Port Changed alert

Related topics
- Windows: Managing printers
- Windows: Exploring printers
- Alert concepts and procedures

Windows: Printer Driver Changed alert

Responding to this alert Alert dialog box Help

This Host Agent for Windows alert triggers when a change is made to the driver of a monitored local printer. You cannot use this alert to monitor network printers. Once the alert is enabled, the agent continuously monitors for a printer driver change.

Enabled by default
No

Monitored resource (source)
The alert monitors the following resource.

Printer name	The name of the printer you want to monitor (for example: `\\myserver\myprinter`). Use wildcards to monitor multiple printers. **Note:** If the driver of a monitored printer changes, Windows changes the name of the printer to the driver name, by default. Any alerts that monitor that printer by name will no longer work. You must update the alerts.

Trigger value
Always set the trigger values to TRUE for this alert.

Evaluation frequency (schedule)
ControlCenter monitors continuously for printer changes when you enable this alert. You cannot change the evaluation frequency of this alert.

Possible uses of this alert
- Windows: Monitoring printers

Related alerts
- Windows: Printer Changed alert
- Windows: Printer Job Changed alert
- Printer Port Changed alert

Related topics
- Windows: Managing printers
- Windows: Exploring printers
- Alert concepts and procedures

Windows: Printer Job Changed alert

Responding to this alert Alert dialog box Help

This Host Agent for Windows alert triggers when a job is added to the queue of a monitored local printer. You cannot use this alert to monitor network printers. Once the alert is enabled, the agent continuously monitors for changes.

Enabled by default

No

Monitored resource (source)

The alert monitors the following resource.

Printer name	The name of the printer you want to monitor (for example: `\\myserver\myprinter`). Use wildcards to monitor multiple printers. **Note:** If the driver of a monitored printer changes, Windows changes the name of the printer to the driver name, by default. Any alerts that monitor that printer by name will no longer work. You must update the alerts.

Trigger value

Always set the trigger values to TRUE for this alert.

Evaluation frequency (schedule)

ControlCenter monitors continuously for printer changes when you enable this alert. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Windows: Monitoring printers

Related alerts

- Windows: Printer Changed alert
- Windows: Printer Driver Changed alert
- Windows: Printer Port Changed alert

Related topics

- Windows: Managing printers
- Windows: Exploring printers
- Alert concepts and procedures

Windows: Printer Port Changed alert

Responding to this alert Alert dialog box Help

This Host Agent for Windows alert triggers when the port for a monitored local printer is changed. You cannot use this alert to monitor network printers. Once the alert is enabled, the agent continuously monitors for changes.

Enabled by default

No

Monitored resource (source)

The alert monitors the following resource.

Printer name	The name of the printer you want to monitor (for example: `\\myserver\myprinter`). Use wildcards to monitor multiple printers. **Note:** If the driver of a monitored printer changes, Windows changes the name of the printer to the driver name, by default. Any alerts that monitor that printer by name will no longer work. You must update the alerts.

Trigger value

Always set the trigger values to TRUE for this alert.

Evaluation frequency (schedule)

ControlCenter monitors continuously for printer changes when you enable this alert. You cannot change the evaluation frequency of this alert.

Possible uses of this alert

- Windows: Monitoring printers

Related alerts

- Windows: Printer Changed alert
- Windows: Printer Driver Changed alert
- Windows: Printer Job Changed alert

Related topics

- Windows: Managing printers
- Windows: Exploring printers
- Alert concepts and procedures

Windows: Process Active alert

Responding to this alert Alert dialog box Help

This Host Agent for Windows alert triggers when a monitored process becomes active. You might use this alert to receive notification when a particular program starts.

Enabled by default

No

Monitored resource (source)

You must specify the following resource for this alert.

Process Name	The name of the process or processes you want to monitor (for example: `payroll.exe`). Use the asterisk wildcard (*) to monitor multiple processes with the same alert.

Trigger values (conditions)

Always specify TRUE as the trigger value. Use the Process Inactive alert to monitor for inactive processes.

Evaluation frequency (schedule)

By default, the alert checks the process list every minute. Apply a schedule that suits the level of monitoring you want to achieve.

Possible uses of this alert

- Windows: Monitoring processes
- Windows: Monitoring security

Related alerts

- Windows: Process Inactive alert

Related topics

- Windows: Managing processes
- Alert concepts and procedures

Windows: Process Inactive alert

Responding to this alert Alert dialog box Help

This Host Agent for Windows alert triggers when a monitored process is not active. You might use this alert to receive notification when a critical program terminates.

Enabled by default

No

Monitored resource (source)

You must specify the following resource for this alert.

Process Name	The name of the process or processes you want to monitor (for example: `payroll.exe`). This alert does not support wildcards.

Trigger values (conditions)

Always specify TRUE as the trigger value. Use the Process Active alert to receive notification when a process starts.

Evaluation frequency (schedule)

By default, the alert checks the process list every minute. Apply a schedule that suits the level of monitoring you want to achieve.

Possible uses of this alert

- Windows: Monitoring processes
- Windows: Monitoring security

Related alerts

- Windows: Process Active alert

Related topics

- Windows: Managing processes
- Alert concepts and procedures

Windows: Processor Congestion (Queue Length) alert

Responding to this alert Alert dialog box Help

This Host Agent for Windows alert monitors the processor queue length for Windows systems. The processor queue length measures the number of threads waiting for processor time. System performance suffers when the queue length is high.

Although this alert has default settings based on recommendations in the Microsoft documentation, you should determine acceptable performance levels at your data center and adjust the settings appropriately.

Enabled by default

No

Monitored resource (source)

You do not have to specify a key for this alert. The alert monitors the System Performance Object's Processor Queue Length counter.

Trigger values

This alert triggers when the Processor Queue Length counter for Windows System Performance Object exceeds a threshold. The processor queue is composed of threads waiting for processor cycles. All processors on a system use the same queue. Generally, if the queue length is greater than two and growing (or greater than double the number of processors on multi-processor systems) and the processor time is high, then you have a processor bottleneck.

Use the Before and After fields on the alert definition dialog box to prevent the alert from triggering when processor activity temporarily spikes but does not remain high.

Evaluation frequency (schedule)

The alert checks the monitored counter every 10 seconds by default. Only the ControlCenter administrator can change the frequency.

Possible uses of this alert

- Windows: Monitoring processor performance

Related alerts

- Windows: Processor Congestion (Processor Time Percent) alerts

Related topics

- Windows: Performance monitoring terminology
- Windows: Creating performance baselines
- Alert concepts and procedures

Windows: Processor Congestion (Processor Time Percent) alerts

Responding to this alert Alert dialog box Help

A strong indication of an impending processor bottleneck is increased processor activity. The Host Agent for Windows Processor Time Percent and Total Processor Time Percent alerts monitor this key indicator. The Processor Time Percent alert monitors the total amount of time the system spends processing requests from applications and services. The Total Processor Time Percent alert monitors the activity of all processors on a system that has multiple processors.

Although this alert has default settings based on recommendations in the Microsoft documentation, you should determine acceptable performance levels at your data center and adjust the settings appropriately.

Enabled by default

No

Monitored resource (source)

These alerts monitor processor activity. For the Processor Time Percent alert, specify the processor you want to monitor. For the Total Processor Time Percent alert, you do not have to specify a source because the alert monitors all processors on the system.

Processor	The index number of the processor you want to monitor. The base index is 0, which is also the default.

Trigger values

The Processor Time Percent alert triggers when the processor performance object's % Processor Time counter exceeds a threshold you define. The Total Processor Time Percent alert triggers when the system performance object's % Total Processor Time counter exceeds a threshold you define. Generally, a % Processor Time greater than 85 percent is considered high on a system with one processor, and greater than 60 percent is considered high on a system with multiple processors.

Use the Before and After fields on the alert definition dialog box to prevent the alert from triggering when processor activity temporarily spikes but does not remain high.

Evaluation frequency (schedule)

The alert checks the monitored counter every 10 seconds by default. Only the ControlCenter administrator can change the frequency.

Possible uses of this alert

- Windows: Monitoring processor performance

Related alerts

- Windows: Processor Congestion (Queue Length) alert

Related topics

- Windows: Performance monitoring terminology
- Windows: Creating performance baselines
- Alert concepts and procedures

Windows: Service Active alert

Responding to this alert Alert dialog box Help

This Host Agent for Windows alert triggers when a specified Windows service becomes active. You might use this alert to receive notification when a critical service starts.

Enabled by default

No

Monitored resource (source)

You must specify the following resource for this alert.

Service Name	The name of the service or services you want to monitor. Use the asterisk wildcard (*) to monitor multiple services with the same alert.

Trigger values (conditions)

Always specify TRUE as the trigger value. Use the Service Inactive alert to receive notification when a service is not active.

Evaluation frequency (schedule)

By default, the alert checks the service list every minute. Select a schedule that provides the level of monitoring you want to achieve.

Possible uses of this alert

- Windows: Monitoring services
- Windows: Monitoring security

Related alerts

- Windows: Service Inactive and Service Failure alerts

Related topics

- Windows: Managing services
- Alert concepts and procedures

Windows: Service Inactive and Service Failure alerts

Responding to this alert Alert dialog box Help

These Host Agent for Windows alerts trigger when a monitored service is not active. You might use these alerts to receive notification when an important service terminates.

There are two alerts that monitor for service inactivity:

- Service Inactive alerttriggers when a service becomes inactive.
- Service Failure alerttriggers when a service becomes inactive and provides an autofix to restart the service.

Enabled by default

Alert: No

Autofix: No

Monitored resource (source)

You must specify the following resource for these alerts.

Service Name	The name of the service or services you want to monitor. Use the asterisk wildcard (*) to monitor multiple services with the same alert.

Trigger values (conditions)

Always specify TRUE as the trigger value. Use the Service Active alert to receive notification when a service is active.

Evaluation frequency (schedule)

By default, the alert checks the service list every minute. Select a schedule that provides the level of monitoring you want to achieve.

Autofixes

The agent provides an autofix for the Service Failure alert called Execute Restart Service. When you attach this autofix to the alert, the agent automatically restarts monitored services when they fail. By default the agent attempts to restart services three times.

Only the ControlCenter administrator can change the number of times the agent attempts to restart the services.

Possible uses of this alert

- Windows: Monitoring services
- Windows: Monitoring security

Related alerts

- Windows: Service Active alert
- Windows: Agent-initiated service alerts

Related topics

- Windows: Managing services
- Alert concepts and procedures

Logical Agent for MVS

Logical: BPXB001E alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXB001E messages issued by the OS/390 operating system. The text of the message is:

```
GROUP ID FOR group_name CANNOT BE OBTAINED. SAF RETURN CODE = saf_return_code,
RACF RETURN CODE = racf_rc, RACF REASON CODE = racf_rsn. TERMINAL GROUP
OWNERSHIP WILL NOT BE UPDATED.
```

The message indicates that, during initialization of pseudo-terminal support, OS/390 UNIX System Services encountered an error from a security package, such as SAF or RACF. The initialization continues but some programs will not be able to access the OS/390 UNIX System Services terminals. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXB002E alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXB002E messages issued by the OS/390 operating system. The text of the message is:

```
OCS REQUIRES TCP/IP TO BE ACTIVE. START TCP/IP OR HAVE THE SYSTEM ADMINISTRATOR
UNCONFIGURE THE OCS NODES.
```

The message indicates that OS/390 UNIX System Services outboard communication server (OCS) could not start because TCP/IP is not active. OCS waits for TCP/IP to be started. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXB003I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXB002E messages issued by the OS/390 operating system. The text of the message is:

`OCS text`

The message indicates that one of OS/390 UNIX System Services' Outboard Communication Server (OCS) kernel services failed. OCS teminates after issuing this message. The name of the service that failed and the return and reason codes are provided in the message text. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXB004E alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXB002E messages issued by the OS/390 operating system. The text of the message is:

`OCS text`

The message indicates that the socket connection between the OS/390 UNIX System Services outboard communication server (OCS) host and one or more of the OCS nodes has broken. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF001I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF001I messages issued by the OS/390 operating system. The text of the message is:

`A FILE SYSTEM WITH FILESYSTYPE` *`type`* `FAILED TO INITIALIZE. THE SOFTWARE LEVEL IS INCORRECT.`

This message indicates that, during initialization, UNIX System Services failed to initialize a physical file system because the software level of the file system is not valid. The system prompts you to restart the file system or continues to initialize without the file system, depending on how the system is configured. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF002I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF002I messages issued by the OS/390 operating system. The text of the message is:

`FILE SYSTEM name WAS NOT MOUNTED.  RETURN CODE = return_code, REASON CODE = reason_code`

This message indicates that OS/390's UNIX System Services failed to mount a file system. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF003I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF003I messages issued by the OS/390 operating system. The text of the message is:

`THE FILE SYSTEM DID NOT INITIALIZE.  IT FAILED TO ESTABLISH AN ESTAE. RETURN CODE = return_code`

During initialization, OS/390 UNIX System Services could not initialize the file system because it could not establish an ESTAE. UNIX System Services terminates abnormally. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF004I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF004I messages issued by the OS/390 operating system. The text of the message is:

`THE FILE SYSTEM DID NOT INITIALIZE. NO ROOT STATEMENT WAS FOUND IN PARMLIB MEMBER member-name.`

This message indicates that, during initialization, OS/390 UNIX System Services could not initialize the file system because a root statement was missing from a parmlib member. UNIX System Services terminates abnormally. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF005I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF005I messages issued by the OS/390 operating system. The text of the message is:

`THE ROOT STATEMENT IN PARMLIB MEMBER member-name DID NOT SPECIFY A TYPE THAT MATCHES ANY FILESYSTYPE STATEMENT.`

This message indicates that, during initialization, OS/390 UNIX System Services could not initialize the file system because a root statement in a parmlib member did not specify a valid file system type. UNIX System Services terminates abnormally. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF006I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF006I messages issued by the OS/390 operating system. The text of the message is:

`A FILE SYSTEM WITH FILESYSTYPE` *`type`* `FAILED TO INITIALIZE. IT TERMINATED DURING INITIALIZATION.`

This message indicates that, during initialization, UNIX System Services failed to initialize a physical file system. The system prompts you to restart the file system or continues to initialize without the file system, depending on how the system is configured. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF007I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF007I messages issued by the OS/390 operating system. The text of the message is:

`FILE SYSTEM` *`name`* `WAS NOT MOUNTED. FILE SYSTEM TYPE` *`type`*`, SPECIFIED IN` *`member-name`*`, IS NOT ACTIVE.`

This message indicates that, during initialization, UNIX System Services failed to mount a file system. The system continues to mount other file systems. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF008I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF008I messages issued by the OS/390 operating system. The text of the message is:

`FILE SYSTEM` *`name`* `WAS NOT MOUNTED. THE MOUNT POINT SPECIFIED IN` *`member-name`* `DOES NOT EXIST.`

This message indicates that, during initialization, UNIX System Services failed to mount a file system because the mount point specified does not exist. The system continues to mount other file systems. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF009I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF009I messages issued by the OS/390 operating system. The text of the message is:

`FILE SYSTEM name WAS NOT MOUNTED. THE MOUNT POINT SPECIFIED IN member-name IS NOT A DIRECTORY.`

This message indicates that, during initialization, UNIX System Services failed to mount a file system because the mount point specified is not a directory; you can only mount file systems on directories. The system continues to mount other file systems. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF011I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF011I messages issued by the OS/390 operating system. The text of the message is:

`A FILE SYSTEM WITH FILESYSTYPE OR SUBFILESYSTYPE type FAILED TO INITIALIZE. A DUPLICATE FILESYSTYPE/SUBFILESYSTYPE STATEMENT WAS FOUND IN PARMLIB MEMBER member-name.`

This message indicates that, during initialization, UNIX System Services failed to mount a file system because the file system was a duplicate of one already found in a parmlib member. The system continues to mount other file systems. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF012I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF012I messages issued by the OS/390 operating system. The text of the message is:

`NEITHER FILESYSTEM NOR DDNAME WAS SPECIFIED ON EITHER A MOUNT OR A ROOT STATEMENT IN PARMLIB MEMBER` *`member-name`*`.`

This message indicates that, during initialization, UNIX System Services encountered an error while processing a parmlib member. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF016I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF016I messages issued by the OS/390 operating system. The text of the message is:
procname TERMINATING. THE ROOT FILE SYSTEM, FILESYSTYPE *type*, TERMINATED.

This message indicates that the root physical file system for UNIX System Services terminated. UNIX System Services also terminates because it cannot run without a root file system. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF017I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF017I messages issued by the OS/390 operating system. The text of the message is:
AN ABEND OCCURRED WHILE PROCESSING DEVICE DRIVER INITIALIZATION ROUTINE *modname*.

This message indicates that a severe error occurred while a UNIX System Services file system was processing a request, possibly damaging the file system. Processing continues, which could cause further harm to the file system. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF018I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF018I messages issued by the OS/390 operating system. The text of the message is:
`DEVICE DRIVER INITIALIZATION ROUTINE` *`modname`* `FAILED. RETURN CODE =` *`return_code`*

This message indicates that during initialization of the character special file system, UNIX System Services failed to initialize a device driver. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF019I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF019I messages issued by the OS/390 operating system. The text of the message is:
`AN ABEND OCCURRED WHILE PROCESSING DEVICE DRIVER INITIALIZATION ROUTINE` *`modname`*`.`

This message indicates that during initialization of the character special file system, an abend occurred. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF010I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF010I messages issued by the OS/390 operating system. The text of the message is:

`FILE SYSTEM` *`name`* `WAS NOT MOUNTED. THE MOUNT POINT SPECIFIED IN` *`member-name`* `ALREADY HAS A FILE SYSTEM MOUNTED ON IT.`

This message indicates that, during initialization, UNIX System Services failed to mount a file system because the mount point specified already has a file system mounted on it. The system continues to mount other file systems. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF020I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF020I messages issued by the OS/390 operating system. The text of the message is:

`AN ABEND OCCURRED WHILE PROCESSING DEVICE DRIVER INITIALIZATION ROUTINE` *`modname`*`.`

This message indicates that a severe error occurred while a UNIX System Services file system was processing a request, possibly damaging the file system. Processing continues, which could cause further harm to the file system. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF022I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF022I messages issued by the OS/390 operating system. The text of the message is:

`A FILE SYSTEM WITH FILESYSTYPE` *`type`* `FAILED TO INITIALIZE. THE FILE SYSTEM MUST RUN IN THE OMVS ADDRESS SPACE.`

This message indicates that, during initialization, UNIX System Services failed to initialize a file system because the file system specification attempted to start the file system in an address space other than OMVS. UNIX System Services file systems must run in the kernel address space. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF023I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF023I messages issued by the OS/390 operating system. The text of the message is:

`FILE SYSTEM` *`name`* `SPECIFIED ON EITHER A MOUNT OR A ROOT STATEMENT IN PARMLIB MEMBER` *`member-name`* `MAY NOT BE MOUNTED ASYNCHRONOUSLY.`

This message indicates that, during initialization, UNIX System Services failed to mount a physical file system because the file system specification indicated that the file system should mount asynchronously. Unless the file system is the root file system, the system continues mounting other file systems. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF202I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF202I messages issued by the OS/390 operating system. The text of the message is:

`DOMAIN` *`domain-name`* `WAS NOT ACTIVATED FOR FILE SYSTEM TYPE` *`type`*`. RETURN CODE =` *`return_code`*`, REASON CODE =` *`reason_code`*

This message indicates that, during initialization, UNIX System Services failed to activate a domain. The system continues to process other requests. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF203I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF203I messages issued by the OS/390 operating system. The text of the message is:

`DOMAIN domain-name WAS SUCCESSFULLY ACTIVATED.`

This message indicates that, during initialization, UNIX System Services successfully initialized a domain. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF205I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF205I messages issued by the OS/390 operating system. The text of the message is:

`UNABLE TO ESTABLISH A CONNECTION TO TRANSPORT DRIVER tdname FOR ROUTING INFORMATION.  RETURN CODE = return_code, REASON CODE = reason.`

This message indicates that UNIX System Services encountered a general error in trying to establish a connection to a transport driver used for retrieving routing information. If possible, the system will use the driver in a degraded state. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF208I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF208I messages issued by the OS/390 operating system. The text of this message is:

`A SOCKETS PORT ASSIGNMENT CONFLICT EXISTS BETWEEN OPENEDITION MVS AND name.`

Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF209I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF209I messages issued by the OS/390 operating system. The text of this message is:

```
ALL OF THE OPENEDITION MVS RESERVED SOCKET PORTS ARE IN USE.
```

Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXF210I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXF210I messages issued by the OS/390 operating system. The text of the message is:

```
A BIND REQUEST COULD NOT BE PROCESSED.  NO PORT 0, INADDR_ANY PORTS WERE
RESERVED.
```

This message indicates that UNIX System Services received a bind request that specified port 0 and internet protocol (IP) address INADDR_ANY; however, there are no ports reserved for that type of bind. You must explicitly reserve ports for binds to port 0 and address INADDR_ANY. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXO001I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXO001I messages issued by the OS/390 operating system. The text for this message is:

hh.mm.ss DISPLAY OMVS

Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXO003I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPX0003I messages issued by the OS/390 operating system. The text for this message is:

hh.mm.ss DISPLAY OMVS

Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXP001I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXP001I messages issued by the OS/390 operating system. The text of the message is:

`OPENMVS INIT PROCESS CANNOT BE CREATED. FAILURE REASON CODE = reason_code. APPC/MVS RETURN CODE = return_code.`

This message indicates that, during initialization, UNIX System Services encountered an error while trying to create INIT process, which is the first process it creates. The initialization of the system ends. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled control group. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXP003E alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXP003I messages issued by the OS/390 operating system. The text of the message is:

`OPENMVS INIT PROCESS CANNOT BE STARTED. AN ERROR OCCURRED DURING APPC PROCESSING. APPC RETURN CODE = returncode. VERIFY APPC AND APPC SCHEDULER ARE OPERATIVE, OR ENTER FORCE jobname, ARM TO END PROCESSING.`

This message indicates that, during initialization of UNIX System Services, APPC/MVS reported an error. The system waits until you correct the error or force the initialization process to end. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: BPXT001I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for BPXT001I messages issued by the OS/390 operating system. The text of the message is:

`THE MAXSOCKETS VALUE OF max-sockets-val ON THE NETWORK STATEMENT IN PARMLIB MEMBER member-name EXCEEDS THE MAXIMUM NUMBER OF SOCKETS SUPPORTED BY THE text.`

This message indicates that, during initialization, UNIX System Services encountered on the NETWORK statement a MAXSOCKETS value that exceeds the maximum allowable sockets number for the sockets file system. The system uses the actual maximum number of sockets allowed. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring UNIX System Services (OpenEdition)

Related topics

- General alert concepts and procedures

Logical: Catalog Sharing alert

Responding to this alert Alert dialog box Help

This alert monitors the user catalog share attributes. The alert detects user catalogs that have share options defined other than (3,4). ControlCenter uses its SCAN command to collect the catalog information.

Enabled by default

Yes

Monitored resources (source)

The alert monitors the following resource, also referred to as the alert key.

User Catalog	The fully-qualified name of the user catalog you want to monitor. You can use a mask to monitor multiple catalogs.

Trigger values

The alert triggers when the number of user catalogs detected meets a value that you specify. For example, the Harmless alert is set to trigger when the number of user catalogs with share options other than (3,4) exceeds zero.

Evaluation frequency (schedule)

Select a control group that provides the level of monitoring you want to achieve and that works with your processing schedules.

Possible uses of this alert

- Monitoring user catalogs

Related topics

- General alert concepts and procedures

Logical: Dataset Extents alert

Responding to this alert Alert dialog box Help

There are two common extent limits for data sets: 16 extents per DASD volume for standard (physical sequential) data sets and 123 extents per volume for extended format data sets. Use separate alerts for each type of data set. Set the alert source appropriately to warn you when data sets are approaching their extent limit. The alert triggers when the number of datasets that have the amount of extents specified in the alert key meets the trigger values you specify.

Enabled by default

No

Monitored resources (source)

The alert monitors the following resources, also referred to as the alert source.

Data Set Mask	A mask that specifies the data sets you want to monitor.
Extended/Nonextended	The type of data set to monitor: Extended or Nonextended. The default is Nonextended.
Min. Extent Count	The number of extents that the monitored data sets must have .

Trigger values

Specify the number of data sets that must have the minimum number of extents as specified in the alert key for the alert to trigger.

Evaluation frequency (schedule)

Specify a control group that provides the level of monitoring you want to achieve. Generally, you should use a control group that evaluates the alert once per day.

Possible uses of this alert

- Monitoring data set growth

Related topics

- General alert concepts and procedures

Logical: DCOLLECT alert

Alert dialog box Help

Space use alerts use data collected by a DCOLLECT operation at regular intervals. This alert controls the scheduling of the data collection.

On the Assign To tab, you should also restrict the DCOLLECT alert to a single OS/390 host.

Enabled by default

Yes

Monitored resources (source)

This alert is used to schedule the collection of space use statistics. There are no sources for this alert.

Trigger values

The trigger values for this alert are ignored.

Evaluation frequency (schedule)

ControlCenter will run the DCOLLECT process according to the control group you specify. The default is once per day. Do not specify a control group more frequent than this (such as twice per day or hourly). To optimize response time when you create reports, schedule the DCOLLECT to finish just before midnight (12:00 a.m.). Also consider timing DCOLLECT processing to avoid contention with other processing requirements.

Possible uses of this alert

- Monitoring space use

Related topics

- General alert concepts and procedures

Logical: Examine alert

Responding to this alert Alert dialog box Help

The Examine alert allows you to monitor the health of catalogs on OS/390 systems. The structural integrity of catalogs is critical to OS/390 systems because jobs and procedures use catalogs to access data sets. The alert runs OS/390's IDCAMS EXAMINE command to detect structural errors in ICF and VSAM catalogs. Using this alert you can schedule ControlCenter to run Examine on a regular basis and report any problems that it finds.

Enabled by default

Yes

Monitored resources (source)

The alert monitors the following resource, also referred to as the alert key.

Catalog Name	The fully-qualified name of the catalog you want to monitor. You can use a mask to monitor multiple catalogs.

Trigger values

The trigger values for this alert are the possible return codes from the Examine command. The possible return codes, which are part of the default alert specification, are:

- 12
- 8
- 4
- 1
- 0

Edit the trigger values to match the level of notification you want to receive. For example, change the trigger value for the Warning severity level to 4 if you want to receive a Warning alert for that return code. By default, a Fatal alert is triggered for a return code of 12, Critical for 8, and Warning for 4.

Evaluation frequency (schedule)

By default, ControlCenter runs the Examine and analyzes the return codes every day at 2 A.M. Select a control group that provides the level of monitoring you want to achieve and that does not interfere with your processing schedules.

Possible uses of this alert

- Monitoring OS/390 catalog health

Related topics

- General alert concepts and procedures

Logical: GDG Scan alert

Responding to this alert Alert dialog box Help

This alert detects whether generation data groups (GDGs) are defined incorrectly. By default, the alert triggers when it detects even one incorrectly defined GDG. ControlCenter uses its SCAN command to collect the information.

Enabled by default

Yes

Monitored resources (source)

The alert monitors the following resource, also referred to as the alert key.

GDG Mask	The fully-qualified name of the GDG you want to monitor. You can use a mask to monitor multiple GDGs.

Trigger values

The alert triggers when the number of incorrectly defined GDGs meets a threshold value you define. By default, the Warning alert is set to trigger when the SCAN command detects just one incorrectly defined GDG.

Evaluation frequency (schedule)

Select a control group that provides the level of monitoring you want to achieve and that works with your processing schedules.

Possible uses of this alert

- Monitoring OS/390 catalog health

Related topics

- General alert concepts and procedures

Logical: IEC304I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for IEC304I messages issued by the OS/390 operating system. The text of the message is:

`SYSCTLG ENTRY SEQUENCE ERROR, off , vol, dsn`

This message indicates that an entry in an OS/390 catalog is out of sequence. Jobs and procedures that use the catalog to access data sets may fail. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring OS/390 catalog health

Related topics

- Responding to this alert
- General alert concepts and procedures

Logical: IEC331I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for IEC331I messages issued by the OS/390 operating system. The text of the message is:

rc-crs[*sfierror*],*job*, *stp*,*proc*[*func*],*mmm* VOL,*ser*,NAME,*dsn*

OS/390 generates this message when it encounters an error while processing catalog management requests. The reason for the error is given by the return and reason codes (*rc* and *crs*). Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring OS/390 catalog health

Related topics

- General alert concepts and procedures

Logical: IEC333I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for IEC333I messages issued by the OS/390 operating system. The text of the message is:

terr[vvv],xx, cat,yyy

OS/390 generates this message when it encounters an I/O error while processing catalog management requests. The message generally follows messages IEC331I and IEC332I. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring OS/390 catalog health

Related topics

- General alert concepts and procedures

Logical: IEC341I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for IEC341I messages issued by the OS/390 operating system. The text of the message is:

IGGOCLHB, CATALOG SERVICE TASK ABENDED - DURING CATALOG PROCESSING.

OS/390 generates this message when a task processing a request ends abnormally in the catalog address space. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring OS/390 catalog health

Related topic

- General alert concepts and procedures

Logical: IEC342I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for IEC342I messages issued by the OS/390 operating system. The text of the message is:

`CATALOG ABEND OCCURRED CATALOG ABEND DIAGNOSTIC INFORMATION JOB=`*`jobname`*`,CAS ESTAE-566528418 R310 ABEND`*`xxx`*`,`*`modname`*`+`*`yyyy`*` FMID=`*`fmid`*`,MAINT=`*`level`*

OS/390 generates this message when a task ends abnormally in a catalog module. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring OS/390 catalog health

Related topics

- General alert concepts and procedures

Logical: IEC355I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for IEC355I messages issued by the OS/390 operating system. The text of the message is:

`CATALOG ADDRESS SPACE IS RESTARTING`

OS/390 generates this message upon restarting a catalog address space after the address space has stopped. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring OS/390 catalog health

Related topics

- General alert concepts and procedures

Logical: IEC356W alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for IEC356W messages issued by the OS/390 operating system. The text of the message is:

```
CATALOG ADDRESS SPACE IS RESTARTING
```

OS/390 generates this message upon restarting a catalog address space after the address space has stopped. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring OS/390 catalog health

Related topics

- General alert concepts and procedures

Logical: IEC358D alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for IEC358D messages issued by the OS/390 operating system. The text of the message is:

```
CATALOG RESTART FAILED, REPLY 'Y' TO RE-INITIATE RESTART
```

OS/390 generates this message when it fails to automatically restart a catalog address space. The message prompts the OS/390 system operator to retry the attempts to restart the catalog address space. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring OS/390 catalog health

Related topics

- General alert concepts and procedures

Logical: IEC372I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for IEC372I messages issued by the OS/390 operating system. The text of the message is:

`CATALOG SEARCH FUNCTION CATALOG MULTI-LEVEL ALIAS HAS DETECTED AN INVALID MASTER CATALOG RECORD NAMED` *`recname`*

OS/390 generates this message when the catalog search function detects an invalid record in a master catalog. You will have to correct the bad record, and then restart the catalog. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring OS/390 catalog health

Related topics

- General alert concepts and procedures

Logical: IEC373I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for IEC373I messages issued by the OS/390 operating system. The text of the message is:

`CATALOG SEARCH FUNCTION CATALOG MULTI-LEVEL ALIAS HAS DETECTED AN INVALID RECORD`

OS/390 generates this message when the catalog search function detects an error in a user catalog alias or connector record. You will have to correct the bad record and then restart the catalog. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring OS/390 catalog health

Related topics

- General alert concepts and procedures

Logical: IEC374I alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for IEC374I messages issued by the OS/390 operating system. The text of the message is:

```
INSUFFICIENT STORAGE FOR CATALOG MULTI-LEVEL ALIAS FACILITY
```

OS/390 generates this message when there is insufficient space for the catalog's multilevel alias facility. The catalog search function cannot function properly. Consult the IBM OS/390 documentation for a full explanation of the message and its implications.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 system for the message. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Critical alert.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Evaluation frequency (schedule)

This alert's scheduling is agent-controlled. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring OS/390 catalog health

Related topics

- General alert concepts and procedures

Logical: PDS Directory Full alert

Responding to this alert Alert dialog box Help

This alert detects partitioned data sets (PDSs) for which the directory space is full or almost full. ControlCenter uses its SCAN command to collect the information.

Enabled by default

Yes

Monitored resources (source)

The alert monitors the following resource, also referred to as the alert key.

Data Set Mask	The fully-qualified name of the data set you want to monitor. You can use a mask to monitor multiple data sets.
Volser Mask	The volume serial number (volser) of the volume you want to monitor. You can use a mask to monitor multiple volumes.

Trigger values

Specify the number of data sets that must have no directory space for the alert to trigger.

Evaluation frequency (schedule)

Select a control group that provides the level of monitoring you want to achieve and that works with your processing schedules.

Possible uses of this alert

- Monitoring OS/390 data sets

Related topics

- General alert concepts and procedures

Logical: Processing Failed alert

Responding to this alert Alert dialog box Help

Use this alert to detect when an error occurs while ControlCenter is processing alerts related to OS/390 logical storage. This alert can help you ensure that you do not miss critical alerts related to OS/390.

Enabled by default

No

Monitored resource (source)

The alert monitors ControlCenter processing of alerts related to OS/390 alert processing. You do not have to specify a key for this alert.

Trigger values

This is a state alert. The trigger value should be TRUE. Select the severity level ControlCenter should report the alert as; by default ControlCenter issues a Warning alert.

Evaluation frequency (schedule)

This alert has an AgentControlled control group. When the alert is enabled, ControlCenter continuously monitors for the message.

Possible uses for this alert

- Monitoring ControlCenter processing

Related topics

- General alert concepts and procedures

Logical: Space activity alerts

Responding to this alert Alert dialog box Help

The space activity alerts check each day for excessive space use growth. You can monitor by high-level qualifier (HLQ) or user ID (UID) for the following intervals:

- hourly
- daily
- weekly
- monthly (over 28 day period)

You can also monitor space use by new HLQs or UIDs.

Enabled by default

No

Monitored resources (source)

The alert monitors the following resource, also referred to as the alert key.

High-level Qualifier or UID	The HLQ or UID you want to monitor. Use masks to monitor multiple HLQs or UIDs.

Trigger values

Specify the amount that the space used by an HLQ or UID must have changed for the alert to trigger.

Evaluation frequency (schedule)

Select a control group that provides the level of monitoring you want to achieve and that works with your processing schedules.

Possible uses of this alert

- Monitoring space use

Related topics

- General alert concepts and procedures

Logical: Space use alerts

Responding to this alert Alert dialog box Help

The space use alerts monitor allocation and use of space by high-level qualifiers (users) and application resources as defined by you in application IDs. ControlCenter provides alerts to monitor by:

- data set name (DSN)
- growth percentage
- number of megabytes used
- percentage of space used

Enabled by default

No

Monitored resources (source)

The alert monitors space resources, also referred to as the alert key.

Special requirements

You must configure the DCOLLECT alert to schedule the time of day ControlCenter should run the DCOLLECT procedure to collect the space use information for these alerts.

Trigger values

Specify the amount that the space used by an HLQ or application ID must have changed for the alert to trigger.

Evaluation frequency (schedule)

Select a control group that provides the level of monitoring you want to achieve and that works with your processing schedules.

Possible uses of this alert

- Monitoring space use

Related topics

- General alert concepts and procedures

Logical: SystemCheck alert

Responding to this alert Alert dialog box Help

The SystemCheck alert allows you to monitor the health of catalogs on OS/390 systems. The structural integrity of catalogs is critical to OS/390 systems because jobs and procedures use catalogs to access data sets. The alert runs ControlCenter's System Check command to detect structural errors in basic catalog structures (BCSs) and VSAM volume data sets (VVDSs). Using this alert you can schedule ControlCenter to run System Check on a regular basis and report any problems that it finds.

Enabled by default

Yes

Monitored resources (source)

The alert monitors the following resource, also referred to as the alert key.

Catalog Name	The fully-qualified name of the catalog you want to monitor. You can use a mask to monitor multiple catalogs.

Trigger values

The trigger values for this alert are the possible return codes from the System Check command. The possible return codes, which are part of the default alert specification, are:

- 12
- 8
- 1
- 4
- 0

Edit the trigger values to match the level of notification you want to receive. For example, change the trigger value for the Warning severity level to 4 if you want to receive a Warning alert for that return code. By default, a Fatal alert is triggered for a return code of 12, Critical for 8, and Minor for 4.

Evaluation frequency (schedule)

By default, ControlCenter runs the System Check and analyzes the return codes every day at 2 A.M. Select a control group that provides the level of monitoring you want to achieve and that works with your processing schedules.

Possible uses of this alert

- Monitoring OS/390 catalog health

Related topics

- Responding to this alert
- General alert concepts and procedures

Logical: TeraSAM Candidates alert

Responding to this alert Alert dialog box Help

This alert detects partitioned data sets (PDSs) for which the high-used RBA value (HURBA) meets a threshold you define. ControlCenter uses its SCAN command to collect the information.

Enabled by default

Yes

Monitored resources (source)

The alert monitors the following resource, also referred to as the alert key.

Data Set Mask	The fully-qualified name of the data set you want to monitor. You can use a mask to monitor multiple data sets.

Trigger values

Specify the HURBA value at which the various alert severity levels should trigger.

Evaluation frequency (schedule)

Select a control group that provides the level of monitoring you want to achieve and that works with your processing schedules.

Possible uses of this alert

- Monitoring OS/390 data sets

Related topics

- General alert concepts and procedures

Logical: VSAM Reorg alert

Responding to this alert Alert dialog box Help

This alert monitors for VSAM data sets that have an excessive number of CA splits, indicating that the data set must be reorganized. ControlCenter uses its SCAN command to collect the information. The alert triggers when the number of data sets with excessive CA splits meets a threshold you define.

Enabled by default

Yes

Monitored resources (source)

The alert monitors the following resource, also referred to as the alert key.

Data Set Mask	The fully-qualified name of the data set you want to monitor. You can use a mask to monitor multiple data sets.

Trigger values

Specify the number of data sets with excessive CA splits at which ControlCenter should trigger the alert.

Evaluation frequency (schedule)

Select a control group that provides the level of monitoring you want to achieve and that works with your processing schedules.

Possible uses of this alert

- Monitoring OS/390 data sets

Related topics

- General alert concepts and procedures

Logical: UNIX System Services (OpenEdition) message alerts

ControlCenter can help you monitor UNIX System Services (USS), formerly called OpenEdition, on OS/390 by triggering alerts when OS/390 issues important messages related to USS. The following table lists the numbers and text of the USS messages ControlCenter can monitor for. Click any message number to see a complete description of the alert for that message.

Message	Message text	Brief explanation
BPXO001I	*hh.mm.ss* DISPLAY OMVS	This message displays information about the status of OS/390 UNIX and its processes.
BPXO003I	*hh.mm.ss* DISPLAY OMVS	This message displays information about the status of OS/390 UNIX and its processes.
BPXB001E	GROUP ID FOR *group_name* CANNOT BE OBTAINED. SAF RETURN CODE = *saf_return_code*, RACF RETURN CODE = *racf_rc*, RACF REASON CODE = *racf_rsn*. TERMINAL GROUP OWNERSHIP WILL NOT BE UPDATED.	During initialization of pseudo-terminal support, OS/390 USS encountered an error from a security package, such as SAF or RACF.
BPXB002E	OCS REQUIRES TCP/IP TO BE ACTIVE. START TCP/IP OR HAVE THE SYSTEM ADMINISTRATOR UNCONFIGURE THE OCS NODES.	OS/390 USS Outboard Communication Server (OCS) could not start because TCP/IP is not active.
BPXB003I	OCS *text*	One of OS/390 USS Outboard Communication Server (OCS) kernel services failed.
BPXB004E	OCS HAS LOST ITS CONNECTION TO THE FOLLOWING NODE(S): *ocsnodename* [, *ocsnodename* [, *ocsnodename*]]]	The socket connection between the OS/390 USS Outboard Communication Server (OCS) host and one or more of the OCS nodes has broken.

BPXF001I	A FILE SYSTEM WITH FILESYSTYPE *type* FAILED TO INITIALIZE. THE SOFTWARE LEVEL IS INCORRECT.	During initialization, OS/390 USS failed to initialize a physical file system because the software level was incorrect.
BPXF002I	FILE SYSTEM name WAS NOT MOUNTED. RETURN CODE = *return_code*, REASON CODE = *reason_code*	OS/390 USS failed to mount a file system.
BPXF003I	THE FILE SYSTEM DID NOT INITIALIZE. IT FAILED TO ESTABLISH AN ESTAE. RETURN CODE = *return_code*	During initialization, OS/390 USS could not initialize the file system because it could not establish an ESTAE.
BPXF004I	THE FILE SYSTEM DID NOT INITIALIZE. NO ROOT STATEMENT WAS FOUND IN PARMLIB MEMBER *member-name*.	OS/390 USS could not initialize the file system because a root statement was missing from a parmlib member.
BPXF005I	THE ROOT STATEMENT IN PARMLIB MEMBER *member-name* DID NOT SPECIFY A TYPE THAT MATCHES ANY FILESYSTYPE STATEMENT.	OS/390 USS could not initialize the file system because a root statement in a parmlib member did not specify a valid file system type
BPXF006I	A FILE SYSTEM WITH FILESYSTYPE *type* FAILED TO INITIALIZE. IT TERMINATED DURING INITIALIZATION.	During initialization, OS/390 USS failed to initialize a physical file system.
BXFP007I	FILE SYSTEM *name* WAS NOT MOUNTED. FILE SYSTEM TYPE *type*, SPECIFIED IN *member-name*, IS NOT ACTIVE.	During initialization, OS/390 USS failed to mount a file system.
BXFP008I	FILE SYSTEM *name* WAS NOT MOUNTED. THE MOUNT POINT SPECIFIED IN *member-name* DOES NOT EXIST.	During initialization, USS failed to mount a file system because the mount point specified does not exist.
BPXF009I	FILE SYSTEM *name* WAS NOT MOUNTED. THE MOUNT POINT SPECIFIED IN *member-name* IS NOT A DIRECTORY.	During initialization, USS failed to mount a file system because the mount point specified is not a directory; you can only mount file systems on directories.
BPXF010I	FILE SYSTEM *name* WAS NOT MOUNTED. THE MOUNT POINT SPECIFIED IN *member-name* ALREADY HAS A FILE SYSTEM MOUNTED ON IT.	During initialization, USS failed to mount a file system because the mount point specified already has a file system mounted on it.
BPXF011I	A FILE SYSTEM WITH FILESYSTYPE OR SUBFILESYSTYPE *type* FAILED TO INITIALIZE. A DUPLICATE FILESYSTYPE/SUBFILESYSTYPE STATEMENT WAS FOUND IN PARMLIB MEMBER *member-name*.	During initialization, USS failed to mount a file system because the file system was a duplicate of one already found in a parmlib member
BPXF012I	NEITHER FILESYSTEM NOR DDNAME WAS SPECIFIED ON EITHER A MOUNT OR A ROOT STATEMENT IN PARMLIB MEMBER *member-name*.	During initialization, USS encountered an error while processing a parmlib member.
BPXF016I	*procname* TERMINATING. THE ROOT FILE SYSTEM, FILESYSTYPE *type*, TERMINATED.	The root physical file system for USS terminated. USS also terminates.
BPXF017I	*procname* TERMINATING. FILE SYSTEM, FILESYSTYPE *type*, TERMINATED.	A physical file system required for USS to run terminated. USS also terminates.
BPXF018I	DEVICE DRIVER INITIALIZATION ROUTINE *modname* FAILED. RETURN CODE = *return_code*	During initialization of the character special file system, USS failed to initialize a device driver.
BPXF019I	AN ABEND OCCURRED WHILE PROCESSING DEVICE DRIVER INITIALIZATION ROUTINE *modname*.	During initialization of the character special file system, an abend occurred
BPXF020I	FILE SYSTEM *name* MAY BE DAMAGED. RETURN CODE = *return_code*, REASON CODE = *reason_code*	A severe error occurred while a USS file system was processing a request, possibly damaging the file system.

BPXF022I	A FILE SYSTEM WITH FILESYSTYPE *type* FAILED TO INITIALIZE. THE FILE SYSTEM MUST RUN IN THE OMVS ADDRESS SPACE.	During initialization, USS failed to initialize a file system because the file system specification attempted to start the file system in an address space other than OMVS.
BPXF023I	FILE SYSTEM *name* SPECIFIED ON EITHER A MOUNT OR A ROOT STATEMENT IN PARMLIB MEMBER *member-name* MAY NOT BE MOUNTED ASYNCHRONOUSLY.	During initialization, USS failed to mount a physical file system because the file system specification indicated that the file system should mount asynchronously.
BPXF202I	DOMAIN *domain-name* WAS NOT ACTIVATED FOR FILE SYSTEM TYPE *type*. RETURN CODE = *return_code*, REASON CODE = *reason_code*	During initialization, USS failed to activate a domain.
BPXF203I	DOMAIN *domain-name* WAS SUCCESSFULLY ACTIVATED.	During initialization, USS successfully initialized a domain.
BPXF205I	UNABLE TO ESTABLISH A CONNECTION TO TRANSPORT DRIVER *tdname* FOR ROUTING INFORMATION. RETURN CODE = *return_code*, REASON CODE = *reason*.	USS encountered a general error in trying to establish a connection to a transport driver used for retrieving routing information.
BPXF208I	A SOCKETS PORT ASSIGNMENT CONFLICT EXISTS BETWEEN OPENEDITION MVS AND *name*.	A bind request specified port number 0 and Internet Protocol (IP) address INADDR_ANY failed because a port number that is reserved for use by OS/390 UNIX Common INET is currently being used by the named transport provider.
BPXF209I	ALL OF THE OPENEDITION MVS RESERVED SOCKET PORTS ARE IN USE.	A bind request that specified port number 0 and Internet Protocol (IP) address INADDR_ANY failed because all of the port numbers reserved for those binds are currently in use.
BPXF210I	A BIND REQUEST COULD NOT BE PROCESSED. NO PORT 0, INADDR_ANY PORTS WERE RESERVED.	UNIX System Services received a bind request that specified port 0 and internet protocol (IP) address INADDR_ANY; however, there are no ports reserved for that type of bind.
BPXP001I	OPENMVS INIT PROCESS CANNOT BE CREATED. FAILURE REASON CODE = *reason_code*. APPC/MVS RETURN CODE = *return_code*.	During initialization, USS encountered an error while trying to create INIT process, which is the first process it creates.
BPXP003E	OPENMVS INIT PROCESS CANNOT BE STARTED. AN ERROR OCCURRED DURING APPC PROCESSING. APPC RETURN CODE = *returncode*. VERIFY APPC AND APPC SCHEDULER ARE OPERATIVE, OR ENTER FORCE *jobname*, ARM TO END PROCESSING.	During initialization of USS, APPC/MVS reported an error.
BPXT001I	THE MAXSOCKETS VALUE OF *max-sockets-val* ON THE NETWORK STATEMENT IN PARMLIB MEMBER *member-name* EXCEEDS THE MAXIMUM NUMBER OF SOCKETS SUPPORTED BY THE *text.*	During initialization, USS encountered on the NETWORK statement a MAXSOCKETS value that exceeds the maximum allowable sockets number for the sockets file system.

Related topics

- Responding to UNIX System Services (OpenEdition) alerts
- General alert concepts and procedures

Logical: User Count alert

Responding to this alert Alert dialog box Help

Use this alert to monitor a group of data sets for a threshold value. You use the ControlCenter SCAN command to specify what you are monitoring. You might use the SCAN command to identify data sets with specific:

- SMS constructs
- date attributes
- VSAM attributes
- GDG attributes
- non-VSAM attributes
- various other parameters

The alert triggers when the number of data sets that meet the criteria specified in the SCAN command meet a threshold value defined in the alert.

See the SCAN command topic for more information. ControlCenter runs the SCAN command according to a schedule you define, such as daily, weekly, or monthly.

Enabled by default

No

Monitored resources (source)

The alert monitors the following resource, also referred to as the alert key.

Scan Description	The name of a ControlCenter SCAN command, either one you have created or one of the commands supplied by ControlCenter. The syntax must match the SCAN command name exactly.

Trigger values

Specify the number of data sets that must match criteria specified in the SCAN command for the alert to trigger.

Evaluation frequency (schedule)

ControlCenter runs the SCAN command and evaluates the number of matching data sets according to the schedule defined in the control group you choose.

Possible uses of this alert

- Monitoring OS/390 data sets

Related topics

- General alert concepts and procedures

Logical: User-defined alert

Responding to this alert Alert dialog box Help

Use this alert to monitor for specific messages issued by the OS/390 operating system.

Enabled by default

No

Monitored resource (source)

The alert monitors the OS/390 0system for a specific message.

Message ID	The ID of the OS/390 message you want to be notified about. Use wild cards to monitor for multiple messages.

Trigger values

Specify TRUE as the trigger value for the severity level you want to use to classify the alert.

Evaluation frequency (schedule)

This alert has an AgentControlled control group. When the alert is enabled, ControlCenter continuously monitors for the message.

Use the **Before** field to indicate how many messages the OS/390 system must issue within the time specified by the control group before ControlCenter triggers the alert.

Possible uses for this alert

- Monitoring OS/390

Related topics

- General alert concepts and procedures

Logical: User RC alert

Responding to this alert Alert dialog box Help

Use this alert to monitor a group of data sets for a specific condition. You use the ControlCenter SCAN command to specify what you are monitoring. The alert triggers when the return code from the SCAN command meets one of the trigger values you specify for the alert.

You can use the SCAN command to identify data sets with specific:

- SMS constructs
- date attributes
- VSAM attributes
- GDG attributes
- non-VSAM attributes
- various other parameters

See the SCAN command topic for more information. ControlCenter runs the SCAN command according to a schedule you define, such as daily, weekly, or monthly.

Enabled by default

No

Monitored resources (source)

The alert monitors the following resource, also referred to as the alert key.

Scan Description	The name of a ControlCenter SCAN command, either one you have created or one of the commands supplied by ControlCenter. The syntax must match the SCAN command name exactly.

Trigger values

Specify the return codes from the SCAN command that should cause the alert severity levels to trigger.

Evaluation frequency (schedule)

ControlCenter runs the SCAN command and evaluates the number of matching data sets according to the schedule defined in the control group you choose.

Possible uses of this alert

- Monitoring OS/390 data sets

Related topics

- General alert concepts and procedures

Physical Agent for MVS

Physical: % Free Space alert

Responding to this alert Alert dialog box Help

This alert issues in response to the free space on a disk reaching a certain level.

Enabled by default
No

Monitored resource (source)
By default, this alert warns you when a disk reaches less than 10 percent free space. You can change this value to receive additional warnings as a disk's capacity decreases.

Trigger values
The default trigger value for this alert is less than 10 percent free space on the disk.

Evaluation frequency (schedule)
This alert evaluates conditions once an hour, but you can change the frequency with which it monitors this condition.

Possible uses of this alert
- Monitor amount of free space available on volumes.

Related topics
- Alert concepts and procedures

Physical: Allocation Without Mount alert

Responding to this alert Alert dialog box Help

This alert is issued when a tape allocated for storage is not mounted within a certain amount of time.

Enabled by default
No

Monitored resource (source)
This agent monitors the elapsed time that it takes to mount a tape.

Trigger values
The alert triggers if it takes more than 30 minutes to mount a tape. This is the default value.

Evaluation frequency (schedule)
This alert's evaluation frequency is agent-controlled and managed by internal settings. However, you can define this alert to monitor and issue alerts at varying time increments (such as at 5-, 10-, 15-, 20-, and 30-minute increments).

Possible uses of this alert
- Notifies you of excessively long backup intervals

Related topics
- Alert concepts and procedures

Physical: DASD Init alert

Responding to this alert Agent dialog box Help

This alert monitors an OS/390 environment and issues a notice when Physical Agent initializes DASD volumes.

Enabled by default
No

Monitored resource (source)
This alert monitors the volume list that you specify and watches for physical volumes fitting those criteria for the agent to initialize.

Trigger values
This is a state alert. It triggers when the agent initializes a physical volume matching the specified volume mask.

Evaluation frequency (schedule)
This alert is controlled by the agent and evaluates system conditions based on internal agent settings.

Possible uses of this alert
- Confirms successful initialization of a volume by the agent

Related topics

- Alert concepts and procedures

Physical: Fragmentation alert

Responding to this alert Alert dialog box Help

This alert triggers in response to fragmentation on a volume reaching a threshold.

Enabled by default

No

Monitored resource (source)

This alert monitors the level of fragmentation on a drive.

Trigger values

By default this alert triggers when fragmentation is less than 100.

Evaluation frequency (schedule)

This alert checks the fragmentation status of the volumes it monitors hourly. You can change this value.

Possible uses of this alert

- Monitor volume fragmentation

Related topics

- Alert concepts and procedures

Physical: Free DSCBs alert

Responding to this alert Alert dialog box Help

This alert activates based on the number of free DSCBs available on a volume. If the DSCBs on a volume fall below a certain level, users cannot store more data on that volume.

Enabled by default

No

Monitored resource (source)

This alert monitors the number of free DSCBs available on a volume and issues an alert when that number falls below 100 by default. This number can be modified by the user.

Trigger values

The trigger value for this alert is based on the number of free DSCBs on a given volume. If that number is reached on a volume, the alert is issued.

Evaluation frequency (schedule)

By default, this alert checks hourly for this condition on all physical volumes that it sees.

Possible uses of this alert

- Monitor DSCB counts on volumes

Related topics

- Alert concepts and procedures

Physical: Integrity alert

Responding to this alert Agent dialog box Help

This alert monitors DASD Volume Tables of Contents (VTOCs) for losses of integrity.

Enabled by default

No

Monitored resource (source)
This alert monitors DASD VTOCs and issues an alert when a volume's VTOC is found to be corrupted.

Trigger values
This alert is a state alert and triggers when a VTOC is found that has lost its integrity.

Evaluation frequency (schedule)
This alert is agent-controlled and activates when it detects this condition. By default, the agent checks for this condition every hour. By modifying the schedule settings, you can change the frequency.

Possible uses of this alert
- Issues notices about corrupted DASD VTOCs

Related topics
- Alert concepts and procedures

Physical: Intervention (Disk) alert

Responding to this alert Alert dialog box Help

This alert activates when the agent determines that a disk unit requires human intervention.

Enabled by default
No

Monitored resource (source)
The agent monitors disks for this information. If a disk is flagged as needing intervention, this alert issues.

Trigger values
Triggers when the device has been flagged as needing user intervention.

Evaluation frequency (schedule)
This is a state alert controlled by the agent. The agent determines when it will run this alert based on internal parameters.

Possible uses of this alert
- Issues notices about disks requiring operator attention

Related topics
- General alert concepts and procedures

Physical: Intervention (Tape) alert

Responding to this alert Alert dialog box Help

This alert is issued when a tape drive is flagged as requiring user intervention.

Enabled by default
No

Monitored resource (source)
This alert monitors the tape drive and issues alerts in response to it.

Trigger values
The default trigger values are 1, 5, 10, and 30 minutes. By default, only the 30-minute warning is enabled.

Evaluation frequency (schedule)
This alert is agent-controlled and checks for new alerts based on internal settings.

Possible uses of this alert
- Monitoring tape drives requiring user intervention.

Related topics

- Alert concepts and procedures

Storage Agent for CLARiiON

CLARiiON: RAID Group Free Space

Responding to this alert Alert dialog box Help

This alert is issued when the free space of a RAID Group is less than some value.

Enabled by default

Yes.

Monitored resource (source)

The following table describes the keys for the RAID Group Free Space alert.

SP A Host Name	The SP A host name of the disk-array storage subsystem where the RAID Group is located. Can include wildcards.
RAID Group Name	The RAID Group ID of the RAID Groups the agent monitors. Can include wildcards.

Trigger values

This alert triggers when the free space of the RAID Group specified by the alert key, meets the conditions specified by the alert trigger and comparison values. The trigger value is a number, and the unit used is MB.

Evaluation frequency (schedule)

ControlCenter monitors every hour for the message.

Possible uses for this alert

Use this alert to receive notification when the free space of a RAID Group is less than a certain value.

Related topics

- Alert concepts and procedures

CLARiiON: RAID Group Percent Free Space

Responding to this alert Alert dialog box Help

This alert is issued when the percent free space of a RAID Group is less than some value.

Enabled by default

Yes.

Monitored resource (source)

The following table describes the keys for the RAID Group Percent Free Space alert.

SP A Host Name	The SP A host name of the disk-array storage subsystem where the RAID Group is located. Can include wildcards.
RAID Group Name	The RAID Group ID of the RAID Groups the agent monitors. Can include wildcards.

Trigger values

The alert triggers is a number, and the unit used is %.

Evaluation frequency (schedule)

ControlCenter monitors every hour for the message.

Possible uses for this alert

Use this alert to receive notification when the percent free space of a RAID Group is less than a certain value.

Related topics

- Alert concepts and procedures

CLARiiON: Storage Array Fault

Responding to this alert Alert dialog box Help

This alert is issued when a storage array fault is detected.

Enabled by default

Yes.

Monitored resource (key)

SP A Host Name

Trigger values

This alert triggers when a storage-array fault is discovered and meets the conditions specified by the alert trigger. The trigger value should be TRUE.

Evaluation frequency (schedule)

ControlCenter monitors every hour for the message.

Possible uses for this alert

Use this alert to receive notification whenever a storage array faults.

Related topics

- Alert concepts and procedures

Storage Agent for Compaq StorageWorks

StorageWorks: Battery Days to Expiration alert

Responding to this alert Alert dialog box Help

This Storage Agent for Compaq StorageWorks alert monitors the expiration date of a subsystem controller's external cache battery. If you continue using a battery after its expiration date, you could lose or corrupt data in the event that the subsystem loses power. The battery allows the cache module to maintain data that has not been written to disk.

Enabled by default

Yes

Monitored resource (source)

The alert monitors the following resource.

Controller	The name of the controller you want to monitor. Use the asterisk (*) and question mark (?) wildcards to monitor multiple controllers with the same alert.

Trigger values

Specify how many days before the battery expires you want to be notified. Select multiple trigger values to receive multiple notifications.

Evaluation frequency (schedule)

By default, the alert checks the battery expiration date every day at midnight. Select a schedule that provides the level of monitoring that you want to achieve.

Possible uses of this alert

- Monitoring Compaq StorageWorks subsystems

Related topics

- Alert concepts and procedures
- StorageWorks: Exploring controller cache properties
- Storage Agent for Compaq StorageWorks overview

StorageWorks: Device Not Mapped alert

Responding to this alert Alert dialog box Help

This Storage Agent for Compaq StorageWorks alert monitors the subsystem containers (disks, partitions, storagesets, and so on) to detect storage space you are not using. You may be able to take advantage of this unused space in your storage environment.

A device is not mapped if:

- It is not part of a storageset and is not mapped to a unit
- It is a partition that is not mapped to a unit
- It is a storageset that is not mapped to a unit

Enabled by default

Yes

Monitored resource (source)

The alert monitors the following resource.

Device Name	The name of the device you want to monitor. Use the asterisk (*) and question mark (?) wildcards to monitor multiple devices with the same alert.

Trigger values

This is a state alert. The trigger values should always be TRUE.

Evaluation frequency (schedule)

By default, the alert checks for unused containers every day at midnight. Select a schedule that provides the level of monitoring that you want to achieve.

Possible uses of this alert

- Monitoring Compaq StorageWorks subsystems

Related topics

- Alert concepts and procedures
- Storage Agent for Compaq StorageWorks overview

StorageWorks: Failed Set Device Count alert

Responding to this alert Alert dialog box Help

This Storage Agent for Compaq StorageWorks alert triggers when the number of disks in the monitored subsystem's failed set exceeds a trigger value that you specify.

Enabled by default

Yes

Monitored resource (source)

The alert monitors the following resource.

Subsystem	The name of the subsystem you want to monitor. Use the asterisk (*) and question mark (?) wildcards to monitor multiple subsystems with the same alert.

Trigger values

Specify how many devices must be in the monitored subsystem's failed set for the alert to trigger. Enable one or more severity levels.

Evaluation frequency (schedule)

By default, the alert checks the failed set every hour. Select a schedule that provides the level of monitoring that you want to achieve.

Possible uses of this alert

- StorageWorks: Monitoring storageset device counts

Related topics

- Alert concepts and procedures
- StorageWorks: Exploring spare and failed sets
- Storage Agent for Compaq StorageWorks overview

StorageWorks: Set Is Reduced alert

Responding to this alert Alert dialog box Help

This Storage Agent for Compaq StorageWorks alert triggers when a disk is removed from a specified storageset in a StorageWorks subsystem. This alert is useful if you do not have a failed device replacement policy enabled.

Enabled by default

Yes

Monitored resource (source)

The alert monitors the following resource.

Set Name	The name of the storageset you want to monitor. Use the asterisk (*) and question mark (?) wildcards to monitor multiple storagesets with the same alert.

Trigger values

This is a state alert. The trigger values should always be TRUE.

Evaluation frequency (schedule)

By default, the alert checks the storageset every day at midnight. Select a schedule that provides the level of monitoring that you want to achieve.

Possible uses of this alert

- StorageWorks: Monitoring storageset device counts

Related topics

- Alert concepts and procedures
- StorageWorks: Exploring storagesets
- Storage Agent for Compaq StorageWorks overview

StorageWorks: Spare Set Device Count alert

Responding to this alert Alert dialog box Help

This Storage Agent for Compaq StorageWorks alert triggers when the number of disks in the monitored StorageWorks subsystem's spare set falls below a trigger value that you specify.

Enabled by default

Yes

Monitored resource (source)

The alert monitors the following resource.

Subsystem	The name of the subsystem you want to monitor. Use the asterisk (*) and question mark (?) wildcards to monitor multiple subsystems with the same alert.

Trigger values

Specify how many devices must be in the monitored subsystem's spare set for the alert to trigger. Enable one or more severity levels.

Evaluation frequency (schedule)

By default, the alert checks the spare set every hour. Select a schedule that provides the level of monitoring that you want to achieve.

Possible uses of this alert

- StorageWorks: Monitoring storageset device counts

Related topics

- Alert concepts and procedures
- StorageWorks: Exploring spare and failed sets
- Storage Agent for Compaq StorageWorks overview

Storage Agent for HDS

HDS: Illegal Paired Volumes

Responding to this alert Alert dialog box Help

This alert reports an error inside the XP disk array. If this alert is triggered, the administrator must fix it or correct the wrong disk (path). With this error, the disk array cannot provide data (disk) protection.

Enabled by default

Yes

Monitored resource (source)

You do not have to specify a key for this alert.

Trigger values

If the agent finds the error, the alert is triggered.

Evaluation frequency (schedule)

ControlCenter monitors every hour for the message.

Related topics

- Alert concepts and procedures

HDS: Volumes Not Paired

Responding to this alert Alert dialog box Help

This alert notifies the storage administrator when a RAID Manager controlled volume is not being hardware backed (pair). Some volumes are not in a data protection state. Make a pair for those unpaired volumes.

Enabled by default

Yes

Monitored resource (source)

You do not have to specify a key for this alert.

Evaluation frequency (schedule)

The default is one hour, but this can be changed in the XML file.

Related topics

- Alert concepts and procedures

Storage Agent for IBM ESS

IBM ESS: Write Sequential Hit Ratio alert

Responding to this alert Alert dialog box help

This alert checks if the Write Sequential hit ratio for an IBM ESS volume is less than a specified value.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Specify a numeric value. This alert triggers whenever the Write Sequential hit ratio for an IBM ESS subsystem is less than a specific number.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Write Normal Hit Ratio alert

Responding to this alert Alert dialog box help

This alert checks if the Write Normal hit ratio for an IBM ESS volume is less than a specified value.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Specify a numeric value. This alert triggers whenever the Write Normal hit ratio for an IBM ESS subsystem is less than a specific number.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Unavailable Cache alert

Responding to this alert Alert dialog box help

This alert checks if a subsystem error has caused one of the IBM ESS cache controllers to become unavailable.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Set the trigger value to TRUE. This alert triggers whenever one of the IBM ESS cache controllers becomes unavailable.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Search Read Cache Fast Write Hit Ratio alert

Responding to this alert Alert dialog box help

This alert checks if an IBM ESS volume's search read cache fast write (CFW) hit ratio is less than a specified value.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Specify a numeric value. This alert triggers whenever an IBM ESS volume's search read cache fast write hit ratio is less than a specific number.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Read Sequential Hit Ratio alert

Responding to this alert Alert dialog box help

This alert checks if the Read Sequential hit ratio for an IBM ESS volume is less than a specified value.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Specify a numeric value. This alert triggers whenever the Read Sequential hit ratio for an IBM ESS volume is less than a specific number.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Read Normal Hit Ratio alert

Responding to this alert Alert dialog box help

This alert checks if the Search Read Normal hit ratio for an IBM ESS volume is less than a specified value.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Specify a numeric value. This alert triggers whenever the Search Read Normal hit ratio for an IBM ESS volume is less than a specific number.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: RAID Rebuild alert

Responding to this alert Alert dialog box help

This alert checks if an IBM ESS volume is part of a RAID rank (disk array) that is undergoing a rebuild.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Set the trigger value to TRUE. This alert triggers whenever an IBM ESS volume is part of a RAID rank (disk array) that is undergoing a rebuild.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Pinned NVS for Device alert

Responding to this alert Alert dialog box help

This alert checks if an IBM ESS volume has data pinned in non volatile storage (NVS) for a specific device. Non volatile storage is battery-powered memory that contains data that the IBM ESS has not yet written to disk.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Set the trigger value to TRUE. This alert triggers whenever an IBM ESS volume has data pinned in non volatile storage.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Pinned NVS alert

Responding to this alert Alert dialog box help

This alert checks the amount (in KB) of pinned non volatile storage (NVS) in an IBM ESS subsystem. non volatile storage is battery-powered memory that contains data that the IBM ESS has not yet written to disk.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Specify a numeric value. This alert triggers whenever the amount of an IBM ESS subsystem's pinned non volatile storage exceeds a specific number.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Pinned Cache alert

Responding to this alert Alert dialog box help

This alert checks the amount of pinned data (in KB) in an IBM ESS subsystem's cache.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Specify a numeric value. This alert triggers whenever the amount of pinned data (in KB) in an IBM ESS subsystem's cache exceeds a specific number.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Offline Cache alert

Responding to this alert Alert dialog box help

This alert monitors the amount of an IBM ESS subsystem's cache that is offline due to cache storage errors.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Specify a numeric value. This alert triggers whenever the amount of an IBM ESS subsystem's cache that is offline exceeds a specific number.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: NVS Pending alert

Responding to this alert Alert dialog box help

This alert checks to see if non volatile storage (NVS) in an IBM ESS subsystem is pending due to a subsystem error. non volatile storage is battery-powered memory that contains data that IBM ESS has not yet written to disk.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Set the trigger value to TRUE. This alert triggers whenever non volatile storage in an IBM ESS subsystem is pending.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: NVS Failed alert

Responding to this alert Alert dialog box help

This alert checks if non volatile storage (NVS) for an IBM ESS subsystem has failed. non volatile storage is battery-powered memory that contains data that IBM ESS has not yet written to disk.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Set the trigger value to TRUE. This alert triggers whenever an IBM ESS subsystem's non volatile storage fails.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: NVS Disabled alert

Responding to this alert Alert dialog box help

This alert checks if one non volatile storage (NVS) in an IBM ESS subsystem is disabled. For example, this alert triggers if customer service disables a non volatile storage for maintenance. non volatile storage is battery-powered memory that contains data that IBM ESS has not yet written to disk.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Set the trigger value to TRUE. This alert triggers whenever non volatile storage in an IBM ESS subsystem is disabled.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: DFW Inhibited alert

Responding to this alert Alert dialog box help

This alert checks to see if DASD fast write (DFW) is inhibited for an IBM ESS subsystem. IBM ESS uses DFW to write data directly to disk, instead of storing it in cache. You can disable DFW during installation.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Set the trigger value to TRUE. This alert triggers whenever DASD fast write is inhibited for an IBM ESS subsystem.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Device Pinned Data alert

Responding to this alert Alert dialog box help

This alert checks if an IBM ESS volume has pinned data in the cache that IBM ESS cannot write to disk.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Set the trigger value to TRUE. This alert triggers whenever an IBM ESS volume has pinned data in the cache that cannot be written to disk.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Delayed DASD Fast Write alert

Responding to this alert Alert dialog box help

This alert checks if the number of delayed DASD fast write (DFW) requests for an IBM ESS subsystem exceeds a specified value. IBM ESS uses DFW to write data directly to disk, instead of storing it in cache. You can disable DFW during installation.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Specify a numeric value. This alert triggers whenever the number of delayed DASD fast write requests for an IBM ESS subsystem exceed a specific number.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: CFW Deactivated alert

Responding to this alert Alert dialog box help

The CFW Deactivated alert checks if cache fast write (CFW) is deactivated for an IBM ESS subsystem.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Set the trigger value to TRUE. This alert triggers whenever an IBM ESS subsystem's cache fast write deactivates.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: CFW and DFW Suspended alert

Responding to this alert Alert dialog box help

This alert checks if cache fast write (CFW) and DASD fast write (DFW) are suspended for an IBM ESS subsystem. IBM ESS uses DFW to write data directly to disk, instead of storing it in cache, and uses CFW to write data directly to cache. You can disable DFW during installation.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Set the trigger value to TRUE. This alert triggers whenever CFW or DFW are suspended for a subsystem.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Cache Fast Write Hit Ratio alert

Responding to this alert Alert dialog box help

This alert checks if the cache fast write (CFW) hit ratio for an IBM ESS subsystem is less than a specified value.

Enabled by default

No

Monitored resource (source)

Subsystem Serial Number	The serial number of the subsystem you want to monitor. You can use wildcards to monitor all subsystems.

Trigger values

Specify a numeric value. This alert triggers whenever the cache fast write hit ratio for an IBM ESS subsystem is less than a specific number.

Evaluation frequency (schedule)

The Storage Agent for IBM ESS evaluates this alert every hour, by default. Select a schedule that provides the level of monitoring that you want to achieve.

Related topics

- Alert concepts and procedures
- Storage Agent for IBM ESS overview

Storage Agent for RVA/SVA

RVA/SVA: Agent Initiated Alter Subsystem

Responding to this alert Alert dialog box Help

This alert triggers when you or another user modifies the subsystem.

When a user modifies the subsystem name, all users working with that subsystem should explore the agent again. Close the window for the Storage Agent for RVA/SVA. Right-click the host you want, then click **Storage Agent for RVA/SVA.** A new agent window displays. This allows the agent to process commands related to the modified subsystem properly.

Enabled by default

No.

Monitored resource (source)

Subsystem Name	The previous name of a subsystem whose name a user changed.

Special requirements

The alert can only monitor commands executed within the EMC ControlCenter console.

Trigger value

You do not need to change trigger values for this alert. However, you may want to change the severity level that the alert displays when triggered. Check the severity level you want for the alert: harmless, minor, warning, critical, or fatal.

Evaluation frequency (schedule)

The agent checks the trigger values continually. You cannot change the scheduling of this alert.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Agent Initiated DDSR Change

Responding to this alert Alert dialog box Help

The alert triggers when you or another ControlCenter user uses the agent to:

- start, stop, suspend, or resume one or more DDSR processes
- start an interval DDSR process (standard or single)
- modify the dynamic DDSR process or an interval DDSR process

Enabled by default

No.

Monitored resource (source)

DDSR Process ID	The DDSR process on which an agent command was executed. This is a unique name for interval processes or "Dynamic" for the dynamic DDSR process.

Special requirements

The alert can only monitor commands executed within the EMC ControlCenter console.

Trigger value

You do not need to change trigger values for this alert. However, you may want to change the severity level that the alert displays when triggered. Check the severity level you want for the alert: harmless, minor, warning, critical, or fatal.

Evaluation frequency (schedule)

The agent checks the trigger values continually. You cannot change the scheduling of this alert.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Agent Initiated Channel Alteration

Responding to this alert Alert dialog box Help

This alert triggers when you or another user modifies the channel interface. When you define the alert, you define only the subsystem name key. A value of * is recommended for this specification.

Enabled by default

Monitored resources (source)

RVA Subsystem Name	The name of the RVA or SVA subsystem where a user modified a channel interface.
Channel Interface ID	The interface ID of the channel interface a user modified.

Special requirements

The alert can only monitor commands executed within the EMC ControlCenter console.

Trigger value

You do not need to change trigger values for this alert. However, you may want to change the severity level that the alert displays when triggered. Check the severity level you want for the alert: harmless, minor, warning, critical, or fatal.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Agent Initiated MVS Device Alteration

Responding to this alert Alert dialog box Help

This alert triggers when you or another user modifies an MVS device.

Enabled by default

No.

Monitored resources (source)

RVA Subsystem Name	The name of the RVA or SVA subsystem where a user modified device characteristics.
Functional Device ID	The functional device ID (FDID) of the device a user modified.

Special requirements

The alert can only monitor commands executed within the EMC ControlCenter console.

Trigger value

You do not need to change trigger values for this alert. However, you may want to change the severity level that the alert displays when triggered. Check the severity level you want for the alert: harmless, minor, warning, critical, or fatal.

Evaluation frequency (schedule)

The agent checks the trigger values continually. You cannot change the scheduling of this alert.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Agent Initiated Vary of MVS Device

Responding to this alert Alert dialog box Help

This alert triggers when you or another user varies an MVS device online or offline.

Enabled by default

Monitored resource (source)

MVS Unit Address	The MVS device that a user varied online or offline.

Special requirements

The alert can only monitor Vary commands executed within the EMC ControlCenter console.

Trigger value

You do not need to change trigger values for this alert. However, you may want to change the severity level that the alert displays when triggered. Check the severity level you want for the alert: harmless, minor, warning, critical, or fatal.

Evaluation frequency (schedule)

The agent checks the trigger values continually. You cannot change the scheduling of this alert.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Channel Interface Disabled

Responding to this alert Alert dialog box Help

This alert triggers when the agent finds a channel interface that is disabled in an RVA or SVA subsystem. The agent checks the channel interfaces periodically, using the interval in the schedule applied to the alert.

Enabled by default

A pre-configured alert is enabled. However, you must check one or more severity levels (on the alert Conditions tab) for the alert to trigger.

Monitored resources (source)

Channel Interface	The channel interfaces you want to monitor with this alert. Specify either an exact ID or * for all interfaces.
Subsystem Name	The name of the subsystems you want to monitor. Specify either an exact subsystem name or * for all subsystems.

Note: You cannot combine wildcards and partial text.

Trigger value

Whether a channel interface is disabled.

Evaluation frequency (schedule)

Once per day by default.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: DDSR Not Active

Responding to this alert Alert dialog box Help

This alert triggers when the host has stopped informing RVA or SVA subsystems of deleted data sets. The space is not being released on those subsystems for data sets deleted on the current host.

Enabled by default

Yes.

Monitored resource (source)

Subsystem Name	The name of the subsystems you want to monitor. Specify either an exact subsystem name or * for all subsystems. The name of a subsystem not receiving information about deleted data sets from the current host.

Trigger value

Whether a DDSR process is monitoring space release on the host for data sets on the specified subsystems.

Evaluation frequency (schedule)

Once per hour by default.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: DDSR Not Active for a Volume

Responding to this alert Alert dialog box Help

This alert triggers when one or more volumes are not set up for release of storage space they are using. Data sets deleted on such volumes disappear from the host but continue to fill space on the RVA or SVA subsystem.

This alert, which monitors at the volume level, is more granular than the DDSR Not Active alert, which monitors at the host level. The current alert provides more specific information about how DDSR is working. For example, if multiple volumes are not being monitored by DDSR, or if unmonitored volumes have high deletion activity, the subsystem could experience performance problems as free space declines and space collection (for monitored volumes) increases automatically to compensate. In that case, create or modify DDSR processes on the current host to include the volumes for which this alert triggers.

Enabled by default

A pre-configured alert is enabled. However, you must check one or more severity levels (on the alert Conditions tab) for the alert to trigger.

Monitored resources (source)

Subsystem Name	The name of the subsystems you want to monitor. Specify either an exact subsystem name or * for all subsystems.
Volser	The volumes you want to monitor with this alert. Specify either an exact volume name or a * for all volumes.

Note: You cannot combine wildcards and partial text.

Trigger value

Whether a DDSR process is monitoring space release on the host volumes for data sets on the specified subsystems.

Evaluation frequency (schedule)

Once per day by default.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Interval DDSR with excessive interval

Responding to this alert Alert dialog box Help

This alert triggers when you define a DDSR process that waits too long between space release activity. Use the agent to modify the interval DDSR process and decrease the interval.

Enabled by default

A pre-configured alert is enabled. However, you must check one or more severity levels (on the alert Conditions tab) for the alert to trigger.

Monitored resource (source

DDSR Process ID	The name of the DDSR process you want to monitor. Specify either an exact name or a * for all interval processes. You cannot combine wildcards and partial text.

Trigger value

The length of the interval, in minutes, for DDSR processes.

Evaluation frequency (schedule)

Once per day by default.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: MVS Device Disabled

Responding to this alert Alert dialog box Help

This alert triggers when the agent finds an MVS device that is disabled in an RVA or SVA subsystem. In the keys, specify the devices and subsystems you want to monitor.

Enabled by default

A pre-configured alert is enabled. However, you must check one or more severity levels (on the alert Conditions tab) for the alert to trigger.

Monitored resources (source)

Subsystem Name	The name of the subsystems you want to monitor. Specify either an exact subsystem name or * for all subsystems.
Unit address	The MVS devices you want to monitor with this alert. Specify either an exact address (four-digit hex number) or * for all devices.

Note: You cannot combine wildcards and partial text.

Trigger value

You do not need to change trigger values for this alert. However, you may want to change the severity level that the alert displays when triggered. Check the severity level you want for the alert: harmless, minor, warning, critical, or fatal.

Evaluation frequency (schedule)

Once per day by default.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: NCL threshold

Responding to this alert Alert dialog box Help

This alert triggers when the Net Capacity Load (NCL) of the RVA or SVA subsystem exceeds a threshold. The NCL is a statistic that indicates how full the subsystem is.

Net Capacity Load is the most important status indicator for a subsystem. NCL ranges from 0 to 100. An NCL of 40-60 is healthy, while an NCL over 85 could result in increasingly severe performance problems and eventual shutdown. Because the RVA and SVA use virtual storage, including compression, host-based free space statistics are not as helpful as Net Capacity Load.

The alert checks Net Capacity Load once per hour by default. The alert triggers if it finds a high NCL at the time that it checks. Use a more frequent schedule if desired.

Enabled by default

Yes.

Monitored resource (source)

The alert monitors the RVA or SVA subsystems that you indicate in the following field.

Subsystem Name	Modify Alert Keys dialog box: The name of the subsystems you want to monitor. Specify either an exact subsystem name or a * for all subsystems.

Trigger values

The Net Capacity Load is the trigger value. Net Capacity Load is a percentage of actual disk capacity used in the RVA or SVA. This probably differs from the operating system view of the storage, as the subsystem compresses the data before writing it. In ordinary conditions, healthy production subsystems have a Net Capacity Load ranging from 40-60, though 40 could indicate poor utilization of the subsystem. An NCL over 85 merits at least a warning, and 95 or over is critical or even fatal.

Evaluation frequency (schedule)

Once per hour on the hour by default. You can select a schedule with a different frequency if desired.

Note: The Net Capacity Load may exceed a threshold value without notification until the interval set by the schedule expires. Use a schedule that ensures an evaluation frequency to suit your needs. Alternatively, set the NCL trigger values slightly lower to allow more time to react.

Recommended notifications (Management Policies)

Create or add a management policy that will alert multiple personnel of a Net Capacity Load alert at severity warning, fatal, or critical.

Autofixes

There are no pre-configured autofixes for this alert. Automated responses to the alert could include:

- Automatically deleting older log data sets and other low-priority data from the RVA or SVA
- Increasing interval DDSR frequency or switching to dynamic DDSR

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: NCL Change Over Time

Responding to this alert Alert dialog box Help

This alert triggers when the Net Capacity Load (NCL) changes more than a certain amount during a period of time. For example: If a subsystem's NCL grows from 20% to 25% in an hour, then the alert would show an increase of 5 and trigger a critical alert.

For this alert, it is suggested that you set a management policy to email an appropriate staff member of the occurrence. This is because the alert may reset (and disappear from your console) if the problem does not recur in the next scheduled check. If it occurs overnight you may want to know that the problem occurred even though the condition did not continue to worsen.

Enabled by default

A pre-configured alert is enabled. However, you must check one or more severity levels (on the alert Conditions tab) for the alert to trigger.

Monitored resource (source)

Subsystem Name	The name of the subsystems you want to monitor. Specify either an exact subsystem name or a * for all subsystems.

Trigger value

The percentage increase in the Net Capacity Load during the scheduled interval. Define a trigger value in conjunction with the schedule that you set for the alert. For example, a trigger value of 3% might trigger a warning when the scheduled evaluation is every hour. In contrast, a trigger value of 6% might trigger a warning when the scheduled evaluation is every two hours.

Evaluation frequency (schedule)

Once per hour by default. If you change the schedule, ensure that this interval remains long enough for the percentage change to have significance. See "Trigger value" for more information about how the schedule affects the triggering of the alert.

Possible uses of this alert

- Monitoring the RVA or SVA subsystem
- Monitoring the Net Capacity Load of an RVA or SVA

Related alerts

- Net Capacity Load threshold alert

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Uncollected Free Space Threshold

Responding to this alert Alert dialog box Help

This alert triggers when the percentage of uncollected free space in an RVA or SVA subsystem exceeds a threshold. If you are observing performance delays for the subsystem, excessive uncollected free space could be a contributor to the problem. The subsystem is overtaxed in terms of collection activity. Use this statistic in combination with other factors such as NCL and performance behavior to ascertain whether there is a problem.

Enabled by default

Yes.

Monitored resource (source)

Subsystem Name	The name of the subsystems you want to monitor. Specify either an exact subsystem name or * for all subsystems.

Trigger value

The uncollected free space divided by the total capacity of the subsystem.

Evaluation frequency (schedule)

Once per hour by default.

Possible uses of this alert

Monitoring collection activity

Related alerts

- DDSR Not Active alert
- DDSR Not Active for a Volume alert

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

Storage Agent for Symmetrix

Symmetrix general statistics alerts

Responding to this alert Alert dialog box Help

The following alerts can be configured to monitor statistics associated with a Symmetrix unit.

The alert message is displayed in the Active Alerts panel, is formatted with variables, and may contain additional text not described in this topic. The alert name is the formal name of the alert and can be viewed by navigating to Administration, Alert Management, Alert Templates, <*AgentName*>, <*AlertType*>.

Alert Name	Alert Message	Trigger value	Description
I/O per second	Symmetrix *SymmID*: I/O per second is *value*	Critical >= 20000 Warning >= 15000 Minor >= 12000	Symmetrix I/Os per second exceed specified value
Kbytes read per second	Symmetrix *SymmID*: KB/sec read is *value*	Critical >= 20000 Warning >= 15000 Minor >= 12000	Symmetrix kilobytes read per second is specified value
Kbytes written per second	Symmetrix *SymmID*: KB/sec written is *value*	Critical >= 20000 Warning >= 15000 Minor >= 12000	Symmetrix kilobytes written per second is specified value
Reads per second	Symmetrix *SymmID*: Reads/sec is *value*	Critical >= 20000 Warning >= 15000 Minor >= 12000	Symmetrix reads per second is the specified value
Throughput	Symmetrix *SymmID*: Throughput is *value*	Critical >= 20000 Warning >= 15000 Minor >= 12000	Symmetrix total throughput is specified value
Total Hit Ratio %	Symmetrix *SymmID*: Hit ratio is *value*	Critical >= 50 Minor >= 65	Symmetrix total hit ratio is specified value
Write Ratio %	Symmetrix *SymmID*: Write ratio is *value*	Warning >= 70 Minor >= 60	Symmetrix write ratio is specified value
Writes per second	Symmetrix *SymmID*: Writes/sec is *value*	Critical >= 20000 Warning >= 15000 Minor >= 12000	Symmetrix writes per second is the specified value

Alert type

Count

Enabled by default

Performance alerts are disabled by default.

Monitored resource (source)

You do not specify a source for this alert.

Evaluation frequency (schedule)

The evaluation frequency is controlled by the Symmetrix Agent. The default is every 15 minutes.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for Symmetrix storage. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

Monitoring Symmetrix I/O and throughput.

Note: The Symmetrix general alerts are not enabled by default when you install the Symmetrix Agent. If you want to receive one of these alerts, you should ensure that the alert settings are appropriate for your environment. Create a baseline of statistics for Symmetrix performance, and adjust the alert settings for acceptable performance levels.

Related topics

- Introduction to alerts
- Alert concepts and procedures
- Viewing real-time performance statistics
- Responding to Symmetrix device alerts
- Responding to Symmetrix director alerts
- Responding to Symmetrix disk alerts
- Responding to Symmetrix alarm alerts
- Responding to Symmetrix general alerts
- Responding to Symmetrix port alerts
- Symmetrix device alerts
- Symmetrix director alerts
- Symmetrix disk alerts
- Symmetrix alarm alerts
- Symmetrix port alerts

Symmetrix alarm alerts

Responding to this alert Alert dialog box Help

The Symmetrix alarm alerts trigger when one of the following events occurs.

The alert message is displayed in the Active Alerts panel, is formatted with variables, and may contain additional text not described in this topic. The alert name is the formal name of the alert and can be viewed by navigating to Administration, Alert Management, Alert Templates, <*AgentName*>, <*AlertType*>.

Alert Name	Alert Message	Description
12 Volts On (Not Normal Mode)	12 Volts On (Not Normal Mode) - Symmetrix *symmID*	
AC Line Problems Detected Alert	AC line problems detected - Symmetrix *symmID*	AC line problems detected
Alarm Signal Set, But No Alarm Found	Alarm Signal Set, But No Alarm Found - Symmetrix *symmID*	
All SRDF Links Not Operational Alert	All SRDF links not operational	All SRDF links not operational
Base Only Access Alert	Agent only has Base Access to Symmetrix *symmID*	
Comm Board SW Data Does Not Match Expected Data	Comm Board Software Data Does Not Match Data Expected by the Utility Program - Symmetrix *symmID*	Comm board SW data does not match expected data. This is an environmental error for Symmetrix 5 only.

Device Resynchronization Process Has Started	Device Resynchronization Process Has Started- Symmetrix *symmID*	
Director A Fault Alert	Director A fault - Symmetrix *symmID*	Fault in director A
Director B Fault Alert	Director B fault - Symmetrix *symmID*	Fault in director B
Director Status Alert	Director *symmID.DirectorID* is *message*	This alert displays the status of a Symmetrix Director.
Disk Adapter Dual Initiator Failed to Impl Monitor	Disk Adapter Dual Initiator Failed to Impl Monitor- Symmetrix *symmID*	
Environmental Alarm Alert	Environmental Alarm - Symm *symmID*	Environmental alarm
Environment Sense Cable is Missing	Environment Sense Cable is Missing - Symmetrix *symmID*	
Fibre Low Light Level Alert	Fibre low light level- Symmetrix *SymmID*	Fibre Channel Optical module problem adapter reported error.
High Charge State Missing	Symmetrix Battery Error. The battery is not completely charged - Symmetrix *symmID*	High Charge State Missing, expected within two minutes after a power-up or a clock inconsistency found or a director was plugged in without system power-up.
Hot Spare Device Invoked Alert	Hot Spare device invoked - Symmetrix *symmID*	Hot Spare invoked
Latched Alarms Discovered for Power System	Latched Alarms Discovered for Power System - Symmetrix *symmID*	
M1 Resynchronized with M2 Alert	M1 resynchronized with M2 - Symmetrix *symmID*	M1 resynchronization with M2 has completed successfully
M2 Resynchronized with M1 Alert	M2 resynchronized with M1- Symmetrix *symmID*	M2 resynchronization with M1 has completed successfully
Memory Banks Automatically Disabled	Memory Banks Automatically Disabled Due to Cache Error - Symmetrix *symmID*	
Migration Completed	Migration System Completed- Symmetrix *symmID*	
No Access Alert	Agent has no access to Symmetrix *symmID*	Agent cannot communicate with the Symmetrix. Access failure.
No PC Connection Time Found in Table	No PC Connection Time Found in Table - Symmetrix *symmID*	Microcode error: No PC connection time found in PC table.
No statistics for remote Symmetrix	Cannot get statistics for remote Symmetrix *symmID*	Unable to retrieve statistics from the remote Symmetrix
Old Board Information Does Not Match Current Read	Old Director Board Information Does Not Match That Expected - Symmetrix *symmID*	Contact EMC Hardware Support.
PC Communications Error Alert	PC Communications Error - Symmetrix *SymmID*	The Service Processor could not complete a call for service.
PC Successfully Called Home	PC Successfully Called Home - Symmetrix *symmID*	The PC successfully called home to report an error.
Power-on Time For Env Inconsistency During Env Tests	Power-on Time For Env Inconsistency During Env Tests - Symmetrix *symmID*	
Power Subsystem Error	Power Subsystem Error - *Description* Symmetrix *SymmID*	Alarm signals set - power subsystem error.

RAID Device Not Ready Alert	RAID device not ready - *SymmID.DeviceID (DirID)*	RAID device not ready
RAID Device Write Disabled Alert	RAID device write disabled - *SymmID.DeviceID (DirID)*	RAID device write disabled
Report 'Disabled Memory Bank' to Host	Report 'Disabled Memory Bank' to Host - Symmetrix *symmID*	
Service Processor Down Alert	Service processor down- Symmetrix *SymmID*	The Service Processor is not communicating with the Symmetrix, forces a reboot of the Service Processor.
SRDF Error	SRDF Error- Symmetrix *symmID*	
SRDF Hot Spare Device Invoked	SRDF Hot Spare device invoked - Symmetrix *symmID*	A Hot Spare was automatically invoked by Enginuity for an SRDF R2 device on another box.
SRDF Initiated SIM Message	SRDF Initiated SIM Message - Symmetrix *symmID*	
SRDF Link Error Alert	SRDF link error - Symmetrix *symmID*	A single SRDF link in an SRDF group is not operational.
SRDF Link Operational	SRDF link now operational - Symmetrix *symmID*	A single SRDF link in an SRDF group is now operational after a previous error.
SRDF Links All Operational	SRDF Links All Operational- Symmetrix *symmID*	All SRDF links are operational now (after a previous failure).
SRDF M2 Device Not Ready	SRDF M2 Device Not Ready - Symmetrix *symmID*	
SRDF Operations Suspended for Some Devices	SRDF operations suspended for some devices - Symmetrix *symmID*	
SRDF Symmetrix Diagnostic Event Trace Trigger	Remote SRDF Diagnostic Event Trace Trigger - Symmetrix *symmID*	
Symmetrix Diagnostic Event Trace Trigger	Diagnostic Event Trace Trigger - Symmetrix *symmID*	
Temperature Alert	Temperature - Symmetrix *symmID*	Temperature alert
Thermal Detector Test Failure	Thermal Detector Test Failure - Symmetrix *symmID*	
Thermal Event	Thermal Event - Symmetrix *symmI*D	
Too Many Suspend/Halt Chains Switching to Adaptive Copywrite Pending	Too Many Suspend/Halt Chains Switching to Adaptive Copywrite Pending - Symmetrix *symmID*	
Validity Problem With Bits Collected in Environment	Validity Problem With Bits Collected in Environment - Symmetrix *symmID*	
Volume Not Ready Alert	Volume not ready - *SymmID.DeviceID* (*DirID*)	Volume is not ready

Alert type

State

Enabled by default

Yes

Monitored resource (source)

You do not specify a source for this alert.

Trigger values

Triggered by TRUE for all values.

Evaluation frequency (schedule)

The default frequency is controlled by the Alert Polling Data Collection Policy.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for Symmetrix storage. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

Monitoring Symmetrix alarms and error messages.

Note: The Symmetrix alarm alerts are enabled by default when you install the Symmetrix Agent. The informational alerts are disabled by default.

Related topics

- Introduction to alerts
- Alert concepts and procedures
- Viewing real-time performance statistics
- Responding to Symmetrix device alerts
- Responding to Symmetrix director alerts
- Responding to Symmetrix disk alerts
- Responding to Symmetrix alarm alerts
- Responding to Symmetrix general alerts
- Responding to Symmetrix port alerts
- Symmetrix device alerts
- Symmetrix director alerts
- Symmetrix disk alerts
- Symmetrix general alerts
- Symmetrix port alerts

Symmetrix director statistics alerts

Responding to this alert Alert dialog box Help

The following alerts can be configured to monitor a Symmetrix back end disk director.

The alert message is displayed in the Active Alerts panel, is formatted with variables, and may contain additional text not described in this topic. The alert name is the formal name of the alert and can be viewed by navigating to Administration, Alert Management, Alert Templates, *<AgentName>*, *<AlertType>*.

Alert Name	Alert Message	Alert Type	Trigger value	Description
% Hit Ratio	Director *SymmID. directorID:* Hit Ratio is *value*	Count	Critical >= 50 Minor >= 65	Symmetrix back end disk director hit ratio status
% Write Ratio	Director *SymmID. directorID:* Write Ratio is *value*	Count	Warning >= 70 Minor >= 60	Symmetrix back end disk director write ratio status
I/O per second	Director *SymmID. directorID:* I/O per second is *value*	Count	Critical >= 8000 Warning >= 6000 Minor >= 4000	Symmetrix back end disk director I/O per second status

The following alerts can be configured to monitor a Symmetrix front end Fibre Channel host director.

Alert Name	Alert Message	Alert Type	Trigger value	Description
% Hit Ratio	Director *SymmID. directorID:* Hit Ratio is *value*	Count	Critical >= 50 Minor >= 65	Symmetrix front end Fibre Channel host director hit ratio status
% Write Ratio	Director *SymmID. directorID:* Write Ratio is *value*	Count	Warning >= 70 Minor >= 60	Symmetrix front end Fibre Channel host director write ratio status
I/O per second	Director *SymmID. directorID:* I/O per second is *value*	Count	Critical >= 8000 Warning >= 6000 Minor >= 4000	Symmetrix front end Fibre Channel host director I/O per second status

The following alerts can be configured to monitor a Symmetrix front end SCSI host director.

Alert Name	Alert Message	Alert Type	Trigger value	Description
% Hit Ratio	Director *SymmID. directorID:* Hit Ratio is *value*	Count	Critical >= 50 Minor >= 65	Symmetrix front end SCSI host director hit ratio status
% Write Ratio	Director *SymmID. directorID:* Write Ratio is *value*	Count	Warning >= 70 Minor >= 60	Symmetrix front end SCSI host director write ratio status
I/O per second	Director *SymmID. directorID:* I/O per second is *value*	Count	Critical >= 8000 Warning >= 6000 Minor >= 4000	Symmetrix front end SCSI host director I/O per second status

Enabled by default

No.

Monitored resource (source)

You do not specify a source for this alert.

Evaluation frequency (schedule)

The evaluation frequency is controlled by the Symmetrix Agent. The default is every 15 minutes.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for Symmetrix storage. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

Being notified when a Symmetrix director goes offline or becomes inoperational.

Related topics

- Introduction to alerts
- Alert concepts and procedures
- Viewing real-time performance statistics
- Responding to Symmetrix device alerts
- Responding to Symmetrix director alerts
- Responding to Symmetrix disk alerts
- Responding to Symmetrix alarm alerts
- Responding to Symmetrix general alerts
- Responding to Symmetrix port alerts
- Symmetrix device alerts
- Symmetrix disk alerts
- Symmetrix alarm alerts
- Symmetrix general alerts
- Symmetrix port alerts

Symmetrix disk statistics alerts

Responding to this alert Alert dialog box Help

The following alerts can be configured to monitor statistics associated with Symmetrix disks.

The alert message is displayed in the Active Alerts panel, is formatted with variables, and may contain additional text not described in this topic. The alert name is the formal name of the alert and can be viewed by navigating to Administration, Alert Management, Alert Templates, <*AgentName*>, <*AlertType*>.

Alert Name	Alert Message	Trigger value	Description
Kbytes read per second	Disk *symmID.diskID:* KB/sec read is *value*	Critical >= 20000 Warning >= 16000 Minor >= 12000	Kilobytes read per second for the disk
Kbytes written per second	Disk *symmID.diskID:* KB/sec written is *value*	Critical >= 20000 Warning >= 16000 Minor >= 12000	Kilobytes written per second for the disk
Reads per second	Disk *symmID.diskID:* Reads/sec is *value*	Critical >= 150 Warning >= 120 Minor >= 100	The reads per second for the disk
Writes per second	Disk *symmID.diskID:* Writes/sec is *value*	Critical >= 150 Warning >= 120 Minor >= 100	The writes per second for the disk

Alert type

Count

Enabled by default

Performance alerts are disabled by default.

Monitored resource (source)

You do not specify a source for this alert.

Evaluation frequency (schedule)

The evaluation frequency is controlled by the Symmetrix Agent The default is every 15 minutes.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for Symmetrix storage. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

Monitoring Symmetrix disk I/O and throughput.

Note: The Symmetrix disk alerts are not enabled by default when you install the Symmetrix Agent. If you want to receive one of these alerts, you should ensure that the alert settings are appropriate for your environment. Create a baseline of statistics for disk performance, and adjust the alert settings for acceptable performance levels.

Related topics

- Introduction to alerts
- Alert concepts and procedures
- Viewing real-time performance statistics
- Responding to Symmetrix device alerts
- Responding to Symmetrix director alerts
- Responding to Symmetrix disk alerts
- Responding to Symmetrix alarm alerts
- Responding to Symmetrix general alerts
- Responding to Symmetrix port alerts
- Symmetrix device alerts
- Symmetrix director alerts
- Symmetrix alarm alerts
- Symmetrix general alerts
- Symmetrix port alerts

Symmetrix device statistics alerts

Responding to this alert Alert dialog box Help

The following alerts can be configured to monitor statistics associated with Symmetrix devices.

The alert message is displayed in the Active Alerts panel, is formatted with variables, and may contain additional text not described in this topic. The alert name is the formal name of the alert and can be viewed by navigating to Administration, Alert Management, Alert Templates, *<AgentName>*, *<AlertType>*.

Alert Name	Alert Message	Trigger value	Description
Hits per second	Device *symmID.deviceID:* Hits/sec is *value*	Critical >= 8000 Warning >= 6000 Minor >= 4000	The device hits per second is the specified value
I/O per second	Device *symmID.deviceID:* I/O per sec is *value*	Critical >= 8000 Warning >= 6000 Minor >= 4000	The device I/Os per second is the specified value
Kbytes read per second	Device *symmID.deviceID:* KB/sec read is *value*	Critical >= 20000 Warning >= 15000 Minor >= 12000	The device kilobytes read per second is the specified value
Kbytes written per second	Device *symmID.deviceID:* KB/sec written is *value*	Critical >= 20000 Warning >= 15000 Minor >= 12000	The device kilobytes written per second is the specified value
Reads per second	Device *symmID.deviceID:* Reads/sec is *value*	Critical >= 8000 Warning >= 6000 Minor >= 4000	The device reads per second is the specified value
Writes per second	Device *symmID.deviceID:* Writes/sec is *value*	Critical >= 8000 Warning >= 6000 Minor >= 4000	The device writes per second is the specified value

Alert type

Count

Enabled by default

Performance alerts are disabled by default.

Monitored resource (source)

You do not specify a source for this alert.

Evaluation frequency (schedule)

The evaluation frequency is controlled by the Symmetrix Agent. The default is every 15 minutes.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for Symmetrix storage. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

Monitoring Symmetrix device I/O and throughput.

Note: The Symmetrix device alerts are not enabled by default when you install the Symmetrix Agent. If you want to receive one of these alerts, you should ensure that the alert settings are appropriate for your environment. Create a baseline of statistics for device performance, and adjust the alert settings for acceptable performance levels.

Related topics

- Introduction to alerts
- Alert concepts and procedures
- Viewing real-time performance statistics
- Responding to Symmetrix device alerts
- Responding to Symmetrix director alerts
- Responding to Symmetrix disk alerts
- Responding to Symmetrix alarm alerts
- Responding to Symmetrix general alerts
- Responding to Symmetrix port alerts
- Symmetrix director alerts
- Symmetrix disk alerts
- Symmetrix alarm alerts
- Symmetrix general alerts
- Symmetrix port alerts

Symmetrix front end port statistics alerts

Responding to this alert Alert dialog box Help

The alert message is displayed in the Active Alerts panel, is formatted with variables, and may contain additional text not described in this topic. The alert name is the formal name of the alert and can be viewed by navigating to Administration, Alert Management, Alert Templates, *<AgentName>*, *<AlertType>*.

The following alerts can be configured to monitor statistics associated with Symmetrix Fibre Channel front end ports.

Alert Name	Alert Message	Trigger value	Description
Port I/O per second	Port s*ymmID.dirID.portID:* I/O per second is *value*	Critical >= 8000 Warning >= 6000 Minor >= 4000	I/Os per second for the Fibre Channel port
Port Throughput	Port s*ymmID.dirID.portID:* Throughput is *value*	Critical >= 70000 Warning >= 60000 Minor >= 50000	Throughput for the Fibre Channel port

The following alerts can be configured to monitor statistics associated with Symmetrix SCSI front end ports.

Alert Name	Alert Message	Trigger value	Description
Port I/O per second	Port s*ymmID.dirID.portID:* Port I/O per second is *value*	Critical >= 8000 Warning >= 6000 Minor >= 4000	I/Os per second for the SCSI port
Port Throughput	Port s*ymmID.dirID.portID:* Throughput is *value*	Critical >= 70000 Warning >= 60000 Minor >= 50000	Throughput for the SCSI port

Alert type

Count

Enabled by default

Performance alerts are disabled by default.

Monitored resource (source)

You do not specify a source for this alert.

Evaluation frequency (schedule)

The evaluation frequency is controlled by the Symmetrix Agent. The default is every 15 minutes.

Notification policies (management policies)

Set up management policies that route these messages to the ControlCenter administrator or the individual responsible for Symmetrix storage. If you do not attach a management policy to this alert, all ControlCenter users receive it.

Possible uses of this alert

Monitoring Symmetrix port I/O and throughput.

Note: The Symmetrix port alerts are not enabled by default when you install the Symmetrix Agent. If you want to receive one of these alerts, you should ensure that the alert settings are appropriate for your environment. Create a baseline of statistics for port performance, and adjust the alert settings for acceptable performance levels.

Related topics

- Introduction to alerts
- Alert concepts and procedures
- Viewing real-time performance statistics
- Responding to Symmetrix device alerts
- Responding to Symmetrix director alerts
- Responding to Symmetrix disk alerts
- Responding to Symmetrix alarm alerts
- Responding to Symmetrix general alerts
- Responding to Symmetrix port alerts
- Symmetrix device alerts
- Symmetrix director alerts
- Symmetrix disk alerts
- Symmetrix alarm alerts
- Symmetrix general alerts

Tape Agent for MVS

STK Tape: ACS Disconnected alert

Responding to this alert Alerts dialog box help

The alert triggers when an Automated Cartridge System (ACS) becomes disconnected from an MVS host. The host can no longer communicate with the StorageTek tape library. Volume mounts are impossible for reads or writes, and any data sets needed in the tape library are inaccessible to the applications running on the given host. The alert clears when the ACS is no longer disconnected. It is possible for an ACS to be disconnected from one host and remain connected to others. The alert triggers for any disconnected host.

Enabled by default

Yes

Monitored resource (source)

There is only one monitored resource for this alert: ACS. Type the hexadecimal number of the ACS or * for all ACSs.

When specifying keys, pay special attention to the monitoring of ACSs by multiple MVS hosts. The ACSs attached to a host are numbered consecutively (00 for the first ACS, then 01, 02 and so forth). When a single ACS is connected to multiple hosts, it may have a different number on different hosts.

The ACSs you want to monitor must be connected to one or more hosts that you specify in the Hosts tab of the Edit Alert dialog box.

Trigger values

You do not need to change the trigger values for this alert.

Evaluation frequency

Agent monitors HSC messages continually for this alert condition.

Autofixes

There are no pre-defined autofixes for this alert.

Possible uses of this alert

- Monitoring ACS and LSM availability

Related topics

- Alert concepts and procedures
- Learning which ACSs are connected to a host

STK Tape: Cells Free_Percentage alert

Responding to this alert Alerts dialog box help

This alert triggers when the percentage of free cells in the location given by the keys falls below the threshold values. Different alerts can be set for different Library Storage Modules (LSM) or not, depending on preference.

Enabled by default

Yes

Monitored resource (source)

The alert monitors the following resources.

ACS	The hex ACS number to which this alert applies. If ACS is not specified (or specified as *), LSM is ignored.
LSM	The hex LSM number to which this alert applies. LSM is effective only if ACS has a definite value.

To monitor a single LSM with this alert, specify keys for the ACS and LSM (for example, an ACS named 01 and an LSM named 03).

Trigger value

The percentage of free cells in the monitored resources.

Evaluation frequency (schedule)

Every day at midnight by default.

Possible uses of this alert

- Ensuring sufficient free cells
- Reducing operator intervention

Related alerts

- Volumes Inactive_Count alert

Related topics

- Alert concepts and procedures

STK Tape: Cleaners Select_Count alert

Responding to this alert Alerts dialog box help

This alert triggers if the average select count for cleaning cartridges in the location and with the media type given by the keys rises above the threshold value. Different alerts can be set for different locations and for different media types.

Enabled by default

Yes

Monitored resource (source)

The alert monitors the following resources.

ACS	The hex ACS number to which this alert applies. If Automated Cartridge System (ACS) is not specified (or specified as *), Library Storage Modules (LSM) is ignored.
LSM	The hex LSM number to which this alert applies. LSM is effective only if ACS has a definite value.
Media	The media type as displayed on the volume display (for example, STANDARD and ECART). Filtering status, reports, or alerts by media type

Trigger value

The average number of uses of the cleaning cartridges that are in the monitored resources (and of a given media type, if specified).

Evaluation frequency (schedule)

Every day at midnight.

Related topics

- Ensuring sufficient cleaning cartridges
- Understanding select count for cleaning cartridge alerts and reports

STK Tape: Drives Mount_Eject alert

Responding to this alert Alerts dialog box help

This alert triggers whenever a mount is issued for a volume in a StorageTek library to a drive not in a StorageTek library. The alert occurs when the event takes place. The alert occurs when the event takes place. The alert is not cleared by the agent. You must reset the alert manually after you resolve the condition.

Enabled by default

Yes

Monitored resource (source)

The alert monitors the following resources.

Unit address	The unit on which the mount occurred.
Volume	The volser to be mounted. Available wildcards are % for a single character or * for multiple characters anywhere in the input string.

Trigger value

A volume is in the monitored library resource, but the drive is not in a library.

Evaluation frequency (schedule)

Agent continuously monitors MVS messages for the alert condition.

Possible uses of this alert

- Reducing operator intervention
- Monitoring drives for excessive operator intervention
- Monitoring mistargeted or inefficient mount requests

Related topics

- Managing tape drives in a tape library
- Managing volumes in a StorageTek tape library

STK Tape: Drives Mount_Enter alert

Responding to this alert Alerts dialog box help

This alert triggers whenever a mount is issued for a volume not in a StorageTek library to a drive inside a StorageTek library. The alert occurs when the event takes place. The alert occurs when the event takes place. The alert is not cleared by the agent. You must reset the alert manually after you resolve the condition.

Enabled by default

Yes

Monitored resource (source)

The alert monitors the following resources.

Unit address	The unit on which the mount occurred.
Volume	The volser to be mounted. Available wildcards are % for a single character or * for multiple characters anywhere in the input string.

Trigger value

A drive in the monitored library needs a volume, but the volume is not in the library.

Evaluation frequency (schedule)

Agent continuously monitors MVS messages for the alert condition.

Possible uses of this alert

- Reducing operator intervention
- Monitoring drives for excessive operator intervention
- Monitoring mistargeted or inefficient mount requests

Related topics

- Managing tape drives in a tape library
- Managing volumes in a StorageTek tape library

STK Tape: Drives Mount_Manual_Scratch alert

Responding to this alert Alerts dialog box help

This alert triggers whenever a scratch mount is issued to a drive not in a StorageTek library, unless the drive has a Cartridge Stack Loader, also called an ACL. The alert occurs when the event takes place. The alert is not cleared by the agent. You must reset the alert manually after you resolve the condition.

Enabled by default

No

Monitored resource (source)

The alert monitors the following resources.

Unit address	The unit on which the mount occurred.

Trigger value

A scratch mount is called for on a non-library drive that does not have ACL installed.

Evaluation frequency (schedule)

Once per hour.

Possible uses of this alert

- Reducing operator intervention
- Monitoring drives for excessive operator intervention
- Monitoring mistargeted or inefficient mount requests

Related topics

- Managing tape drives in a tape library
- Managing volumes in a StorageTek tape library

STK Tape: Drives Mount_Eject_Enter alert

Responding to this alert Alerts dialog box help

This alert triggers whenever a mount is issued for a volume in a StorageTek library to a drive in a different StorageTek library. The alert occurs when the event takes place. The alert is not cleared by the agent; you must clear it yourself.

Enabled by default

Yes

Monitored resource (source)

The alert monitors the following resources.

Unit address	The unit on which the mount occurred.
Volume	The volser to be mounted. Available wildcards are % for a single character or * for multiple characters anywhere in the input string.

Trigger value

A volume is in the monitored library resource, but the drive is not in a library.

Evaluation frequency (schedule)

Agent continuously monitors MVS messages for the alert condition.

Possible uses of this alert

- Reducing operator intervention
- Monitoring drives for excessive operator intervention
- Monitoring mistargeted or inefficient mount requests

Related topics

- Managing tape drives in a tape library
- Managing volumes in a StorageTek tape library

STK Tape: Drives Mount_Eject_Enter alert

Responding to this alert Alerts dialog box help

This alert triggers whenever a mount is issued for a volume in a StorageTek library to a drive in a different StorageTek library. The alert occurs when the event takes place. The alert is not cleared by the MVS agent; you must clear it yourself.

Enabled by default

Yes

Monitored resource (source)

The alert monitors the following resources.

Unit address	The unit on which the mount occurred.
Volume	The volser to be mounted. Available wildcards are % for a single character or * for multiple characters anywhere in the input string.

Trigger value

A volume is in the monitored library resource, but the drive is not in a library.

Evaluation frequency (schedule)

Agent continuously monitors MVS messages for the alert condition.

Possible uses of this alert

- Reducing operator intervention
- Monitoring drives for excessive operator intervention

Possible uses of this alert

- Reducing operator intervention
- Monitoring drives for excessive operator intervention
- Monitoring mistargeted or inefficient mount requests

Related topics

- Managing tape drives in a tape library
- Managing volumes in a StorageTek tape library

STK Tape: Drives Mount Pass Thru alert

Responding to this alert Alerts dialog box help

This alert triggers whenever an MVS mount requires a mechanical pass-through from one LSM to another within the same ACS. This alert can help you identify volumes that need to be placed in a different LSM to increase responsiveness and decrease the mechanical activity needed to satisfy mount requests. The alert occurs when the event takes place. The alert is not cleared by the agent. You must reset the alert manually after you resolve the condition.

Enabled by default

No

Monitored resource (source)

The alert monitors the following resources.

Unit Address	The unit on which the mount occurred.
Volume	The volser to be mounted. Available wildcards are % for a single character or * for multiple characters anywhere in the input string.

Trigger value

The alert triggers whenever a pass-through is required.

Evaluation frequency (schedule)

The alert monitors for pass-throughs continuously. You cannot change the evaluation frequency.

Possible uses of this alert

- Monitoring mistargeted or inefficient mount requests

Related alerts

- Drives Mount_Pass_Thru_Count Alert

Related topics

- Alert concepts and procedures

STK Tape: Drives Mount_Pass_Thru_Count alert

Responding to this alert Alerts dialog box help

This alert triggers whenever the number of pass-throughs exceeds a threshold for a single MVS image. The alert monitors the MVS image on which the agent is running.

Enabled by default

No

Monitored resource (source)

The alert monitors the following resources.

System	The MVS system whose pass-through count should be monitored.

Trigger value

The number of pass-throughs required for mount requests from a single MVS system in a given period of time. The time period is the interval defined by the schedule. For example, a pass-through count of 3 for a schedule of Hour_01 means that 3 pass-throughs occurred in a single hour for the MVS system.

Evaluation frequency (schedule)

Every hour by default.

Possible uses of this alert

- Monitoring mistargeted or inefficient mount requests

Related alerts

- Drives Mount Pass Thru alert

Related topics

- Alert concepts and procedures

STK Tape: HSC Inactive alert

Responding to this alert Alerts dialog box help

This alert triggers whenever the Host Software Component (HSC) is not active or is not running at FULL service level. The alert is cleared whenever the HSC is at FULL service level. This is an agent-controlled alert and has no keys and no schedule.

Enabled by default

Yes. The alert is enabled to trigger with a severity of Critical.

Monitored resource (source)

This is an agent-controlled alert. You cannot specify monitored resources or a schedule. The agent checks hosts to see whether the HSC is running, and alerts you if it is not.

Trigger values

The alert triggers when the HSC software is not active or running at service level of FULL on a host. You do not need to change the trigger values for this alert.

Evaluation frequency (schedule)

Agent monitors HSC messages continually for this alert condition. If you want to change the severity of the alert, clear the checkbox next to the severity you no longer want to use, then check the severity you want.

Autofixes

There are no predefined autofixes for this alert.

Possible uses of this alert

- Monitoring host software (HSC) for StorageTek libraries

Related topics

- Alert concepts and procedures

STK Tape: LMU Error alert

Responding to this alert Alerts dialog box help

The alert informs you when an Library Management Unit (LMU) error occurs that the Host Software Component (HSC) cannot correct. The alert triggers when the HSC issues messages SLS0698I and SLS0699I (which are issued simultaneously). A variety of conditions could trigger the LMU error alert. Usually these conditions are hardware-related. They can require attention by StorageTek support.

Enabled by default

Yes

Monitored resource (source)

The alert monitors the following resources.

ACS	The hex Automated Cartridge System (ACS) number to which this alert applies. This key is defined so you know which ACS has the problem when the alert triggers. When you create the alert, the recommended specification is * (all ACSs). When the alert triggers, the exact ACS is given in the Active Alerts window.
Action code	A one- or two-letter code given in message SLS0698I. This key is defined to provide you information about the alert condition when the alert actually triggers. Consult StorageTek documentation of message SLS698I to research the meaning of the request code.
Error code	An error code given in message SLS699I. The format of the code is *nn/mm.* This key is defined to provide you information about the alert condition when the alert is actually triggered. Consult StorageTek documentation of message SLS699I to research the meaning of the error code.

Trigger values

You do not need to change the trigger values for this alert.

Evaluation frequency (schedule)

An agent monitors HSC messages continually for this alert condition.

Autofixes
There are no predefined autofixes for this alert.

Possible uses of this alert
- Monitoring Library Management Unit errors

Related topics
- Alert concepts and procedures
- Learning which ACSs are connected to a host

STK Tape: LSM_Offline alert

Responding to this alert Alerts dialog box help

The alert triggers whenever a Library Storage Module (LSM) goes offline to an MVS host (enters manual mode). The host can no longer use data stored in the LSM. Volume mounts are impossible for reads or writes, and any data sets needed in the LSM are inaccessible to the applications running on the given host. The alert clears when the LSM goes back online. It is possible for an LSM to be offline to one host and remain online to others. The alert triggers for any host where the LSM is offline.

Enabled by default
Yes

Monitored resource (source)
The alert monitors the following resources.

ACS	The hex Automated Cartridge System (ACS) number to which this alert applies. If ACS is not specified (or specified as *), LSM is ignored.
LSM	The hex LSM number to which this alert applies. LSM is effective only if ACS has a definite value.

Trigger Value
You do not need to change the trigger values for this alert.

Evaluation frequency (schedule)
Agent monitors HSC messages continually for this alert condition.

Possible uses of this alert
- Monitoring ACS and LSM availability

Related alerts
- ACS Disconnected alert

Related topics
- Alert concepts and procedures

STK Tape: Scratch Counts alert

Responding to this alert Alerts dialog box help

This alert triggers if the number of scratch volumes in the location and subpool, with the specified media type, falls below the threshold value. You can set different alerts for different locations, subpools, and media types.

Enabled by default
Yes

Monitored resource (source)

The alert monitors the following resources.

ACS	The hex Automated Cartridge System (ACS) number to which this alert applies. If ACS is not specified (or specified as *), Library Storage Module (LSM) is ignored.
LSM	The hex LSM number to which this alert applies. LSM is effective only if ACS has a definite value.
Media	The media type as displayed on the volume display (for example, STANDARD and ECART). Filtering status, reports, or alerts by media type
Subpool	The subpool number. Subpool 0 means all scratches without regard to subpool.

Trigger value

The number of scratch tapes in the monitored resources.

Evaluation frequency (schedule)

Every day at midnight.

Possible uses of this alert

- Ensuring sufficient scratch volumes
- Monitoring silos for low numbers of scratch volumes

Related alerts

- Drives Mount_Manual_Scratch

Related topics

- Monitoring silos for low numbers of scratch volumes

STK Tape: Volumes Inactive_Count alert

Responding to this alert Alerts dialog box help

This alert triggers if the number of volumes that have not been mounted for at least the number of days given by the key exceeds the threshold value. You can further refine alerts by location and media type. Also, you can set multiple alerts for different locations, media types, and days since last mount.

Enabled by default

Yes

Monitored resource (source)

The alert monitors the following resources.

ACS	The hex Automated Cartridge System (ACS) number to which this alert applies. If ACS is not specified (or specified as *), Library Storage Module (LSM) is ignored.
LSM	The hex LSM number to which this alert applies. LSM is effective only if ACS has a definite value.
Media	The media type as displayed on the volume display (for example, STANDARD and ECART).
Days since last mount	The minimum number of days since the volume was mounted. For example, a value of 30 means that volumes are included in the count only if it has been 30 or more days since they were last mounted by the Host Software Component (HSC).

Trigger value

The number of volumes not mounted in a time period specified by Days Since Last Mount.

Evaluation frequency (schedule)

Every day at midnight

Possible uses of this alert

- Monitoring silos for high numbers of inactive volumes

Related topics

- Alert concepts and procedures

WLA Archiver

Disk Space Status alert

Responding to this alert Alert dialog box Help

This alert triggers when there is less than 1 MB of disk space left on the host running WLA (Workload Analyzer) Archiver.

Status

Fatal

By default, this alert presents a Fatal status, however you can change the alert status to: Critical, Warning, Minor, or Harmless.

Enabled by default

Yes

To disable the alert, right-click **Archive Process Status Alert** in the tree, select **Edit Alert**, clear the **Enabled** checkbox, and click **OK** to close the dialog box.

Monitored resource (source)

The alert monitors the amount of disk space of the host running the WLA Archiver.

Trigger values

You cannot modify the trigger values for this alert. The alert is triggered automatically when the disk on which you are storing WLA statistical data is almost full.

Evaluation frequency (schedule)

By default, the WLA Archiver automatically sends the alert immediately after it detects that the host disk is almost full.

Possible uses of this alert

- Informing you that the host on which the WLA Archiver is running is just about out of disk space

Related topics

- Alert concepts and procedures
- WLA Archiver
- Changing the alert severity

Archive Errors alert

Responding to this alert Alert dialog box Help

This alert triggers when an error occurs when generating a Workload Analyzer (WLA) data collection.

Status

Warning

By default, this alert presents a Warning status, however you can change the alert status to Fatal, Critical, Harmless, or Error.

Enabled by default

Yes

To disable the alert, right-click **Archive Errors Alert** in the tree, select **Edit Alert**, clear the **Enabled** checkbox, and click **OK** to close the dialog box.

Monitored resource (source)

The alert monitors the following resources:

Data Collection Type	The type of collection that has been processed: Daily, Revolving, or Analyst.
Data Collection Name or date	The name of the collection if the error occurred on an Analyst collection. The time of the collection if the error occurred on a Revolving collection. The date of the collection if the error occurred on a Daily collection.
Data Provider	The monitored resource from which data is being collected, for example Symmetrix 00001234, or Host LA01234.

The monitored resource information is automatically included in the Archive Error alert message, for example:

`Error processing WLA Daily collection 20010910 for Symmetrix=000012345.`

You can not modify the monitored resource for this alert.

Trigger values

You cannot modify the trigger values for this alert. The alert triggers automatically when an error occurs while the WLA Archiver is generating the Daily, Revolving, or Analyst data collection.

Evaluation frequency (schedule)

By default, the WLA Archiver sends the alert each time an error occurs when the Daily, Revolving, or Analyst collection is being generated.

Possible uses of this alert

- Informing you that an error occurred while generating the data for WLA data collections.

Related topics

- Alert concepts and procedures
- WLA Archiver
- Changing alert severity

Archive Process Status alert

Responding to this alert Alert dialog box Help

This alert triggers when a data for a specific WLA (Workload Analyzer) Daily, Revolving, or Analyst collection has been successfully generated and is ready for viewing through WLA Performance View.

Status

Harmless

By default this alert presents a Harmless status, however you can change the alert status to Fatal, Critical, Warning, or Error.

Enabled by default

Yes

To disable the alert, right-click **Archive Process Status Alert** in the tree, select **Edit Alert**, clear the **Enabled** checkbox, and click **OK** to close the dialog box.

Monitored resource (source)

The alert monitors the following resources:

Data Collection Type	The type of collection that has been processed can be Daily, Revolving, or Analyst.
Data Collection Date	The date that the data in the collection represents.
Data Provider	The monitored resource from which data is being collected, for example Symmetrix 00001234, or Host LA01234.

The monitored resource information is automatically included in the Archive Process Status alert message, for example:

WLA Daily collection *20010817* for *Symmetrix=00001234* is processed.

You cannot modify the monitored resource for this alert.

Trigger values

You cannot modify the trigger values for this alert. The alert is triggered automatically when a Daily, Revolving, or Analyst collection has been processed.

Evaluation frequency (schedule)

By default the WLA Archiver sends the alert each time a Daily, Revolving, or Analyst collection is successfully generated.

Possible uses of this alert

- Reminding you that your collection is ready for viewing from WLA Performance View

Related topics

- Alert concepts and procedures
- WLA Archiver
- Changing the alert severity

Responding to alerts

Overview of responding to alerts

When an alert triggers, determine the impact of the alert and take any necessary actions to alleviate the condition that caused the alert or to prevent it from worsening.

Assessing the impact of an alert

When an alert triggers, ControlCenter provides the following information:

- Alert severity
- Host or storage device for which the alert triggered
- Names of the affected resources
- Values that caused the alert to trigger

The first step in responding to an alert is viewing this information and assessing the impact on your environment.

For more information, see Viewing triggered alerts.

Taking immediate action

In the Active Alerts view, you can take immediate action on an alert by right-clicking it. ControlCenter provides the following commands for all alerts.

Command	Description
Remove alert from your display	If the alert is informational or you determine that you do not need to respond to it, you can remove it from the triggered alerts list. Doing this helps you keep track of which alerts you have responded to, and keeps the triggered alerts list manageable.
Reset alert for all users	After you respond to an alert, you can reset it so that it no longer appears in your Console or that of other users. This helps your storage management team focus on critical issues.
Edit alert	Modify the settings that caused the alert to trigger.
Edit note	Add, edit, or view a text note. For example, use notes to describe any actions you have taken to resolve the alert.
View alert Help	View an online Help topic that discusses possible responses to the alert.

Some triggered alerts provide additional commands when you right-click, for example to display a report associated with the alert. For descriptions of these commands, see the online Help topics for those alerts.

Planning automated responses

You can create automated responses to alerts using management policies and autofixes. ControlCenter provides some autofixes, and you can also create your own using new or existing scripts, batch files, and utilities.

For more information, see:

- Creating a management policy
- Creating an autofix

Note

- If a monitored resource falls back to within the acceptable levels you defined in the alert, ControlCenter automatically removes the alert from the Active Alerts view.

Tip

- To prevent alerts from triggering too frequently, specify spike-controlling values for the alert.

Related topics

- Introduction to alerts
- Overview of creating alerts
- Overview of viewing alerts
- Understanding alert terminology
- Alert concepts and procedures

Automatically responding to alerts with commands and scripts

To automate your responses to alerts, you can have ControlCenter run scripts, batch files, commands, or executables when an alert triggers. Do this by creating autofixes.

To respond to an alert using an autofix:

1. Create the autofix. In the autofix definition, you can pass information from the alert to your script or executable, such as the name of the monitored resource and the severity of the alert.
2. Create the alert and attach the autofix. You attach an autofix on the **Actions** tab of the alert dialog box.

When the alert triggers, ControlCenter automatically sends the autofix command to the host where the alert triggered.

Related topics

- Creating an autofix
- Creating an alert from a template
- Copying an existing alert
- Introduction to alerts
- Alert concepts and procedures

Creating, editing, and viewing alert notes

To better track the actions you have taken to resolve an alert, you can document your actions by attaching a note to an alert. You can continue to update the alert notes to create a log of your actions.

To create, edit, or view a note for an alert:

1. Display the active alerts.
2. In the Active Alerts view, right-click the alert and select **Edit note**. The Alert Notes dialog box displays.
3. To add to or edit the note, type in the text box.
4. Click **OK** to save your changes.

Notes

- All ControlCenter users who see the alert can also see and edit the alert note.
- If the alert is reset either by a user or because the condition that caused it has been corrected, then ControlCenter deletes the note. If you remove the alert from your Console only, other users still see the note.

Related topics

- Introduction to alerts
- Overview of viewing alerts

Removing unneeded alerts from your Console

After you receive and review an alert, you can remove that alert from the Active Alerts view. By removing unneeded alerts, you can better track which alerts you have responded to and which need further attention.

To remove an alert from your Console:

1. View the active alerts.
2. Right-click the alert you want to remove and select **Remove alert from your display**. The alert does not reappear until it triggers again based on the conditions in the alert definition.

Note

- This procedure removes the alert from your Console only, not from the Consoles of other ControlCenter users.

Tips

- To remove the alert from all users' Consoles, right-click the alert and select **Reset alert for all users**.
- To permanently remove the alert, disable or delete the alert.

Related topics

- Reducing the number of alerts that display
- Enabling or disabling an alert
- Enabling or disabling multiple alerts
- Deleting an alert
- Overview of responding to alerts
- Alert concepts and procedures

Resetting an alert whose condition has been resolved

After you resolve the condition that caused an alert to trigger, reset the alert so that ControlCenter removes it from the Consoles of all ControlCenter users. Resetting an alert ensures that you or other users do not waste time responding to resolved conditions.

To reset an alert for all users:

1. View the currently triggered alerts if you are not already doing so.
2. Right-click the alert you want to reset and select **Reset this alert for all users**. ControlCenter removes the alert from all users' displays. The alert does not reappear until it triggers again based on the conditions in the alert definition.

Tips

- To remove the alert from your Active Alerts view only, right-click the alert and select **Remove alert from your display**.
- To permanently remove the alert, disable or delete the alert.

Related topics

- Reducing the number of alerts that display
- Enabling or disabling an alert
- Enabling or disabling multiple alerts
- Deleting an alert
- Overview of responding to alerts
- Alert concepts and procedures

All agents

Responding to Generic Agent Alerts

Each ControlCenter agent, or software component, generates messages as it runs. The components write these messages to a log file. However, you can also receive these messages in the Console as alerts. Each component's Generic Agent Alert determines:

- Which of a component's messages appear as alerts (all, Fatal messages only , and so on)
- Which ControlCenter users receive the alerts

Getting more information about a message

For more information about a specific message, view the message description in the error message online help.

To view the error message help:

1. In the main Console window, select **Error Message Help** from the **Help** menu. The Help Navigator window appears.
2. On the **Contents** tab, expand the book that corresponds to the first three letters of the message ID. For example, if the message ID is MNRESN103E, expand the book titled **MNR Messages**.
3. Double-click the message ID. A secondary window appears, displaying a reason and action for the message.

Alternatively, use the **Search** tab to search for the message ID.

Clearing message alerts from the Active Alerts view

To clear a message alert from the Active Alerts view, right-click the alert and select:

- **Reset alert for all users**to remove the alert from all users' Consoles
- **Remove alert from your display**to remove the alert from your Console only

The alert does not reappear until it triggers again based on the conditions in the alert definition.

Preventing message alerts from appearing

If you do not want the message alerts to appear in the Console, you can:

- Disable the alerts. You must disable the alerts for each component separately.
- Attach a management policy to the alerts. In the management policy, specify that only the ControlCenter administrator (or the user responsible for a particular agent or component) should receive the message alerts.

Related topics

- Generic Agent Alerts
- Monitoring ControlCenter status and security
- Introduction to alerts
- Alert concepts and procedures

ControlCenter infrastructure

Responding to ControlCenter infrastructure alerts

These alerts trigger when significant events occur within the ControlCenter infrastructure.

Alert	Problem	Immediate response	Long-term prevention
Agent Inactive	A ControlCenter component is no longer available.	View the alert message to determine which component is affected. If necessary, restart the component or reestablish its connection.	Use these alerts to create an audit trail of configuration changes and problem histories. You can view the ControlCenter log files to help troubleshoot problems with the ControlCenter infrastructure. To receive immediate notification about potential infrastructure problems, the security administrator can have ControlCenter send this alert to an e-mail account or pager. See: Automatically notifying staff members by e-mail or page
MO has been added/removed by user	A user has removed a managed object (such as a host or subsystem) from ControlCenter.	The alert message identifies which component was removed and who removed it. View the alert message to determine if any action is necessary.	
Repository alert	The ECC Server has received an alert regarding the ControlCenter Repository database.	View the alert message to determine if any action is necessary.	
Server message logged	A message about the ECC Server has been written to the log file.	View the log file to determine if any action is necessary.	
Server shutdown	The ECC Server has been shut down under normal conditions.	No action necessary.	
Primary/Secondary Assignment	A ControlCenter component that was serving as a data source has failed, and ControlCenter has automatically changed the data source.	Investigate why the component failed. Correct the problem and switch the data source back if necessary.	
Store message logged	A message about the Store has been written to the log file.	View the log file to determine if any action is necessary.	

Note

- By default, these alerts appear in all users' Consoles. To route these alerts to a specific user, such as the ControlCenter administrator, attach a management policy to the alerts. For more information, see: Reducing the number of alerts that display.

Related topics

- Monitoring ControlCenter status and security
- Introduction to alerts
- Overview of responding to alerts
- Alert concepts and procedures

ControlCenter security

Responding to ControlCenter user management alerts

These alerts trigger when significant ControlCenter user management events occur.

Alert	Problem	Immediate response	Long-term prevention
User Change	A user has been added to or deleted from ControlCenter, or has had an attribute changed.	If an unauthorized user has logged on to ControlCenter, the security administrator can delete the user or remove the user's privileges. See: Managing a ControlCenter user's permissions	Use these alerts to create an audit trail of user activities. You can view the ControlCenter log files to track user activity and to troubleshoot security breaches.
User Logged On/Off	A user has logged on to or off of ControlCenter.		
User Group Change	A user group has been added to or deleted from ControlCenter, or has had an attribute changed.	ControlCenter users can gain permissions by inheriting the permissions of user groups to which they belong. The security administrator can use this alert to ensure users are not placed in the wrong user groups. See: Using ControlCenter groups effectively	
User Logon Failure	A user failed to log on to ControlCenter.	Repeated failed logon attempts could indicate someone is trying to access ControlCenter without the proper authorization. The security administrator should immediately address these issues.	To receive immediate notification about potential security breaches, the security administrator can have ControlCenter send this alert to an e-mail account or pager. See: Automatically notifying staff members by e-mail or page

Note

- By default, these alerts appear in all users' Consoles. To route these alerts to a specific user, such as the ControlCenter security administrator, attach a management policy to the alerts. For more information, see: Reducing the number of alerts that display.

Related topics

- Monitoring ControlCenter status and security
- Alert concepts and procedures
- Overview of Responding to alerts
- ControlCenter security management overview

Connectivity Agent for SNMP

Responding to Connectivity Agent for SNMP alerts

Connectivity Agent for SNMP alerts are generated by the Connectivity Agent for SNMP when it detects configuration or status changes to devices in the SAN or when a device cannot be reached. The Connectivity Agent for SNMP detects these changes by polling the SNMP agents running on the specific devices it is monitoring.

Note: See Connectivity Agent for SNMP alerts for information on viewing alerts generated by this agent.

Alert responses

Alert	Problem	Immediate response	Long-term prevention
SNMP Agent Configuration Change	The configuration of a device being monitored by the Connectivity Agent for SNMP has changed.	If the device generating the alert is not required for your task, ignore this alert.	1. Check the physical configuration of the device and change it to the correct one. 2. Launch the device management software and check the physical device related to the alert.
SNMP Agent Port Status Change	The status of a port being monitored by the Connectivity Agent for SNMP has changed. For example: the status of port 2 of switch A has changed from `OK` to `FAILURE`.	If the device generating the alert is not required for your task, ignore this alert.	1. Check the hardware, including the power source, for physical problems, and fix the problem. 2. Launch the device management software and check the physical device related to the alert.
SNMP Agent Unit Status Change	The status of a device being monitored by the Connectivity Agent for SNMP has changed. For example: a switch status has changed from `OK` to `WARNING`.	If the device generating the alert is not required for your task, ignore this alert.	1. Check the hardware, including the power source, for physical problems, and fix the problem. 2. Launch the device management software and check the physical device related to the alert.
SNMP Agent Unreachable	A device being monitored by the Connectivity Agent for SNMP cannot be detected.	If the device generating the alert is not required for your task, ignore this alert.	1. Fix the physical device or the network problem to bring back the SNMP agent running on the device. 2. Check the SNMP agent process running on the device.

Related topics

- Connectivity Agent for SNMP alerts
- Connectivity Agent for SNMP administration

Backup Agent for TSM

TSM: Responding to activity log search alerts

The response to this alert depends on the string that the alert identified in the activity log. This alert is issued by the Backup Agent for TSM.

Alert	Problem	Immediate response	Long-term prevention
Activity Log Search	In the activity log for a TSM server, a string appeared that a user has configured to trigger this alert.	Note the string that appears in the alert message text, then search for that string in the activity log. Gather the information you need by exploring the activity log for the TSM server on the host indicated by the alert.	None required.

Related topics

- Searching the activity log
- Alert concepts and procedures

TSM: Responding to alerts for failed, missed, and severed events in TSM

These alerts are issued by the Backup Agent for TSM.

Alert	Problem	Immediate response	Long-term prevention
Event Log Failed Events	A backup or archive event failed.	Check the utilization of the storage pool. For more information: • Search the activity log for message number **ANR2579E**. • Read the schedule log on the node (client).	Ensure that files to be backed up are valid. Set up an overflow pool as described in TSM documentation from Tivoli. If the node is not configured to keep a schedule log, see Tivoli Storage Manager documentation to configure it.
Event Log Missed Events	A backup or archive event was missed (did not occur).	For more information: • Search the activity log for message number **ANR2578I**. • Read the schedule log on the node (client).	Check to see whether the affected node is running and whether the client scheduler is running. If the node is not configured to keep a schedule log, see Tivoli Storage Manager documentation to configure it.
Event Log Severed Events	A backup or archive event was interrupted by network problems or a system outage.	For more information: • Search the activity log for message number **ANR0480W** and **ANR0568W**. • Read the schedule log on the node (client).	Create more reliable or redundant connections between the node and the backup server host machine. If the node is not configured to keep a schedule log, see Tivoli Storage Manager documentation to configure it.
Activity Log Failure Count	For a node (client), one or potentially many backup events failed in the previous 24 hours.	For more information: • Search the activity log for the string **4959**. • Read the schedule log on the node (client).	Monitor volume availability, database and log utilization, and backup size. If the node is not configured to keep a schedule log, see Tivoli Storage Manager documentation to configure it.

Related topics

- Searching the activity log
- Alert concepts and procedures
- Monitoring nodes for failed, missed, and severed events

TSM: Responding to TSM client backup size alerts

These alerts are issued by the Backup Agent for TSM.

Alert	Problem	Immediate response	Long-term prevention
Size Backup Storage Size (KB)	A node (client) is backing up a large amount of data.	Ensure that clients are not backing up through mount points and NFS mounts. This may require access to the TSM client machine and interface. See if TSM is backing up the same networked storage through multiple clients.	Determine if the node was recently registered. If so, it may be performing an initial full backup. View the client option file (on the client system) or the client option set to see which files the client backs up. Determine whether incremental or selective backups are in use. Selective backups back up entire files.
Size Archive Storage Size (KB)	A node is archiving a large amount of data.		
Size Space Managed Storage Size (KB)	A node is transferring a large amount of space-managed data.		

To determine if a node is recently registered:

1. Explore the TSM server.
2. Explore **Nodes**.
3. In the target panel, find the node that triggered the alert.
4. Scroll to the right to the **Registered** column. If the date and time are recent, the node may be performing a full backup as its initial session.

To view the client option file:

This procedure requires that you go to the client machine. Use Tivoli Storage Manager documentation to view the client options file and the files the client is configured to back up.

Ensure that clients are backing up only necessary data. See that system files, temporary files, and personal files are excluded.

To view the client option set:

1. Explore the TSM server.
2. Explore **Nodes.**
3. In the target panel, find the node that triggered the alert.
4. Scroll to the right to the **Option Set** column and note the name of the option set.
5. Expand **Server** and **Option Sets.**
6. Explore **Client Option Sets.**
7. Explore the option set used by the node.
8. Explore **Client Options**.
9. Look for **INCLEXCL**. If it is present, note the **Option Value** for the included and excluded files and directories.

   Ensure that clients are backing up only necessary data. See that system files, temporary files, and personal files are excluded.

To determine the type of backups in use:

1. Explore the TSM server.
2. Explore **Nodes**.
3. Explore the desired node.
4. Under the node, explore **Schedules**.
5. In the target panel, note the **Action** listed for the schedule. The usual action is Incremental. An action of **Selective** causes entire files to be backed up as defined in the client option file or the client option set.

Related topics

- Monitoring client backup and archive size

TSM: Responding to TSM client management alerts

Use the following table for recommendations. These alerts are issued by the Backup Agent for TSM.

Alert	Problem	Immediate response	Long-term prevention
Client Licenses *This alert available for TSM 3.7 only*	The number of available client licenses is almost exhausted. If client licenses run out, you will not be able to install the client software on new nodes.	Remove nodes that are no longer needed.	Prioritize deployment of TSM client software to the most important systems. Request additional licenses from the product vendor.
Invalid Sign On Count	An excessive number of logon attempts failed for a TSM client in a given period. An attempted security breach may have occurred.	Check the schedule of the alert (24 hours by default) to see the time period in which the failed attempts occurred. Follow security procedures in place at your site.	Refer to security procedures at your site.

Related topics

- Alert concepts and procedures

TSM: Responding to TSM database performance alerts

The cache, or buffer pool, may experience poor performance if it is too small or not being tuned automatically by TSM. Use the following table for recommendations and suggestions. These alerts are issued by the Backup Agent for TSM.

Alert	Problem	Immediate response	Long-term prevention
DB Cache Hit Percent	The percentage of database requests being met from the cache is too low. Backup performance may be slowed.	Check cache utilization of the database. If cache hit percentage is less than 98% or if cache wait percentage is greater than zero, increase the size of the database buffer pool using the TSM interface.	Determine whether the server is tuning cache size automatically by checking the server options. If not, consider setting server option SELFTUNEBUFpoolsize to Yes using Tivoli Storage Manager software.
DB Cache Wait Percent	The percentage of database requests having to wait for the cache is too high. Backup performance may be slowed.		

To explore the database for current cache statistics:

1. Explore the TSM server.
2. Click (+) to expand **Server**.
3. Right-click **Database** and select **Explore**. The target panel displays a view.

Scroll to the right to see the following useful fields:

- **Buff Pool Pgs** The number of buffer pool pages.
- **Tot Buf Requests** The number of requests since the last time the statistic was reset.
- **Cache Hit %** The percentage of requests satisfied from a buffer pool page. A value less than 98% means increase the size of the cache.
- **Cache Wait %** The percentage of requests that could not immediately access a buffer. A nonzero value means increase the size of the cache.

To increase the size of the cache, use Tivoli Storage Manager documentation and interface.

To determine whether the server is tuning cache size automatically:

1. Explore the TSM server.
2. Click (+) to expand **Server**.
3. Click (+) to expand **Options**.
4. Right-click **Server Options** and select **Explore**. The MGYGRID dialog box displays the server options and their values.

Scroll down to **SELFTUNEBUFpoolsize**.

- If the value is **Yes**, the server is adjusting its size automatically.
- If the value is **No**, the server is not adjusting the buffer pool size automatically. You may want to change the option to Yes or adjust the size of the buffer pool manually. Use the Tivoli Storage Manager web interface to perform either measure.

Related topics

- Monitoring TSM database performance
- Responding to activity log search alerts
- Responding to alerts for failed, missed, and severed events

TSM: Responding to utilization alerts for the database, logs, and their volumes

Database and log utilization alerts trigger when the space available for TSM's critical files is running low. Low severity alerts are a positive sign as they remind you to add resources only when you need them, rather than preemptively adding excessive storage to TSM's operational files. As the alerts increase in severity, the TSM system is at increased risk of an outage. These alerts are issued by the Backup Agent for TSM.

Alert	Problem	Immediate response	Long-term prevention
Database			
Database Utilization	The TSM database is using a high percentage of its allocated space. If it reaches 100%, the TSM backup server will no longer be able to function.	If backups are in progress, either allow them to complete or stop them. Once no backups are in progress, add a database volume and extend the database.	The database size increases with the total number of files being backed up. Audit clients to ensure that no unnecessary files are backed up. When the TSM database becomes excessively large or experiences large increases or fluctuations, consider dividing backed-up clients among multiple TSM servers.
Database Volume Percent	A file that stores TSM database data is filling up beyond an acceptable percentage.	Check the percent utilization of the TSM database. If it is higher than acceptable at your site, then add a database volume and extend the database.	The database size increases with the total number of files being backed up. Audit clients to ensure that no unnecessary files are backed up.
Recovery log			
Log LogPool	The buffer pages that hold data to be written to the recovery log are filling up.	Check the cache performance of the recovery log. If backups are in progress, either allow them to complete or stop them. Once no backups are in progress, add space to the recovery log buffer pool using TSM documentation and the TSM interface. Add a recovery log volume and extend the recovery log.	None.

Log Utilization	The TSM recovery log is using a high percentage of its allocated space. In roll-forward mode, you may lose data if the recovery log reaches 100%.	If backups are in progress, either allow them to complete or stop them. If backups are not in progress, add a recovery log volume and extend the recovery log. Then back up the database.	For utilization of 90% or more, increase the size of the recovery log. In roll-forward mode, increase the frequency of scheduled database backups or increase the capacity of the recovery log.
Log Volume Utilization	A volume used to store logs is running out of space.	If backups are in progress, either allow them to complete or stop them. Check the percent utilization of the recovery log. If it is higher than acceptable at your site, then add a recovery log volume and extend the recovery log.	None.

Related topics

- Monitoring TSM databases and logs for space problems
- Managing backup databases and logs in TSM
- Alert concepts and procedures
- Responding to TSM database performance alerts

TSM: Responding to utilization alerts for volumes and storage pools in TSM

Volume and storage pool utilization alerts trigger when the storage available for TSM backups is filling up. As the alerts increase in severity, backup events are at greater risk of failure due to space errors. These alerts are issued by the Backup Agent for TSM.

Alert	Problem	Immediate response	Long-term prevention
Storage Pool Utilization	The percentage utilization of a storage pool has crossed a threshold. The storage pool may be filling up.	Determine if the storage pool has enough space for upcoming backups. Listing upcoming backups. Add more volumes to the storage pool. Search the activity log for failed events related to the storage pool.	Consider migrating disk storage pools to tape more frequently. Consider configuring a subordinate storage pool to use when the main storage pool fills up. Increase the limit of scratch volumes a sequential pool can access.
Volume Utilization	Informational: A volume in a storage pool is filling up.	Check utilization of the storage pool and volumes.	

Related topics

- Alert concepts and procedures
- Monitoring volumes and storage pools for space problems

TSM: Responding to volume availability alerts in TSM

Use the recommendations here to respond to volume status alerts and volume read and write error alerts. These alerts are issued by the Backup Agent for TSM.

Alert	Problem	Immediate response	Long-term prevention
Status Filling	Informational: The volume contains data but is not full.	No action is required.	No action is required.
Status Offline	A backup volume is offline. TSM may attempt to access files from the copy storage pool.	Ensure that remaining volumes have enough space for the next backup cycle. Listing upcoming backups Check utilization of storage pools and volumes.	Focus prevention efforts on administrator actions and system startup configuration.
Status Unavailable	A backup volume is unavailable. TSM may attempt to access files from the copy storage pool.	Ensure that remaining volumes have enough space for the next backup cycle. Listing upcoming backups Check utilization of storage pools and volumes.	Focus prevention efforts on network and system connectivity.
Volume Read Errors	A volume has excessive read errors in the last 24 hours (or user-defined period).	Check the alert's schedule for the period over which the errors occurred (24 hours by default). Add another volume to the same storage pool. Migrate the data and remove the current volume from the storage pool. Attempt a restore (to another client or location) of the data on the volume. Read and write errors could prevent successful restore operations and make the backup unusable.	Once the data is safely moved off the volume and you have been able to restore it successfully, test the volume thoroughly and remove it from use if it is unreliable.
Volume Write Errors	A volume has excessive write errors in the last 24 hours (or user-defined period).		

Related topics

- Alert concepts and procedures
- Monitoring availability of backup volumes

Database Agent for DB2

DB2: Responding to DB2 active and dropped table alerts

DB2 table alerts inform you when dropped tables containing unneeded data are taking excessive space.

Use the suggested responses and DB2 documentation to resolve these alerts. Click the alert name for a description of the alert.

Alert	Problem	Immediate response	Long-term prevention
Tablespace Partition Percent Active Table	The percentage of space occupied by active tables has fallen below a threshold. Database performance may suffer.	If you are sure you will not need to roll back the database, issue the SQL COMMIT statement. Issuing SQL statements.	None.
Tablespace Partition Percent Dropped Table	The percentage of space occupied by dropped tables has exceeded a threshold. Database performance may suffer.	If you are sure you will not need to roll back the database, issue the SQL COMMIT statement. Issuing SQL statements.	None.

Related topics

- Database Agent for DB2 overview
- Issuing SQL statements
- Monitoring databases for dropped tables

DB2: Responding to DB2 database integrity alerts

DB2 database integrity alerts inform you when objects are in Check Pending status and when detector-initiated Check Data and Check Index utilities fail. Use the suggested responses and DB2 documentation to resolve these alerts. Click the alert name for a description of the alert.

Note: If you are performing recovery operations, use caution and follow DB2 documentation. This will help avoid data integrity problems and decrease the number of utilities you need to run.

Alert	Problem	Immediate response	Long-term prevention
Index Check Index Return Code	Fatal: a detector-initiated Check Index operation failed (return code 8). Warning: a detector-initiated Check Index operation completed with errors (return code 4).	Run the detector report to view errors and reasons. • Error status report • Error history status report • Running reports	None.
Table Check Pending Status	A table is in Check Pending status. *Possible problems:* The last Check Data operation found errors in constraints. An ALTER TABLE command added a constraint to a populated table. Recovered tables may be from different points in time.	*In recovery situations, see DB2 documentation.* Run Check Data against the table, find and fix the errors, and re-run Check Data.	None.

Table Definition Incomplete	A table definition is incomplete. The table may lack: • a primary index • a required index on a row ID • a required index on a unique key • an auxiliary table or auxiliary index for an LOB column	View the system tables for the affected database. View table SYSIBM.SYSTABLES and find the Table Status field. Create the necessary index or auxiliary table.	None.
Tablespace Check Data Return Code	Fatal: a detector-initiated Check Data operation failed (return code 8). Warning: a detector-initiated Check Data operation completed with non-fatal errors (return code 4). Harmless: a Check Data operation completed with return code 0.	Run the detector report to view errors and reasons. • Error status report • Error history status report • Running reports	Follow DB2 documentation for preparation measures before running Check Data.
Tablespace Check Pending Scope	A table space is in a Check Pending status with the scope less than the entire table space.	Run Check Data utility against unchecked data.	None.
Tablespace Check Pending Status	A table space is in Check Pending status. *Possible problems:* The last Check Data operation found violations of referential and table check constraints. Data in the table space does not comply with a recently added table constraint. A recovery placed the table in Check Pending status.	Run Check Data against the table space, fix the errors, and re-run Check Data.	To avoid Check Pending status during recovery, follow IBM DB2 recommendations for point-in-time recovery .

Tablespace Lack Partitioned Index Status	A partitioned table space lacks a partitioned index.	Create the partitioned index. Issuing SQL statements	None.
Tablespace Partition Check Pending	A table space partition is in Check Pending status. *Possible problems:* The last Check Data operation found errors in the data. Data in the partition does not comply with a recently added table A recovery placed the table in Check Pending status.constraint.	Run Check Data against the table space partition, fix the errors, and re-run Check Data.	None.

Removing Check Pending status

See DB2 documentation for prerequisites and complete instructions.

To remove Check Pending status:

1. Run the Check Data utility against the table, table space, or partition to identify errors.
2. Use SQL UPDATE or DELETE commands to correct the errors.
3. Run Check Data again to remove the Check Pending status and allow table access.

You can perform all these steps using the Database Agent for DB2. Use the following topics for instructions on running utilities and issuing SQL statements:

- DB2: Running DB2 utilities
- DB2: Issuing SQL statements

Related topics

- Monitoring DB2 database integrity
- Running DB2 utilities
- Error history status report

DB2: Responding to DB2 row position alerts

Depending on the alert that triggered, DB2 row position alerts inform you of row position statistics that may justify a REORG.

For table spaces, alerts inform you when

- A large number of rows have been written to different pages from their original location, whether **near** or **far**. (possible problem)
- A high percentage of rows have been relocated **far** from their original position. (possible problem)
- A given percentage of rows are relocated **near** their original position. (informational)

Any or all of these conditions may justify running the REORG utility against the table space or partition.

For indexes, alerts inform you when

- A large number of rows have been written to different pages from their optimal location, whether **near** or **far**. (possible problem)
- A high percentage of relocated rows are **far** from their optimal position. (possible problem)
- A given percentage of relocated rows are **near** their optimal position. (informational)

Any or all of these conditions may justify running the REORG utility against the index or index partition.

General responses

Consider a reorganization of the tablespace, partition, or index.

Note the following:

- A premature REORG can actually decrease performance.
- Performance of certain catalog tables is unaffected by row position statistics.

Index partition alerts Table space partition alerts

Alert	Problem	Immediate response
Index partition		
DB2 Index Partition Percent Rows Far From Optimal alert	In an index partition, the *percentage* of referred-to rows *far from* their original position is high. A reorganization may be advisable, depending on the actual number of rows.	Consider running a REORG if: • A high percentage and a high absolute number of rows are far from their optimal position. • The absolute number of non-optimally placed rows is at warning or higher for both "near" and "far" alerts. Running DB2 utilities
DB2 Index Partition Percent Rows Near Optimal alert	In an index partition, the *percentage* of referred-to rows *near* their original position is high. This is not a problem condition.	
DB2 Index Partition Rows Far From Optimal alert	In an index partition, a large number of referred-to rows are *far* from their optimal position.	
DB2 Index Partition Rows Near Optimal alert	In an index partition, a large number of rows are not at optimal position but are near optimal position.	
Table space partition		
DB2 Tablespace Partition Percent Rows Far From Original alert	In a table space partition, the *percentage* of relocated rows *far from* their original position is high. A reorganization may be advisable, depending on the actual number of relocated rows.	Consider running a REORG if: • A high percentage and a high absolute number of rows are far from their original position. • The absolute number of relocated rows is at warning or higher for both "near" and "far" alerts. Running DB2 utilities
DB2 Tablespace Partition Percent Rows Near Original alert	In a table space partition, the *percentage* of relocated rows *near* their original position is high. This may not be a problem condition.	
DB2 Tablespace Partition Rows Far From Original alert	In a table space partition, a large number of rows have been relocated. This alert provides the *number* of rows *far from* their original position.	
DB2 Tablespace Partition Rows Near Original alert	In a table space partition, a large number of rows have been relocated. This alert provides the *number* of rows *near* their original position.	

Related topics

- Monitoring for reorganization candidates

DB2: Responding to DB2 RUNSTATS return code alerts

RUNSTATS return code alerts inform you when a RUNSTATS operation fails or has warning messages. Find the return code in the alert message, then use the following table to respond.

TableSpace RUNSTATS Return Code alert description

Return code	Problem	Immediate response
0	None. RUNSTATS completed normally.	None is required.
4	RUNSTATS completed with warning messages.	Run the detector report to view errors and reasons. • Error status report • Error history status report • Running reports
8	RUNSTATS failed to complete.	
12	RUNSTATS did not complete because of an authorization error.	

Related topics

- Configuring data collection for DB2 alerts and reports
- Monitoring DB2 RUNSTATS execution
- Error status report
- Error history status report

DB2: Responding to DB2 space alerts

DB2 space alerts inform you when space usage crosses a threshold for databases, indexes, stogroups, and table spaces. Also, other alerts inform you when the number of rows exceeds a threshold for table rows and index rows in a partition. The alerts inform you when the space allocation of DB2 resources is excessive as defined by the trigger values in the alert. They do not necessarily mean that the resources are running out of space.

Use the suggested responses to provide information needed to resolve the alert. Click the alert name for a description of the alert.

General responses

Run the equivalent space usage report as soon as possible. Only the most recent space usage data is available for alerts and reports. As soon as the next detector runs, the last set of data is lost. To keep a body of trend data available to you, run the space reports ideally after each detector process completes, or at least as often as a space alert triggers.

Alert	Problem	Immediate response
Subsystem database space alert	A database has exceeded a given space threshold.	Run the database space usage report.
Index space usage alert	An index has exceeded a given space threshold.	Run the index space usage report.
Subsystem stogroup space alert	A stogroup has exceeded a given space threshold.	Run the stogroup space usage report.
Table rows usage alert	A table has exceeded a given number of rows.	Run the table status report.
Tablespace space usage alert	A table space has exceeded a given space threshold.	Run the tablespace space usage report.
Index partition space alert	Partition space has exceeded a threshold.	Run the index space usage report.
Index partition rows alert	An index partition has exceeded a given number of rows.	Run the index status report.

Related topics

- Monitoring DB2 space utilization and trends
- Running reports
- DB2 reports

DB2: Responding to DB2 trend alerts

DB2 trend alerts inform you when space usage increases by an excessive amount for databases, indexes, stogroups, tables, and table spaces. Use the suggested responses to provide information needed to resolve the alert.

General responses

Run the equivalent trend report as soon as possible. Only the most recent trend data is available for trend alerts and reports. As soon as the next detector runs, the last set of trend data is lost. To keep a body of trend data available to you, run the trend reports ideally after each detector process completes, or at least as often as a trend alert triggers.

Click the alert name for a description of the alert.

Alert	Problem	Immediate response
Subsystem database trend alert	A database has grown by a high percentage since the last detector execution.	Run the database trend report.
Subsystem index trend alert	An index has grown by a high percentage since the last detector execution.	Run the index trend report.
Subsystem stogroup trend alert	A stogroup has grown by a high percentage since the last detector execution.	Run the stogroup trend report.
Subsystem table trend alert	A table has grown by a high percentage since the last detector execution.	Run the table trend report.
Subsystem tablespace trend alert	A tablespace has grown by a high percentage since the last detector execution.	Run the tablespace trend report.

Related topics

- Monitoring DB2 space utilization and trends
- Running reports
- DB2 reports

Database Agent for Oracle alerts

Responding to the Storage Agent for Celerra alert

This is the alert that can be generated by the Storage Agent for Celerra.

Alert name	Problem/Display	Immediate response	Long-term prevention
Celerra Agent Unit Status Changes	The status of the Celerra has changed from OK to Warning or Critical	Launch the Celerra Manager URL to review the Celerra data.	Long-term prevention requires historical data and an experienced storage manager to resolve.

Related topics

- Storage Agent for Celerra overview
- Storage Agent for Celerra administration
- Storage Agent for Celerra alert
- Storage Agent for Celerra data collection policies

Responding to Database Agent for Oracle Space alerts

These are the space-related alerts that can be generated by the Database Agent for Oracle.

Alert name	Problem/Display	Immediate response	Long-term prevention
Table Size % Used	Table Used percent for *sid* table : *value*	Notify your DBA of the remaining percentage free in the table extents.	Your DBA should either reset the alert threshold or allocate more table extents.
Table Blocks % Free	Table Blocks Free(%) for *sid* table : *value*	Notify your DBA of the remaining percentage free in the table blocks.	Your DBA should either reset the alert threshold or allocate more table blocks.
Index Extents % Used	Index extents Used percent for *sid* index: *value*	Notify your DBA of the remaining percentage free in the index extents.	Your DBA should either reset the alert threshold or allocate more index extents.
Used Megs	Tablespace used Megabytes for *sid* tablespace: *value*	Notify your DBA of the remaining tablespace MBs.	Your DBA should either reset the alert threshold or allocate more MBs for the tablespace.
Used % of Tablespace	Tablespace used Percent for *sid* tablespace: *value*	Notify your DBA of the remaining percentage free in the tablespace.	Your DBA should either reset the alert threshold or allocate more MBs for the tablespace.
Free Megs in Tablespace	Tablespace Megabytes free for *sid* tablespace: *value*	Notify your DBA of the remaining tablespace MBs.	Your DBA should either reset the alert threshold or allocate more MBs for the tablespace.
Free % of Tablespace	Tablespace Free % for *sid* tablespace: *value*	Notify your DBA of the remaining percentage free in the tablespace.	Your DBA should either reset the alert threshold or allocate more MBs for the tablespace.
Used % of total SID datafiles space	Total Tablespace percent of SID *sid* tablespace: *value*	Notify your DBA of the remaining percentage free in the database instance datafiles space.	Your DBA should either reset the alert threshold or allocate more datafiles space.

Related topics

- Database Agent for Oracle overview
- Database Agent for Oracle administration
- Database Agent for Oracle data collection policies
- Database Agent for Oracle Space alerts
- Database Agent for Oracle Environment alerts
- Responding to Database Agent for Oracle Environment alerts

Responding to Database Agent for Oracle Environment alerts

These are the environment-related alerts that can be generated by the Database Agent for Oracle.

Alert name	Problem/Display	Immediate response	Long-term prevention
Oracle SID Up	Oracle SID is up for *sid*	No response is required. This is a system tracking mechanism cataloging when a particular database instance is available.	N/A
Oracle SID Down	Oracle SID is down for *sid*	Notify your database administrator (DBA) that the database instance is down.	Long-term prevention requires historical data and an experienced DBA to resolve.

Oracle Error	Oracle Error error found in SID *sid*	Notify your DBA that the database instance is producing errors.	Long-term prevention requires historical data and an experienced DBA to resolve.
Count of Oracle Errors	Oracle Error error in SID *sid* occurs value times	Notify your DBA that the database instance is producing errors.	Long-term prevention requires historical data and an experienced DBA to resolve.
Num Chained Rows	Chained Rows for *sid* table: *value*	Notify your DBA that the database instance is chaining rows.	Long-term prevention requires historical data and an experienced DBA to resolve.
User Connected to Oracle	User Connected SID *sid oracleid osid*	No response is required. This is a system tracking mechanism cataloging when a particular database instance is accessed by a particular user.	N/A

Related topics

- Database Agent for Oracle overview
- Database Agent for Oracle administration
- Database Agent for Oracle data collection policies
- Database Agent for Oracle Space alerts
- Database Agent for Oracle Environment alerts
- Responding to Database Agent for Oracle Space alerts

Host Agents for AIX, HP-UX, and Solaris

UNIX: Responding to quota alerts

Alerts covered:

- Hard Quotas: Free Disk Space or Files alerts
- Soft Quotas: Free Disk Space or Files alerts

Your response to user quota alerts will vary depending on the severity of the alert and the user that the alert monitors.

If the alert severity is critical or fatal, you should take immediate action to identify the users's storage space needs. To obtain this information, you can contact the user directly or view the files the user owns. If you decide that the user should be allocated more space, you can modify the user's quota. To ensure that the user does not exceed the specified quota, enable quota enforcement on the file system on which the user quota is defined.

If the alert severity is harmless, minor, or warning, determine what you steps you need to take to ensure that the user does not exceed their quota limit, for example:

- Notify the user of the approaching quota limit
- Modify the user's quota and allocate more storage space as needed
- Enable or disable quota enforcement on the file system
- Identify and delete, compress, or back up non-mission-critical files in the user's directories

You may also want to create an autofix for these alerts. See General alert topics for more information.

Related topics

- Alert concepts and procedures
- Performance monitoring guidelines
- Monitoring AIX, HP-UX, and Solaris hosts
- Checking the status of UNIX Host Agents
- Host Agents for AIX, HP-UX, and Solaris overview

UNIX: Responding to storage space-related alerts

Alerts covered:

- UNIX: Disk Space Free on a File System alert
- UNIX: Disk Space Percent Free on the File System alert
- UNIX: File and Directory Size alert
- UNIX: Inodes (files) free on the file system alert
- Solaris: VERITAS Disk Group Free Space alerts
- UNIX: Volume Group Free Space alerts

Your response to storage space-related alerts will vary depending on the severity of the alert.

If the alert severity is critical or fatal, you should take immediate action to free up storage space for mission critical applications and users. This may include solutions such as:

- Adding new physical storage devices
- Recovering wasted disk space
- Compressing unused or large files
- Extending a file system, logical volume, or volume group

If the alert severity is harmless, minor, or warning, determine what you steps you need to take to ensure that the host maintains an adequate level of free storage space, for example:

- Identify the users and groups consuming the greatest amount of storage resources and find alternative storage resources for them
- Enable user quota enforcement
- Add new physical storage devices
- Extend file systems, logical volumes, or volume groups to meet your storage needs

You may also want to create an autofix for these alerts. See General alert topics for more information.

Related topics

- Alert concepts and procedures
- Performance monitoring guidelines
- Monitoring AIX, HP-UX, and Solaris hosts
- Checking the status of UNIX Host Agents
- Host Agents for AIX, HP-UX, and Solaris overview

UNIX: Responding to swap space-related performance alerts

Alerts covered:

- Swap Space Megabytes Free alert (Solaris)
- Swap Space Percent Free alert (Solaris)

Your response to swap space-related performance alerts will vary depending on the severity of the alert.

If the alert severity is critical or fatal, you should take immediate action to allocate more device-type or file-type page space on the host on which the alert was triggered. You may also want to explore the processes running on the system and try to identify any processes that may be using up a disproportional amount of system resources. Using ControlCenter, you can also determine the system resources that a process consumes, and kill processes that may be dangerous to system health. You may also want to identify those users logged on to the host and notify them that system resources are critically low. Ignoring critical swap space-related issues could have a severe impact on host system performance.

If the alert severity is harmless, minor, or warning, determine what you steps you need to take to ensure that the amount of swap space available does not shrink to a critical size, for example:

- Allocate more device-type or file-type page space on the host
- Search for and kill unnecessary or zombie processes
- Explore and view the resources consumed by all processes on the system
- Limit access to the system to only those users performing mission-critical operations

You may also want to create an autofix for these alerts. See General alert topics for more information.

Related topics

- Alert concepts and procedures
- Performance monitoring guidelines
- Monitoring AIX, HP-UX, and Solaris hosts
- Checking the status of UNIX Host Agents
- Host Agents for AIX, HP-UX, and Solaris overview

Host Agent for MVS HSM

MVS HSM: Responding to ARC message alerts

Host Agent for MVS HSM reports on a wide variety of ARC messages that can appear in the HSM logs. Some of the ARC message alerts come enabled at installation time, but if you find that these ARC messages are not critical to your operation, you can disable them.

Each ARC message alert works based on a True/False condition. If you set an alert to False, it will not trigger when a particular ARC message appears in the HSM logs.

To address an ARC message, consult the IBM DFSMShsm message documentation.

Related topics

- Host Agent for MVS HSM overview

MVS HSM: Responding to failed alerts

Host Agent for MVS HSM issues alerts when certain tasks fail to execute correctly. The items that the agent notifies you when failures occur are:

- Automatic Backup Failed alert
- Automatic Dump Failed alert
- CDS Backup Failed alert
- Failed Parse Error alert
- Primary Space Management Failed alert
- Secondary Space Management Failed alert

Consult the HSM logs to determine why these failures occurred.

Related topics

- Host Agent for MVS HSM overview

MVS HSM: Responding to the HSM Address Space Inactive alert

Host Agent for MVS HSM issues a notice when the HSM address space becomes inactive.

To correct this condition, restart HSM.

Related topics

- Host Agent for MVS HSM overview

MVS HSM: Responding to the ML1/ML2 Space Usage alert

Host Agent for MVS HSM issues an alert when certain return codes are issued during migration level 1 (disk) and migration level 2 (tape) space usage.

The ML1/ML2 Space Usage alert issues when these return codes are detected.

Consult the documentation for DFSMShsm to determine the proper response.

Related topics

- Host Agent for MVS HSM overview

MVS HSM: Responding to user alerts

Host Agent for MVS HSM provides two alerts that you can configure to detect message IDs the agent does not include alerts for.

The alerts are:

- User-defined alert
- User-specified alert

Consult the documentation for DFSMShsm for the proper response to either of these custom alerts.

Related topics

- Host Agent for MVS HSM overview

Host Agent for MVS SMS

MVS SMS: Responding to Automate and Environment alerts

These alerts monitor changes in the environment including:

- Occupancy alert
- Quiesce alert
- DASD Init alert
- SCDS Activate alert
- SCDS Update alert

The Occupancy alert issues a notification when a storage group begins to run out of space. Contact the storage group owner and tell them to clean up their disk space, or allocate more space for the storage group.

Quiesce alerts indicate that a storage group of quiesced volumes are running out of space. Contact the storage group owner and tell them to clean up their disk space, or allocate more space for the storage group.

A DASD Init alert (DASD Initialization) indicates volumes were successfully initialized. No response is required for these alerts.

SCDS Activate alerts indicate that a new SMS Control Data Set configuration has been enabled. No response is required. This alert informs the SMS administrator when someone has made an update to the SCDS. Unless someone with the authorization was not supposed to update this dataset, no action is required.

SMS SCDS update notifications are strictly informational. This alert informs the SMS administrator when someone has made an update to the SCDS. Unless someone with the authorization was not supposed to update this dataset, no action is required.

MVS SMS: Responding to SMS Error alerts

Alerts containing IGD messages are issued by the DFSMS subsystem. When you receive an alert with one of these message IDs, consult your IBM documentation for the appropriate response to the message.

MVS SMS: Responding to user defined alerts

Host Agent for MVS SMS permits you to create alerts that you define. These alerts can be configured to detect DFSMS message IDs or to detect message text that appears from multiple messages.

To respond to these types of alerts, consult your IBM DFSMS documentation for more information about the message that the user defined alert detected, or consult the creator of the alert to determine why that person created it, and what their intent for the alert is.

Host Agent for Novell

Novell: Responding to the Deleted File Space Threshold alert

Your response to the Deleted File Space Threshold alert will vary depending on the severity of the alert.

If the alert severity is critical or fatal, you should take immediate action to purge the deleted files or to allocate more space to the volume in which the file sits.

If the alert severity is harmless, minor, or warning, you should determine what steps you need to take to ensure that the deleted files do not grow to a critical size, for example:

- Purge the oldest deleted files, thereby allowing the possible salvage of more recently deleted files if necessary
- Add extra storage devices or increase volume size if necessary

You may want to create autofixes for the Deleted File Space Threshold alert. For example, the autofix might:

- purge all deleted files
- automatically delete other temporary files that are wasting space

See Alert concepts and procedures for more information about autofixes.

Related topics

- Deleted File Space Threshold alert
- Monitoring NetWare servers and file systems
- Host Agent for Novell overview

Novell: Responding to the Large File alert

Your response to the Large File alert will vary depending on the severity of the alert.

If the alert severity is critical or fatal, you should take immediate action to compress the file, to allocate more space to the volume in which the file sits, or to migrate the file to subsystem storage.

If the alert severity is harmless, minor, or warning, determine what you steps you need to take to ensure that the file does not grow to a critical size, for example:

- Contact the file's owner and determine the file's purpose and function
- Add extra storage devices or increase volume size if necessary

You may also want to create autofixes for the Large File alert. For example, an autofix might:

- automatically delete other temporary files that are wasting space
- compress the file
- migrate the file to subsystem storage

See Alert concepts and procedures for more information about autofixes.

Related alerts

- Large File alert

Related topics

- Monitoring NetWare servers and file systems
- Host Agent for Novell overview

Novell: Responding to the user space alerts

Your response to a user space alert will vary depending on the severity of the alert.

If the alert severity is critical or fatal, you should take immediate action to allot more space for the user, to compress the user's data, or to contact the user and identify files to be moved or deleted. For example, you might:

- Search for and delete temporary, log, and obsolete files from the user's account
- Set large files to Compress Immediate status
- Migrate the user's least critical files to subsystem storage
- Modify the user's space restriction to allow for greater storage space

If the alert severity is harmless, minor, or warning, determine what you steps you need to take to ensure that the user does not exceed their quota, for example:

- Contact the user and determine if greater space is needed
- Add extra storage devices if necessary

You may also want to create an autofix for these alerts. See Alert concepts and procedures for more information about autofixes.

Related alerts

- User Quota alert
- Space Usage alert

Related topics

- Monitoring NetWare servers and file systems
- Host Agent for Novell overview

Novell: Responding to volume alerts

Your response to a volume alert will vary depending on the severity of the alert.

If the alert severity is critical or fatal, you should take immediate action to create space on the volume. For example, you might:

- Search for and delete temporary, log, and obsolete files.
- Attempt to control the programs and files that are consuming the space if the free space has declined very rapidly.

If the alert severity is harmless, minor, or warning, determine what you steps you need to take to ensure the host has adequate storage, for example:

- Monitor files and folders to see how rapidly they are consuming space.
- Add storage devices if necessary.

You may also want to create an autofix for these alerts. See Alert concepts and procedures for more information about autofixes.

Related alerts

- Volume % Free Space alert
- Volume Free Space alert

Related topics

- Monitoring NetWare servers and file systems
- Host Agent for Novell overview

Host Agent for Windows

Windows: Responding to agent-initiated event log alerts

These alerts trigger after the Host Agent for Windows attempts to back up or clear a Windows event log, either as a result of an autofix attached to an event log size alert or the manual execution of the agent's back up or clear command.

Alert	Problem	Immediate response	Long-term prevention
Application, Security, or System Event Log Backup Failed	The Host Agent for Windows failed to back up the specified event log.	If the backup was part of a backup and clear event, the agent aborts the clear event. The event log may be empty or may not have any messages of the type you are trying to back up. For an explanation of why the backup failed, see the accompanying error messages in the Console, Active Alerts view, or log files.	Review the error messages that accompany the alert to see whether you can take steps to prevent future failures.
Application, Security, or System Event Log Clear Failed	The Host Agent for Windows failed to clear the specified event log.	The event log may be empty or may not have any messages of the type you are trying to clear. For an explanation of why the clear failed, see the accompanying error messages in the Console, Active Alerts view, or log files.	
Application, Security, or System Event Log Backup Completed	The Host Agent for Windows successfully backed up the specified event log.	By default, the agent saves the backup file in its working directory in a folder named `\EventLogBk\`*logname*, where *logname* is the name of the log the agent is backing up. The agent uses the following format in naming the backup file: *yyyydddhhmm*`.log`, where *yyyy* is the year, *ddd* is the julian day, *hh* is the hour in 24-hour format, and *mm* is the minutes. The ECC Administrator can change the directory to which the agent backs up the event logs.	You can disable these alerts if you only want to receive notification when the agent fails to back up or clear an event log.
Application, Security, or System Event Log Clear Completed	The Host Agent for Windows successfully cleared the specified event log.	This is an informational alert. No action is necessary.	

Note

- Note that these alerts trigger only when the agent is used to back up or clear an event log. You do not receive notification when other prgrams, such as Windows native programs, back up or clear an event log.

Related topics

- Windows: Monitoring event logs
- Windows: Backing up and clearing event logs
- Alert concepts and procedures

Windows: Responding to agent-initiated performance alerts

The agent-initiated performance alerts notify you after the Host Agent for Windows has completed the final performance recording of the day for a particular performance object.

Alert	Problem	Immediate response	Long-term prevention
Cache Recorder Complete Logical Storage Recorder Complete Memory Recorder Complete Page File Recorder Complete Physical Storage Recorder Complete Process Recorder Complete Server Recorder Complete Operating System Recorder Complete	The Host Agent for Windows recorded the final set of statistics for the specified performance object for the day.	Use a spreadsheet or database program, such as Microsoft Excel or Microsoft Access, to view and analyze the performance statistics.	Analyze the data after several weeks statistics have accumulated to perform capacity planning. Use the accumulated statistics to create baselines for performance monitoring. If you do not want to receive these alerts every day, you can disable them.

Related topics

- Windows: Recording performance statistics
- Windows: Viewing recorded performance statistics
- Windows: Creating performance baselines
- Windows: Performance monitoring terminology
- Windows: Monitoring performance
- Alert concepts and procedures

Windows: Responding to agent-initiated service alerts

These alerts trigger after the Host Agent for Windows attempts to restart a service as the result of the MNR_AUTOFIXSERSTART autofix, which is attached to the Service Failure alert.

Alert	Problem	Immediate response	Long-term prevention
Service Restart Failed	The Host Agent for Windows failed to restart a service that failed.	By default, the agent attempts to restart a failed service three times. For an explanation of why the agent could not restart the service, see the accompanying error messages in the Console, Active Alerts view, or log files. Also, browse the application and system event logs to see why the service failed to restart. If necessary, attempt to restart the service manually.	The ECC Administrator can change the number of restart attempts. Review the error messages that accompany the alert, and review the application and system event logs to see whether you can take steps to prevent future failures.
Service Restart Completed	The Host Agent for Windows successfully restarted a failed service.	Review the application and system event logs to see why the service failed and to determine whether steps must be taken to prevent future failures.	Disable this alert if you only want to receive notification when the agent fails to restart a service.

Related topics

- Windows: Monitoring services
- Windows: Exploring services
- Windows: Starting and stopping services
- Windows: Modifying the startup properties for a service
- Windows: Browsing event logs
- Alert concepts and procedures

Windows: Responding to event log size alerts

The event log size alerts, provided by the Host Agent for Windows, trigger when a Windows event log exceeds a size threshold you specified.

Alert	Problem	Immediate response	Long-term prevention
Application Event Log Size (KB) Limit Security Event Log Size (KB) Limit System Event Log Size (KB) Limit	A Windows event log has exceeded a size threshold you specified.	The Host Agent for Windows provides two autofixes for this alert, one that backs up and then clears the specified event log, and one that just clears the event log. See the alert description for more information on the autofixes. If you attached either autofix to the alert, the agent runs the autofix. Look for additional alerts indicating the result of the autofix (if those alerts are enabled). If you have not attached an autofix, use the agent to back up and clear, or just clear, the event log manually.	In addition to using the agent's autofixes to manage the size of your Windows event logs, you can use Windows native policies to manage them. For example, you can have Windows overwrite existing messages when an event log reaches a certain size. See the Windows documentation for more information.

Related alerts

- Agent-initiated event log alerts

Related topics

- Windows: Monitoring event logs
- Windows: Browsing event logs
- Alert concepts and procedures

Windows: Responding to event logged alerts

The event logged alerts trigger when a Windows application or service writes an event containing a text string that you have specified to the application, system, or security event log. These alerts are provided by the Host Agent for Windows.

Alert	Problem	Immediate response	Long-term prevention
Application Error Event Logged Application Warning Event Logged Application Information Event Logged	An event containing text that you specified was written to the Application event log.	Browse the application or system event log to view the complete event text and to determine whether additional action is necessary.	Create a user autofix that automatically corrects a problematic condition.
System Error Event Logged System Warning Event Logged System Information Event Logged	An event containing text that you specified was written to the System event log.		
Security AuditFailure Event Logged Security AuditSuccess Event Logged	An event containing text that you specified was written to the Security event log.	Browse the security event log to view the complete event text and to determine whether additional action is necessary.	If you are monitoring for repeated events, you can set up the alert to trigger when an event occurs a certain number of times within a specific period (such as 50 failed logon attempts within a minute). ControlCenter also provides additional features for monitoring Windows security.

Related topics

- Windows: Monitoring event logs
- Alert concepts and procedures

Windows: Responding to file and directory changed alerts

The File and Directory Changed alerts trigger when a monitored file or directory is created, renamed, deleted, or has any attribute changed.

Alert	Problem	Immediate response	Long-term prevention
File Changed Directory Changed	A monitored file or directory has been created, renamed, deleted, or had any attribute change.	Explore the file or directory to determine whether additional action is necessary. Modify the file or directory's permissions to prevent further changes. Change the file or directory attributes as necessary.	To monitor a high-security file or directory, use the agent's I/O monitoring feature to record all I/O activity against the file or directory.

Related topics

- Windows: Monitoring files and folders
- Alert concepts and procedures

Windows: Responding to file and directory size alerts

The File and Directory Size alerts trigger when the size of a monitored file or directory on a Windows host reach a threshold you specify.

Alert	Problem	Immediate response	Long-term prevention
File Size Directory Size	A monitored file or directory has reached a size threshold you specified. The threshold was specified in bytes.	Compress the file or directory. Windows may take more time read from and write to the file or directory, but it will occupy less disk space. See Compressing files, Compressing folders. Move the file or directory to another local disk that has more space, if necessary. To see which programs have a file or directory open, view the open files on the system. If a particular program is causing the file or directory to grow at an excessive rate, stop the program.	Create a user autofix that automatically corrects a problematic condition. For example, automatically delete files that are wasting space, such as files in a temporary directory. If specific users or groups are consuming the space on a particular Windows 2000 NTFS volume, create volume quotas to control their consumption.
File Size Change Percent Directory Size Change Percent	The size of a monitored file or folder has changed by a percentage that you specified.	Explore the file or directory to determine whether any immediate action is necessary. To see which programs have a file or directory open, view the open files on the system. If a particular program is causing the file or directory to grow at an excessive rate, stop the program. If you have set up the agent to monitor the I/O against the file, view the I/O monitoring log to determine what caused the size change.	To identify specific reasons why the size of a file or directory is changing, monitor all I/O events against the file or directory.
File Size Change Directory Size Change	The size of a monitored file or folder has changed by an amount (in bytes) that you specified.		

Related topics

- Windows: Monitoring files and folders
- Alert concepts and procedures

Windows: Responding to file count alerts

The File Count alerts trigger when the number of files in a monitored directory changes by an amount you specified in the alert definition. These alerts are provided by the Host Agent for Windows.

Alert	Problem	Immediate response	Long-term prevention
File Count	The number of files in a monitored directory has reached a threshold you defined.	Explore the directory to determine whether additional action is required. If necessary, delete files from the directory. To determine which programs are causing the file count to change, view the open files and directories on the system, which also reveals the processes that have a file or directory open. If a particular program is causing the file count to change at an excessive rate, stop the program.	Create a user autofix that automatically deletes files from a directory when the count reaches some threshold.
File Count Changed	The number of files in a monitored directory has changed by an amount you specified.	Explore the directory to determine whether additional action is required. To determine which programs are causing the file count to change, view the open files and directories on the system, which also reveals the processes that have a file or directory open. If a particular program is causing the file count to change at an excessive rate, stop the program.	To monitor a high-security directory, use the agent's I/O monitoring feature to record all I/O activity against the directory.
File Count Changed Percent	The number of files in a monitored directory has changed by a percentage you specified.		

Related topics

- Windows: Monitoring file I/O
- Windows: Monitoring files and folders
- Alert concepts and procedures

Windows: Responding to logical volume alerts

The logical volume space alerts trigger when the amount of free space on a logical volume, or drive, reaches a threshold you specified.

Alert	Problem	Immediate response	Long-term prevention
Logical Volume Percent Free	The percentage of free space on a monitored logical volume has reached a threshold you specified.	Explore the logical volume to determine whether additional action is necessary. If free space is declining very rapidly, attempt to control the programs or users that are consuming the space. Use the agent to determine which programs are accessing a volume. If necessary, stop a program that is consuming space excessively. Search for temporary, log, obsolete, or very large files. Create space by removing duplicate or unnecessary files.	Add storage devices to accommodate applications that need more disk space. Move large files to volumes with sufficient space. Create a user autofix that automatically deletes files that are wasting space, such as files in a temporary directory. If specific users or groups are consuming the space on a particular Windows 2000 NTFS volume, create volume quotas to control their consumption. To identify specific reasons why the size of a file or directory is changing, monitor all I/O events against the file or directory.
Logical Volume Size Free	A monitored logical volume has reached a size threshold you specified.		

Related alerts

- File and Folder Size alerts
- File and Folder Size Changed alerts
- File and Folder Size Changed Percent alerts

Related topics

- Windows: Monitoring volumes
- Windows: Searching volumes and folders
- Windows: Removing files and folders
- Windows: Monitoring files and folders
- Windows: Monitoring file I/O
- Windows: Managing volumes
- Alert concepts and procedures

Windows: Responding to memory-related performance alerts

If you have received one or more of the memory-related performance alerts, the monitored Windows host may be experiencing a memory bottleneck. A memory bottleneck affects host performance because the processor must devote most of its time and resources to managing memory.

Alert	Problem	Immediate response	Long-term prevention
Memory Usage Bottleneck (Pages Per Second)	The number of pages per second occurring on a monitored host has exceeded a threshold. Excessive paging can cause a memory bottleneck and affect the host's performance.	Determine the cause of the bottleneck. Use the Host Agent for Windows to view snapshots of various Windows performance counters. If a particular program is consuming excessive memory, stop the program to release the memory it has allocated. If a service is consuming excessive memory, stop the service. If the memory problem is severely affecting the host's performance, you may have to restart the host.	Rewrite host applications to use memory more efficiently or add memory to the host. Determine whether any programs have memory leaks and rewrite the programs to correct the leaks.
Memory Usage Bottleneck (Percent of I/O)	The amount of I/O activity a monitored host is devoting to paging has exceeded a threshold. As the host devotes more time to paging, there are fewer resources available for normal I/O operations.		
Pagefile Capacity	The number of times allocations from the paged pool have failed on a monitored host has exceeded a threshold. A high number of failures can indicate that the host does not have enough physical memory or that the paging file is too small.	Increase the size of the paging file or span the paging file across multiple disks.	Use the agent's recording feature to chart the % Usage and % Usage Peak values for the host's paging file performance object. Monitor these values over time to determine the minimum (average % Usage) and maximum (% Usage Peak) values for your paging file.

Related topics

- Windows: Creating performance baselines
- Windows: Viewing real-time performance statistics (snapshots)
- Alert concepts and procedures

Windows: Responding to physical disk performance alerts

A lengthy disk queue and a high transfer rate are key indicators that a disk is not handling I/O requests sufficiently. When the disk subsystem does not handle I/O requests well, system performance suffers as services and programs wait for the disk subsystem to satisfy their read and write requests.

Alert	Problem	Immediate response	Long-term prevention
Physical Disk Bottleneck (Transfer Rate)	The time the processor is taking to read from and write to disks on a monitored host has exceeded a threshold. A high transfer rate may affect the host's performance.	Determine whether a memory bottleneck is not the real problem. If memory is not the problem, diagnose the disk bottleneck. Determine which programs and files are causing the high level of activity on the disk. Balance the I/O load on the host by moving heavily accessed files to disks with less activity.	Move the paging file off the system's root disk, which is the disk where the key operating system files are located Minimize the number of programs installed on the root disk. If your system only has one disk, consider purchasing additional disks or moving heavily accessed files to another server. If insufficient memory is the cause of the disk bottleneck, use memory tuning techniques to reduce the amount of paging and increase the system's use of cache.
Physical Disk Bottleneck (Queue Length)	The number of read and write requests in a disk queue on a monitored host has exceeded a threshold, indicating that the disk may not be handling I/O requests sufficiently.		

Note

- These alerts have default settings based on Microsoft documentation. However, you should create a baseline of statistics for disk performance to determine acceptable levels for your data center, and adjust the alert settings for acceptable performance levels.

Related topics

- Windows: Monitoring disk performance
- Windows: Creating performance baselines
- Windows: Viewing real-time performance statistics (snapshots)
- Alert concepts and procedures

Windows: Responding to printer alerts

The Host Agent for Windows printer alerts trigger when significant changes occur on local printers of monitored Windows hosts. Use these alerts to track printer changes and detect problems before they affect work flow.

Alert	Problem	Immediate response	Long-term prevention
Printer Changed	A local printer has been added to or deleted from a monitored Windows system.	Explore the printers on the host to determine whether additional action is necessary. Pause, resume, or cancel a print job. Or, clear a printer's queue. Start or stop the printer, if necessary. See Stopping printers, Starting printers.	For high-security printers, such as printers used for payroll or accounts receivable, you can monitor the security event log for significant printer-related events, such as attempts to change the ownership of a printer.
Printer Driver Changed	The driver for a local printer on a monitored host has changed.		
Printer Job Changed	A job was added to the queue of a local printer on a monitored host.		
Printer Port Changed	A change has been made to the port of a local printer on a monitored host.		

Related topics

- Windows: Managing printers
- Windows: Monitoring printers
- Alert concepts and procedures

Windows: Responding to process alerts

The Host Agent for Windows process alerts trigger when Windows processes become either active or inactive.

Alert	Problem	Immediate response	Long-term prevention
Process Active	A specific process has started on a monitored host.	If the process is a virus or another potentially harmful program, stop the process immediately. To learn more about the process and the resources it is consuming, explore the processes on the host. Determine which other process started the process by viewing the process relationship tree. Determine which files the process is accessing by viewing the open files on the host. If the process is low priority, change its processing priority to lessen its impact on other resources.	If this is a harmful process, create an autofix to kill it automatically when it starts.
Process Inactive	A specific process has become inactive on a monitored host.	Browse the system and application event logs to determine why the process stopped. If you have created a service for the process, restart the service. Restart the process manually on the host. You cannot restart the process using the agent.	Create an autofix to automatically restart the process when it fails. Set up the process as a service and use the agent's service restart autofix to automatically restart the service when it fails. To receive early warning that an important process may fail, use the event logged alerts to monitor the system and application event logs for events that previously led to the process failing. Use the agent's recording feature to gather performance trending data that may help determine why a process fails.

Related alerts

- Service Active alert
- Service Inactive and Service Failure alerts

Related topics

- Windows: Monitoring processes
- Windows: Managing processes
- Alert concepts and procedures

Windows: Responding to processor performance alerts

The Host Agent for Windows processor performance alerts trigger when the agent detects conditions that may cause a processor bottleneck. To fix a processor bottleneck, first consider processor activity in relation to other indicators. A busy processor is not necessarily bad. You want your system to take advantage of your processor's power, but you do not want programs to have to wait for access to the processor. If you receive a Processor Time Percent alert in combination with a Processor Queue Length alert, you likely have a processor bottleneck.

<table>
<tr><th>Alert</th><th>Problem</th><th>Immediate response</th><th>Long-term prevention</th></tr>
<tr><td>Processor Congestion (Processor Time Percent)</td><td>The % Processor Time counter for a processor on a monitored host has reached a threshold, indicating a possible processor bottleneck.</td><td rowspan="3">Determine whether a memory or disk bottleneck is the real problem. See Diagnosing memory bottlenecks, Diagnosing disk bottlenecks.
After you rule out other bottlenecks, diagnose the processor bottleneck.
To fix the processor bottleneck, first identify which programs are demanding the most CPU time. Use the agent's recording and process snapshot features to track these statistics.
Stop processes that are monopolizing the CPU time.
Alternatively, lower the priority of demanding processes to allow other programs to perform.</td><td rowspan="3">Rewrite or replace programs that cause bottlenecks.
Upgrade your CPU if most of your programs are single-threaded.
Add CPUs if you have a multiuser environment and your programs are mult-threaded.</td></tr>
<tr><td>Processor Congestion (Total Processor Time Percent)</td><td>The % Total Processor Time counter for a monitored host that has multiple processors has reached a threshold, indicating a possible processor bottleneck.</td></tr>
<tr><td>Processor Congestion (Queue Length)</td><td>The number of threads waiting on the processor of a monitored host has reached a threshold, indicating a possible processor bottleneck.</td></tr>
</table>

Related topics

- Windows: Monitoring processor performance
- Windows: Creating performance baselines
- Windows: Viewing real-time performance statistics (snapshots)
- Alert concepts and procedures

Windows: Responding to service alerts

The Host Agent for Windows service alerts trigger when a monitored service becomes either active or inactive on a Windows host.

Alert	Problem	Immediate response	Long-term prevention
Service Active	A monitored service has become active.	If the service is potentially harmful, stop the service immediately. Explore the services on the host to determine learn more about the service.	If this is a harmful service, create an autofix to stop it automatically when it starts.
Service Inactive	A monitored service has become inactive.	Restart the service manually. Browse the system and application event logs to determine why the service stopped.	To have the service restart automatically when it stops, use the Service Failure alert and attach its predefined autofix. To receive early warning that an important service may fail, use the event logged alerts to monitor the system and application event logs for events that previously led to the service failing.
Service Failure	A monitored service has become inactive. This is a duplicate of the Service Inactive alert, except that you can attach an autofix that automatically restarts the failed service.	If you have attached the service restart autofix to this alert, the agent attempts to restart the service three times.	The ControlCenter administrator can change the number of times the agent attempts to restart the services.

Related alerts

- Windows: Agent-initiated service alerts

Related topics

- Windows: Monitoring services
- Windows: Exploring services
- Windows: Starting and stopping services
- Windows: Browsing event logs
- Alert concepts and procedures

Logical Agent for MVS

Logical: Responding to Alias Space alerts

The Alias Space alert monitors the amount of alias space in user catalogs. ControlCenter uses its SCAN command to collect the alert information. When the alert triggers, you can view the specific SCAN command report associated with the alert. To do this:

1. View the triggered alerts for the monitored OS/390 system.
2. Right-click the alert and select **Display Alias Space Check report**. A new dialog box displays, listing the SCAN reports that ControlCenter has run.
3. Locate the SCAN report that generated the alert.
4. Right-click the report and select **View Last Ouput**. A list of the data sets that matched the criteria of the SCAN command appears. You can manipulate the data sets by right-clicking them and selecting from the list of commands provided.

Related topics

- Alias Space alert
- General alert concepts and procedures

Logical: Responding to Allocation Failures alerts

The Allocation Failures alert monitors the number of DASD allocation failures occurring from creates and extends. When you receive this alert, check the message output to determine what caused the failures. Once you determine the cause of the failures, address it.

Related topics

- Allocation Failures alert
- General alert concepts and procedures

Logical: Responding to catalog message alerts

Work with your system programmers to resolve the conditions identified in the error message. Consult the IBM OS/390 documentation for more information on the error messages and for recommended actions.

Related topics

- Catalog error message alerts
- General alert concepts and procedures

Logical: Responding to Catalog Sharing alerts

The Catalog Sharing alert monitors for user catalogs with their share options attribute set to something other than (3,4). ControlCenter uses its SCAN command to collect the alert information. When the alert triggers, you can view the specific SCAN command report associated with the alert. To do this:

1. View the triggered alerts for the monitored OS/390 system.
2. Right-click the alert and select **Display the List of Saved CSL Scans**. A new dialog box displays listing the SCAN reports that ControlCenter has run.
3. Locate the SCAN report that generated the alert.
4. Right-click the report and select **View Last Ouput**. A list of the data sets that matched the criteria of the SCAN command appears. You can manipulate the data sets by right-clicking them and selecting from the list of commands provided.

Related topics

- Catalog Sharing alert
- General alert concepts and procedures

Logical: Responding to Data Set Extents alert

The alert triggers when the number of extents for a data set exceeds a threshold. When a data set reaches its extent limit, it can no longer grow. To reduce the number of extents, you must reorganize the data set.
In response to this alert, you can view a report of the number of extents of data sets monitored by the alert. To do this:

1. View the triggered alerts for the monitored OS/390 system.
2. Right-click the alert and select **Display the Extent Summary report**. A new dialog box displays, listing the data sets or data set masks for which ControlCenter has run Extent reports.
3. Locate the report that generated the alert. Sort the report by the Data Set Name or Last Scanned columns to help locate the report.
4. Right-click the report and select **View Detail**.
5. Examine the report.

Related topics

- Dataset Extents alert
- General alert concepts and procedures

Logical: Responding to Examine alerts

The Examine command monitors the health of OS/390 ICF catalogs. The alert triggers when the return code from the OS/390 IDCAMS EXAMINE command matches the trigger value for one of the alert severity levels. By default, the Fatal alert triggers for a return code of 12, Critical for 8, and Minor for 4.

In response to the alert, you can view the results of the Examine command that issued the return code. To do this:

1. View the triggered alerts for the monitored OS/390 system.
2. Right-click the alert and select **Display the Examine summary report**. A new dialog box displays listing the Examine reports that ControlCenter has run.
3. Locate the Examine report that generated the alert. Sort the report by the Catalog Name, Status, or Last Scanned columns to help locate the report.
4. Right-click the report, and select **Examine**, **View Last**.
5. View the report to determine the cause of the return code.

Related topics

- Examine alert
- General alert concepts and Examine

Logical: Responding to GDG Scan alerts

The GDG Scan alert detects generation data groups (GDGs) that are not defined correctly. ControlCenter uses the SCAN command to detect these GDGs. When the alert triggers, you can view a report of the incorrectly defined GDGs. To do this:

1. View the triggered alerts for the monitored OS/390 system.
2. Right-click the alert and select **Display GDGs that were incorrectly defined**. A new dialog box displays listing the GDGs. You can manipulate them by right-clicking them and selecting from the list of commands provided.

Related topics

- GDG Scan alert
- General alert concepts and procedures

Logical: Responding to PDS Directory Full alerts

The PDS Directory Full alert detects partitioned data sets (PDSs) that are out of directory space. ControlCenter uses its SCAN command to collect the information. When the alert triggers, you can view a report of the data sets that are out of directory space. To do this:

1. View the triggered alerts for the monitored OS/390 system.
2. Right-click the alert and select **Display the PDS Directory Space report**. A new dialog box appears, listing the PDSs.

Related topics

- PDS Directory Full alert
- General alert concepts and procedures

Logical: Responding to Processing Failed alerts

The Processing Failed alert detects when ControlCenter encounters an error while processing alerts related to OS/390 logical storage. When you receive this alert, you should consult with the ControlCenter administrator to determine why the alert processing failed. Check the ControlCenter logs for error messages. If you cannot determine the cause of the failure, contact EMC technical support.

Related topics

- Processing Failed alert
- General alert concepts and procedures

Logical: Responding to Space Activity alerts

The Space Activity alerts check each day for excessive space use growth. When you receive a space activity alert, determine how much space has been used.

Your options are to tell the people who used the space to clean it up, to make more storage space available, or to change storage management policies to make more room available for mission-critical data.

Related topics

- Space Activity alerts
- General alert concepts and procedures

Logical: Responding to Space Use alerts

The Space Use alerts monitor allocation and use of space by high-level qualifiers (users) and application resources as defined by you in application IDs.

Related topics

- Space Use alerts
- Creating application IDs
- General alert concepts and procedures

Logical: Responding to System Check alerts

The System Check command monitors the health of OS/390 ICF catalogs. The alert triggers when the return code from the ControlCenter System Check command matches the trigger value for one of the alert severity levels. By default, the Fatal alert triggers for a return code of 12, Critical for 8, and Minor for 4.

In response to the alert, you can view the results of the System Check command that issued the return code. To do this:

1. View the triggered alerts for the monitored OS/390 system.
2. Right-click the alert and select **Display the SystemCheck summary report**. A new dialog box displays listing the System Check reports that ControlCenter has run.
3. Locate the System Check report that generated the alert. Sort the report by the Catalog/VVDS Name, Status, or Last Scanned columns to help locate the report.
4. Right-click the report, select **System Check**, **View Last**.
5. Examine the report to determine the cause of the return code.

Related topics

- System Check alert
- General alert concepts and procedures

Logical: Responding to TeraSAM Candidates alerts

The TeraSAM Candidates alert detects data sets for which the high-used RBA value (HURBA) meets a threshold you define. ControlCenter uses its SCAN command to collect the information. When the alert triggers, you can view a report of the data sets that match the alert criteria. To do this:

1. View the triggered alerts for the monitored OS/390 system.
2. Right-click the alert and select **Display the CSL HURBA status report**. A new dialog box appears, listing the data sets that meet the alert criteria.

Related topics

- TeraSAM Candidates alert
- General alert concepts and procedures

Logical: Responding to user-defined alerts

Work with your system programmers to resolve the conditions identified in the error message. Consult the IBM OS/390 documentation for more information on the error messages and for recommended actions.

Related topics

- User-defined alert
- General alert concepts and procedures

Logical: Responding to VSAM Reorg alerts

The VSAM Reorg alert detects data sets for which the number of CA splits is excessive, indicating that the data set should be reorganized. ControlCenter uses its SCAN command to collect the information. When the alert triggers, you can view a report of the data sets that match the alert criteria. To do this:

1. View the triggered alerts for the monitored OS/390 system.
2. Right-click the alert and select **Display the CSL CA Splits status report**. A new dialog box appears, listing the data sets that meet the alert criteria.

Related topics

- VSAM Reorg alert
- General alert concepts and procedures

Physical Agent for MVS

Physical: Responding to DASD status alerts

The Physical Agent for MVS offers three alerts that allow you to monitor status conditions on DASD. Status in this context refers to conditions involving DASD integrity, user intervention with DASD, and changes in the DASD environment.

Related alerts

- Physical: Integrity alert
- Physical: Intervention (Disk) alert
- Physical: DASD Init alert

Related topics

- General alert concepts and procedures

Physical: Responding to DASD Space alerts

The Physical Agent for MVS offers three alerts that monitor DASD space conditions. The typical response to these types of alerts is to free space from existing volumes, make new volumes available, or to run a defragmentation job. These alerts can be associated with REXX executables or CLISTs you have created to automatically address these problems.

Related alerts

- Physical: % Free Space alert
- Physical: Free DSCBs alert
- Physical: Fragmentation alert

Related topics

- General alert concepts and procedures

Physical: Responding to Tape alerts

The Physical Agent for MVS offers two tape alerts: One notifies you when user intervention is needed for a tape, and the other when an allocation has been made without a tape being mounted.

Related alerts

- Physical: Intervention (Tape) alert
- Physical: Allocation Without Mount alert

Related topics

- General alert concepts and procedures

Storage Agent for CLARiiON

CLARiiON: Responding to RAID Group Free Space

When responding to a RAID Group Free Space alert, you should either recover some space in that RAID Group or add new disks to it to extend its size (if that type of RAID group allows you to add new disks to it).

Alert Name	Problem	Immediate Response	Long Term Prevention
RAID Group Free Space alert	The free space on the RAID group is below a specified value.	Either add new space to that RAID Group or clean it to restore some free space.	Create a new RAID Group; reorganize its data distribution.

Related topics

- Alert concepts and procedures

CLARiiON: Responding to RAID Group Percent Free Space

When responding to RAID Group Percent Free Space alert, you should either recover some space in that RAID Group or add new disks to it to extend its size (if that type of RAID Group allows you to add new disks to it).

Alert Name	Problem	Immediate Response	Long Term Prevention
RAID Group Percent Free Space alert	The free space on the RAID group is below a specified value.	Either add new space to that RAID Group or clean it to restore some free space.	Create a new RAID group; reorganize its data distribution.

Related topics

- Alert concepts and procedures

CLARiiON: Responding to Storage Array Fault

When responding to Storage Array Fault alert, you should fix it.

Alert Name	Problem	Immediate Response	Long Term Prevention
Storage Array Fault alert	There are faults with some customer replaceable units (CRUs) in the disk array.	View the customer replaceable units report to which faults are broken.	N/A

Related topics

- Alert concepts and procedures

Storage Agent for Compaq StorageWorks

StorageWorks: Responding to Battery Days to Expiration alerts

This Storage Agent for Compaq StorageWorks alert triggers when the number of days until the external cache battery for a subsystem controller expires reaches a threshold you specify. The external cache battery ensures that you do not lose or corrupt data that is in cache but has not been written to disk if an array's power supply is interrupted.

Alert	Problem	Immediate response	Long-term prevention
Battery Days to Expiration	The external cache battery for a monitored subsystem controller is approaching its expiration date.	To view more information about the battery and controller cache, explore the controller cache properties. Replace the affected array's external cache battery before the expiration date.	Continue using the alert to receive notification when batteries must be changed.

Related topics

- StorageWorks: Monitoring subsystems
- Storage Agent for Compaq StorageWorks overview
- Alert concepts and procedures

StorageWorks: Responding to device count alerts

These Storage Agent for Compaq StorageWorks alerts trigger when the number of devices in a monitored subsystem's spare and failed sets meet a threshold you specify.

Alert	Problem	Immediate response	Long-term prevention
Failed Set Device Count	The number of devices in a monitored subsystem's failed set has exceeded a threshold you specified.	Explore the failed set to determine which disks have failed.	Replace or fix the disks in the failed set so that they can be used in the subsystem.
Set Is Reduced	A disk has been removed from a storageset or a disk has failed and there is a failed device replacement policy.	Explore the storageset to determine the current configuration of the storageset.	Continue using this alert to monitor for unexpected removals of devices from storagesets.
Spare Set Device Count	The number of devices in a monitored subsystem's spare set has fallen below a trigger value that you specified.	Explore the spare set to determine whether you need to add devices.	Add devices to the spare set, if necessary.

Note

- Use the StorageWorks Command Console (SWCC) or command line interpreter (CLI) to add or remove devices.

Related topics

- StorageWorks: Monitoring storageset device counts
- Storage Agent for Compaq StorageWorks overview
- Alert concepts and procedures

StorageWorks: Responding to Device Not Mapped alerts

This Storage Agent for Compaq StorageWorks alert triggers when the agent discovers a device that is not currently mapped to a unit in the monitored subsystem.

Alert	Problem	Immediate response	Long-term prevention
Device Not Mapped	The agent discovered a subsystem device that is not mapped to a unit and, therefore, not available to hosts in your storage network.	Evaluate whether the device should be in use in your storage environment. Use the agent to explore the subsystem configuration. Use the StorageWorks Command Console (SWCC) or command line interpreter (CLI) to make the container available.	Continue using the alert to monitor for unmapped devices.

Related topics

- StorageWorks: Monitoring subsystems
- Storage Agent for Compaq StorageWorks overview
- Alert concepts and procedures

Storage Agent for HDS

HDS: Responding to Illegal Paired Volumes

Contact the HDS administrator or HP Customer Engineer (CE) for the XP system.

Alert Name	Problem	Immediate Response	Long Term Prevention
Illegal Paired Volumes alert	Internal error.	Contact the HP CE or HDS administrator.	Contact the HP CE or HDS administrator.

Related topics

- Alert concepts and procedures

HDS: Responding to Volume Not Paired

You can pair these volumes, or pass this alert (do nothing) at the risk of losing data.

Alert Name	Problem	Immediate Response	Long Term Prevention
Volumes Not Paired alert	Some volumes were not yet in data protection.	Make a pair of these volumes.	Make a pair of these volumes.

Related topics

- Alert concepts and procedures

Storage Agent for IBM ESS

IBM ESS: Responding to Unavailable Cache alert

If you receive this alert, a subsystem error has caused one of the IBM ESS cache controllers to become unavailable. If you have remote hardware support enabled, the call home feature sends information about this problem to IBM technical support. See your IBM ESS documentation for more information.

Do the following:

- Notify your hardware customer support engineer.
- Check that IBM ESS has notified IBM of this problem.
- Check the IBM ESS Configuration and Status report to see configured, available, and offline cache.
  ..

Related topics

- IBM ESS: Unavailable Cache alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to Offline Cache alert

If you receive this alert, caching errors have caused cache in the IBM ESS to be offline. If you have remote hardware support enabled, the call home feature sends information about this problem to IBM technical support. See your IBM ESS documentation for more information.

Do the following:

- Notify your hardware customer support engineer.
- Check that IBM ESS has notified IBM of this problem.
- Check the IBM ESS Status and Configuration report to see configured, available, and offline cache.

Related topics

- IBM ESS: Offline Cache alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to DFW Inhibited alert

If you receive this alert, IBM ESS DASD fast write (DFW) is inhibited. If you have remote hardware support enabled, the call home feature sends information about this problem to IBM technical support. See your IBM ESS documentation for more information.

Do the following:

- Notify your hardware customer support engineer.
- Check that IBM ESS has notified IBM of this problem.

Related topics

- IBM ESS: DFW Inhibited alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to CFW Deactivated alert

If you receive this alert, IBM ESS cache fast write (CFW) has deactivated. If you have remote hardware support enabled, the call home feature sends information about this problem to IBM technical support. See your IBM ESS documentation for more information.

Do the following:

- Notify your hardware customer support engineer.
- Check that IBM ESS has notified IBM of this problem.

Related topics

- IBM ESS: CFW Deactivated alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to Cache Fast Write Hit Ratio alert

If you receive this alert, the IBM ESS cache fast write (CFW) hit ratio is less than a specified value. This is usually a transient event. If the alert continues to display, do the following:

1. Notify your performance group, which may need to increase the cache capacity or balance the workload.
2. Check the cache summary reports for detailed information about IBM ESS caching activity. You can select to view hourly, daily, weekly, or monthly summaries of cache activity.

   You can use these reports to see if there is a trend with this alert, in which you could adjust the hit ratio, or if the period that caused the alert to trigger was only a transient event, which you could probably ignore.

Related topics

- IBM ESS: Cache fast write Hit Ratio alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to CFW and DFW Suspended alert

If you receive this alert, caching errors have suspended both IBM ESS cache fast write (CFW) and DASD fast write (DFW). If you have remote hardware support enabled, the call home feature sends information about this problem to IBM technical support. See your IBM ESS documentation for more information.

Do the following:

- Notify your hardware customer engineer.
- Check that IBM ESS has notified IBM of this problem.

Related topics

- IBM ESS: CFW and DFW Suspended alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to Delayed DASD Fast Write alert

If you receive this alert, IBM ESS DASD fast write (DFW) is currently delayed. If you have remote hardware support enabled, the call home feature sends information about this problem to IBM technical support. See your IBM ESS documentation for more information.

Do the following:

- Notify your hardware customer support engineer.
- Check that IBM ESS has notified IBM of this problem.

Related topics

- IBM ESS: Delayed DASD Fast Write alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to Device Pinned Data alert

If you receive this alert, an IBM ESS subsystem has pinned data in its cache that IBM ESS cannot write to disk. If you have remote hardware support enabled, the call home feature sends information about this problem to IBM technical support. See your IBM ESS documentation for more information.

Do the following:

1. Notify your hardware customer support engineer.
2. Check that IBM ESS has notified IBM of this problem.
3. Check the Pinned Tracks report to see which datasets have pinned tracks.

Related topics

- IBM ESS: Device Pinned Data alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to NVS Disabled alert

If you receive this alert, non volatile storage (NVS) in IBM ESS is disabled. If you have remote hardware support enabled, the call home feature sends information about this problem to IBM technical support. See your IBM ESS documentation for more information.

Do the following:

1. Notify your hardware customer support engineer.
2. Check that IBM ESS has notified IBM of this problem.

Related topics

- IBM ESS: NVS Disabled alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to NVS Failed alert

If you receive this alert, non volatile storage (NVS) in IBM ESS has failed. If you have remote hardware support enabled, the call home feature sends information about this problem to IBM technical support. See your IBM ESS documentation for more information.

Do the following:

1. Notify your hardware customer support engineer.
2. Check that IBM ESS has notified IBM of this problem.

Related topics

- IBM ESS: NVS Failed alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to NVS Pending alert

If you receive this alert, non volatile storage (NVS) in IBM ESS is pending and IBM ESS is unable to write the data to disk. If you have remote hardware support enabled, the call home feature sends information about this problem to IBM technical support. See your IBM ESS documentation for more information.

Do the following:

1. Notify your hardware customer support engineer.
2. Check that IBM ESS has notified IBM of this problem.

Related topics

- IBM ESS: NVS Pending alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to Pinned Cache alert

If you receive this alert, caching errors have caused pinned cache in the IBM ESS. If you have remote hardware support enabled, the call home feature sends information about this problem to IBM technical support. See your IBM ESS documentation for more information.

Do the following:

- Notify your hardware customer support engineer.
- Check that IBM ESS has notified IBM of this problem.
- Check the IBM ESS Status and Configuration report to see configured, available, and offline cache.

Related topics

- IBM ESS: Pinned Cache alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to Pinned NVS alert

If you receive this alert, an IBM ESS subsystem's pinned non volatile storage (NVS) has exceeded its limit (in KB). If you have remote hardware support enabled, the call home feature sends information about this problem to IBM technical support. See your IBM ESS documentation for more information.

Do the following:

1. Notify your hardware customer support engineer.
2. Check that IBM ESS has notified IBM of this problem.
3. Check the Pinned Tracks report to see which datasets have pinned tracks.

Related topics

- IBM ESS: Pinned NVS alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to Pinned NVS for Device alert

If you receive this alert, an IBM ESS devices's pinned non volatile storage (NVS) has exceeded its limit (in KB). If you have remote hardware support enabled, the call home feature sends information about this problem to IBM technical support. See your IBM ESS documentation for more information.

Do the following:

1. Notify your hardware customer support engineer.
2. Check that IBM ESS has notified IBM of this problem.
3. Check the Display Pinned Tracks report to see which datasets have pinned tracks.

Related topics

- IBM ESS: Pinned NVS for Device alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to RAID Rebuild alert

If you receive this alert, an IBM ESS volume is part of a RAID rank (disk array) that is undergoing a rebuild. This alert is typically transient. If the alert recurs, do the following:

- Notify your hardware customer support engineer.
- Use the MVS Volumes report to see which volumes are affected.

Related topics

- IBM ESS: RAID Rebuild alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to Read Normal Hit Ratio alert

If you receive this alert, the IBM ESS Read Normal hit ratio is less than a specified value. This is usually a transient event. If the alert recurs, do the following:

1. Notify your performance group, which may need to increase the cache capacity or balance the workload.
2. Check the cache summary reports for detailed information about IBM ESS caching activity. You can select to view hourly, daily, weekly, or monthly summaries of cache activity.

   You can use these reports to see if there is a trend with this alert, in which you could adjust the hit ratio, or if the period that caused the alert to trigger was only a transient event, which you could probably ignore.

Related topics

- IBM ESS: Read Normal Hit Ratio alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to Read Sequential Hit Ratio alert

If you receive this alert, the IBM ESS Read Sequential hit ratio is less than a specified value. This alert may be a transient event. If the alert continues to display, do the following:

1. Notify your performance group, which may need to increase the cache capacity or balance the workload.
2. Check the cache summary reports for detailed information about IBM ESS caching activity. You can select to view hourly, daily, weekly, or monthly summaries of cache activity.

   You can use these reports to see if there is a trend with this alert, in which you could adjust the hit ratio, or if the period that caused the alert to trigger was only a transient event, which you could probably ignore.

Related topics

- IBM ESS: Read Sequential Hit Ratio alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to Search Read Cache Fast Write Hit Ratio alert

If you receive this alert, the IBM ESS search read cache fast write hit ratio is less than a specified value. This is usually a transient event. If the alert recurs, do the following:

1. Notify your performance group, which may need to increase the cache capacity or balance the workload.
2. Check the cache summary reports for detailed information about IBM ESS caching activity. You can select to view hourly, daily, weekly, or monthly summaries of cache activity.

   You can use these reports to see if there is a trend with this alert, in which you could adjust the hit ratio, or if the period that caused the alert to trigger was only a transient event, which you could probably ignore.

Related topics

- IBM ESS: Search Read Cache fast write Hit Ratio alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to Write Normal Hit Ratio alert

If you receive this alert, the IBM ESS Write Normal hit ratio is less than a specified value. This is usually a transient event. If the alert recurs, do the following:

1. Notify your performance group, which may need to increase the cache capacity or balance the workload.
2. Check the cache summary reports for detailed information about IBM ESS caching activity. You can select to view hourly, daily, weekly, or monthly summaries of cache activity.

   You can use these reports to see if there is a trend with this alert, in which you could adjust the hit ratio, or if the period that caused the alert to trigger was only a transient event, which you could probably ignore.

Related topics

- IBM ESS: Write Normal Hit Ratio alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

IBM ESS: Responding to Write Sequential Hit Ratio alert

If you receive this alert, the IBM ESS Write Sequential hit ratio is less than a specified value. This is usually a transient event. If the alert recurs, do the following:

1. Notify your performance group, which may need to increase the cache capacity or balance the workload.
2. Check the cache summary reports for detailed information about IBM ESS caching activity. You can select to view hourly, daily, weekly, or monthly summaries of cache activity.

   You can use these reports to see if there is a trend with this alert, in which you could adjust the hit ratio, or if the period that caused the alert to trigger was only a transient event, which you could probably ignore.

Related topics

- IBM ESS: Write Sequential Hit Ratio alert
- Alert concepts and procedures
- Storage Agent for IBM ESS overview

Storage Agent for RVA/SVA

RVA/SVA: Responding to Agent Initiated Alter Subsystem

When responding to this alert, use the Storage Agent for RVA/SVA. Right-click the affected host, and then select **Storage Agent for RVA/SVA**, **Explore**.

Alert Name	Problem	Immediate Response	Long Term Prevention
Agent Initiated Alter Subsystem Alert	A ControlCenter user has changed the name of an RVA or SVA subsystem. This can affect console users and prevent alerts from monitoring the affected RVA. This alert may be informational or may indicate an undesirable change or a security exposure.	When a user modifies the subsystem name, all users working with that subsystem should explore the agent again. Edit Storage Agent for RVA/SVA configured alerts to ensure the new subsystem name is included in the specification on the Source tab.	If you want to prevent this change in the future, use RACF and ControlCenter security to restrict user privileges.

To explore the Storage Agent for RVA/SVA again:

1. Close the window for the Storage Agent for RVA/SVA.
2. Right-click the host you want, then click Storage Agent for RVA/SVA. A new agent window displays.

This allows the agent to process commands related to the modified subsystem properly.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Responding to Agent Initiated DDSR Change

When responding to this alert, use the Storage Agent for RVA/SVA. Right-click the affected host, and then select **Storage Agent for RVA/SVA**, **Explore**.

Alert Name	Problem	Immediate Response	Long Term Prevention
Agent Initiated DDSR Change alert	A ControlCenter user has modified a DDSR process. This alert may be informational or may indicate an undesirable change or a security exposure.	Explore DDSR processes and ensure the process will release space appropriately.	If you want to prevent this change in the future, use RACF and ControlCenter security to restrict user privileges.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Responding to Agent Initiated Channel Alteration

When responding to this alert, use the Storage Agent for RVA/SVA. Right-click the affected host, and then select **Storage Agent for RVA/SVA**, **Explore**.

Alert Name	Problem	Immediate Response	Long Term Prevention
Agent Initiated Channel Alteration alert	A ControlCenter user has modified a channel interface. This alert may be informational or may indicate an undesirable change or a security exposure.	Explore Channel Interfaces and ensure that the new properties are acceptable.	If you want to prevent this change in the future, use RACF and ControlCenter security to restrict user privileges.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Responding to Agent Initiated MVS Device Alteration

When responding to this alert, use the Storage Agent for RVA/SVA. Right-click the affected host, and then select **Storage Agent for RVA/SVA**, **Explore**.

Alert Name	Problem	Immediate Response	Long Term Prevention
Agent Initiated MVS Device Alteration alert	A ControlCenter user has modified an MVS device configuration on the RVA or SVA. This alert may be informational or may indicate an undesirable change or a security exposure.	Explore MVS devices to ensure that the modified device has the correct properties.	If you want to prevent this change in the future, use RACF and ControlCenter security to restrict user privileges.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Responding to Channel Interface Disabled

When responding to this alert:

Alert Name	Problem	Immediate Response	Long Term Prevention
Channel Interface Disabled alert	A channel interface is disabled. Subsystem performance could be diminished. The cause is either hardware failure or intentional deactivation.	Explore Channel Interfaces to see if sufficient interfaces remain enabled. Use the LOP (the console) on the subsystem to investigate the problem. The subsystem may already have "phoned home." Consider pausing or terminating lower priority processing.	Use RMF data to check average response time from the MVS devices on the subsystem. This will tell you the impact of the disabled channel interface and help you make contingency plans.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Responding to DDSR Not Active

When responding to this alert, use the Storage Agent for RVA/SVA. Right-click the affected host, and then select **Storage Agent for RVA/SVA**, **Explore**.

Alert Name	Problem	Immediate Response	Long Term Prevention
DDSR Not Active alert	DDSR is not active for a host. No DDSR processes are active on the host. Data deleted on the host will not be recovered by the subsystem.	See if IXFP is running and, if not, start it from the MVS console. On the host, start the dynamic DDSR process so space collection will occur for future deletions. A backlog of deleted data may exist. To recover the space with minimal impact, start interval DDSR processes that cover separate groups of volumes. Stagger the start of these processes to minimize impact.	Check automatic startup configuration of IXFP and DDSR. Ensure IXFP starts automatically at IPL, Also, configure DDSR to start automatically as well. Alternatively, allow a staff member to start DDSR manually through ControlCenter.

Related topics

- Alert concepts and procedures
- RVA/SVA: Responding to DDSR alerts (more detailed procedures for responding to this alert)
- RVA/SVA: Exploring DDSR (starting, stopping, suspending, and resuming DDSR processes)
- Storage Agent for RVA/SVA overview

RVA/SVA: Responding to DDSR Not Active for a Volume

When responding to this alert, use the Storage Agent for RVA/SVA. Right-click the affected host, and then select **Storage Agent for RVA/SVA**, **Explore**.

Alert Name	Problem	Immediate Response	Long Term Prevention
DDSR Not Active for a Volume alert	DDSR is not active for a host volume. For this volume, space occupied by deleted data will not be recovered by the subsystem.	On the host, start the dynamic DDSR or, if it is started, check its configuration to ensure that the affected volume is included in the specification. A backlog of deleted data may exist. To recover the space with minimal impact, start an interval DDSR process that specifies the volume.	None.

Related topics

- Alert concepts and procedures
- RVA/SVA: Responding to DDSR alerts (more detailed procedures for responding to this alert)
- RVA/SVA: Exploring DDSR (starting, stopping, suspending, and resuming DDSR processes)
- Storage Agent for RVA/SVA overview

RVA/SVA: Responding to Interval DDSR with Excessive Interval

When responding to this alert, use the Storage Agent for RVA/SVA. Right-click the affected host, and then select **Storage Agent for RVA/SVA**, **Explore**.

Alert Name	Problem	Immediate Response	Long Term Prevention
Interval DDSR with Excessive Interval alert	An interval DDSR process may wait too long before checking for deletions on the host. This can impact the subsystem by causing undesirable spikes in space release activity. Also, Net Capacity Load may decrease to unacceptable levels between interval DDSR processing.	For the affected subsystem, explore **Net Capacity Load** to ensure sufficient space remains. Explore the affected DDSR process and edit it to shorten its interval. Intervals are specified in minutes.	Ideal interval length depends on volume activity levels. Volumes with little deletion activity (such as an archive) can have DDSR intervals as long as many days. Volumes with frequent deletion activity (such as TSO data sets) may require intervals as short as 15 minutes.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Responding to MVS Device Disabled

When responding to this alert, use the Storage Agent for RVA/SVA. Right-click the affected host, and then select **Storage Agent for RVA/SVA**, **Explore**.

Alert Name	Problem	Immediate Response	Long Term Prevention
MVS Device Disabled alert	An MVS device is disabled. The device is unavailable to any MVS host. The Intentional disabling through the Storage Agent for RVA/SVA or through IXFP.	Verify whether the device is supposed to be offline. Before restarting the device, ensure that it is offline to all other hosts. Explore **MVS Devices** and locate the device. The status will probably be **Offline Disabled**. Right-click the device and click **Modify**. For **Enabled** field, select **Yes**, then click **OK**.	To prevent inadvertent or unauthorized changes in status, use ControlCenter and RACF security to restrict access to this command.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Responding to NCL Threshold

When responding to this alert, use the Storage Agent for RVA/SVA. Right-click the affected host, and then select **Storage Agent for RVA/SVA**, **Explore**.

Alert Name	Problem	Immediate Response	Long Term Prevention
NCL Threshold alert	The Net Capacity Load of an RVA or SVA subsystem exceeded a threshold. The subsystem may be running out of configured physical disk space.	Explore MVS logical volumes on the subsystem. Add capacity to the subsystem. Move some MVS volumes off the subsystem. See if DDSR is running on the connected hosts. Start both interval and dynamic DDSR processes.	Run the NCL Trend report. More long term prevention.

Related topics

- Alert concepts and procedures
- RVA/SVA: Responding to Net Capacity Load alerts
- Storage Agent for RVA/SVA overview

RVA/SVA: Responding to NCL Change Over Time

When responding to this alert, use the Storage Agent for RVA/SVA. Right-click the affected host, and then select **Storage Agent for RVA/SVA**, **Explore**.

Alert Name	Problem	Immediate Response	Long Term Prevention
NCL Change Over Time alert	The Net Capacity Load of an RVA or SVA subsystem has increased by an excessive percentage since the last time the alert checked it. Configured disk space is being consumed too quickly or not recovered after deletions.	Explore MVS logical volumes on the subsystem. Move some MVS volumes to another disk subsystem. Check to see if DDSR (space release) is running for hosts connected to the subsystem. Start both interval and dynamic DDSR processes.	Run the NCL Trend report. More long term prevention for NCL alerts.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

RVA/SVA: Responding to Net Capacity Load alerts

If the Net Capacity Load (NCL) threshold alert or change over time alert is critical, the affected RVA or SVA subsystem could become full at any time. In this situation, application continuity and data availability are both at serious risk.

Responding to an immediate need, including Warning, Critical, or Fatal alerts

- Explore MVS logical volumes on the subsystem. Move some MVS volumes to another disk subsystem.
- Check to see if DDSR (space release) is running for hosts connected to the subsystem. Start both interval and dynamic DDSR processes.

Add capacity to the subsystem

To add capacity to the RVA or SVA subsystem:

1. Locate spares.
2. Form an array.
3. Create MVS devices.
4. Vary MVS devices online.

Move data off the subsystem

1. Explore hosts connected to the RVA/SVA subsystem.
2. For a given host, explore MVS devices on the subsystem.
3. Identify volumes to remove from the subsystem to other disk subsystems.
4. Move the volumes.

Start space release if it has been stopped

1. Explore hosts connected to the RVA/SVA subsystem with high NCL.
2. Explore Deleted Data Space Release.
3. Determine if any DDSR processes are running. If no DDSR processes are listed, or if all the listed DDSR processes are suspended, then start DDSR processes as follows:
4. Start an interval DDSR process on one host (assuming a shared DASD environment). For the Defer field, select No. This step initiates space release built up while no DDSR process was running.
5. Start the dynamic DDSR process on all hosts connected to the subsystem. This step takes care of space release for new deletions on each host.

Investigating sources of NCL growth

Run the NCL Trend report. You can get hourly, daily, weekly, and monthly trend data showing the fluctuations in Net Capacity Load.

Using the report, correlate trend data with the following types of events:

- A new application brought online
- MVS devices drained and returned to the Media Acceptance Partition
- Triggered alerts, including
  - DDSR Not Active
  - DDSR Not Active for a Volume
  - Uncollected Free Space

Implementing long-term prevention approaches

Consider the following measures to help prevent Net Capacity Load from rising too high:

- Identify physical disks in the spares partition and bring them into test or production use.
- Troubleshoot compression problems.
- Ensure that applications or hosts are not compressing data before sending it to the RVA or SVA subsystem. Subsystem compression is more efficient when hosts do not compress data first.
- Consider whether an application's data format may be compressing less efficiently than expected when it reaches the RVA or SVA. This can be difficult to test experimentally in the subsystem. Consider contacting IBM or StorageTek technical support for advice on compression.
- Optimize DDSR monitoring and space collection. Tune interval length and ensure that active DDSR processes are covering all hosts and volumes.
- Set the DDSR Not Active and DDSR Not Active for a Volume alerts. These will inform you when DDSR is not running in the future.

Related topics

- NCL Threshold alert
- NCL Change Over Time alert
- Storage Agent for RVA/SVA overview

RVA/SVA: Responding to Uncollected Free Space

When responding to this alert, use the Storage Agent for RVA/SVA. Right-click the affected host, and then select **Storage Agent for RVA/SVA**, **Explore**.

A high percentage of uncollected free space means the subsystem could start dedicating resources to space collection instead of I/O. Performance problems can result.

In response to the alert:

- Suspend DDSR to prevent further space release requests from being sent to the subsystem.
- Check DDSR processes to configure them more effectively.
- Resume the DDSR processes when performance is no longer critical.

Suspend DDSR

If short-term performance is the most serious concern, then suspend one or more DDSR processes temporarily to relieve the subsystem of new collection activity. To keep collection activity from increasing and possibly harming performance:

- Suspend DDSR processes, or edit them to use a longer interval.
- Check Collected Free Space, which should remain large enough for applications to have sufficient storage even though space is not being collected.

If available space is more important than performance, you may choose to accept degraded performance to allow space collection to continue. Alternatively, add more physical disks if spares are available. If you consider moving volumes to a different subsystem, take into account that this only increases the space the RVA or SVA has to collect.

Even after you suspend DDSR, the subsystem continues to collect free space from previous deletions. If applications are writing new data, Net Capacity Load may increase and collected free space may decrease.

Reduce unnecessary space collection

For certain applications, dynamic DDSR and short-interval DDSR can cause unnecessary space collection. Switch to a longer-interval DDSR process for the volumes used by such applications.

Do not use dynamic DDSR for applications that frequently create and delete data sets. A certain application may write and delete the same data set name numerous times. Dynamic DDSR instructs the subsystem to collect the free space for every single repeated deletion at the time it occurs. This is unnecessary because the application is only going to create the same data set again soon anyway. A similar problem occurs when a DDSR interval is too short.

You can reduce unnecessary space collection by monitoring the application's volumes with interval DDSR instead of dynamic DDSR, and with a longer interval as opposed to a shorter one. Interval DDSR ignores repetitious creations and deletions--it only checks to see whether a data set is deleted at the end of the interval, then informs the subsystem at that time.

To reduce unnecessary space collection:

1. Edit the dynamic DDSR process.
2. Change the volume specification to exclude the volumes that have frequent creations and deletions for the same data set names.
3. Start or edit an interval DDSR process.
4. Include the volumes you removed from the dynamic process.

Reduce spikes caused by converging DDSR intervals

Check interval DDSR processes to make sure they are not sending deletions to the subsystem all at the same time. One potential strategy:

1. Edit or create multiple interval DDSR processes to use the same interval (for example, every 30 minutes).
2. Start the DDSR processes five minutes apart from one another.

Resume DDSR at an advantageous time

Resume DDSR processes before the subsystem begins to have space problems (high NCL and low collected free space). To avoid a spike in the uncollected free space, stagger the DDSR processes when you resume them.

Related topics

- Uncollected Free Space Threshold alert
- Storage Agent for RVA/SVA overview

RVA/SVA: Responding to Agent Initiated Vary of MVS Device

When responding to this alert, use the Storage Agent for RVA/SVA. Right-click the affected host, and then select **Storage Agent for RVA/SVA**, **Explore**.

Alert Name	Problem	Immediate Response	Long Term Prevention
Agent Initiated Vary of MVS Devices alert	An ControlCenter user has varied an MVS device on- or offlline on an RVA or SVA subsystem.	Explore MVS Devices to ensure that the affected device is in the proper state. Right-click to vary it on- or offline as needed.	If you want to prevent this change in the future, use RACF and ControlCenter security to restrict user privileges.

Related topics

- Alert concepts and procedures
- Storage Agent for RVA/SVA overview

Storage Agent for Symmetrix

Responding to general Symmetrix alerts

The following alerts can be configured for the general performance of a Symmetrix system. If the I/O for a particular Symmetrix unit becomes excessive, you may need to direct activity to other Symmetrix units. Services and applications run more slowly if they must wait for the disk subsystem to respond to their read and write requests.

Alert Name	Immediate response	Long-term prevention
Reads per second	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.
Writes per second		
I/O per second		
Kbytes read per second		
Kbytes written per second		
Total Hit Ratio %		
% Write Ratio		
Throughput		

Note: The Symmetrix general alerts are not enabled by default when you install the Symmetrix Agent. If you want to receive one of these alerts, you should ensure that the alert settings are appropriate for your environment. Create a baseline of statistics for Symmetrix performance, and adjust the alert settings for acceptable performance levels.

Related topics

- Introduction to alerts
- Alert concepts and procedures
- Viewing real-time performance statistics
- Responding to Symmetrix device alerts
- Responding to Symmetrix director alerts
- Responding to Symmetrix disk alerts
- Responding to Symmetrix alarm alerts
- Responding to Symmetrix port alerts
- Symmetrix device alerts
- Symmetrix director alerts
- Symmetrix disk alerts
- Symmetrix alarm alerts
- Symmetrix general alerts
- Symmetrix port alerts

Responding to Symmetrix alarm alerts

The following alerts are configured by default. Note that most of them are automatic Dial Home Calls to the EMC Customer Support Center with no user action required.

Alert Name	Immediate response	Long-term prevention
12 Volts On (Not Normal Mode)	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
AC Line Problems Detected Alert	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
Alarm Signal Set, But No Alarm Found	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
All SRDF Links Not Operational Alert	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
Base Only Access Alert	Contact EMC Customer Support Center.	
Comm Board SW Data Does Not Match Expected Data	Comm board SW data does not match expected data. This is an environmental error for Symmetrix 5 only. Contact EMC Customer Support Center.	
Device Resynchronization Process Has Started	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
Director A Fault Alert	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
Director B Fault Alert	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
Director Status Alert	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
Disk Adapter Dual Initiator Failed to Impl Monitor	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
Environmental Alarm Alert	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
Environment Sense Cable is Missing	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
Fibre Low Light Level Alert	Fibre Channel Optical module problem adapter reported error. Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
High Charge State Missing	Symmetrix battery is not fully charged. Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
Hot Spare Device Invoked Alert	Hot spare was invoked. No action required.	
Latched Alarms Discovered for Power System	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
M1 Resynchronized with M2 Alert	M1 resynchronization with M2 has completed successfully. No action required.	
M2 Resynchronized with M1 Alert	M2 resynchronization with M1 has completed successfully. No action required.	
Memory Banks Automatically Disabled	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
Migration Completed	Status report. No action required.	
No Access Alert	Agent cannot communicate with the Symmetrix. Access failure. Contact EMC Customer Support Center.	
No PC Connection Time Found in Table	Microcode error: No PC connection time found in PC table. Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
No statistics for remote Symmetrix	Unable to retrieve statistics from the remote Symmetrix. Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.	
Old Board Information Does Not Match Current Read	Contact EMC Customer Support Center.	

PC Communications Error Alert	The Service Processor could not complete a call for service. Contact EMC Customer Support Center.
PC Successfully Called Home	The PC successfully called home to report an error. No action required.
Power-on Time For Env Inconsistency During Env Tests	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
Power Subsystem Error	Alarm signals set - power subsystem error. Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
RAID Device Not Ready Alert	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
RAID Device Write Disabled Alert	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
Report 'Disabled Memory Bank' to Host	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
Service Processor Down Alert	The Service Processor is not communicating with the Symmetrix, forcing a reboot of the Service Processor. Contact EMC Customer Support Center.
SRDF Error	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
SRDF Hot Spare Device Invoked	A Hot Spare was automatically invoked by Enginuity for an SRDF R2 device on another box. No action required.
SRDF Initiated SIM Message	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
SRDF Link Error Alert	A single SRDF link in an SRDF group is not operational. Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
SRDF Link Operational	A single SRDF link in an SRDF group is now operational after a previous error. No action required.
SRDF Links All Operational	All SRDF links are operational now (after a previous failure). No action required.
SRDF M2 Device Not Ready	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
SRDF Operations Suspended for Some Devices	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
SRDF Symmetrix Diagnostic Event Trace Trigger	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
Symmetrix Diagnostic Event Trace Trigger	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
Temperature Alert	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
Thermal Detector Test Failure	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
Thermal Event	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
Too Many Suspend/Halt Chains Switching to Adaptive Copywrite Pending	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
Validity Problem With Bits Collected in Environment	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.
Volume Not Ready Alert	Unless manually overridden, this is an automatic Dial Home Call to the EMC Customer Support Center. No user action required.

Note: The Symmetrix alarm alerts are enabled by default when you install the Symmetrix Agent.

Related topics

- Introduction to alerts
- Alert concepts and procedures
- Viewing real-time performance statistics
- Responding to Symmetrix device alerts
- Responding to Symmetrix director alerts
- Responding to Symmetrix disk alerts
- Responding to Symmetrix general alerts
- Responding to Symmetrix port alerts
- Symmetrix device alerts
- Symmetrix director alerts
- Symmetrix disk alerts
- Symmetrix alarm alerts
- Symmetrix general alerts
- Symmetrix port alerts

Responding to Symmetrix director alerts

The following alerts can be configured for a Symmetrix back end disk director.

Alert Name	Immediate response	Long-term prevention
% Hit Ratio	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.
% Write Ratio		
I/O per second		

The following alerts can be configured for a Symmetrix front end Fibre Channel host director.

Alert Name	Immediate response	Long-term prevention
% Hit Ratio	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.
% Write Ratio		
I/O per second		

The following alerts can be configured for a Symmetrix front end SCSI host director.

Alert Name	Immediate response	Long-term prevention
% Hit Ratio	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.
% Write Ratio		
I/O per second		

Note: The Symmetrix director alerts are not enabled by default when you install the Symmetrix Agent. If you want to receive one of these alerts, you should ensure that the alert settings are appropriate for your environment. Create a baseline of statistics for director performance, and adjust the alert settings for acceptable performance levels.

Related topics

- Introduction to alerts
- Alert concepts and procedures
- Viewing real-time performance statistics
- Responding to Symmetrix device alerts
- Responding to Symmetrix disk alerts
- Responding to Symmetrix alarm alerts
- Responding to Symmetrix general alerts
- Responding to Symmetrix port alerts
- Symmetrix device alerts
- Symmetrix director alerts
- Symmetrix disk alerts
- Symmetrix alarm alerts
- Symmetrix general alerts
- Symmetrix port alerts

Responding to Symmetrix disk alerts

The following alerts can be configured for a Symmetrix disk. If the I/O for a particular disk becomes excessive, you may need to direct activity to other disks. Services and applications run more slowly if they must wait for the disk subsystem to respond to their read and write requests.

Alert Name	Immediate response	Long-term prevention
Reads per second	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.
Writes per second		
Kbytes read per second		
Kbytes written per second		

Note: The Symmetrix disk alerts are not enabled by default when you install the Symmetrix Agent. When you first receive one of these alerts, you should ensure that the alert settings are appropriate for your environment. Create a baseline of statistics for disk performance, and adjust the alert settings for acceptable performance levels.

Related topics

- Introduction to alerts
- Alert concepts and procedures
- Viewing real-time performance statistics
- Responding to Symmetrix device alerts
- Responding to Symmetrix director alerts
- Responding to Symmetrix alarm alerts
- Responding to Symmetrix general alerts
- Responding to Symmetrix port alerts
- Symmetrix device alerts
- Symmetrix director alerts
- Symmetrix disk alerts
- Symmetrix alarm alerts
- Symmetrix general alerts
- Symmetrix port alerts

Responding to Symmetrix device alerts

The following alerts can be configured for a Symmetrix device. If the I/O for a particular device becomes excessive, you may need to direct activity to other devices. Services and applications run more slowly if they must wait for the disk subsystem to respond to their read and write requests.

Alert Name	Immediate response	Long-term prevention
Reads per second	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.
Writes per second		
I/O per second		
Hits per second		
Kbytes read per second		
Kbytes written per second		

Note: The Symmetrix device alerts are not enabled by default when you install the Symmetrix Agent. If you want to receive one of these alerts, you should ensure that the alert settings are appropriate for your environment. Create a baseline of statistics for device performance, and adjust the alert settings for acceptable performance levels.

Related topics

- Introduction to alerts
- Alert concepts and procedures
- Viewing real-time performance statistics
- Responding to Symmetrix director alerts
- Responding to Symmetrix disk alerts
- Responding to Symmetrix alarm alerts
- Responding to Symmetrix general alerts
- Responding to Symmetrix port alerts
- Symmetrix device alerts
- Symmetrix director alerts
- Symmetrix disk alerts
- Symmetrix alarm alerts
- Symmetrix general alerts
- Symmetrix port alerts

Responding to Symmetrix front end port alerts

The following alerts can be configured for a Symmetrix front end port. If the I/O for a particular port becomes excessive, you may need to direct activity to other ports. Services and applications run more slowly if they must wait for the disk subsystem to respond to their read and write requests.

The Symmetrix agent can generate the following alerts to monitor statistics associated with Symmetrix SCSI front end ports.

Alert Name	Immediate response	Long-term prevention
Port Throughput Port I/O per second	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.

The Symmetrix agent can generate the following alerts to monitor statistics associated with Symmetrix Fibre Channel front end ports.

Alert Name	Immediate response	Long-term prevention
Port Throughput Port I/O per second	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.	This is a statistical message, triggered by a user-specified threshold. Refer to Storage Agent for Symmetrix Agent: Performance statistics for more information on controlling these alerts.

Note: The Symmetrix port alerts are not enabled by default when you install the Symmetrix Agent. If you want to receive one of these alerts, you should ensure that the alert settings are appropriate for your environment. Create a baseline of statistics for port performance, and adjust the alert settings for acceptable performance levels.

Related topics

- Introduction to alerts
- Alert concepts and procedures
- Viewing real-time performance statistics
- Responding to Symmetrix device alerts
- Responding to Symmetrix director alerts
- Responding to Symmetrix disk alerts
- Responding to Symmetrix alarm alerts
- Responding to Symmetrix general alerts
- Symmetrix device alerts
- Symmetrix director alerts
- Symmetrix disk alerts
- Symmetrix alarm alerts
- Symmetrix general alerts
- Symmetrix port alerts

Tape Agent for MVS

STK Tape: Responding to ACS and LSM availability alerts

ACS_Disconnected alerts and LSM_Offline alerts may or may not indicate a problem. An ACS or LSM may be unavailable for known maintenance attention, in which case no response is necessary. If this is not the case, then use the following information to find the problem.

ACS_Disconnected alert

ACSs are connected to an MVS host via a 3270 terminal-type connection. A coaxial cable connects the ACS's Library Management Unit (LMU) to a 3174 or similar controller, which is connected to a channel to the MVS host.

Connection can be lost for many reasons, including

- The LMU is varied offline to HSC
- The LMU is varied offline to MVS
- The LMU is powered off or not functioning properly
- The controller is varied offline or powered off
- All cable connections are physically broken

Regarding cable connections: If there are multiple redundant connections from a host to an ACS, the ACS_Disconnected alert triggers only if all these connections are lost.

Check these potential problems to see why the ACS is disconnected.

LSM_Offline alert

Determine why the LSM is offline. You may need to go to the library console to bring it back online.

Related topics

- Monitoring ACS and LSM availability
- ACS_Disconnected alert
- LSM_Offline alert

STK Tape: Responding to cleaning cartridge alerts

Use these tips and guidelines to respond to the alert.

Alert	Problem	Immediate response
Cleaners Select_Count alert	The average use levels of cleaning cartridges is high. The cleaning cartridges in the library (of a given media type) may be reaching the end of their useful life.	Check the media type monitored by the alert and add cleaning cartridges of the appropriate type.

Related topics

- Monitoring silos for an aging supply of cleaning cartridges
- Understanding select count for cleaning cartridge alerts and reports
- Searching for volumes by volser, media type, and scratch status
- Filtering status, reports, or alerts by media type

STK Tape: Responding to drive mount alerts

Use the following table to respond to situations when drive mounts require manual intervention or mechanical pass-through to place a volume where it is needed.

Alert	Problem	Immediate response	Long-term prevention
Drives_Mount_Eject	A volume in a library is needed in a non-library drive.	Eject the volume from the library and mount it in the non-library drive.	Ask the user to check the JCL. Check the media type of the volume and the drives. Ensure the volume is in a silo with a compatible drive type. Consider adding drives of the given type in the library.
Drives_Mount_Enter	The library needs a volume that is not located inside it.	Enter the needed volume into the library.	Ask the user of the volume how frequently it is needed. Consider entering it permanently in the library.
Drives_Mount_Eject_Enter	A volume in one library is needed in another.	Eject the needed volume from one library and enter it into the library that needs it.	Ask the user to check the JCL. Check the media type of the volume and the drives. Ensure the volume is in a silo with a compatible drive type.
Drives_Mount_Manual_Scratch	A non-library drive needs a scratch volume.	Mount a scratch volume manually in the non-library drive.	Enter scratch volumes of the given media type in the library. Set an alert to monitor scratch volume counts for that media type.
Drives Mount Pass Thru	A volume requires a mechanical pass-through from one LSM to another in the same ACS.	Record the affected volume and LSM names.	If a pattern develops, consider moving the volume to the LSM that requests it most frequently.
Drives Mount Pass Thru Count	Mount requests for an MVS system required an excessive number of pass-throughs since the last time the alert processed.	To determine the period of time elapsed, edit the alert and check the schedule, or see the alert description for the default schedule.	Use the related Drives Mount Pass Thru alert to track the actual volumes and LSMs that are causing pass-throughs. Move volumes to the LSMs that request them most frequently. Also, drive configuration may cause excessive pass-throughs and other problems.

Related topics

- Ejecting a volume
- Exploring drives
- Searching for volumes by volser, media type, and scratch status
- Monitoring mistargeted or inefficient mount requests
- Monitoring drives for excessive operator intervention

STK Tape: Responding to free cell alerts

Use these tips and guidelines to respond to the Cells Free_Percentage alert.

Alert	Problem	Immediate response	Long-term prevention
Cells Free_Percentage alert	The percentage of free cells is too low in an ACS or LSM.	Eject the volume from the library and mount it in the non-library drive. Remove inactive volumes.	Ask the user to check the JCL. Check the media type of the volume and the drives. Ensure the volume is in a silo with a compatible drive type. Consider adding drives of the given type in the library. Run a free cells historical report for information about the buildup of the problem. Cells historical report

Related topics

- Listing and removing inactive volumes from silos
- Monitoring silos for low number of free cells

STK Tape: Responding to inactive volume alerts

The Volumes Inactive_Count alert informs you of the number of inactive volumes in the library. Use the following guidelines to respond to the alert.

Alert	Problem	Immediate response
Volumes Inactive_Count alert	The number of inactive volumes is high.	Identify the exact volumes that are inactive and then eject them.

Related topics

- Managing volumes in a StorageTek tape library
- Listing and removing inactive volumes from silos
- Monitoring silos for high numbers of inactive volumes

STK Tape: Responding to LMU error alerts

Use the following guidelines to respond to the alert.

Alert	Problem	Immediate response
LMU Error alert	An LMU error occurred.	View the data provided by the alert, then consult StorageTek documentation for a resolution.

When the LMU_Error alert triggers, it provides the following information:

- The LMU error number that occurred.
- The ACS.
- A one- or two-letter code given when HSC message SLS0698I issued. Consult StorageTek documentation for the meaning of the code.
- An error code given when HSC message SLS699I issued. The format of the code is *nn/mm*. Consult StorageTek documentation.

The alert only triggers if a retry failed. For help in diagnosing the reason for an LMU error alert, view details in the MVS syslog or HSC job log.

Related topics

- Monitoring Library Management Unit errors

STK Tape: Responding to scratch count alerts

Use these tips and guidelines to respond to the alert.

Alert	Problem	Immediate response
Scratch_counts alert	The number of scratch volumes in the library is low. This may be total scratch volumes, or for specific media types, or for a specific subpool, depending on how the alert is configured.	Add scratch volumes to the library. If the alert specifies a media type or subpool, add the scratch volumes of the necessary type to the necessary subpool.

Related topics

- Filtering status, reports, or alerts by media type
- Monitoring silos for low numbers of scratch volumes

STK Tape: Responding to StorageTek Host Software alerts

Use the following guidelines to respond to the alert.

Alert	Problem	Immediate response
HSC Inactive alert	The Host Software Component is not running properly on one of the MVS hosts. For the given MVS host, the service level should be FULL but it is not.	Unless maintenance is underway, restore the HSC to full operating condition as soon as possible. HSC is necessary for all I/O activity to the StorageTek tape libraries from the host. Consider running important jobs from a different host if possible.

Related topics

- Monitoring host software (HSC) for StorageTek libraries

Responding to WLA Archiver alerts

This topic describes how to respond to the following alerts:

- Disk Space Status
- Archive Errors
- Archive Process Status

These alerts are set for the WLA Archiver. Respond in the following manner:

Alert	Problem	Immediate Response	Long-term Prevention
Disk Space Status	There is less than 1 MB of disk space left on the host running WLA Archiver.	Clear some data from the disk*.	• Add more disk space to the host. • Move other applications off of the host. • Re-examine your WLA Archiver Retention polices to ensure that you are only saving data that you need.
Archive Errors	An error occurred while the WLA Archiver was generating a WLA collection.	Review the ENW_SST.log file located on the WLA Archiver host. This log file provides information about where the error may have occurred.	N/A
Archive Process Status	There is no problem. A WLA Daily, Revolving, or Analyst collection has been successfully generated.	N/A	N/A

*If you move any of the WLA data collections from the host you will not be able to access them automatically from WLA Performance View. You will have to point to the new location when performing WLA Performance View data selection.

Related Topics

- Alert concepts and procedures
- WLA Archiver

Viewing alerts

Finding out about alerts that trigger outside your work hours

Often, alerts trigger when you are not in front of the Console. To receive notification of alerts through other means, configure ControlCenter to send:

- An e-mail to any valid e-mail address
- An SNMP trap to a management framework like HP OpenView Network Node Manager or Computer Associates Unicenter TNG, which can then send a page to you

For specific procedures, see Automatically notifying staff members by e-mail or page.

Use custom scripts

You can implement a more custom solution by creating an autofix that runs a script or batch file. For example, program automated responses for critical alerts or create a specialized notification script. For more information, see Creating an autofix.

Related topics

- Introduction to alerts
- Alert concepts and procedures

Viewing alert templates

You can view alert templates categorized by agent, host, or subsystem. Or, you can view all the alert templates at one time.

To view the alert templates:

1. In the selection tree, expand **Administration**, **Alert Management**, and **Alert Templates**. The alert templates are organized by agent or component.
2. Expand the tree to view the templates for the area of functionality you want to monitor. Beneath the agent name, the alert templates are grouped into categories.

To view the templates of one or more agents in a single view:

1. Click **Properties** on the toolbar.
2. In the selection tree, select the folders for the templates you want to view by placing checkmarks next to them in the tree. ControlCenter displays detailed information about the selected templates in the target panel. For descriptions of the column headings, see Alert Templates view.

Related topics

- Overview of viewing alerts
- Viewing all triggered alerts for a host or subsystem
- Viewing an overview of all triggered alerts
- Viewing triggered alerts
- Introduction to alerts
- Alert concepts and procedures

Viewing all alert definitions

You can view detailed information on all defined alerts, which include alerts you have defined and alerts that came pre-defined when you installed ControlCenter or one of its components.

To view the alert definitions:

1. On the toolbar, click **Properties**.
2. In the selection tree, expand **Administration** and **Alert Management**.
3. Double-click **Alerts**. Detailed information on all the defined alerts appears in the Alerts view. For descriptions of the column headings, see Alerts view.

Tips

- To view the defined alerts for a particular component only, double-click the folder for that component.
- To edit, copy, or delete an alert, right-click the alert and select the corresponding command.
- Click any column heading to sort the view by that column.
- Click and drag the column headings to rearrange the columns.

Related topics

- Overview of viewing alerts
- Viewing all triggered alerts for a host or subsystem
- Viewing an overview of all triggered alerts
- Viewing triggered alerts
- Introduction to alerts
- Alert concepts and procedures

Viewing triggered alerts

To view all triggered alerts, click **Alerts**in the upper-right corner of the Console window. For descriptions of the column headings, see Active Alerts view.

To view a series of bar charts showing the number and types of triggered alerts for each host or storage device, click **Chart** in the Active Alerts view title bar.

Filtering the active alerts

You can filter the Active Alerts view. For more information, see:

- Viewing all triggered alerts for a host or subsystem
- Viewing an overview of all triggered alerts

Responding to triggered alerts

To respond to the alerts in the Active Alerts view, right-click them and select from the commands provided. For more information, see:

- Reducing the number of alerts that display
- Removing unneeded alerts from your Console
- Resetting an alert whose condition has been resolved

Tip

- The online Help provides topics on responding to each alert. To see a topic, right-click the alert and select **View alert Help**.

Related topics

- Overview of viewing alerts
- Overview of responding to alerts
- Introduction to alerts
- Understanding alert terminology
- Alert concepts and procedures

Viewing all triggered alerts for a host or subsystem

To view all the active (triggered) alerts for a particular host or subsystem:

1. On the toolbar, click **Alerts**.
2. In the selection tree, select the host or subsystem by placing a checkmark next to it in the tree. All the active alerts and the alert definitions for the selected host or subsystem display in the target panel. For column heading descriptions, see the Active Alerts and Alert Definitions view descriptions.

Tips

- To add the alerts for another host or subsystem to the views, double-click that host or subsystem.
- To see an overview of the alerts for the host, click **Chart** in the view title bar.

Related topics

- Overview of viewing alerts
- Viewing triggered alerts
- Introduction to alerts
- Alert concepts and procedures

Viewing an overview of all triggered alerts

The Active Alerts view provides both table and graphical views of the active alerts. For a visual overview of the total number of alerts for all the systems ControlCenter is monitoring or for individual systems, use the Alert Chart view.

To view active alerts as a series of bar charts:

1. In the toolbar, click **Alerts**.
2. In the Alerts view title bar, click **Chart**.
3. In the selection tree, select the **Storage** and **Hosts** folders by placing a checkmark next to them in the tree. This selects all storage subsystems and hosts that ControlCenter is monitoring. A series of bar charts appears in the Active Alerts view.
4. Click the title of a bar chart to see only the alerts for that host or subsystem. Click the individual bars to see only the alerts of that severity for the selected subsystem or host.

Tip

- To reduce the number of charts, select individual hosts or subsystems in the selection tree.

Related topics

- Overview of viewing alerts
- Viewing triggered alerts
- Introduction to alerts
- Alert concepts and procedures

Reducing the number of alerts that display

If there are too many non-critical alerts in your Active Alerts view, do the following to reduce the number so you can focus on critical alerts.

Action	Description	Procedures
Disable all alerts, then enable only those critical to you.	Many alerts are enabled by default when you install ControlCenter components. Although we identified these alerts as important, they may not be significant in your environment or on every host. Or, the default settings may not be appropriate.	Disabling or enabling multiple alerts
Assign management policies.	If you do not assign a management policy to an alert, the alert displays for all users when it triggers. Use management policies to direct alerts to appropriate personnel. For example, assign all of the ECC Server alerts to the ControlCenter administrator. Many alerts are pre-configured when you install ControlCenter components. However, these alerts do not have management policies attached. Make sure you assign management policies to them.	Assigning a management policy to multiple alerts
Reset or remove active alerts.	After you address a triggered alert, you can remove it from the Active Alerts view by resetting it for all users or by removing it from your Console only.	Resetting an alert whose condition has been resolved Removing unneeded alert from your Console

Related topics

- Overview of viewing alerts
- Overview of responding to alerts
- Introduction to alerts
- Alert concepts and procedures

Working with autofixes

Attaching an autofix to an alert

To have an autofix run when an alert triggers, attach the autofix to the alert. The autofix runs when the alert first triggers and then each time the alert moves from one severity level to another.

To attach an autofix to an alert:

1. In the selection tree, expand **Administration**, **Alert Management**, and **Alerts**.
2. Expand the folder for the agent that contains the alert to which you want to attach the autofix.
3. Expand the sub-folders to locate the alert.
4. Right-click the alert and select **Edit Alert**.
5. Click **Actions**.
6. Select the autofix in **Available Autofixes**.
7. Click **Move**.
8. Click **Apply To**.
9. Verify that you want the autofix to run on all the selected hosts or subsystems. The script, executable, or batch file specified in the autofix must exist in the same place on all selected hosts or subsystems.

Tip

- If the autofix script exists in different directories on the hosts to which you want to apply the autofix, create separate alerts for each host.

Related topics

- Creating an autofix
- Autofix syntax
- Automatically responding to alerts with commands and scripts
- Introduction to alerts
- Alert concepts and procedures

Autofix syntax

For autofixes, ControlCenter sends to the host exactly what you enter in the **Command** field on the New Autofix or Edit Autofix dialog boxes. Therefore, the syntax for the autofix commands depends on what is required for the host to run your command.

Passing alert information to an autofix script

ControlCenter allows you to pass the following information with your autofix command:

- Alert name
- Alert severity level
- Value that caused the alert to trigger
- Specific resource for which the alert triggered (also called the alert source or key)

Use the following syntax to pass this information with your autofix command:

```
your_autofix_command &METRIC &LEVEL &KEY &VALUE
```

- &METRIC is the alert name.
- &LEVEL is the severity level of the alert, in string format: Fatal, Critical, Warning, Minor, and Information.
- &KEY is the alert key (or source). On UNIX and Windows, if the alert has more than one key, then append a number to &KEY for each key you want to pass, for example: &KEY1, &KEY2, and so on. On MVS and OS/390, ControlCenter passes the first key only.
- &VALUE is the value at which the alert triggered.

Platform-specific requirements and examples

Following are the requirements and examples for specifying autofixes for UNIX, Windows, MVS, and OS/390 hosts.

Platform	Requirements and examples

UNIX	• Specify the file path and the name of a shell command, shell script, or executable.
	• Ensure that files or programs referenced in a script are in the same directory as the script, or specify the complete path in the script.
	Examples
	`/admin/tools/backup/backup.sh &KEY &VALUE`
	`/utility/cleanup/fixit.pl`

Windows	• Specify the name of a command, script, batch file, or executable.
	• Include `cmd.exe /c` or `cmd /c` in front of the autofix string.
	• If the script, batch file, or executable is not included in the Windows path, then specify the full path in the autofix command.
	• Ensure that files or programs referenced in a script are in the same directory as the script, or specify the complete path in the script.
	Examples
	`cmd.exe /c C:\utilities\cleanup.bat &METRIC &LEVEL &KEY1 &KEY2 &VALUE`
	`cmd /c C:\backup\delete.wsh`
	`cmd /c cp &KEY1 C:\backup`

MVS, OS/390	• Specify the fully qualified dataset name of the REXX executable or CLIST.
	• Enclose the autofix within quotes. (ControlCenter submits autofixes as TSO commands.)
	• Place the alert value substitutions outside of the quotes.
	• Separate multiple commands with semi-colons.
	Examples
	`"system.utility.cleanup" &METRIC &VALUE &KEY`
	`"test.batch.restart(rexxfix)"`

Related topics

- Creating an autofix
- Attaching an autofix to an alert
- Automatically responding to alerts with commands and scripts
- Alert concepts and procedures

Creating an autofix

Through autofixes, ControlCenter allows you to specify commands or scripts that should run when an alert triggers. Autofixes consist of a unique name, a descriptive name, and the text of the command or script ControlCenter sends to the host when an alert triggers. ControlCenter provides some autofixes; you can also create autofixes from new or existing scripts, batch files, or executables.

To create an autofix:

1. In the selection tree, expand **Administration**, **Alert Management**, and **Autofixes**.
2. Right-click **User** and select **New Autofix**. The Create New Autofix dialog box appears.
3. Type a brief but unique name in **Internal Name**. This name cannot contain spaces.
4. Type a succinct description in **Display Name**. This field can contain spaces but should not be too long, as it displays in many tables throughout the interface.
5. In **Command**, type the syntax of the command or the name of a script or batch file. When an alert triggers, ControlCenter sends the text to the host exactly as the text appears in this field. You can also pass alert information to your autofix commands. See Autofix syntax for complete information.
6. Attach the autofix to the appropriate alerts when you create or edit alerts.

Notes

- ControlCenter executes an autofix any time an alert to which the autofix is attached triggers or moves from one severity to another, whether the alert increases or decreases in severity.
- Autofixes generally display alphabetically in the Console. Use a naming scheme, such as consistent prefixes, that will logically group the autofixes when they display alphabetically. This allows you to find specific autofixes more quickly.

Related topics

- Overview of creating alerts
- Overview of responding to alerts
- Automatically responding to alerts with commands and scripts
- Automatically notifying staff members by e-mail or page
- Introduction to alerts
- Alert concepts and procedures

Deleting an autofix

Autofixes provide automatic actions ControlCenter can take when an alert triggers. ControlCenter provides some autofixes; you can also create your own using existing or new scripts, batch commands, or executables.

To delete an autofix:

1. In the selection tree, expand **Administration**, **Alert Management**, **Autofixes**, and **User**.
2. Right-click the autofix and select **Delete Autofix**.

Notes

- Make sure you remove the deleted autofix from all of the alerts to which it is attached.
- You cannot delete the autofixes supplied by ControlCenter.

Related topics

- Automatically responding to alerts with commands and scripts
- Attaching an autofix to an alert
- Creating an autofix
- Editing an autofix
- Introduction to alerts
- Alerts concepts and procedures

Editing an autofix

Edit an autofix to change its unique internal name, descriptive name, or the syntax of the autofix command.

To edit an autofix:

1. In the selection tree, expand **Administration**, **Alert Management**, **Autofixes**, and **User**.
2. Right-click the autofix and select **Edit Autofix**. The Edit Autofix dialog box appears.
3. Type your changes to the internal name, display name, or autofix command.

Notes

- For more information on the syntax rules for autofixes, see Autofix syntax.
- An autofix might be attached to more than one alert. Make sure your edits are appropriate for all the alerts to which the autofix is attached.
- Autofixes generally display alphabetically in the Console. You may want to use a naming scheme, such as consistent prefixes, that logically groups the autofixes when they display alphabetically. This allows you to find specific autofixes more quickly.
- You cannot edit the autofixes supplied by ControlCenter.

Related topics

- Attaching an autofix to an alert
- Creating an autofix
- Deleting an autofix
- Automatically responding to alerts with commands and scripts
- Introduction to alerts
- Alerts concepts and procedures

System autofixes

ControlCenter provides several system autofixes that you can attach to alerts. You can attach system autofixes to specific alerts only.

- Logical Agent for MVS system autofixes
- Host Agent for SMS system autofixes
- Host Agent for Windows system autofixes

Logical Agent for MVS system autofixes

Autofix name	Description	Associated alerts
Notify the MVS operator of this event using a nonscrollable WTO	Issues a nonscrollable WTO message to the MVS console.	Any Logical Agent for MVS alert
Notify the MVS operator of this event using a WTO	Issues a nonscrollable WTO message to the MVS console.	Any Logical Agent for MVS alert

Host Agent for SMS system autofixes

Autofix name	Description	Associated alerts
Notify the MVS operator of this event using a nonscrollable WTO	Issues a nonscrollable WTO message to the MVS console.	Any Host Agent for SMS alert
Notify the MVS operator of this event using a WTO	Issues a nonscrollable WTO message to the MVS console.	Any Host Agent for SMS alert

Host Agent for Windows system autofixes

Autofix name	Description	Associated alerts
Execute Backup and Clear the Event Log	Backs up and clears a Windows event log when the log reaches a size threshold.	Event log size alerts
Execute Clear The Event Log	Clears a Windows event log when the log reaches a size threshold.	Event log size alerts
Execute Restart Service	Attempts to restart a Windows service when it fails.	Service Failure alert

Note

- You cannot edit the system autofixes.

Tip

- You can also create your own *user* autofixes using commands, scripts, and executables. You can attach user autofixes to any alert.

Related topics

- Automatically responding to alerts with commands and scripts
- Creating an autofix
- Attaching an autofix to an alert
- Autofix syntax
- Troubleshooting alerts and autofixes
- Introduction to alerts
- Alert concepts and procedures

Working with management policies

Assigning a management policy to multiple alerts

You can assign management policies to groups of alerts. For example, you might want to assign to the ECC Server alerts a management policy that sends them only to the ControlCenter administrator.

To assign a management policy to multiple alerts:

1. In the selection tree, expand **Administration** and **Alert Management**.
2. Right-click **Alert Templates** or **Alerts**, or any folder beneath them, and select **Assign Management Policy**. The Assign Management Policy dialog box appears.
3. Select a management policy from the list and click **OK**. ControlCenter applies the management policy to all the alerts in the selected folder and all sub-folders.

Notes

- To assign a management policy to an individual alert or alert template, right-click the alert and select **Edit Alert**. Select the management policy on the **Actions** tab.
- Be careful when assigning management policies to multiple alerts. You cannot undo the assignment of multiple policies. You must reassign the policies in groups or individually.

Related topics

- Creating a management policy
- Overview of responding to alerts
- Introduction to alerts
- Alerts concepts and procedures

Creating a management policy

Management policies identify what ControlCenter should do when an alert triggers. Possible actions include: displaying an alert in the Console of a specific ControlCenter user, sending an e-mail message, and sending a message to a management framework.

To create a management policy:

1. In the selection tree, expand **Administration** and **Alert Management**.
2. Right-click **Management Policies** and select **New Management Policy**. The New Management Policy dialog box appears.
3. In the **Name** box, type a descriptive name. Choose a name that gives some indication of the actions you want the management policy to perform.
4. To create the management policy, drag the icons from the palette on the left side of the dialog box to the work area on the right side of the dialog box.
   - To have the alert display in the Console of a specific ControlCenter user, drag **ECC User** and type the user's ControlCenter ID.
   - To notify a user through e-mail, drag **Email** and type the e-mail address in standard format (for example, doe_john@mycompany.com).
   - To notify a management framework such as the Tivoli Management Framework, drag **Notify SNMP**.
   - To repeat a step, drag **Begin Loop**, drag the icons for one or more steps, and then drag **End Loop**.
   - To have ControlCenter wait before performing a step, drag **Wait** and select a time period.

Notes

- Sending e-mails or SNMP messages requires additional configuration steps. The ControlCenter administrator typically performs these steps during installation of the ECC Server.
- To delete a management policy step, click it and then click **Remove**.
- ControlCenter executes the management policy steps in the order they appear in this dialog box, from top to bottom.
- ControlCenter executes the management policy steps each time an alert triggers, including when an alert moves from one severity to another (such as when an alert increases in severity from Warning to Critical, or decreases from Minor to Harmless).
- If ControlCenter evaluates an alert again before all the management policy steps have run and the conditions that caused the alert to trigger have been resolved, then ControlCenter does not complete the management policy steps. This could happen, for example, if ControlCenter evaluates the alert every 10 minutes according to the alert's schedule, and the management policy has a wait step greater than 10 minutes.

Tips

- Management policies generally display alphabetically in the Console. You may want to use a naming scheme, such as consistent prefixes, that logically groups the management policies when they display alphabetically. This allows you to find specific management policies more quickly.
- To further automate your responses to alerts, have ControlCenter run an autofix when an alert triggers.

Related topics

- Copying a management policy
- Editing a management policy
- Assigning a management policy to multiple alerts
- Introduction to alerts
- Alert concepts and procedures

Copying a management policy

Management policies identify what ControlCenter should do when an alert triggers. You can create new management policies by copying existing ones.

To create a management policy by copying an existing one:

1. In the selection tree, expand **Administration**, **Alert Management**, and **Management Policies**.
2. Locate the management policy you want to copy, right-click it, and select **Copy Management Policy**. The Copy Management Policy dialog box appears.
3. Change the name in the **Name** field. You cannot have duplicate management policy names. Choose a name that gives some indication of the actions you want the management policy to perform.
4. If desired, edit the management policy steps.
   - Edit the user IDs, e-mail addresses, and other notifications as appropriate.
   - To add a management policy step, drag an icon from the palette on the left to the work area on the right.
   - To delete a step, click it and then click **Remove**.
   - To rearrange the steps, drag them up or down in the work area.

Notes

- ControlCenter executes the management policy steps in the sequence they appear in this dialog box, from top to bottom.
- Sending SMTP or SNMP messages requires additional configuration steps. The ControlCenter administrator typically performs these steps during installation of the ECC Server.
- ControlCenter executes the management policy steps each time an alert triggers, including when an alert moves from one severity to another (such as when an alert increases in severity from Warning to Critical, or decreases from Minor to Harmless).
- If ControlCenter evaluates an alert again before all the management policy steps have run and the conditions that caused the alert to trigger have been resolved, then ControlCenter does not complete the management policy steps. This could happen, for example, if ControlCenter evaluates the alert every 10 minutes according to the alert's schedule, and the management policy has a wait step greater than 10 minutes.

Tips

- Management policies generally display alphabetically in the Console. You may want to use a naming scheme, such as consistent prefixes, that logically groups the management policies when they display alphabetically. This allows you to find specific management policies more quickly.
- To further automate your responses to alerts, have ControlCenter run an autofix when an alert triggers.

Related topics

- Automatically notifying staff members by e-mail or page
- Creating a management policy
- Editing a management policy
- Introduction to alerts
- Alert concepts and procedures

Deleting a management policy

Deleting a management policy completely removes it from ControlCenter. The management policy is no longer available to any ControlCenter users.

To delete a management policy:

1. In the selection tree, expand **Administration**, **Alert Management**, and **Management Policies**.
2. Locate the management policy you want to edit, right-click it, and click **Delete Management Policy**. ControlCenter removes the management policy from any alerts to which it is attached.

Notes

- If there is no management policy attached to an alert, the alert appears in the Consoles of all ControlCenter users.
- A management policy might be attached to more than one alert. Before you delete a management policy, ensure that you want to remove the management policy from all the alerts.

Related topics

- Creating a management policy
- Editing a management policy
- Copying a management policy
- Introduction to alerts
- Alerts concepts and procedures

Determining which alerts use a management policy

Before you edit or delete a management policy, determine which alerts use the management policy so you can assess the impact of your changes. If necessary, assign new management policies to the affected alerts. If you do not attach a management policy to an alert, the alert appears in the Consoles of all ControlCenter users.

To determine which alerts use a management policy:

1. Click **Properties** on the toolbar.
2. Select the **Alerts** folder in the selection tree by placing a checkmark next to it. The Properties - Alerts view appears in the target panel.
3. Sort the view by the **Management Policy** column. If desired, rearrange the columns so that the Management Policy column appears next to the Agent Name or Element columns. To rearrange the columns, click a column heading and drag it to the left or right.
4. Scroll to locate the alerts to which the management policy is attached.
5. If necessary, change the management policy for those alerts before editing or deleting the management policy. To do this quickly, you can assign management policies to groups of alerts.

Related topics

- Editing a management policy
- Deleting a management policy
- Editing an alert
- Assigning a management policy to multiple alerts
- Introduction to alerts
- Alert concepts and procedures

Editing a management policy

Management policies identify what ControlCenter should do when an alert triggers. Edit a management policy to change the notification actions ControlCenter performs when an alert triggers, for example, the ControlCenter users who receive an alert or the e-mail address to which ControlCenter sends an alert.

To edit a management policy:

1. In the selection tree, expand **Administration**, **Alert Management**, and **Management Policies**.
2. Locate the management policy you want to edit, right-click it, and select **Edit Management Policy**. The Edit Management Policy dialog box appears.
3. If desired, type a new name in the **Name** box. Choose a name that gives some indication of the actions you want the management policy to perform.
4. Edit the management policy.
    - To add a management policy step, drag an icon from the palette on the left to the work area on the right.
    - To delete a step, click it and then click **Remove**.
    - To rearrange the steps, drag them up or down in the work area.

Notes

- A management policy might be used by more than one alert. If you change a management policy, make sure your changes are appropriate for all the alerts to which the management policy is attached.
- ControlCenter executes the management policy steps in the sequence they appear in this dialog box, from top to bottom.
- ControlCenter executes the management policy steps each time an alert triggers, including when an alert moves from one severity to another (such as when an alert increases in severity from Warning to Critical, or decreases from Minor to Harmless).
- Sending e-mails or SNMP messages requires additional configuration steps. The ControlCenter administrator typically performs these steps during installation of the ECC Server.

Tips

- Management policies generally display alphabetically in the Console. You may want to use a naming scheme, such as consistent prefixes, that logically groups the management policies when they display alphabetically. This allows you to find specific management policies more quickly.
- To further automate your responses to alerts, have ControlCenter run an autofix when an alert triggers.

Related topics

- Determining which alerts use a management policy
- Creating a management policy
- Deleting a management policy
- Introduction to alerts
- Alert concepts and procedures

Automatically notifying staff members by e-mail or page

Often, alerts trigger when you are not at the ControlCenter Console. To ensure you receive notification of critical alerts in a timely manner, set up ControlCenter to send alert messages by e-mail or to a management framework like HP OpenView Network Node Manager or Computer Associates Unicenter TNG. The management framework can then page you with the alert text.

To set up ControlCenter to send e-mails or pages:

1. To send e-mails, the ControlCenter administrator must configure ControlCenter for SMTP notification during installation of the ECC Server.
2. To send a page, the ControlCenter administrator must configure ControlCenter to send SNMP traps to a management framework during installation of the ECC Server. The management framework then sends the page.
3. In the Management Policy Definition dialog box, drag the **Email** or **SNMP** icon into the management policy and then, for e-mails, specify the address.

Related topics

- Introduction to alerts
- Creating a management policy
- Assigning a management policy to multiple alerts
- Determining which alerts use a management policy
- Alerts concepts and procedures
- Working with schedules

Managing hosts, databases, and subsystems

Managing host storage

Adding and removing host storage

The ControlCenter host agents allow you to add and remove storage to help meet the demands of your environment. Consult the following table for procedures on adding and removing storage on Windows, UNIX, and MVS hosts.

File system tasks	**Procedures**
Creating file systems	UNIX host
Extending or shrinking a VERITAS file system	Solaris (VERITAS) host
Mounting or mapping file systems	Windows host UNIX host
Removing a file system	UNIX host
Unmounting or disconnecting file systems	Windows host UNIX host
Physical device tasks	**Procedures**
Adding physical volumes to volume groups	AIX or HP-UX host
Creating physical volumes	HP-UX host
Removing physical volumes	UNIX host
Logical volume tasks	**Procedures**
Adding volumes to a storage group	MVS, OS/390 host (SMS)
Creating or initializing volumes	UNIX host MVS, OS/390 host
Extending, shrinking, or draining volumes	UNIX host MVS, OS/390 host (SMS)
Removing volumes	UNIX host MVS, OS/390 host (SMS)
Volume group tasks	**Procedures**
Activating volume groups	AIX or HP-UX host
Creating volume groups	AIX or HP-UX host
Deactivating volume groups	AIX or HP-UX host
Extending or reducing volume groups	AIX or HP-UX host
Removing volume groups	AIX or HP-UX host
VERITAS-specific tasks	**Procedures**
Adding VM disks to disk groups	Solaris (VERITAS) host
Creating disk groups	Solaris (VERITAS) host
Removing disk groups	Solaris (VERITAS) host
Removing VM disks from Volume Manager control	Solaris (VERITAS) host
Removing VM disks from disk groups	Solaris (VERITAS) host

For more information about the capabilities of any host agent, see the overview topic for that agent:

- Host Agents for AIX, HP-UX, and Solaris overview
- Host Agent for Novell overview
- Host Agent for Windows overview
- Host Agent for HSM overview
- Host Agent for SMS overview
- Logical Agent for MVS overview
- Physical Agent for MVS overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Capacity planning for host systems

Capacity planning is the process of predicting and planning for the future workload of computer systems. The goal of capacity planning is to increase the capacity of a computing system before the workload causes system performance to suffer. At the same time, you must balance capacity increases with how quickly the capabilities and price of technology change. You do not want to buy too far ahead because the technology you buy today may cost half as much in six months.

The benefits of capacity planning are:

- Reduced downtime and costs
- Improved performance and productivity
- Greater customer satisfaction

The results of not planning usually include reduced system reliability, potentially expensive business system outages, and inefficient purchasing practices.

Capacity planning should be an ongoing and regularly scheduled activity. Although it is an inexact process, comparing estimates to actual demand will help you make more accurate predictions. Additionally, comparing capacity needs over time will reveal whether the performance and efficiency of your systems is improving.

Aspects of your systems to consider

You should consider the following aspects of your computing environment in capacity planning:

- Storagewill you have enough disk space to store and protect (through backups and redundancy) critical data as your business grows?
- Processing and application performancecan your CPUs and applications perform quickly enough to satisfy future business needs?
- Network bandwidthwill the capacity of your network handle predicted data and transaction growth?

The capacity planning process

Capacity planning generally includes the following tasks:

- Determine the extent and capabilities of your current environment
- Clean up your system
- Log data to create baselines
- Talk to business planners
- Evaluate future needs and plan six months ahead

Determine the extent and capabilities of your current environment

Accurate capacity planning requires a thorough understanding of your business systems. If you do not already have an inventory of your systems, you should create one. Perform the following tasks:

1. Determine how much storage you currently have and how it is being used.
2. Evaluate the performance of your network and CPUs.
3. Gain an understanding of how your CPUs and storage systems relate to your critical business applications.

The following table provides links to information on how ControlCenter can help you with these tasks.

Tasks	Topics
Use reports to create your inventory	Viewing asset management reports Viewing utilization and free space reports Viewing configuration reports Generating historical reports on UNIX hosts
Use topology maps to explore your storage network	Topology features Viewing your network topology
Monitor performance	Performance management features Analyzing performance with Workload Analyzer (WLA) Monitoring performance on Windows

Clean up your system

Before purchasing additional storage, ensure that the storage you have is being used efficiently. Identify legacy and log files that you can archive or delete. And remove files that should not be stored on company servers, such as users' personal multimedia files.

See Recovering disk space.

Log data to create baselines

To predict capacity needs, you need baseline statistics that will help you identify trends and growth rates. To create your baselines, you should log storage statistics and network and CPU performance data from all your critical systems. The level of activity for most business systems has peaks and valleys. Make sure you capture data during your systems' daily, weekly, monthly, and yearly peaks.

Tasks	Topics
Use reports to create baselines	Viewing asset management reports Viewing utilization and free space reports Viewing configuration reports
Create baselines on Windows hosts	Creating performance baselines

Talk to business planners

A key to successful capacity planning is being informed about new business activities and significant changes. Keep in close contact with business planners to ensure your systems can meet new demands. For example, if the Marketing department is planning a new advertising campaign, you will want know well ahead of time so that you can make sure the systems hosting your Internet applications and databases can handle the increased traffic.

Evaluate future needs and plan six months ahead

Make capacity planning a part of your routine by putting it on your schedule of regular activities. After creating your initial baselines, review your trending reports on a schedule that meets your business' needs, whether that is every month, quarter, or six months. Capacity planning experts generally recommend planning six months ahead. Purchasing capacity too far ahead is inefficient because of the rate at which technology and prices change.

For more information about the capabilities of any host agent, see the overview topic for that agent:

- Host Agents for AIX, HP-UX, and Solaris overview
- Host Agent for Novell overview
- Host Agent for Windows overview
- Host Agent for HSM overview
- Host Agent for SMS overview
- Logical Agent for MVS overview
- Physical Agent for MVS overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Controlling disk consumption on hosts

Controlling rapid consumption of storage resources is crucial to keeping data center costs in check and maintaining a stable environment. ControlCenter helps you control disk consumption by providing access to native tools on your Windows, UNIX, Novell, and MVS hosts, such as creating disk quotas. In addition, ControlCenter provides alerts for monitoring free space and features for identifying who is consuming storage resource, such as the DASD Space Summary and DASD Space Activity reports provided by the Logical Agent for MVS.

See the following for links to procedures for controlling disk consumption on Windows, UNIX, Novell, and MVS hosts:

- Using a host's native tools
- Monitoring disk consumption with alerts
- Discovering who is consuming storage space

Using a host's native tools

Tasks	Procedures
Using volume or disk quotas	Windows host UNIX host Novell host

Monitoring disk consumption with alerts

Tasks	Procedures
Monitoring logical volume or file system free space	Windows host UNIX host MVS, OS/390 host Novell host
Monitoring file and directory size	Windows host UNIX host MVS, OS/390 host Novell host

Discovering who is consuming storage space

Tasks	Procedures
Searching for large files	Windows host UNIX host Novell host
Identifying who owns files and directories	Windows host UNIX host Identifying users Identifying groups Novell host

For more information about the capabilities of any host agent, see the overview topic for that agent:

- Host Agents for AIX, HP-UX, and Solaris overview
- Host Agent for Novell overview
- Host Agent for Windows overview
- Host Agent for HSM overview
- Host Agent for SMS overview
- Logical Agent for MVS overview
- Physical Agent for MVS overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Ensuring space availability on hosts

ControlCenter provides numerous alerts to monitor space availability and data integrity, key tasks to ensuring a stable storage environment.

See the following table for links to useful alerts for monitoring space availability on Windows, UNIX, and MVS hosts.

Tasks	Procedures
Monitoring logical volume or file system free space	Windows host UNIX host MVS, OS/390 host MVS, OS/390 host (SMS)
Monitoring disk fragmentation	MVS, OS/390 host
Monitoring disk integrity	MVS, OS/390 host
Monitoring storage group occupancy	MVS, OS/390 host (SMS)

For more information about the capabilities of any host agent, see the overview topic for that agent:

- Host Agents for AIX, HP-UX, and Solaris overview
- Host Agent for Novell overview
- Host Agent for Windows overview
- Host Agent for HSM overview
- Host Agent for SMS overview
- Logical Agent for MVS overview
- Physical Agent for MVS overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Exploring host storage

Use ControlCenter to explore the logical and physical storage configurations of your hosts. In addition, ControlCenter agents allow you to directly manipulate many storage resources from the Console to reduce the complexity of managing a heterogeneous and geographically diverse storage environment.

See the following table for links for exploring the storage resources of your Windows, UNIX, Novell, and MVS hosts.

Tasks	Procedures
Exploring physical devices	Windows host UNIX host MVS, OS/390 host
Exploring logical volumes	Windows host UNIX host Novell host
Exploring file systems	UNIX host MVS, OS/390 host (OpenEdition)
Exploring files and directories	Windows host UNIX host Novell host MVS, OS/390 host

For more information about the capabilities of any host agent, see the overview topic for that agent:

- Host Agents for AIX, HP-UX, and Solaris overview
- Host Agent for Novell overview
- Host Agent for Windows overview
- Host Agent for HSM overview
- Host Agent for SMS overview
- Logical Agent for MVS overview
- Physical Agent for MVS overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing applications

Ensuring application availability, performance, and integrity is *the* critical function of IT organizations. ControlCenter provides numerous features to assist storage and system administrators in managing their organizations' critical applications.

- Logically grouping application elements in ControlCenter
- Ensuring the availability of storage resources
- Managing database storage
- Monitoring vital processes or tasks
- Managing application security
- Managing application files or data sets
- Capacity planning

Logically grouping application elements in ControlCenter

In ControlCenter, you can use object groups to logically group the objects (hosts, Symmetrix devices, and so on) that comprise an application. Grouping an application's objects not only allows you to visually organize the elements in the interface, but also enables you to centrally manage access to these objects by ControlCenter users.

See Managing ControlCenter object groups.

Ensuring the availability of storage resources

A crucial task for ensuring application availability is monitoring the storage resources an application uses. ControlCenter provides functions to monitor space availability and data integrity whether the application data resides on a host device or in a disk or tape subsystem.

See Ensuring space availability.

Managing database storage

Most application data is stored in databases. Therefore, ensuring space availability and the integrity of databases is critical to keeping an application online.

See Managing database storage, space use, and growth.

Monitoring vital processes or tasks

An important aspect of application management is keeping track of the various processes or tasksoften running on multiple platformsthat comprise an application. ControlCenter automates monitoring the status of these processes and tasks and can even automatically restart them when they fail.

Tasks	Procedures
Monitoring processes or tasks	Windows host UNIX host
Monitoring and automatically restarting services	Windows

Managing application security

Use ControlCenter to help automate security management tasks on your hosts.

See Monitoring host security.

Managing application files or data sets

Most applications are composed of numerous individual files on several different platforms. ControlCenter can help you automate the management of application files by monitoring their size and how they are accessed. Additionally, you can change the location and properties of files and directories.

Tasks	Procedures
Monitoring file sizes	Windows host UNIX host
Monitoring file access	Windows host
Managing files and directories	Windows host UNIX host

For more information about the capabilities of any host agent, see the overview topic for that agent:

- Host Agents for AIX, HP-UX, and Solaris overview
- Host Agent for Novell overview
- Host Agent for Windows overview
- Host Agent for HSM overview
- Host Agent for SMS overview
- Logical Agent for MVS overview
- Physical Agent for MVS overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Monitoring host security

ControlCenter provides features to help automate monitoring the security of your Windows hosts, such as monitoring the Windows security event log or monitoring who is accessing critical files.

In addition, from a single ControlCenter Console, you can manage the permissions of Windows and UNIX files and directories on hosts across your enterprise.

Tasks	Procedures
Monitoring host security	Windows host
Managing file and directory permissions	Windows host UNIX host
Managing ControlCenter security	All hosts

For more information about the capabilities of any host agent, see the overview topic for that agent:

- Host Agents for AIX, HP-UX, and Solaris overview
- Host Agent for Novell overview
- Host Agent for Windows overview
- Host Agent for HSM overview
- Host Agent for SMS overview
- Logical Agent for MVS overview
- Physical Agent for MVS overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Monitoring host performance

Use ControlCenter to monitor and improve the performance of your host storage resources.

See the following table for links to procedures for monitoring the performance of your UNIX and Windows hosts.

Tasks	Procedures
Monitoring disk performance	Windows host
Monitoring memory performance	Windows host UNIX host
Monitoring processor performance	Windows host

For more information about the capabilities of any host agent, see the overview topic for that agent:

- Host Agents for AIX, HP-UX, and Solaris overview
- Host Agent for Novell overview
- Host Agent for Windows overview
- Host Agent for HSM overview
- Host Agent for SMS overview
- Logical Agent for MVS overview
- Physical Agent for MVS overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Recovering disk space on hosts

The ControlCenter host agents provide a variety of functions for recovering inefficient disk space. On MVS hosts, you can use the DASD Space Utilization and DASD Space Activity reports to identify users or jobs that are:

- Using excessive space
- Consuming space at an excessive rate

The following table describes space recovery procedures for Windows, UNIX, and Novell hosts.

Tasks	Procedures
Compressing files, directories, or volumes	Windows host Files Directories UNIX host Novell host
Searching for large, obsolete, or log files	Windows host UNIX host Novell host
Deleting files	Windows host UNIX host Novell host
Removing deleted files	Windows host Novell host
Clearing log files	Windows host
Migrating files	Novell host

For more information about the capabilities of any host agent, see the overview topic for that agent:

- Host Agents for AIX, HP-UX, and Solaris overview
- Host Agent for Novell overview
- Host Agent for Windows overview
- Host Agent for HSM overview
- Host Agent for SMS overview
- Logical Agent for MVS overview
- Physical Agent for MVS overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing database storage

Collecting database statistics

You can use the database agents to collect statistics about the databases managed by ControlCenter.

The following table provides procedures for collecting DB2 database statistics.

Tasks	Procedures
Configuring data collection for DB2 alerts and reports	DB2
Configuring DB2 detector execution frequency	DB2
Learning how often DB2 detector statistics are collected	DB2
Configuring collection of DB2 summary data	DB2
Monitoring DB2 RUNSTATS execution	DB2

The Database Agent for Oracle also provides data collection policies for collecting performance statistics.

For more information on the capabilities of a database agent, see the overview topic for that agent:

- Database Agent for DB2 overview
- Database Agent for Oracle overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing database applications

You can use the database agents to manage databases from the application perspective.

The following table provides procedures for managing application database resources in DB2 and Oracle databases.

Tasks	Procedures
Exploring application resources: collections, DBRMs, databases, stogroups, and stored procedures	DB2

For more information on the capabilities of a database agent, see the overview topic for that agent:

- Database Agent for DB2 overview
- Database Agent for Oracle overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing database storage, space use, and growth

You can use the database agents to monitor database storage, space use, and growth in databases managed by ControlCenter.

The following table provides procedures for monitoring storage in DB2 and Oracle databases.

Tasks	Procedures
Ensuring sufficient space for database resources	DB2 Oracle
Monitoring utilization and trends	DB2
Monitoring for reorganization candidates	DB2
Exploring database subsystems	DB2

For more information on the capabilities of a database agent, see the overview topic for that agent:

- Database Agent for DB2 overview
- Database Agent for Oracle overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing database structure

You can use the database agents to explore and monitor the structure of databases managed by ControlCenter.
The following table provides procedures for managing database structure in DB2 and Oracle databases.

Tasks	Procedures
Exploring collections, databases, DBRMs, packages, and stored procedures	DB2
Viewing object definition language	DB2
Monitoring database integrity	DB2 Oracle

For more information on the capabilities of a database agent, see the overview topic for that agent:

- Database Agent for DB2 overview
- Database Agent for Oracle overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Running database utilities and reports

You can use the database agents to run utilities and reports for databases managed by ControlCenter.
The following table provides procedures for running utilities and reports in DB2 databases.

Tasks	Procedures
Running utilities	DB2
Running reports	DB2
Viewing a list of all reports	DB2

For more information on the capabilities of a database agent, see the overview topic for that agent:

- Database Agent for DB2 overview
- Database Agent for Oracle overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing disk subsystem storage

Exploring physical devices in disk subsystems

You can use the storage agents to explore the size, types, and status of physical devices in the storage arrays managed with ControlCenter.

The following table provides procedures for exploring physical devices in HDS/XP, EMC CLARiiON, Compaq StorageWorks, IBM RVA, and StorageTek SVA subsystems.

Tasks	Procedures
Exploring physical devices in the subsystem	HDS CLARiiON StorageWorks RVA/SVA

For procedures on exploring and configuring physical devices in a Symmetrix system, see:

- Configuration Manager: Overview
- Physical Display

For more information on any disk subsystem storage agent, see the overview topic for the agent:

- Storage Agent for Celerra overview
- Storage Agent for CLARiiON overview
- Storage Agent for Compaq StorageWorks overview
- Storage Agent for HDS/XP overview
- Storage Agent for IBM ESS overview
- Storage Agent for Symmetrix overview
- Storage Agent for RVA/SVA overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing data protection in disk subsystems

You can use the storage agents to help manage the data protection schemes in the disk subsystems managed by ControlCenter.

The following table provides procedures for managing data protection in HDS/XP and Compaq StorageWorks subsystems.

Tasks	Procedures
Exploring Business Continuance Volumes	HDS
Creating Business Continuance Volumes	HDS
Monitoring data protection	HDS
Monitoring for data protection errors	HDS
Monitoring backup (spare) devices	StorageWorks

For procedures on managing data protection in a Symmetrix system, see Data Protection: Overview.

For more information on any disk subsystem storage agent, see the overview topic for the agent:

- Storage Agent for Celerra overview
- Storage Agent for CLARiiON overview
- Storage Agent for Compaq StorageWorks overview
- Storage Agent for HDS/XP overview
- Storage Agent for IBM ESS overview
- Storage Agent for Symmetrix overview
- Storage Agent for RVA/SVA overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing host connections in disk subsystems

You can use the storage agents to explore and monitor the connections between your hosts and disk subsystems.

The following table provides procedures for managing connections in EMC CLARiiON, Compaq StorageWorks, IBM RVA, and StorageTek SVA subsystems.

Tasks	Procedures
Exploring active connections	StorageWorks RVA/SVA
Exploring port configurations	HDS StorageWorks
Exploring logical units	CLARiiON StorageWorks
Monitoring connections	RVA/SVA

For procedures on managing connections in a Symmetrix system, see:

- Configuration Manager: Overview
- Physical Display

For more information on any disk subsystem storage agent, see the overview topic for the agent:

- Storage Agent for Celerra overview
- Storage Agent for CLARiiON overview
- Storage Agent for Compaq StorageWorks overview
- Storage Agent for HDS/XP overview
- Storage Agent for IBM ESS overview
- Storage Agent for Symmetrix overview
- Storage Agent for RVA/SVA overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing host devices in disk subsystems

You can use the storage agents to explore and monitor the host devices defined in the disk subsystems managed by ControlCenter.

The following table provides procedures for managing host devices in HDS/XP, IBM ESS, IBM RVA, and StorageTek SVA subsystems.

Tasks	Procedures
Exploring host devices	HDS IBM ESS RVA/SVA
Creating host devices	RVA/SVA
Making host devices available for use	RVA/SVA

For procedures on managing host devices in a Symmetrix system, see:

- Configuration Manager: Overview
- Physical Display

For more information on any disk subsystem storage agent, see the overview topic for the agent:

- Storage Agent for Celerra overview
- Storage Agent for CLARiiON overview
- Storage Agent for Compaq StorageWorks overview
- Storage Agent for HDS/XP overview
- Storage Agent for IBM ESS overview
- Storage Agent for Symmetrix overview
- Storage Agent for RVA/SVA overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Monitoring disk subsystem configuration and status

You can use the storage agents to explore configuration and status information about the disk subsystems managed by ControlCenter.

The following table provides procedures for exploring configuration information for HDS/XP, EMC CLARiiON, Compaq StorageWorks, IBM ESS, IBM RVA, and StorageTek SVA subsystems.

Tasks	Procedures
Exploring configuration and status	CLARiiON HDS IBM ESS StorageWorks
Monitoring status	IBM ESS StorageWorks
Managing subsystem control devices	CLARiiON RVA/SVA

For procedures on exploring and monitoring the configuration and status of Symmetrix subsystems, see:

- Configuration Manager: Overview
- Visual Storage: Overview

For more information on any disk subsystem storage agent, see the overview topic for the agent:

- Storage Agent for Celerra overview
- Storage Agent for CLARiiON overview
- Storage Agent for Compaq StorageWorks overview
- Storage Agent for HDS/XP overview
- Storage Agent for IBM ESS overview
- Storage Agent for Symmetrix overview
- Storage Agent for RVA/SVA overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Monitoring disk subsystem performance

You can use the storage agents to help monitor the performance of disk subsystems managed by ControlCenter.

The following table provides procedures for monitoring the performance of EMC CLARiiON, IBM ESS, IBM RVA, and StorageTek SVA subsystems.

Tasks	Procedures
Exploring performance statistics	CLARiiON IBM ESS
Monitoring performance	IBM ESS RVA/SVA

For procedures on monitoring the performance of Symmetrix subsystems, see Performance Management: Overview.

For more information on any disk subsystem storage agent, see the overview topic for the agent:

- Storage Agent for Celerra overview
- Storage Agent for CLARiiON overview
- Storage Agent for Compaq StorageWorks overview
- Storage Agent for HDS/XP overview
- Storage Agent for IBM ESS overview
- Storage Agent for Symmetrix overview
- Storage Agent for RVA/SVA overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing RAID configurations in disk subsystems

You can use the storage agents to monitor and explore how the disks in a subsystem are configured for data protection, availability, and performance.

The following table provides procedures for exploring RAID configurations in HDS/XP, EMC CLARiiON, Compaq StorageWorks, IBM RVA, and StorageTek SVA subsystems.

Tasks	Procedures
Exploring RAID sets	HDS CLARiiON StorageWorks RVA/SVA
Monitoring RAID configurations	CLARiiON StorageWorks
Creating RAID configurations	RVA/SVA

For procedures on exploring, monitoring, and creating RAID configurations in a Symmetrix system, see:

- Data Protection: Overview
- Configuration Manager: Overview
- Topology

For more information on any disk subsystem storage agent, see the overview topic for the agent:

- Storage Agent for Celerra overview
- Storage Agent for CLARiiON overview
- Storage Agent for Compaq StorageWorks overview
- Storage Agent for HDS/XP overview
- Storage Agent for IBM ESS overview
- Storage Agent for Symmetrix overview
- Storage Agent for RVA/SVA overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Monitoring space availability in disk subsystems

You can use the storage agents to help monitor space availability in the disk subsystems managed by ControlCenter.

The following table provides procedures for monitoring space availability in EMC CLARiiON, Compaq StorageWorks, IBM RVA, and StorageTek SVA subsystems.

Tasks	Procedures
Monitoring for low space availability	CLARiiON
Identifying unused space	StorageWorks RVA/SVA
Recovering free space	RVA/SVA

For more information on any disk subsystem storage agent, see the overview topic for the agent:

- Storage Agent for Celerra overview
- Storage Agent for CLARiiON overview
- Storage Agent for Compaq StorageWorks overview
- Storage Agent for HDS/XP overview
- Storage Agent for IBM ESS overview
- Storage Agent for Symmetrix overview
- Storage Agent for RVA/SVA overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing tape subsystem storage

Managing tape data sets

ControlCenter's Tape Agent for MVS provides several functions to help control how tape subsystems manage data sets.

The following table provides procedures on managing data sets in RMM and CA-1 tape subsystems.

Tasks	Procedures
Exploring data sets in a subsystem	RMM CA-1
Adding data sets to subsystem control	RMM
Modifying data sets under subsystem control	RMM CA-1
Removing data sets from subsystem control	RMM

For more information on tape agent functionality for a specific subsystem, see Tape Agent for MVS overview.

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing tape subsystem control data

Ensuring the integrity of subsystem control data is a critical aspect of tape subsystem management. Tape subsystems use control data files to keep track of where files under their control are physically located. If a control data file becomes corrupted, you may lose the data sets under the tape subsystem's control. The Tape Agent for MVS can help the storage administrator automate this function by monitoring the health of important control files.

The following table provides procedures on monitoring control files in RMM and CA-1.

Tasks	Procedures
Exploring control data	CA-1
Monitoring control files	RMM

For more information on tape agent functionality for a specific subsystem, see Tape Agent for MVS overview.

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing tape volumes

You can use the Tape Agent for MVS to help manage tape subsystem volumes. The agent provides functions for exploring, adding, modifying, and deleting volumes in various tape software and hardware subsystems.

The following table provides procedures the volume management functions the agent provides for CA-1, RMM, StorageTek, and IBM VTS tape subsystems.

Tasks	Procedures
Exploring volumes	CA-1 RMM StorageTek
Adding volumes	RMM
Modifying volumes	CA-1 RMM StorageTek
Removing volumes	RMM StorageTek
Scratching volumes	CA-1
Ejecting volumes	StorageTek
Monitoring for inactive or underused volumes	StorageTek VTS
Monitoring scratch volume counts	RMM StorageTek VTS
Monitoring for rejected scratch volumes	RMM

For more information on tape agent functionality for a specific subsystem, see Tape Agent for MVS overview.

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Monitoring tape subsystem availability

You can use the Tape Agent for MVS to ensure tape subsystems are available in your storage environment when they are needed.

The following table provides procedures for monitoring the status of RMM, CA-1, StorageTek, IBM VTS, and 3494/3995 subsystems.

Tasks	Procedures
Monitoring subsystem availability	3493/3495 RMM StorageTek VTS
Monitoring for subsystem errors	CA-1 RMM StorageTek

For more information on tape agent functionality for a specific subsystem, see Tape Agent for MVS overview.

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Monitoring tape subsystem performance

You can use the Tape Agent for MVS to monitor the performance of your tape subsystems.

The following table provides procedures for monitoring the performance of IBM Virtual Tape Server (VTS) and StorageTek tape subsystems.

Tasks	Procedures
Monitoring cache performance	VTS
Monitoring volume mount times	VTS
Monitoring transfer rates	VTS
Monitoring free cells in StorageTek	StorageTek
Monitoring cleaning cartridges in StorageTek	StorageTek
Monitoring operator intervention	VTS StorageTek

For more information on tape agent functionality for a specific subsystem, see Tape Agent for MVS overview.

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing backup and archive applications

Configuring backup policies, classes, and schedules

You can use the backup and host agents to help configure policies, classes, and schedules for the backup and archive applications that you manage through ControlCenter.

The following table provides procedures for configuring Tivoli Storage Manager (TSM).

Task	Procedures
Configuring backup policies, classes, and schedules	TSM

For more information on the capabilities of a host or database agent, see the overview topic for that agent:

- Backup Agent for TSM overview
- Host Agent for HSM overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Ensuring backup completion

You can use the backup and host agents to ensure that backups complete for the backup and archive applications that you manage through ControlCenter.

The following table provides procedures for ensuring backup completion in Tivoli Storage Manager (TSM) and DFSMShsm (HSM).

Task	Procedures
Ensuring backup completion	TSM HSM

For more information on the capabilities of a host or database agent, see the overview topic for that agent:

- Backup Agent for TSM overview
- Host Agent for HSM overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing backup clients and nodes

You can use the backup and host agents to help manage clients and nodes for the backup and archive applications that you manage through ControlCenter.

The following table provides procedures for managing clients and nodes in Tivoli Storage Manager (TSM).

Task	Procedures
Managing backup clients and nodes	TSM

For more information on the capabilities of a host or database agent, see the overview topic for that agent:

- Backup Agent for TSM overview
- Host Agent for HSM overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing backup databases and logs

You can use the backup and host agents to help protect the databases used by and the log files generated by the backup and archive applications that you manage through ControlCenter.

The following table provides procedures for protecting and monitoring databases and log files in Tivoli Storage Manager (TSM) and IBM DFSMShsm (HSM).

Tasks	Procedures
Managing backup databases and logs	TSM
Monitoring database performance	TSM
Monitoring for space problems	TSM
Ensuring the integrity of control data sets	HSM
Pointing HSM to different control data sets	HSM

For more information on the capabilities of a host or database agent, see the overview topic for that agent:

- Backup Agent for TSM overview
- Host Agent for HSM overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Managing backup storage resources

You can use the backup and host agents to help manage the storage resources used by the backup and archive applications that you manage through ControlCenter.

The following table provides procedures for managing storage resources in Tivoli Storage Manager (TSM).

Task	Procedures
Managing backup pools and volumes	TSM

For more information on the capabilities of a host or database agent, see the overview topic for that agent:

- Backup Agent for TSM overview
- Host Agent for HSM overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Searching for files in backup and archive applications

You can use the backup and host agents to search for files managed by the backup and archive applications that you manage through ControlCenter.

The following table provides procedures for searching for files in Tivoli Storage Manager (TSM) and IBM DFSMShsm (HSM).

Tasks	Procedures
Searching log files	TSM
Listing backed up files for a node	TSM
Listing migrated files	HSM

For more information on the capabilities of a host or database agent, see the overview topic for that agent:

- Backup Agent for TSM overview
- Host Agent for HSM overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Viewing backup jobs (processes)

You can use the backup and host agents to view the jobs, or processes, that comprise the backup and archive applications that you manage through ControlCenter.

The following table provides procedures for viewing jobs, or processes, in Tivoli Storage Manager (TSM) and IBM DFSMShsm (HSM).

Tasks	Procedures
Viewing current backup processes	TSM HSM

For more information on the capabilities of a host or database agent, see the overview topic for that agent:

- Backup Agent for TSM overview
- Host Agent for HSM overview

Related topics

- Introducing EMC ControlCenter
- ControlCenter agents overview

Reporting

ControlCenter collects voluminous detailed information about the entire storage environment and stores it in a database, extracting specific pieces to populate reports. The resulting reports help storage administrators better analyze and report on the current state of their storage environment, giving managers a variety of perspectives to study. Some reports are predefined, others can be customized for specific needs.

ECC Reports

These pre-configured reports are divided into three general categories:

- Asset Management reports provide lists of their storage assets, counts of different types of assets, installation and maintenance dates and data, and some high level configuration information.
- Configuration reports provide detailed configuration information for hardware such as storage arrays, connectivity devices, and hosts.
- Utilization and Free Space reports give information about current storage capacity, percent utilization, and the amount of available storage.

User Defined Reports

Users can create their own reports using the ECC Reports as templates but tailoring them to their specific needs.

Schedules

All reports have schedules associated with them. Users can create customized schedules to attach to their user defined reports so they run on certain days and at selected times. The schedule can be configured to run the report a given number of times. Further, the schedule can be set to delete a report after a certain number of days.

All reports can be printed, saved, or exported for further study by other programs.

Related topics

- Running a report
- Saving a report
- Viewing report properties
- User Defined reports

Reporting Overview

For an overview of a report, as well as details about each field and column, click the report's title.

Asset Management Reports

- General Assets Detail

Configuration Reports

- Host Details
- Host Device Configuration Details

Utilization and Free Space Reports

- Database Utilization Details
- Database Utilization Summary by Symmetrix
- File System Utilization
- File System Utilization Summary by Host
- File System Utilization Summary by Symmetrix
- File System Utilization Summary by User-Defined Groups
- File Systems with Least Free Space - Top 10
- File Systems with Most Free Space - Top 10
- Host Free Space Summary by Symmetrix
- Host Utilization
- Host Utilization - Most and Least Available Capacity -Top 10
- Host Utilization Summary by Operating System
- Host Utilization by User-Defined Groups
- Symmetrix Configuration Details
- Symmetrix Utilization
- Symmetrix Utilization Summary by Host by User-Defined Groups
- Symmetrix Utilization Summary by User-Defined Groups
- Symmetrix Capacity - Top 10

Related topics

- Running a report
- Saving a report
- Viewing report properties

Viewing report properties

There are two ways to view the properties of a report:

- In the selection panel, select the box to the left of the report.
- In the selection panel, right click a report that is unchecked and select **Properties**.

Using either method, the properties appear in the PropertiesReports table in the target panel.

Field descriptions

Name	Name of the report.
User Defined	Whether this is a user-defined report.
Schedule	Name of the schedule, if any, associated with the report.
Association	The managed object associated with the report.
Object	
Date Modified	Date (mm/dd/yy) and time (hh:mm:ss) the report was last modified.
Who Modified	User ID of the user who made the last modification to the report.

Related topics

- Running a report
- Saving a report

Running a report

Reports can be run against selected managed objects (MOs) or against all MOs.

Right-click the MO, select **Reports**, then **Select Report**. The Select ECC Reports dialog box appears with a list of available reports from which to choose. If the desired report is not visible, click **Show All** to display the remaining available reports.

Click to select the appropriate report, then click **Run**. The Report dialog box appears and displays a progress bar as the report is being prepared and notifies the user when the report has completed. Click **Close** to close the dialog.

When the report is complete, it appears in a separate Web browser window.

Print the report

Click **Print** in the banner at the top of the browser window. A printer-friendly version of the report appears. The Print dialog box appears. Select a printer, click **Print**.

Export the report

You can export the report as a Microsoft Excel Comma Separated Values (.csv) file.

Click **Export** in the banner at the top of the browser window. The File Download dialog box appears.

- To immediately open the file in a spreadsheet, click **Open this file from its current location** and then click **OK**. Microsoft Excel opens and displays the report as a spreadsheet. You can now manipulate the data and customize the spreadsheet to meet your specific needs. To save the spreadsheet, select **Save As** from the **File** menu.
- To save the report directly to a .csv file, click **Save this file to disk**, then click **OK**. The Save As dialog box appears. Specify a file name and location, then click **Save**.

ECC report details

To view general information about a particular report, as well as details about each field and column, select the report from the ECC Reports list.

Related topics

- Saving a report
- Viewing report properties

Saving a report

Right-click the report, select **Save As**. The Edit Report dialog box appears. Complete the fields, click **OK**.

Field descriptions

Name	Name of the report.
Schedule	Select a schedule from the drop-down list box.
Edit	The Edit Schedule dialog box appears.
New	The Create a Schedule dialog box appears.
Activated	If checked, the report runs in the background if it has a schedule associated with it.
Description	Enter a short description to help identify the report later.

Related topics

- Running a report
- Viewing report properties

Edit/Create a Report

This dialog box provides a way to edit an existing report or to create a new report based on one that already exists.

Field and button descriptions

Name	Name of the selected report. To edit the report, do not change its name. To create a new report based on this report, enter a new name.
Schedule	Assign a report schedule. Select an existing schedule from the drop down list.
Edit	Opens the Edit Report Schedule dialog box, populated with existing values, so you can adjust the report schedule as needed.
New	Opens the Create a Report Schedule dialog box so you can set parameters for the new schedule.
Description	Enter text that describes the report.

Click **OK** to save the new report. Click **Cancel** to leave the report in its original form.

Related topics

- Creating a user defined report
- Edit/Copy/Create a Report Schedule
- Viewing report properties

User Defined Reports

You can define your own report by saving any ECC report with a new name. Since the parameters are saved with a new report name, this custom report can be run whenever you need updated information on the same object. For example, if you select Host x, run a report, and save it with a new name you can run the report a week later and you will only see results that apply to Host x.

Alternatively, you can save any report directly from the ECC Reports branch in the tree panel. Using this approach the new report, all objects are applied to the report as appropriate.

Related topics

- Creating a User Defined Report
- Reports overview

Creating a User Defined Report

There are two methods to create user defined reports:

- After running any ECC report, the Report dialog box advises you that the operation is complete. Click **Save As** and the Edit Report dialog box appears. Enter a name for the report and click **OK**. ControlCenter saves your parameters and the new report appears in the tree under User Defined Reports.
- To create a report that executes against all appropriate managed objects, right-click an existing report in the ECC Reports branch of the tree in the selection panel and click **Save As**. The Edit Report dialog box appears. Enter a name for the new report and click **OK**. The new report appears in the tree under User Defined Reports.

Click and drag the report to its appropriate Report Group, if desired.

Related topics

- User Defined Reports
- Creating a Report Group

Creating a Report Group

Provide structure to your User Defined Groups by organizing them into folders known as Report Groups.

To create a Report Group:

1. Expand Reports.
2. Right-click User Defined Reports, select New Report Group. The New Group dialog box appears.
3. Enter a name for the new report group, click OK. The new folder appears in the tree panel.

Click and drag any appropriate user defined reports into the new report group.

Related topics

- User Defined Reports
- Creating a User Defined Report

Save Schedule As

Enter a new name for the schedule you just created.

Click **OK** to save the schedule and exit.

Related topics

- Edit/Create a Report Schedule

Select ECC Reports

This dialog box lists all available reports.

If the report you want is not visible, click **Show All** to display the remaining available reports.

Field descriptions

Category	The category to which the report belongs. All reports associated with a category appear under that category in the selection tree.
Name	The name of the report.
Associated MOs	Managed object(s) associated with the report.
Grouping	Whether the information in the report is organized by user-defined groups.
Description	The description of the report. This description is optional and is entered when a report is created or edited.

Related topics

- Running a report
- Edit/Create a Report

Properties - Report Schedules

The Report Schedules lists all schedules.

Field descriptions

Name	The name of the schedule.
Day to Run	The frequency when the report is scheduled to run.
Time to Run	The time of day when the report is scheduled to run
Recurrence	The frequency that the report is scheduled to recur in *x* minutes

Related topics

- Edit/Create a Schedule

Copy Report Schedule

The purpose of this dialog box is to make a copy of an existing report schedule. You can then change the day, time, recurrence interval, and retention period and save the copy as a new schedule.

When to Run

Day	This drop down list contains a list of options, including weekday names, days of the month, and common intervals.
Time (local)	Enter the time of day you want to assign to this schedule. Time is specified using a 24-hour clock.
Recur *x* minutes	Enter a number to schedule a report to run every x minutes on the day you specified in the Day field. The maximum number of minutes is 1440, which will cause the report to run only once in the 24-hour period. Enter 0 if you do not want the report to run more than once.

When to Automatically Delete Reports

Delete After *x* days	This text field allows you to specify a retention period for a report assigned this schedule. Enter the number of days you want the report retained, after which it will be deleted. Enter 0 to retain the report indefinitely. Leave the field blank if you do not want the report retained.

Click Save As to save and name the schedule.

Related topics

- Edit/Create a Report Schedule
- Save Report As

Copying a ReportSchedule

1. Right-click **Reports**. The Reports tree appears.
2. Expand **Schedules**.
3. Right-click a schedule name. Select **Copy Schedule**. The Edit Schedule: Copy of dialog box appears. For field descriptions, see Edit/Create a Schedule.
4. Click **Save AS**. The Save Schedule as dialog box appears.
5. Type in a schedule name and click **OK**.
6. The Edit Schedule: Copy of dialog box still remains visible for you to make any changes or further copies. Click **OK** to close this dialog box.

Related topics

- Edit/Create a Schedule
- Save Schedule As dialog box

Creating a report schedule

1. Expand **Reports**.
2. Right-click **Schedule**. The Create a Report Schedule dialog box appears. For field descriptions, see Create a Report Schedule.
3. Enter the data to schedule when your report is to run.
4. Click **Save As**. The Save Schedule As dialog box appears.
5. Enter the new schedule name, and click **OK**. The new schedule name appears in the tree panel.

Related topics

- Save Schedule As dialog box

Edit/Create a Report Schedule

The purpose of this dialog box is to create or edit a schedule of when to run the report. You can specify the day, time, recurrence interval, and deletion schedule.

When to Run

Day	This drop down list contains a list of options, including weekday names, days of the month, and common intervals.
Time (local)	Enter the time of day you want to assign to this schedule. Time is specified using a 24-hour clock.
Recur *x* minutes	Enter a number to schedule a report to run every x minutes on the day you specified in the Day field. The maximum number of minutes is 1440, which will cause the report to run only once in the 24-hour period. Enter 0 if you do not want the report to run more than once.

When to Automatically Delete Reports

Delete After *x* days	This text field allows you to specify a retention period for a report assigned this schedule. Enter the number of days you want the report retained, after which it will be deleted. Enter 0 to retain the report indefinitely. Leave the field blank if you do not want the report retained.

Click Save As to save and name the schedule.

Related topics

- Copy Report Schedule
- Save Report As

Deleting a report schedule

1. Expand Reports in the tree panel.
2. Expand **Schedules**.
3. Right-click a schedule name, and select **Delete Schedule**. A confirmation dialog box appears asking 'Do you really want to delete this schedule?'
4. Click **No** to cancel and close the dialog box, OR Click **Yes** to delete the schedule and close the dialog box.

Related topics

- Edit/Create a Schedule
- Copying a Schedule

Viewing Schedule Properties

1. Expand Reports in the tree panel.
2. Right-click **Schedules** and select **Properties**. A table listing all schedules appears in the target panel. OR Expand **Schedules,** right-click a schedule name, and select **Properties**. A table listing the properties of the selected schedule appears in the target panel. For field descriptions, see Properties - Report Schedules.

Related topics

- Save Schedule As
- Copying a Schedule
- Deleting Schedule

Asset Management reports

Asset Management reports provide details about the storage hardware assets of the enterprise.

Reports

General Assets Detail	This is a detail report that provides basic information about the assets in the enterprise, or those that the user has selected. For report field descriptions, see General Assets Detail report.

Related topics:

- Running a report
- Saving a report
- Viewing report properties

General Assets Detail report

This is a detail report that provides basic information about the hardware assets in the enterprise, or those that the user has selected.

Field descriptions

Vendor	Name of the vendor of the asset.
Type	Type of asset.
Serial No.	Serial number of the asset.
Product	Generic name of the asset.
Model	Model number or other vendor description.
Operating System	Operating system installed on the asset.
O/S Version	Operating system version installed on the asset.
O/S Revision	Operating system revision installed on the asset.

For a printable copy of the report, click **Print** at the top of the report. On the Print dialog box choose the printer, set printing options, and click **Print**.

To make changes to the report, click Export at the top of the report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (.csv) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report

Configuration reports

These reports show information about the configuration of hosts on the system. They give additional details on those hosts with storage devices associated with them.

Reports

Host Details	This is a detail report provides basic information about all the hosts on the system. For those hosts with associated storage devices, the report gives figures on storage capacity. For report field descriptions, see Host Details report.
Host Device Configuration Details	This is a summary/detail report that contains information about host devices grouped by host. For report field descriptions, see Host Device Configuration Details report.

Related topics

- Running a report
- Saving a report
- Viewing report properties

Host Details report

This detail report provides basic information about all the hosts on the system. For those hosts with associated storage devices, the report gives figures on storage capacity.

Field description

Host Name	Name of the host.
IP Address	Primary IP address of the host.
Total Capacity	Sum of all volume group and non-volume group device capacities.
Used Capacity	The portion of the host's capacity that is in use.
Free Capacity	Total Capacity less Used capacity.
% Used Capacity	Percent of the total capacity in use.
Memory	Amount of memory installed on the host.
Host Device Count	Total number of host devices for this host.
PowerPath Count	Total number of PowerPath devices for this host.
Operating System	The host's operating system.
O/S Version	Operating system version.
O/S Level	The release level of the operating system.
Host Type	Type of host (for example x86, os/390, 9000/800).
# HBAs	Total number of host bus adapters (HBA) on this host.

For a printable copy, click **Print** at the top of the report.

To make changes, click **Export** at the top of this report. The **File Download** dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (csv.) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties

Host Device Configuration Details report

The first section of this report gives general information about all hosts that have devices associated with them, including counts of all the host devices and PowerPath devices. The hosts are sorted by IP address.

The second section is organized by host. Devices associated with each host are listed along with details about their configuration.

Hosts that do not have associated devices do not appear iin this report.

Field descriptions

Summary section

Host Name	The name of the host.
Host Type	Host type off the related host.
IP Address	Primary IP address.
Operating System	The operating system running on the related host.
# Host Devices	Total number of devices attached to the related host. Details of these devices make up the next section of the report.
# PowerPath Devices	Total number of PowerPath devices for this host.

Detail section

Device	The name of the device attached to the host.
Volume Group	Volume group name.
Vendor	The vendor of this device.
Product	Brief description of the device. Configurable during installation.
Product Revision	Host device product version and revision level information.
Cache	Host device cache size.
Total Capacity	Total capacity of the device.
Free Capacity	Capacity free and available for use.
Removeable	Whether the disk is removable or not.
VCM	Whether the device is under volume control or not.
Symmetrix	Symmetrix ID.
Device ID	ID of the device.
Adaptor No.	Host bus adapter ID.
Port Type	Type of port (for example SCSI, host, fibre device).
Port No.	The port number of the device.

For a printable copy, click **Print** at the top of the report.

To make changes, click **Export** at the top of this report. The **File Download** dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (csv.) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties

Utilization and Free Space reports

The Utilization and Free Space reports provide a number of views storage capacity and usage information. The reports display summary and detail views of database, file system, and host storage utilization and show there the most and least free space can be found.

Reports

Database Utilization Details	This is a simple detail report that provides information on capacity and usage of storage in the selected databases. For report field descriptions, see Database Utilization Details report.
Database Utilization Summary by Symmetrix	This is a summary/detail report organized into two parts. The summary section lists all selected Symmetrixes with general information about the database capacity of each. The detail section lists all database instances and their capacity information, grouped by Symmetrix. For report field descriptions, see Database Utilization Summary by Symmetrix report.
File System Utilization	This detail report provides file system utilization information. For report field descriptions, see File System Utilization (GB) report.
File System Utilization Summary by Host	This is a summary/detail report that provides file system utilization by hosts. The detail section contains the same fields as in the file system utilization detail report, except that the host name and host OS are removed. The summary section contains the totals for all the file systems in that host. The detail section reports on file system capacity and use, grouped by host. For report field descriptions, see File System Utilization Summary by Host report.
File System Utilization Summary by Symmetrix	This is a summary/detail report that provides file system utilization by Symmetrix. It follows a similar logic as the Database Utilization by Symmetrix and show what file systems reside on each Symmetrix and what capacity they have. For report field descriptions, see File System Utilization Summary by Symmetrix report.
File System Utilization Summary by User-Defined Groups	The summary portion of this report provides general information about file system capacity and usage associated with user-defined groups. The detail portion lists each user-defined group and details the file systems on each associated host. For report field descriptions, see File System Utilization Summary by User-Defined Groups.
Host Free Space Summary by Symmetrix	This report shows the amounts of free space on the host and on the storage device attached to it, grouped by specific Symmetrix subsystems. For report field descriptions, see Host Free Space Summary by Symmetrix report.
Host Utilization	This is a summary/detail report providing summary information on capacity and usage of host storage. For report field descriptions, see Host Utilization report.
Host Utilization – Most and Least Available Capacity – Top 10	This two-part summary report lists the 10 hosts with the highest available capacity and those with the least capacity. For report field descriptions, see Host Utilization - Top 10 report.
Host Utilization by User-Defined Groups	This report provides a summary of capacity and usage of host storage by user-defined groups. for report field descriptions, see Host Utilization by User-Defined Groups report.
Host Utilization Summary by Operating System	This is a summary/detail report, and provides summary information on capacity and usage of host storage grouped by operating system. For report field descriptions, see Host Utilization Summary by Operating System report.
Symmetrix Configuration Details	This is a detail report that provides basic information about the Symmetrix configuration. The user can select Symmetrix systems or groups that contain Symmetrix systems to define the population for this report. For report field descriptions, see Symmetrix Configuration report.
Symmetrix Utilization	This is a detail report that provides information on Symmetrix utilization and capacity. For report field descriptions, see Symmetrix Utilization Details report.
Symmetrix Utilization Summary by Host by User-Defined Groups	This report shows the total Symmetrix storage allocated per user-defined group, broken down by hosts. For report field descriptions, see Symmetrix Utilization by Host by User-Defined Groups report.

Symmetrix Utilization Summary by User-Defined Groups	This report provides summary information on capacity and usage of Symmetrix storage by user-defined groups. For report field descriptions, see Symmetrix Utilization Summary by User-Defined Groups report.
Top 10 FileSystems with least free space	This report provides a list of the file systems with least free space. For report field descriptions, see File Systems with least free space – Top 10.
Top 10 FileSystems with most free space	This report provides a list of the file systems with most free space. For report field descriptions, see File Systems with most free space – Top 10.
Symmetrix Capacity – Top 10	This detail report shows Symmetrixes with the largest available capacity, those with the largest unallocated capacity, those with the largest unmapped capacity, those with the largest unconfigured capacity, and those with the largest number of free disk slots. For report field descriptions, see Symmetrix Capacity – Top 10 report.

Related topics

- Running a report
- Saving a report
- Viewing report properties

Database Utilization Details report

This is a simple detail report that provides information on capacity and usage of storage in the selected databases.

Field descriptions

Host	Host name.
DB Instance	Database instance name.
Instance Type	Database instance type.
Instance Version	Version of the database instance.
Total Capacity	Sum of all database files and all raw devices on which the database resides.
Data Capacity	Total space allocated for data file and redo logs.
Free Data Capacity	Amount of free space in all segment of files.
Used Data Capacity	Total data capacity in use.
% Used Data Capacity	Percent of the total capacity in use.
Redo Log Capacity	Total size of redo logs.
# Schemas	Count of schemas in the instance.
# Tablespaces	Count of tablespaces in instance.
# Files	Count of data files in the instance.

For a printable copy of the report, click **Print** at the top of the report. On the Print dialog box choose the printer, set printing options, and click Print.

To make changes to the report, click **Export** at the top of the report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (.csv) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties

File System Utilization Summary by Host report

This is a two-part summary/detail report that provides file system utilization by hosts. The summary section contains the totals for all the file systems on each host. The detail section shows details of every file system for each host listed in the summary section.

Field descriptions

Summary section

Host Name	Name of the host.
Total Capacity	Total capacity on the host.
Free Capacity	Capacity available.
Used Capacity	Capacity currently in use.
% Used Capacity	Percent of total capacity currently in use.
Total Inodes	Total configured Inodes.
Free Inodes	Number of free Inodes.
% Free Inodes	Percent of total Inodes available for use.

Detail section

File System	Name of the file system.
Type	File system type.
Total Capacity	Total capacity of the file system.
Free Capacity	Capacity available on the file system.
Used Capacity	File system capacity currently in use.
% Used Capacity	Percent of total capacity currently in use.
Total Inodes	Total configured Inodes on the file system.
Free Inodes	Number of free Inodes on the file system.
% Free Inodes	Percent of total inodes on the file system available for use.

For a printable copy of the report, click **Print** at the top of the report. On the Print dialog box choose the printer, set printing options, and click Print.

To make changes to the report, click **Export** at the top of the report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (.csv) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties

File System Utilization Summary by Symmetrix

This summary/detail report is in two parts. The first section lists each Symmetrix and provides a summary of file system capacity and use on each. The second part lists details of file systems on hosts, grouped by Symmetrix.

Field descriptions

Summary section

Symmetrix	Serial number of the Symmetrix.
File System Type	Type of file system.
Total Capacity	Total capacity of file systems on the Symmetrix.
Free Capacity	Capacity available for use.
Used Capacity	File system capacity currently in use.
% Used Capacity	Percent of total capacity in use.
Total Inodes	Total inodes associated with the Symmetrix.
Free Inodes	Inodes available for use.
% Free Inodes	Percent of total inodes available.

Detail section

Host Name	Name of the host associated with the Symmetrix.
File System	Name of the file system.
Type	Type of file system.
Total Capacity	Total capacity of file systems on the host.
Free Capacity	Capacity available for use on the host.
Used Capacity	File system capacity currently in use.
% Used Capacity	Percent of total capacity in use.
Total Inodes	Total inodes associated with the host.
Free Inodes	Inodes available for use.
% Free Inodes	Percent of total inodes on the host that are available.

For a printable copy of the report, click Print at the top of the report. On the Print dialog box choose the printer, set printing options, and click Print.

To make changes to the report, click Export at the top of the report. The File Download dialog box appears. Select Open this file from its current location. The report exports in comma-separated values (.csv) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties

File System Utilization Summary by User-Defined Groups

This is a summary/detail report providing summary information on capacity and usage of host storage, organized by user defined groups. To run the report, select the groups that contain the hosts or any parent group. The report includes every host associated with its group, and every group associated with its direct parent group.

Field descriptions

Group	Name of the user-defined group.
Count	The number of hosts associated with the group.
Host Name	Name of the host.
File System	Name of the file system.
Type	Type of file system.
Total Capacity	Total capacity of file systems associated with the group.
Free Capacity	Capacity available for use.
Used Capacity	File system capacity currently in use.
% Used Capacity	Percent of total capacity in use.
Total Inodes	Total inodes associated with the group.
Free Inodes	Inodes available for use.
% Free Inodes	Percent of total inodes available.

For a printable copy of the report, click **Print** at the top of the report. On the Print dialog box choose the printer, set printing options, and click **Print**.

To make changes to the report, click **Export** at the top of the report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (.csv) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties

File System Utilization Summary by User-Defined Groups

This summary/detail report is in two parts. The first section lists each user-defined group and provides a summary of file system capacity and use for each. The second part lists details of file systems on hosts, organized by user group.

Field descriptions

Summary section

Group	Name of the user-defined group.
Count	The number of managed objects associated with the group.
Host Name	The name of the host associated with the group.
File System Type	Type of file system.
Total Capacity	Total capacity of file systems associated with the group.
Free Capacity	Capacity available for use.
Used Capacity	File system capacity currently in use.
% Used Capacity	Percent of total capacity in use.
Total Inodes	Total inodes associated with the group.
Free Inodes	Inodes available for use.
% Free Inodes	Percent of total inodes available.

Detail section

Host Name	Name of the host associated with the group.
File System	Name of the file system.
Type	Type of file system.
Total Capacity	Total capacity of file systems on the host.
Free Capacity	Capacity available for use on the host.
Used Capacity	File system capacity currently in use.
% Used Capacity	Percent of total capacity in use.
Total Inodes	Total inodes associated with the host.
Free Inodes	Inodes available for use.
% Free Inodes	Percent of total inodes on the host that are available.

For a printable copy of the report, click Print at the top of the report. On the Print dialog box choose the printer, set printing options, and click Print.

To make changes to the report, click Export at the top of the report. The File Download dialog box appears. Select Open this file from its current location. The report exports in comma-separated values (.csv) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties

File System Utilization Summary by Symmetrix report

This is a summary/detail report that provides file system utilization by Symmetrix. It follows a similar logic as the Database Utilization by Symmetrix and show what file systems reside on each Symmetrix and what capacity they have.

Field descriptions

Symmetrix	
File System Type	
Total Capacity	
Free Capacity	
Used Capacity	
% Used Capacity	
Total Inodes	
Free Inodes	
% Free Inodes	

For a printable copy, click **Print** at the top of the report.

To make changes, click **Export** at the top of this report. The **File Download** dialog box appears. Select **Open this file from its current location**. The report appears in Microsoft Excel format.

Related topics

- Running a report
- Saving a report
- Viewing report properties

Host Free Space Summary by Symmetrix report

This is a detail/summary report with two levels of summarization, that provides amounts of free space on the host and on the storage array attached to it, grouped by host bus adapters and by specific Symmetrix subsystems.

Field descriptions

Host Name	Name of the host.
Total Capacity	Total of the volume group and host device capacities.
Used Capacity	Total amount of the capacity in use.
% Used Capacity	Percent of the total capacity in use.
Volume Group Free	Total size in volume group that is not part of any logical volume.
File Systems Free	Total capacity of file systems available.
Host Device Free	Total size of host devices not inside any volume group that don't have file systems on them.
Unconfigured	Total capacity of unconfigured Symmetrix devices on all Symmetrix systems that are visible to this host (this includes formatted and unformatted storage).
Total Unmapped	Total size of unmapped Symmetrix devices on all Symmetrix systems that are visible to this host.
STD Unmapped	Total size of unmapped STD Symmetrix devices on all Symmetrix systems that are visible to this host.
BCV Unmapped	Total size of unmapped BCV Symmetrix devices on all Symmetrix systems that are visible to this host.
RDF Unmapped	Total size of unmapped RDF (R1) Symmetrix devices on all Symmetrix systems that are visible to this host.
Total Unallocated	Total size of unallocated (mapped but not allocated to a host) Symmetrix devices on all Symmetrix systems that are visible to this host.
STD Unallocated	Total size of unallocated STD Symmetrix devices on all Symmetrix systems that are visible to this host.
BCV Unallocated	Total size of unallocated BCV Symmetrix devices on all Symmetrix systems that are visible to this host.
RDF Unallocated	Total size of unallocated RDF Symmetrix devices on all Symmetrix systems that are visible to this host.
Symmetrix	Symmetrix ID.

For a printable copy, click **Print** at the top of the report.

To make changes to a report, click **Export** at the top of this report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (csv.) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties

Host Utilization Summary by User-Defined groups report

This is report provides information on capacity and usage of host storage by user-defined groups. The groups are reported by their hierarchy in the tree panel, the highest level group followed by its child group, and so forth.

Field descriptions

Group	Name of the group.
Count	Total number of users in the group.
Host Name	Name of the host.
Total Capacity	Total capacity on the host. The sum of volume groups and host devices.
Used Capacity	Amount of capacity currently in use.
Free Capacity	Amount of capacity available.
% Used Capacity	Percentage of total capacity in use.
FS Total	Total size of logical volumes with file systems.
FS Used	Total size of used file system.
FS Free	Total size of free file systems.
Database Total	Total size of logical volumes that do not contain a file system.
VG Total	Total size of volume groups.
VG Used	Volume group capacity currently used.
VG Free	Amount of free volume group capacity.
HD Total	Total size of host device space.
HD Used	Total size of host device capacity currently in use.
HD Free	Total size of host device capacity available.
# Files Systems	Count of file systems on the host.
# Host Devices	Count of host devices associated with the host.
# Volume Groups	Count of volume groups.
# Logical Volumes	Count of logical volumes on the host.

For a printable copy of the report, click **Print** at the top of the report. On the Print dialog box choose the printer, set printing options, and click **Print**.

To make changes to the report, click **Export** at the top of the report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (.csv) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties
- Utilization and Free Space reports

Host Utilization — Most and Least Available Capacity

This summary report is in two parts. The first section lists, in order, the 10 hosts with the highest available capacity. The second section lists the 10 hosts with the least amount of free capacity.

Field descriptions

Host	Name of the host.
Operating System	Operating system installed on the host.
Total Capacity	Total capacity on the host. The sum of volume groups and host devices.
Used Capacity	Amount of capacity currently in use.
Free Capacity	Amount of capacity available.
% Used Capacity	Percentage of total capacity in use.
FS Total	Total size of logical volumes with file systems.
FS Used	Total size of used file system.
FS Free	Total size of free file systems.
Database Total	Total size of logical volumes that do not contain a file system.
VG Total	Total size of volume groups.
VG Used	Volume group capacity currently used.
VG Free	Amount of free volume group capacity.
HD Total	Total size of host device space.
HD Used	Total size of host device capacity currently in use.
HD Free	Total size of host device capacity available.
# Files Systems	Count of file systems on the host.
# Host Devices	Count of host devices associated with the host.
# Volume Groups	Count of volume groups.
# Logical Volumes	Count of logical volumes on the host.

For a printable copy, click **Print** at the top of the report.

To make changes to a report, click **Export** at the top of this report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (csv.) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties

Host Utilization - Top 10 report

This report provides the top N hosts in different categories.

Field descriptions

Host Name	
Operating System	
Total Capacity	
Used Capacity	
Free Capacity	
% Used Capacity	
FS Total	
FS USed	
FS Free	
Database Total	
VG Total	
VG Used	
VG Free	
HD Total	
HD Used	
HD Free	
# File Systems	
# Host Devices	
# Volume Groups	
# Logical Volumes	

For a printable copy, click **Print** at the top of the report.

To make changes, click **Export** at the top of this report. The **File Download** dialog box appears. Select **Open this file from its current location**. The report appears in Microsoft Excel format.

Related topics

- Running a report
- Saving a report
- Viewing report properties

Host Utilization Summary by User Defined groups report

This is report provides information on capacity and usage of host storage by user-defined groups. The groups are reported by their hierarchy in the tree panel, the highest level group followed by its child group, and so forth.

Field descriptions

Group	Name of the group.
Count	Total number of users in the group.
Host Name	Name of the host.
Total Capacity	Total capacity on the host. The sum of volume groups and host devices.
Used Capacity	Amount of capacity currently in use.
Free Capacity	Amount of capacity available.
% Used Capacity	Percentage of total capacity in use.
FS Total	Total size of logical volumes with file systems.
FS Used	Total size of used file system.
FS Free	Total size of free file systems.
Database Total	Total size of logical volumes that do not contain a file system.
VG Total	Total size of volume groups.
VG Used	Volume group capacity currently used.
VG Free	Amount of free volume group capacity.
HD Total	Total size of host device space.
HD Used	Total size of host device capacity currently in use.
HD Free	Total size of host device capacity available.
# Files Systems	Count of file systems on the host.
# Host Devices	Count of host devices associated with the host.
# Volume Groups	Count of volume groups.
# Logical Volumes	Count of logical volumes on the host.

For a printable copy of the report, click **Print** at the top of the report. On the Print dialog box choose the printer, set printing options, and click **Print**.

To make changes to the report, click **Export** at the top of the report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (.csv) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties
- Utilization and Free Space reports

Host Utilization Summary by Operating System report

This is a summary/detail report, and provides summary information on capacity and usage of host storage grouped by operating system. The user sees how much used and available capacity he has on Windows hosts vs. UNIX hosts vs. MVS hosts.

Field descriptions

Summary section

Operating System	Operating system for the group of hosts.
# Hosts	Number of hosts using this operating system.
Total Capacity	Total storage capacity of hosts using this operating system.
Used Capacity	Total space in use on hosts using this operating system.
Free Capacity	Capacity available on hosts using this operating system.
% Used Capacity	Percent of capacity currently in use on hosts using this operating system.
File System Total	Total size of logical volumes with file system on hosts using this operating system.
Database	Total size of logical volumes that do not contain a file system on hosts using this operating system.
# File Systems	Count of file systems on all hosts using this operating system.
# Host Devices	Count of host devices associated with all hosts using this operating system.

Detail Section

Host	Name of the host.
Total Capacity	Total capacity on the host. The sum of volume groups and host devices.
Used Capacity	Amount of capacity currently in use.
Free Capacity	Amount of capacity available.
% Used Capacity	Percentage of total capacity in use.
FS Total	Total size of logical volumes with file systems.
FS Used	Total size of used file system.
FS Free	Total size of free file systems.
Database Total	Total size of logical volumes that do not contain a file system.
VG Total	Total size of volume groups.
VG Used	Volume group capacity currently used.
VG Free	Amount of free volume group capacity.
HD Total	Total size of host device space.
HD Used	Total size of host device capacity currently in use.
HD Free	Total size of host device capacity available.
# Files Systems	Count of file systems on the host.
# Host Devices	Count of host devices associated with the host.
# Volume Groups	Count of volume groups.
# Logical Volumes	Count of logical volumes on the host.

For a printable copy, click **Print** at the top of the report.

To make changes to a report, click **Export** at the top of this report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (csv.) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties

Symmetrix Configuration Details report

This is a detail report that provides basic information about the configuration of each Symmetrix. The user can select Symmetrix systems or groups that contain Symmetrix systems to define the population for this report.

Field descriptions

Symmetrix	Symmetrix ID.
Model	Symmetrix model number.
Configured Storage	Total amount of storage configured on the Symmetrix.
Micro Code	Microdoce level.
M/C Date	Microcode date.
M/C Patch Level	Microcode patch level.
Patch Date	Microcode patch date.
Cache Size	Total size of configured cache.
# SCSI Ports	Count of all SCSI ports on the Symmetrix.
# Used SCSI Ports	Count of used SCSI ports.
# Available SCSI Ports	Count of available SCSI ports.
# Fibre Ports	Count of all fibre ports.
# Used Fibre Ports	Count of used fibre ports.
# Available Fibre Ports	Count of available fibre ports.
Open Channel Ports	Count of open channel ports.
# 18GB Disks	Count of 18 GB disks.
# 36GB Disks	Count of 36 GB disks.
# 47GB Disks	Count of 47 GB disks.
# 50GB Disks	Count of 50 GB disks.
Total Disk Slots	Count of all disk slots.
Free Disk Slots	Count of open (free) disk slots.

For a printable copy, click **Print** at the top of the report.

To make changes to a report, click **Export** at the top of this report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (csv.) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties

Symmetrix Utilization report

This is a detail report that provides information on utilization and capacity of each Symmetrix selected

Field descriptions

Symmetrix	Symmetrix serial number.
Name	Name of the Symmetrix.
Model	Symmetrix model number.
Micro Code Version	Symmetrix microcode level.
Total Unmapped	Total configured capacity not mapped to front end port.
STD Unmapped	Amount of storage capacity on STD devices that has been configured but not mapped to a front end port.
RDF1 Unmapped	Amount of storage capacity on RDF1 devices that has been configured but not mapped to a host.
Total Unallocated	Total capacity of devices that are not allocated to a host.
STD Unallocated	Capacity of STD devices not allocated to a host.
RDF1 Unallocated	Capacity of RDF1 devices not allocated to a host.
Total Unconfigured	Disk capacity that has not been configured as a Symmetrix device. This includes capacity on disks that currently have no devices (unformatted) and capacity on disks where a portion of the disk has been configured (formatted).
Unconfigured Formatted	Amount of unconfigured storage capacity on disks that have hyper volumes (Symmetrix devices) configured.
Unconfigured Unformatted	Amount of storage capacity on disks that have no hyper volumes configured.
Total Allocated	Total disk space allocated to hosts.
Unprot Allocated	Total unprotected disk space allocated to hosts.
Configured Capacity	Amount of usable storage capacity configured as Symmetrix devices. Note, this is usable capacity and therefore does not include mirrored capacity.

For a printable copy of the report, click **Print** at the top of the report. On the Print dialog box choose the printer, set printing options, and click **Print**.

To make changes to the report, click **Export** at the top of the report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (.csv) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties
- Utilization and Free Space reports

Symmetrix Utilization Summary by Host by User-Defined Groups report

This is a summary/detail report that provides information on utilization and capacity of Symmetrix storage allocated per user-defined group, broken down by hosts.

Field descriptions

Group	Name of the user-defined group selected.
Count	Count of Symmetrixes associated with the group.
Host Name	Name of the host.
Name	Symmetrix serial number.
Sym Device ID	Symmetrix device identification number.
Sym Device Type	Symmetrix device type.
Host Device Name	Name of the host device allocated to this Symmetrix.
Host Device Type	Device type of this host.
Total Capacity	Allocated capacity of the host.

For a printable copy of the report, click **Print** at the top of the report. On the Print dialog box choose the printer, set printing options, and click **Print**.

To make changes to the report, click **Export** at the top of the report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (.csv) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties
- Utilization and Free Space reports

Symmetrix Utilization Summary by User-Defined Groups report

This is a summary/detail report that provides information on utilization and capacity of Symmetrix storage as it relates to user-defined groups. The summary portion lists those selected groups that have associations with Symmetrixes and the count of devices for those groups.

Field descriptions

Group	Name of the user-defined group selected.
Count	Count of Symmetrixes associated with the groups.
Symmetrix	Symmetrix serial number.
Name	Name of the Symmetrix.
Model	Symmetrix model number.
Micro Code Version	Symmetrix microcode level.
Configured Capacity	Amount of usable storage capacity configured as Symmetrix devices. Note, this is usable capacity and therefore does not include mirrored capacity.
Total Unmapped	Total configured capacity not mapped to front end port.
BCV Unmapped	Amount of storage capacity on BCV devices that has been configured but not mapped to a front end port.
STD Unmapped	Amount of storage capacity on STD devices that has been configured but not mapped to a front end port.
RDF1 Unmapped	Amount of storage capacity on RDF1 devices that has been configured but not mapped to a host.
RDF2 Unmapped	Amount of storage capacity on RDF2 devices that has been configured but not mapped to a host.
Total Unallocated	Total capacity of devices that are not allocated to a host.
BCV Unallocated	Capacity of BCV devices not allocated to a host.
STD Unallocated	Capacity of STD devices not allocated to a host.
RDF1 Unallocated	Capacity of RDF1 devices not allocated to a host.
RDF2 Unallocated	Capacity of RDF2 devices not allocated to a host.
Total Mapped	Total configured capacity mapped to front end port.
STD Mapped	Amount of storage capacity on STD devices that has been configured and mapped to a front end port.
BCV Mapped	Amount of storage capacity on BCV devices that has been configured and mapped to a front end port.
RDF1 Mapped	Amount of storage capacity on RDF1 devices that has been configured and mapped to a host.
RDF2 Mapped	Amount of storage capacity on RDF2 devices that has been configured and mapped to a host.
Total Allocated	Total capacity of devices allocated to a host.
BCV Allocated	Capacity of BCV devices allocated to a host.
STD Allocated	Capacity of STD devices allocated to a host.
RDF1 Allocated	Capacity of RDF1 devices allocated to a host.
RDF2 Allocated	Capacity of RDF2 devices allocated to a host.
Unprotected Allocated	Capacity of unprotected devices allocated to a host.

Total Unconfigured	Disk capacity that has not been configured as a Symmetrix device. This includes capacity on disks that currently have no devices (unformatted) and capacity on disks where a portion of the disk has been configured (formatted).
Unconfigured Formatted	Amount of unconfigured storage capacity on disks that have hyper volumes (Symmetrix devices) configured.
Unconfigured Unformatted	Amount of storage capacity on disks that have no hyper volumes configured.

For a printable copy of the report, click **Print** at the top of the report. On the Print dialog box choose the printer, set printing options, and click **Print**.

To make changes to the report, click **Export** at the top of the report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (.csv) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties
- Utilization and Free Space reports

File Systems with most free space — top 10

This report provides a list of the 10 file systems with most free space.

Field descriptions

Host Name	Name of the host on which the file system resides.
Operating System	Operating system of the host.
File System	Name of the file system.
File Path	Path to the file system.
Type	File system type.
Total Space	Total amount of space configured for the file system.
Used Space	Space currently in use.
Free Space	Free space available on the file system.
% Free Space	Free space available for use.
Total Inodes	Total configured Inodes on the file system.
Used Inodes	Inodes currently in use
Free Inodes	Number of free Inodes on the file system.
% Free Inodes	Percent of total Inodes on the file system available for use.

For a printable copy of the report, click **Print** at the top of the report. On the Print dialog box choose the printer, set printing options, and click **Print**.

To make changes to the report, click **Export** at the top of the report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (.csv) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties

File Systems with least free space — top 10

This report provides a list of the 10 file systems with least free space. The file system with the least amount of free space is listed first.

Field descriptions

Host Name	Name of the host on which the file system resides.
Operating System	Operating system of the host.
File System	Name of the file system.
Type	File system type.
Total Space	Total amount of space configured for the file system.
Used Space	Space currently in use.
Free Space	Free space available on the file system.
% Used Space	Percent of total space currently in use.
Total Inodes	Total configured Inodes on the file system.
Used Inodes	Inodes currently in use
Free Inodes	Number of free Inodes on the file system.
% Free Inodes	Percent of total Inodes on the file system available for use.

For a printable copy of the report, click **Print** at the top of the report. On the Print dialog box choose the printer, set printing options, and click **Print**.

To make changes to the report, click **Export** at the top of the report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (.csv) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties

Symmetrix Capacity - Top 10 report

This report contains five sections.

- Symmetrix with Largest Available Capacity
- Symmetrix with Largest Unallocated Capacity
- Symmetrix with Largest Unmapped Capacity
- Symmetrix with Largest Unconfigured Capacity
- Symmetrix with Largest Number of Free Disk Slots

Each section provides appropriate details on the metric being monitored, starting with the larger number.

Field Descriptions

Symmetrix with Largest Available Capacity

Symmetrix	Symmetrix serial number.
Name	Name of the Symmetrix.
Largest Capacity	Largest available capacity (includes unallocated, unmapped, and unconfigured).
Model	Symmetrix model number.
Micro Code Version	Symmetrix microcode level.
Configured Capacity	Amount of usable storage capacity configured as Symmetrix devices. Note, this is usable capacity and therefore does not include mirrored capacity.
Total Unconfigured	Disk capacity that has not been configured as a Symmetrix device. This includes capacity on disks that currently have no devices (unformatted) and capacity on disks where a portion of the disk has been configured (formatted).
Unconfigured Formatted	Amount of unconfigured storage capacity on disks that have hyper volumes (Symmetrix devices) configured.

Unconfigured Unformatted	Amount of storage capacity on disks that have no hyper volumes configured.
Total Unmapped	Total configured capacity not mapped to front end port.
STD Unmapped	Amount of storage capacity on STD devices that has been configured but not mapped to a front end port.
BCV Unmapped	Amount of storage capacity on BCV devices that has been configured but not mapped to a front end port.
RDF1 Unmapped	Amount of storage capacity on RDF1 devices that has been configured but not mapped to a host.
RDF2 Unmapped	Amount of storage capacity on RDF2 devices that has been configured but not mapped to a host.
Total Mapped	Total configured capacity mapped to front end port.
STD Mapped	Amount of storage capacity on STD devices that has been configured and mapped to a front end port.
BCV Mapped	Amount of storage capacity on BCV devices that has been configured and mapped to a front end port.
RDF1 Mapped	Amount of storage capacity on RDF1 devices that has been configured and mapped to a host.
RDF2 Mapped	Amount of storage capacity on RDF2 devices that has been configured and mapped to a host.
Total Unallocated	Total capacity of devices that are not allocated to a host.
STD Unallocated	Capacity of STD devices not allocated to a host.
BCV Unallocated	Capacity of BCV devices not allocated to a host.
RDF1 Unallocated	Capacity of RDF1 devices not allocated to a host.
RDF2 Unallocated	Capacity of RDF2 devices not allocated to a host.
Total Allocated	Total capacity of devices allocated to a host.
Unprotected Allocated	Capacity of unprotected devices allocated to a host.
RDF1 Allocated	Capacity of RDF1 devices allocated to a host.
BCV Allocated	Capacity of BCV devices allocated to a host.
RDF2 Allocated	Capacity of RDF2 devices allocated to a host.

Symmetrix with Largest Unallocated Capacity

Symmetrix	Symmetrix serial number.
Name	Name of the Symmetrix.
Total Unallocated	Total capacity of devices that are not allocated to a host.
Configured Capacity	Amount of usable storage capacity configured as Symmetrix devices. Note, this is usable capacity and therefore does not include mirrored capacity.
Model	Symmetrix model number.
Micro Code Version	Symmetrix microcode level.
Total Unconfigured	Disk capacity that has not been configured as a Symmetrix device. This includes capacity on disks that currently have no devices (unformatted) and capacity on disks where a portion of the disk has been configured (formatted).
Unconfigured Formatted	Amount of unconfigured storage capacity on disks that have hyper volumes (Symmetrix devices) configured.
Unconfigured Unformatted	Amount of storage capacity on disks that have no hyper volumes configured.
Total Unmapped	Total configured capacity not mapped to front end port.
STD Unmapped	Amount of storage capacity on STD devices that has been configured but not mapped to a front end port.
BCV Unmapped	Amount of storage capacity on BCV devices that has been configured but not mapped to a front end port.
RDF1 Unmapped	Amount of storage capacity on RDF1 devices that has been configured but not mapped to a host.

RDF2 Unmapped	Amount of storage capacity on RDF2 devices that has been configured but not mapped to a host.
Total Mapped	Total configured capacity mapped to front end port.
STD Mapped	Amount of storage capacity on STD devices that has been configured and mapped to a front end port.
BCV Mapped	Amount of storage capacity on BCV devices that has been configured and mapped to a front end port.
RDF1 Mapped	Amount of storage capacity on RDF1 devices that has been configured and mapped to a host.
RDF2 Mapped	Amount of storage capacity on RDF2 devices that has been configured and mapped to a host.
STD Unallocated	Capacity of STD devices not allocated to a host.
BCV Unallocated	Capacity of BCV devices not allocated to a host.
RDF1 Unallocated	Capacity of RDF1 devices not allocated to a host.
RDF2 Unallocated	Capacity of RDF2 devices not allocated to a host.
Total Allocated	Total capacity of devices allocated to a host.
Unprotected Allocated	Capacity of unprotected devices allocated to a host.
RDF1 Allocated	Capacity of RDF1 devices allocated to a host.
BCV Allocated	Capacity of BCV devices allocated to a host.
RDF2 Allocated	Capacity of RDF2 devices allocated to a host.

Symmetrix with Largest Unmapped Capacity

Symmetrix	Symmetrix serial number.
Name	Name of the Symmetrix.
Total Unmapped	Total configured capacity not mapped to front end port.
Model	Symmetrix model number.
Micro Code Version	Symmetrix microcode level.
Configured Capacity	Amount of usable storage capacity configured as Symmetrix devices. Note, this is usable capacity and therefore does not include mirrored capacity.
Total Unconfigured	Disk capacity that has not been configured as a Symmetrix device. This includes capacity on disks that currently have no devices (unformatted) and capacity on disks where a portion of the disk has been configured (formatted).
Unconfigured Formatted	Amount of unconfigured storage capacity on disks that have hyper volumes (Symmetrix devices) configured.
Unconfigured Unformatted	Amount of storage capacity on disks that have no hyper volumes configured.
Total Unmapped	Total configured capacity not mapped to front end port.
STD Unmapped	Amount of storage capacity on STD devices that has been configured but not mapped to a front end port.
BCV Unmapped	Amount of storage capacity on BCV devices that has been configured but not mapped to a front end port.
RDF1 Unmapped	Amount of storage capacity on RDF1 devices that has been configured but not mapped to a host.
RDF2 Unmapped	Amount of storage capacity on RDF2 devices that has been configured but not mapped to a host.
Total Mapped	Total configured capacity mapped to front end port.
STD Mapped	Amount of storage capacity on STD devices that has been configured and mapped to a front end port.
BCV Mapped	Amount of storage capacity on BCV devices that has been configured and mapped to a front end port.
RDF1 Mapped	Amount of storage capacity on RDF1 devices that has been configured and mapped to a host.

RDF2 Mapped	Amount of storage capacity on RDF2 devices that has been configured and mapped to a host.
Total Unallocated	Total capacity of devices that are not allocated to a host.
STD Unallocated	Capacity of STD devices not allocated to a host.
BCV Unallocated	Capacity of BCV devices not allocated to a host.
RDF1 Unallocated	Capacity of RDF1 devices not allocated to a host.
RDF2 Unallocated	Capacity of RDF2 devices not allocated to a host.
Total Allocated	Total capacity of devices allocated to a host.
Unprotected Allocated	Capacity of unprotected devices allocated to a host.
RDF1 Allocated	Capacity of RDF1 devices allocated to a host.
BCV Allocated	Capacity of BCV devices allocated to a host.
RDF2 Allocated	Capacity of RDF2 devices allocated to a host.

Symmetrix with Largest Unconfigured Capacity

Symmetrix	Symmetrix serial number.
Name	Name of the Symmetrix.
Total Unconfigured	Disk capacity that has not been configured as a Symmetrix device. This includes capacity on disks that currently have no devices (unformatted) and capacity on disks where a portion of the disk has been configured (formatted).
Model	Symmetrix model number.
Micro Code Version	Symmetrix microcode level.
Configured Capacity	Amount of usable storage capacity configured as Symmetrix devices. Note, this is usable capacity and therefore does not include mirrored capacity.
Unconfigured Formatted	Amount of unconfigured storage capacity on disks that have hyper volumes (Symmetrix devices) configured.
Unconfigured Unformatted	Amount of storage capacity on disks that have no hyper volumes configured.
Total Unmapped	Total configured capacity not mapped to front end port.
STD Unmapped	Amount of storage capacity on STD devices that has been configured but not mapped to a front end port.
BCV Unmapped	Amount of storage capacity on BCV devices that has been configured but not mapped to a front end port.
RDF1 Unmapped	Amount of storage capacity on RDF1 devices that has been configured but not mapped to a host.
RDF2 Unmapped	Amount of storage capacity on RDF2 devices that has been configured but not mapped to a host.
Total Mapped	Total configured capacity mapped to front end port.
STD Mapped	Amount of storage capacity on STD devices that has been configured and mapped to a front end port.
BCV Mapped	Amount of storage capacity on BCV devices that has been configured and mapped to a front end port.
RDF1 Mapped	Amount of storage capacity on RDF1 devices that has been configured and mapped to a host.
RDF2 Mapped	Amount of storage capacity on RDF2 devices that has been configured and mapped to a host.
Total Unallocated	Total capacity of devices that are not allocated to a host.
STD Unallocated	Capacity of STD devices not allocated to a host.
BCV Unallocated	Capacity of BCV devices not allocated to a host.
RDF1 Unallocated	Capacity of RDF1 devices not allocated to a host.
RDF2 Unallocated	Capacity of RDF2 devices not allocated to a host.
Total Allocated	Total capacity of devices allocated to a host.
Unprotected Allocated	Capacity of unprotected devices allocated to a host.

RDF1 Allocated	Capacity of RDF1 devices allocated to a host.
BCV Allocated	Capacity of BCV devices allocated to a host.
RDF2 Allocated	Capacity of RDF2 devices allocated to a host.

Symmetrix with Largest Number of Free Disk Slots

Symmetrix	Symmetrix serial number.
Name	Name of the Symmetrix.
Free Disk Slots	Count of open disk slots on this Symmetrix.
Model	Symmetrix model number.
Configured Storage	Amount of usable storage capacity configured as Symmetrix devices. Note, this is usable capacity and therefore does not include mirrored capacity.
Microcode Level	Symmetrix microcode level.
Microcode Date	Date of Symmetrix microcode.
Microcode Patch Level	Symmetrix microcode patch level.
Patch Date	Date of latest microcode patch.
Cache Size	Total size of configured cache.
Total SCSI Ports	Count of all SCSI ports on the Symmetrix.
Used SCSI Ports	Count of used SCSI ports.
Avail SCSI Ports	Count of available SCSI ports.
Total Fibre Ports	Count of all fibre ports.
Used Fibre Ports	Count of used fibre ports.
Available Fibre Ports	Count of available fibre ports.
Open Channel Ports	Count of open channel ports.
# 18GB Disks	Count of 18GB disks.
# 36GB Disks	Count of 36GB disks.
# 47GB Disks	Count of 47GB disks.
# 50GB Disks	Count of 50GB disks.
Total Disk Slots	Count of all disk slots.
Total Drive Size	Total size of the drive.

For a printable copy of the report, click **Print** at the top of the report. On the Print dialog box choose the printer, set printing options, and click **Print.**

To make changes to the report, click **Export** at the top of the report. The File Download dialog box appears. Select **Open this file from its current location**. The report exports in comma-separated values (.csv) format and populates a Microsoft Excel spreadsheet.

Related topics

- Running a report
- Saving a report
- Viewing report properties
- Utilization and Free Space reports

Troubleshooting

Troubleshooting alerts and autofixes

For troubleshooting tips on alerts and autofixes, see:

- Alert does not trigger as expected
- Autofix does not run
- Too many alerts appear in Console

Alert does not trigger as expected

Ensure that:

- You have used the correct syntax to specify the alert key (or source). For syntax rules, see the specific alert description in the online Help.
- You have attached a schedule to the alert.
- Enough time has passed for the ControlCenter to evaluate the alert. (For example, if you have attached a schedule that causes ControlCenter to evaluate the alert every hour, wait for an hour to pass.)
- The alert is enabled and you have selected at least one alert severity level.
- The alert's management policy is set up to send notification to your Console.
- The alert's spike controlling values are configured properly. The **Before** field in the alert definition indicates how many consecutive times an alert must evaluate to true before ControlCenter triggers the alert.
- Another user has not reset or removed the alert.
- There are no additional requirements for the alert. See the alert description in the online Help for requirements.

See also:

- Viewing all alert definitions
- Editing an alert

Autofix does not run

If your autofix command does not run when the alert it is attached to triggers, ensure that:

- You have used the proper syntax to specify the autofix command.
- Files or programs referenced in a script are in the same directory as the script or have their complete path specified in the script.
- On Windows, you have included `cmd.exe /c` in front of the command and you have specified an executable.

See also Creating an autofix.

Too many alerts appear in Console

If too many alerts appear in your Console, there are several steps you can take to reduce the display, such as applying management policies and disabling alerts that are not important to you.

See also Reducing the number of alerts that display.

Related topics

- Introduction to alerts
- Understanding alert terminology
- Alert concepts and procedures

Troubleshooting context-sensitive help

If you notice that context-sensitive help only displays the help navigation pane, shut down and restart the console. This will reactivate context-sensitive help.

Related Topics

- Getting help with Help
- Contacting EMC

Novell: Troubleshooting host agents

If you are having trouble executing commands on a Novell NetWare server or seeing NetWare servers through the ControlCenter Console, consider the following problems and solutions before contacting technical support.

Problem: I receive the error No privileges for this operation.

Problem: My Host Agent for Novell returns very limited information about my Novell network.

Problem: I cannot see my NetWare 4.x servers.

***Problem*: I receive the error *No privileges for this operation*.**

Solution: Log on to your Novell network with a username that has greater privileges on your NDS tree. To log on using another username and password, first clear the currently buffered username and password, and then perform an operation that requires user privileges. The User Authentication dialog box prompts you to authenticate on your Novell Network. This approach works only if the error occurred when performing a function that prompted for user authentication information. If this problem occurs in general processing, then the ControlCenter administrator agent must re-configure the agent to use a different login account. Note that the agent uses a background account for most of its processing.

***Problem*: My Host Agent for Novell returns very limited information about my Novell network.**

Solution: Re-install the Host Agent for Novell. Your Host Agent for Novell references the username and password that you provided during agent installation when performing commands on your Novell network. If the username and password, which are stored in the `ndsconfig.ini` file in the agent's installation directory, do not have the necessary privileges to explore and take action in your NDS tree, your agent's ability to provide information and to execute commands will be very limited. To fix this problem, remove and then re-install the agent on your NetWare host, specifying the new username and password during the installation process.

***Problem*: I cannot see my NetWare 4.x servers.**

Solution: Enable IPX networking. NetWare 5.x servers can use IP or IPX addressing for connectivity. NetWare 4.x servers use IPX addressing only. If you do not have IPX addressing enabled upon the Windows NT or Windows 2000 host on which the agent is running, the agent will not be able to see NetWare 4.x servers. To solve this problem, enable IPX addressing on the Windows host, or contact your Windows administrator for more information about addressing on your LAN.

Related topics

- Checking the status of the Host Agent for Novell
- Agent Inactive alert
- How the Host Agent for Novell operates
- Contacting EMC Technical Support
- Host Agent for Novell overview

Troubleshooting the Host Agent for Windows

See the following for troubleshooting tips:

- Open Files command does not work
- Cannot view contents of Recycle Bin or contents inaccurate
- Cannot view performance statistics for logical and physical disks
- Browsing event logs returns no data or is slow

Open Files command does not work

You may encounter problems if the Host Agent for Windows driver is not installed on the system running the agent. The following functions do not work without the driver:

- Open Files command
- File I/O logging

The driver is installed as part of a normal installation of the agent.

Cannot view contents of Recycle Bin or contents inaccurate

To see the contents of and empty the Recycle Bin, the Host Agent for Windows requires Internet Explorer version 4 or later to be installed. In addition, the Active Desktop component of Internet Explorer must be installed, although Active Desktop does not have to be active.

Cannot view performance statistics for logical and physical disks

The logical and physical disk counters must be enabled on your Windows NT or Windows 2000 system for the physical and logical disk snapshot commands to work.

See Windows: Enabling disk counters

Browsing event logs returns no data or is slow

Depending on the size of the event log and the capacity of your network, it may take several minutes for the agent to retrieve all the event log messages. The Host Agent for Windows provides several alerts and autofixes to help manage the event logs. These alerts, which trigger based on the size of the event logs and allow you to back up and clear the event logs automatically, can help you keep your event logs at a manageable size.

See Windows: Monitoring event logs, Windows: Event log size alerts

Related topics

- Host Agent for Windows administration
- Host Agent for Windows overview

UNIX: Troubleshooting host agents

If you are having trouble executing commands on a UNIX host or trouble seeing AIX, HP-UX, or Solaris hosts through the ControlCenter Console, consider the following problems and solutions before contacting technical support.

***Problem*: I receive the error *No privileges for this operation*.**

Solution:

Some operations require specific-user or superuser privileges on the host. If the user ID and password that you are currently using for the host do not give you the necessary privileges, you may need to clear the current buffered user ID and password information and then retry the command. ControlCenter will then prompt you for the necessary user ID and password before carrying out the operation.

***Problem*: I believe that VERITAS Volume Manager is installed on my Solaris host, but I cannot use the agent to access Volume Manager functionality.**

Solution:

You can test if VERITAS Volume Manager is installed on a Solaris host by using the command `pkginfo`. If VERITAS information is returned by the command, Volume Manager is installed. The agent uses the command `pkginfo VRTSvxvm` to detect VERITAS. If you cannot detect VERITAS using this method, the agent may have trouble doing so as well.

This issue may also arise if the superuser account used by the agent on your Solaris host does not have a *PATH* environment variable pointing to VERITAS-installed commands.

Related topics

- Checking the status of your UNIX Host Agents
- Host Agents for AIX, HP-UX, and Solaris administration
- Agent Inactive alert
- How the UNIX Host Agents operate
- Contacting EMC Technical Support

Glossary

A	
active alert	An alert for which one or more trigger values have been met. Active alerts display in the Active Alerts view in the Console. Respond to an active alert by right-clicking it and selecting from a list of available commands. An active alert displays until you remove or reset it or the conditions that caused the alert to trigger are alleviated.
Administration folder	A folder in the tree panel that contains a hierarchical tree of ECC administration objects, organized by task: alert management, data collection policies, security management, and so on. Drilling down through the hierarchy displays increasing levels of detail, such as specific definitions and templates.
agent	A program, running on a system, that takes action on behalf of an administrator or user. A ControlCenter agent typically acts on policies, monitors, collects data, and executes commands initiated at the Console.
alert	An expression, based on a metric, that triggers notification when it is observed. For example, an alert could be triggered when 95% or greater storage utilization occurs for a particular device.
alert definition	An alert for which keys, trigger values, and a schedule have been defined, and optionally autofixes and a management policy. You create alert definitions using the alert templates or by copying existing alerts. *See also* management policy.
alert schedule	Defines when ControlCenter should evaluate an alert. In a schedule, you can define the interval at which the evaluation occurs (every 10 seconds, minutes, hours, and so on), the days of the week, and the days of the year. ControlCenter provides several predefined schedules, and you can define additional ones. One predefined schedule is "Agent Controlled". You cannot edit this schedule. It is used in cases where ControlCenter uses intercepts or drivers that rely on an event occurring (for example, a message being written to a log file or ControlCenter itself completing a task).
alert type - count	A count alert monitors values that can be calculated, such as the percentage of free space in a file system or the size of a file. Count alerts have numeric values for the triggers.
alert type - state	A state alert evaluates whether a condition is true or false, such as whether a subsystem or database is active or whether an important file was backed up. State alerts have TRUE or FALSE as the trigger value.
allocated capacity	The amount of storage made available to hosts connected to a Symmetrix system. In a direct-connect (SCSI or ESCON) environment, Symmetrix devices are considered allocated as soon as they are mapped to a front-end port. In a SAN (Fibre Channel) environment, Symmetrix devices are considered allocated when Volume Logix allows access from a specific host to those devices.

authentication agent	A process that maintains user IDs and passwords.
authorization	A mechanism within ControlCenter allowing you (the ControlCenter administrator) to control user access to hosts, Symmetrix systems, and the ControlCenter security management system. You create authorization rules for users or user groups. Although you can only create one authorization rule per user or user group, the security management system provides endless flexibility by allowing you to include users in multiple groups and to nest groups within other groups. Users inherit the authorization rules of the groups to which they belong and, similarly, groups inherit the authorization rules of the groups in which they are nested.
authorization rules	A set of permissions assigned to ControlCenter users and user groups. For example, you might create an authorization rule that grants the user group SymmetrixAdmins permissions to use the TimeFinder and SRDF applications for managing Symmetrix systems. Unless the users are granted these permissions by some other rule, ControlCenter would prevent users not in the SymmetrixAdmins group from making changes to Symmetrix devices.
autofix	An action that ControlCenter can perform automatically when an alert triggers, such as backing up or clearing a log file. ControlCenter provides some autofixes; you can also create your own using existing scripts, batch files, and executables, or by writing new ones.
B	
back-end configuration	The configuration of disk directors and physical disk devices in a Symmetrix system. Back-end components are responsible for staging data from the physical disk devices to cache and the subsequent destaging of data from cache back to the physical devices.
Backup Agent for TSM (Tivoli Storage Manager)	A ControlCenter agent that allows you to monitor your TSM backup systems, looking for events that you define, such as failed backups and increasing space utilization. TSM is a storage management system to manage business information in an enterprise-wide Storage Area Network (SAN) and traditional network environment.
Business Continuance Volume (BCV)	A Symmetrix device that represents an additional mirror image of a standard device. The BCV can be dynamically synchronized, and split at any time, to create point-in-time copies of data. While a BCV is split from the device, it can be allocated to a host. BCVs are located in the same Symmetrix system as the devices they are mirroring.
C	
Celerra File Server	An EMC high-end network file server composed of two cabinets -- one cabinet contains the Symmetrix system, and the other cabinet contains the Celerra File Server components.
CLARiiON	An EMC midrange, scalable, full Fibre Channel storage array.
client	A host that runs the ControlCenter management applications.

Command History	A function within the ControlCenter Console monitoring group that provides a tabular view of the ControlCenter active commands associated with managed objects. It shows who executed which command on which object when.
Common Array Manager	The ControlCenter product that encompasses support for storage systems from other manufacturers such as Compaq StorageWorks, HDS/HP, RVA/SVA, and IBM ESS.
configured capacity	The amount of storage capacity configured into Symmetrix devices. It is the usable capacity (the amount of storage a host can use to build a file system or database). *See also* unconfigured capacity.
connected	In regard to fabrics, a state where all the units comprising the fabric have physically intact links between them to conduct I/O transactions from any unit to any other unit in the fabric. A fabric could have some physical links down and still be connected if there are sufficient physical links to allow I/O to and from all of the units.
Connectivity Agent for SDM	A ControlCenter agent that monitors the VCM database on each Symmetrix system for storage access control configuration changes. The SDM (storage device masking) Agent discovers volume access control information for each Symmetrix system in a storage network and updates the Repository with configuration changes.
Connectivity Agent for SNMP	A ControlCenter agent that manages information gathered by generic SNMP agents in the storage network, updates the Console with current connectivity settings, executes data collection policies, and generates alerts. It is generally installed on the same host as the ECC Server.
Connectivity Agent for Switches	A ControlCenter agent that monitors switch status through vendor-supplied software. The Connectivity Agent for Switches discovers topology and fabric information for switches, runs data collection policies to monitor topology and fabric status, and updates the Repository with switch connection data. Typically, a single instance of the Switch Agent is installed.
connectivity device	Any device that indirectly connects hosts with storage arrays. They may also be devices that allow connections to other connectivity devices, but with the ultimate purpose of connecting hosts to storage arrays. Examples include: switches, hubs, bridges, and patch panels.
Connectivity folder	A folder in the tree panel that contains a hierarchical tree of connectivity objects, organized by connectivity device, links, or unknown ports. Drilling down through the hierarchy displays increasing levels of detail, such as specific switches and ports.
Console	The user interface to ControlCenter. It provides the core functionality; other applications are built into the Console as plug-ins. The Console allows the user to manage objects, views, and actions together in an intuitive flow, to achieve a particular task.
D	

database agents	A collective term for the ControlCenter agents that monitor or manage host databases. Database agents are provided for Oracle and MVS DB2. The agent typically gathers configuration, status, and performance data from the database and may support control actions.
Database Tuner (Symmetrix)	An EMC application that analyzes database and storage objects (for example, an Oracle database and Symmetrix system) from a single location. It monitors and tunes the database object for improved database performance, optimizes it for the storage object, and identifies storage devices that are causing bottlenecks for database access.
data collection policy	A formal set of statements used to manage the data collected by ControlCenter agents. A policy specifies the data to collect and the collection frequency. Most agents have associated predefined collection policies and collection policy templates that can be configured through the ECC Administration task.
data collection policy template	A template that provides default values for the creation of new collection policies. ControlCenter provides one or more policy template for each agent. You can configure your own policies by modifying the collection policy templates.
device group	A group of devices that can be managed using a single device group name. ControlCenter allows you to view, create, and modify SYMCLI device groups and to perform operations on the device group. Device groups (unlike ControlCenter "groups") are associated with a particular host and Symmetrix. For example, you might set up a group of all devices used by a particular host. Another group might be all devices used in a particular database. *See also* group.
device reallocation volume (DRV)	A non-user-addressable device within the Symmetrix that is designated to act as the temporary staging area while a pair of Symmetrix devices are swapped by the Optimizer product.
discoverable object	An connectivity device in the storage network that can be identified by an agent. The following attributes of the object must be identified: IP address, world wide name (WWN), ports, neighboring switches, type, management information base (MIB), Fibre Channel adapter (FA) port, director, and serial number.
discovery	The process of identifying storage systems, hosts, ports, links, switches, and other objects in the storage network. Discovery is performed by the Storage Agent for Symmetrix and Host Agent once they are installed, according to a predefined discovery policy. The user initiates discovery of other objects in the topology using the SNMP Collector, ESN Switch Agent, ESN SDM Agent, Oracle Agent, other ControlCenter agents, and various vendor agents. The agents collect data from the objects in the storage network and correlate it in the Repository. Once the discovered data is in the Repository, it remains persistent and adheres to normal update, delete, and rediscovery constraints.

E	
ECC Server	The primary interface between the Console(s), Repository, and agents. It also provides many of the common services to the ControlCenter infrastructure.
EMC ControlCenter	A family of products that enables you to discover, monitor, automate, provision, and report on host storage resources, networks, and storage across your entire information environment from a single console.
Enterprise Storage Network (ESN)	A storage network implementation that integrates products, technology, and services offering universal data access for every major computing platform, operating system, and application across any combination of SCSI, Ultra SCSI, Fibre Channel, and ESCON technologies.
Enterprise System Connection (ESCON)	A set of IBM and vendor products that interconnect S/390 computers with each other, with attached storage, and with other devices using optical fiber technology and dynamically modifiable ESCON directors.
F	
Framework Integration package (ControlCenter)	ControlCenter software that consists of a component that integrates ControlCenter into various third-party framework applications such as HP OpenView or CA Unicenter, and an agent (the Integration Gateway) that uses SNMP to monitor events and interface to the third-party application.
front-end configuration	The configuration of host channels, SCSI, ESCON, and Fibre Channel directors, ports, and Symmetrix logical devices. Front-end components are responsible for handling I/O requests from hosts and serving the data from cache.
functional device identifier (FDID)	A unique ID that the RVA or SVA uses for an MVS device.
G	
gatekeeper	A Symmetrix device accessible by the host through which the ControlCenter agent communicates with the Symmetrix. The gatekeeper routes low-level SYMAPI commands to the Symmetrix.
group	A group of objects that allows you to logically group hosts, Symmetrix systems, and other objects that ControlCenter manages. Creating object groups simplifies how you manage object permissions. For example, you can create an object group that includes all your UNIX hosts and then grant your UNIX administrators permissions to perform actions on those hosts.
H	
host agents	A group of ControlCenter agents that monitor or manage the host environment. Host agents are provided for AIX, HP-UX, Novell, Solaris, Windows, and various MVS subsystems. The agent typically gathers configuration, status, and performance data from the host on which it is running and may support control actions.
host bus adapter (HBA)	An I/O adapter that sits between the host computer's bus and the Fibre Channel loop, and manages the transfer of information between the two channels.

Hosts folder	A folder in the tree panel that contains a hierarchical tree of host objects, organized by operating system: Solaris, Windows, MVS, and so on. Drilling down through the hierarchy displays increasing levels of detail, such as specific hosts, databases, and tablespaces.
hot spare device	A powered up physical disk drive that a Symmetrix system can use in situations such as the failure of a standard (STD), R1, or R2 device.
hyper volume	The splitting of a physical disk into two or more devices. The host views hyper volumes as individual physical devices. Also called Symmetrix device (logical volume).
I	
infrastructure	A collective term that describes the base ControlCenter components: ECC Server, Store, and Repository.
Integration Gateway	A ControlCenter agent that provides an interface from the ECC Server to management framework applications such as HP OpenView Network Node Manager, Tivoli NetView, or the CA Unicenter TNG Framework, enabling those applications to display ControlCenter information. *See also* Framework integration package.
L	
login history table (LHT)	A table residing on Symmetrix systems that contains the current and historical login information of host HBAs logging into each FA in a Symmetrix system. The information in the table can be used to track changes in a configuration.
log file	A file (one for each ControlCenter component) that contains output messages from component execution. Log files contain messages with different levels of output that indicate message severity. When a log file reaches a maximum size, a new log is created. The number of log files per component is configurable; the default is five. Once the maximum number of logs are created, the first log is reused.
logical device configuration	The process of defining additional storage capacity from unconfigured space within a Symmetrix system.
logical unit number (LUN)	An addressing model for devices in which each separately addressable logical unit in a storage system has a unique LUN ID, which is a hexadecimal number. The default ID for the first new LUN is the smallest available one; for the next new LUN, it is the next smallest available, and so on.
M	
managed object	Hosts, databases, file systems, storage systems, switches, and other connectivity devices in the storage network that can be managed by ControlCenter.

management information base (MIB)	A formal description of each network object and storage component, organized in a hierarchical tree structure. The information for each object is addressed using an object identifier (OID). An application typically reads or writes the information for each object using a network management protocol like SNMP. A basic MIB is defined as part of SNMP. All other MIBs are extensions of this basic MIB. Therefore MIBs (or more accurately, MIB extensions) exist for each set of related network entities that can be managed.
management policy	A formal set of statements that defines the users (scripts, SNMP trap, and so on) that ControlCenter should notify when an alert triggers, and how those users should be notified. Notification options include: a message through the Console, an e-mail, and a message to a management framework such as Hewlett Packard's OpenView.
mapped capacity	Devices that are mapped to front-end ports on a Symmetrix system. Host systems cannot access device unless they are mapped to front-end ports. *See also* unmapped capacity.
Master Agent	A ControlCenter agent that manages the installation, starting, and stopping of other agents on the host. Required on every host running an agent (except for the Connectivity Agent for SNMP).
media repository	An area on the ECC Server to which ControlCenter components are downloaded before they are installed. Installation and licensing information is captured and shared through the media repository tables.
meta device	Meta devices are Symmetrix devices concatenated together to form a larger device. The Symmetrix devices forming the meta device are all accessed through the same target/LUN value. The SDR component reports the Symmetrix meta device number as the device number of the first device in the group, which is also known as the meta head. The remaining members of the group are known as meta members.
mirroring	The concept of maintaining data on both a production volume and a mirror volume. RAID technology (for example RAID Level 1) provides various levels of mirroring at the physical disk level. TimeFinder uses local mirroring to protect data at the logical volume level by maintaining data on both a production volume and a mirror volume within the same storage unit. SRDF uses remote mirroring, which is similar to local mirroring except that the production volume resides in one storage unit while its mirror resides in a different storage unit.
MVS (OS/390)	An operating system from IBM that is installed on most of its mainframe and large server computers. Payroll, accounts receivable, transaction processing, database management, and other programs critical to large businesses typically run on an MVS system.

N	
Navisphere	An EMC application that manages storage for CLARiiON storage systems. It configures, monitors, and tunes CLARiiON disk arrays, provides the Console with the status of CLARiiON systems, and indicates when an alert occurs by changing the color of the CLARiiON icon.
net capacity load (NCL)	In an RVA/SVA storage array, a statistic measuring the percentage of actual total physical capacity of the subsystem or one of its partitions (test or production). A value of 70 to 80 is considered normal for NCL.
O	
OnAlert	An EMC application that provides remote support functionality and, optionally, dial-home capability to Symmetrix systems.
Open Integration Components	The ControlCenter product encompassing the set of common services available to all EMC ControlCenter/Open Edition products, including centralized install, agents for all managed entities, login and access control administration, a Repository, and so on.
Optimizer	A separate product that automatically collects, analyzes, and dynamically balances physical drive I/O load by swapping Symmetrix devices.
P	
Performance view	A view displaying Symmetrix performance statistics about various objects available within ControlCenter. For each object, ongoing real-time data can be displayed in chart form, or point-in-time data can be displayed in table form.
permissions	A set of permissions granted to a ControlCenter user that grant permission to perform specific actions on specific objects. A user's permissions are controlled by an authorization rule applied directly to the user, plus those permissions the user inherits from the user groups to which they belong. ControlCenter provides several default permission sets. The ECCAdministrators Rule is a set of permissions created by default when you first start the ECC Server. It grants to members of the ECCAdminstrators user group all permissions on all objects. The rule is intended for initial set up of your ControlCenter groups and permissions.
point/record	In Workload Analyzer, a point or a record represents the value of data collected by an agent at a specific time. For example, if the agent collects statistical data every 15 minutes, the data collected at 8:15 is represented by one point or one record. When looking at a WLA Performance view graph, each value is represented by one point on the graph. However, when talking about Performance Archives, Revolving data, and Analyst data, you can use the terms record and point interchangeably.
port flags	Settings assigned to front-end ports that tell a Symmetrix system how to communicate with different host types and how to behave in certain situations.
production partition	In the RVA or SVA subsystem, a classification assigned to drives in use (or available) for data storage. The production partition has no functional difference from the test partition.

proxy agent	A Symmetrix agent that provides indirect access to a host running the SYMAPI Server and directly connected to a Symmetrix system. The SYMAPI Server host receives requests for data or commands from the Symmetrix Agent, acts upon the data request or command, and replies to the Symmetrix Agent. A proxy host is typically used in a situation where the SYMAPI Server host is running on a platform not supported for the Symmetrix Agent, such as MVS.
Q	
quality of service (QoS)	A function within the ControlCenter Console that reduces the resources allocated for Business Continuance Volumes (BCVs) or SRDF copy operations on selected devices. QoS allows you to control the balance between standard and BCV/SRDF operations.
R	
RA group	A logical grouping of source (R1) or target (R2) devices associated with a remote link director. Up to 16 RA groups may exist in an SRDF configuration.
rediscover	A process that refreshes ControlCenter by retrieving the latest topology connection settings from the Repository.
Relationship view	A function within the ControlCenter Console that provides a complete mapping of host objects to Symmetrix devices, with physical, logical, and line-of-business views.
remote link director (RLD)	A two-port serial channel or Fibre Channel director microcode-configured as the link between the two Symmetrix systems in a Symmetrix Remote Data Facility (SRDF) configuration.
Reports folder	A folder in the tree panel that contains a hierarchical tree of ControlCenter and user-defined reports, organized by type. Drilling down through the hierarchy displays specific reports.
Repository	A central, relational database that contains the aggregation of all the data about your installation's managed environment.
Resource Availability	A ControlCenter application that allows platform-independent management of logical storage resources. Resource Availability: • Automates event response to storage resource issues, such as backup status and capacity utilization • Contains established business policies designed to improve service levels and availability • Eliminates the need for host-specific configuration and monitoring commands
rules	*See* authorization rules.
S	
schedule	A set of instructions that defines when ControlCenter events should occur, such as the evaluation of an alert or the collection of statistics. In a schedule, you can define the interval at which an event occurs (every 10 seconds, minutes, hours, and so on), the days of the week, and the days of the year. ControlCenter provides several predefined schedules, and you can define additional ones.
Server	*See* ECC Server.

SNMP Agent	Vendor software installed on connectivity devices that responds to management requests through the SNMP protocol. SNMP agents detect changes in the physical connectivity of devices in the SAN. Data generated by SNMP agents is used by the Connectivity Agent for SNMP to update the Console and generate alerts. One SNMP Agent can manage multiple devices.
Solutions Enabler	An EMC product included with ControlCenter that can manage and retrieve configuration, status, and performance information from Symmetrix systems. The Solutions Enabler components include SYMCLI, SYMAPI, and SYMAPI Server.
spares partition	In the RVA or SVA subsystem, the classification assigned to drives that have passed media acceptance testing but are currently unused for data storage. Such drives are called spares.
SRDF (Symmetrix Remote Data Facility)	A ControlCenter plug-in (optional application) that manages business continuance and disaster recovery operations using remote mirroring.
Status Acknowledged folder	A folder in the tree panel in which you can store managed objects that have a warning or error status. If you drag an object that has a warning or error status on it (yellow caution or red X) into this folder, then the object's status will not propagate up the tree causing a parent icon to show the warning or error icon when that parent is collapsed. The purpose is to acknowledge that you saw the status condition without being reminded of it through the parent object.
storage agents	A group of ControlCenter agents that monitor or manage storage arrays. Storage agents are provided for Symmetrix, CLARiiON, Celerra, Compaq StorageWorks, HDS, RVA/SVA, and IBM ESS storage arrays. The agent runs on a host connected to the storage array and typically gathers configuration, status, and performance data and may support control actions.
storage allocation	The process of finding and configuring suitable storage space for use by a host.
storage area network (SAN)	A special-purpose network (or sub network) that interconnects different kinds of data storage devices with associated data servers on behalf of a larger network of users. Typically, a SAN is part of the overall network of computing resources for an enterprise. A SAN is usually clustered in close proximity to other computing resources, but may also extend to remote locations for backup and archival storage, using wide area network carrier technologies such as asynchronous transfer mode or synchronous optical networks.
storage device masking (SDM)	An access control mechanism for Symmetrix systems that regulates which host bus adapters in a Fibre Channel environment can access specific Symmetrix volumes. Synonymous with LUN masking.

Storage folder	A folder in the tree panel that contains a hierarchical tree of storage system objects, organized by type: Celerra, CLARiiON, HDS, StorageWorks, Symmetrix, and so on. Drilling down through the hierarchy displays increasing levels of detail, such as specific storage systems, host directors, and individual storage devices.
StorageScope	A ControlCenter optional application that addresses the storage metering and capacity planning requirements of organizations interested in consolidating their storage, and improving their storage utilization and asset management.
Store	A ControlCenter infrastructure component that populates the Repository with data from the agents, and controls the sending and receiving of data between the agents and the Repository.
Symmetrix	An integrated cache disk array (ICDA) storage array that provides centralized, sharable enterprise storage. It helps create an information infrastructure capable of managing large, complex ultra-dynamic storage area network (SAN) environments by consolidating storage from multiple heterogeneous hosts onto a single system.
Symmetrix Data Mobility Manager (SDMM)	An EMC application that allows you to configure, monitor, and manage the replication of data between Symmetrix devices.
Symmetrix Device Reallocation (SDR)	A function within the ControlCenter Console storage allocation task that allows you to map Symmetrix devices to the front-end director ports of the Symmetrix system. You must map a device to one or more front-end ports to make it available to a host.
Symmetrix Manager	A set of functions accessed from within the ControlCenter Console that allows the user to monitor the status, performance, and configuration of Symmetrix systems and to perform active Symmetrix commands such as TimeFinder, SRDF and configuration changes. The Symmetrix Manager also allows you to modify the configuration of a Symmetrix system. The controllable areas include logical device allocation, device type definition, metadevice configuration, SDR, and port flag settings.
T	
tape agent	A ControlCenter agent for MVS that manages tape systems. It has functions for a Virtual Tape Server (VTS) tape system, a CA-1 tape software package by CA, a StorageTek tape silo environment, and RMM (Removable Media Manager—a software product by IBM).
target panel	The right panel in the Console, displaying one or more views of task data for the managed object(s) currently selected in the tree panel.
taskbar	A blue bar, located by default below the menu bar, providing access to five task buttons: Storage Allocation, Monitoring, Performance Mgt, ECC Administration, and Data Protection. Clicking a task button opens a drop-down menu offering a selection of views.

template	A set of default values for the creation of new alerts. ControlCenter provides templates for every alert. You can specify your own default settings by modifying the alert templates.
test partition	In the RVA or SVA subsystem, a classification assigned to drives in use (or available) for data storage. The test partition has no functional difference from the production partition.
TimeFinder	A ControlCenter plug-in that allows customers to use Business Continuance Volumes (BCVs) to provide a local mirror of Symmetrix devices, while the standard devices are online for regular host operations.
time window	In the context of Optimizer, a period in time during which an aspect of Optimizer's behavior is controlled. *Performance* time windows allow you to specify which samples (past or future) Symmetrix Optimizer should consider when running its swap generation algorithm. *Swap* time windows allow you to specify when Symmetrix Optimizer should or should not perform swap activity.
topology	A description of the physical and logical configuration of the storage network, including storage systems, hosts, ports, connectivity devices, and connecting links.
topology discovery	A ControlCenter core function that automatically identifies storage, hosts, ports, links, switches, and other objects in a storage network. *See also* discovery.
topology editing	A ControlCenter feature that allows display in the topology map of objects that the Console cannot discover automatically. For example, some elements do not have software-based management interfaces (they are entirely hardware entities). Topology editing can depict those elements by providing the desired placement in the map and some basic properties of the object. The Topology Editing feature allows you to display this object in the map, and manually supply missing connectivity information. In addition to properties, user editing allows you to manually define an object's relationship to other entities in the topology map.
topology map	A ControlCenter core function that provides a picture of elements in the storage network. It depicts those objects selected in the tree panel and the connectivity relationships between them in a graphical display. For example, if you select a host, the topology map displays all children of the host and all connections for the host, such as HBAs, connections, switches, and storage. The topology map reflects the state of elements that are discoverable through the Connectivity Agent for SNMP.
tree panel	The left panel in the Console, displaying all the objects in the storage environment, organized by type.
trigger	The logical operator that evaluates an alert condition (for example, >90% storage utilization).

U	
unallocated capacity	The amount of storage formatted into Symmetrix devices but not yet allocated to a host. Unallocated capacity includes both mapped and unmapped devices but does not include unconfigured capacity. *See also* allocated capacity.
unconfigured capacity	The amount of storage capacity that remains unconfigured (often expressed in terms of the raw size of the physical drive, such as 36 GB). *See also* configured capacity.
uncollected free space	The space for deleted data that the RVA or SVA has been informed of (by Deleted Data Space Release (DDSR) processes) but has not yet freed.
undiscoverable object	An object in the storage network that cannot be identified by an agent. An object may remain undiscovered if an agent cannot identify any of the following attributes: IP address, world wide name (WWN), ports, neighboring switch, type, management information base (MIB), Fibre Channel adapter (FA) port, director or serial number.
unmapped capacity	Devices or capacity that have been configured, but not mapped to front-end ports on a Symmetrix system. Host systems cannot access volumes unless they are mapped to front-end ports. *See also* mapped capacity.
user groups	User groups simplify the management of ControlCenter user permissions. You can create authorization rules for user groups and grant permissions to users by including them in specific user groups. For example, you might create a WindowsAdmin user group that has full permissions on all Windows hosts. You would include all of your Windows administrators in that user group.
V	
VCM database	A database, residing on a Symmetrix system, that contains host access information for Symmetrix volumes. Each Symmetrix system has its own VCM database.
Visual Storage	A function in Symmetrix Manager that shows the configuration of a Symmetrix system. The view can include all directors, channels, cache, ports, and devices, as well as the links between them. You can configure Visual Symmetrix to your specific needs, such as to display disk devices that are serviced by any disk assembly, or to display which volumes are in RAID-S groups.
volume	A general term referring to a logical storage device. Synonymous with Symmetrix device.
Volume Logix	An EMC application that controls access to Symmetrix volumes. It avoids conflict, between host-based access control mechanisms, by using a single, centralized monitoring function. Using Volume Logix, you can define a virtual channel connecting each host with its storage volumes in a Symmetrix system, even though there may be many hosts sharing the same Symmetrix port.

W	
WLA Archiver	A ControlCenter agent that retrieves and archives collections of data from individual agents, and organizes (rolls up) collected data into summaries for the reports. The summarized data is saved to a data archive, separate from the Repository.
WLA Performance View	An optional ControlCenter application that is used for viewing historical and revolving performance and configuration data of Symmetrix systems, hosts, and Oracle databases. WLA Archiver manages the statistical data collected for historical analysis through WLA Performance View.
world wide name (WWN)	A unique 48- or 64-bit number assigned by a recognized naming authority (often via block assignment to a manufacturer) that identifies a connection or set of connections to a network. A WWN is assigned for the life of the connection or device.

Index