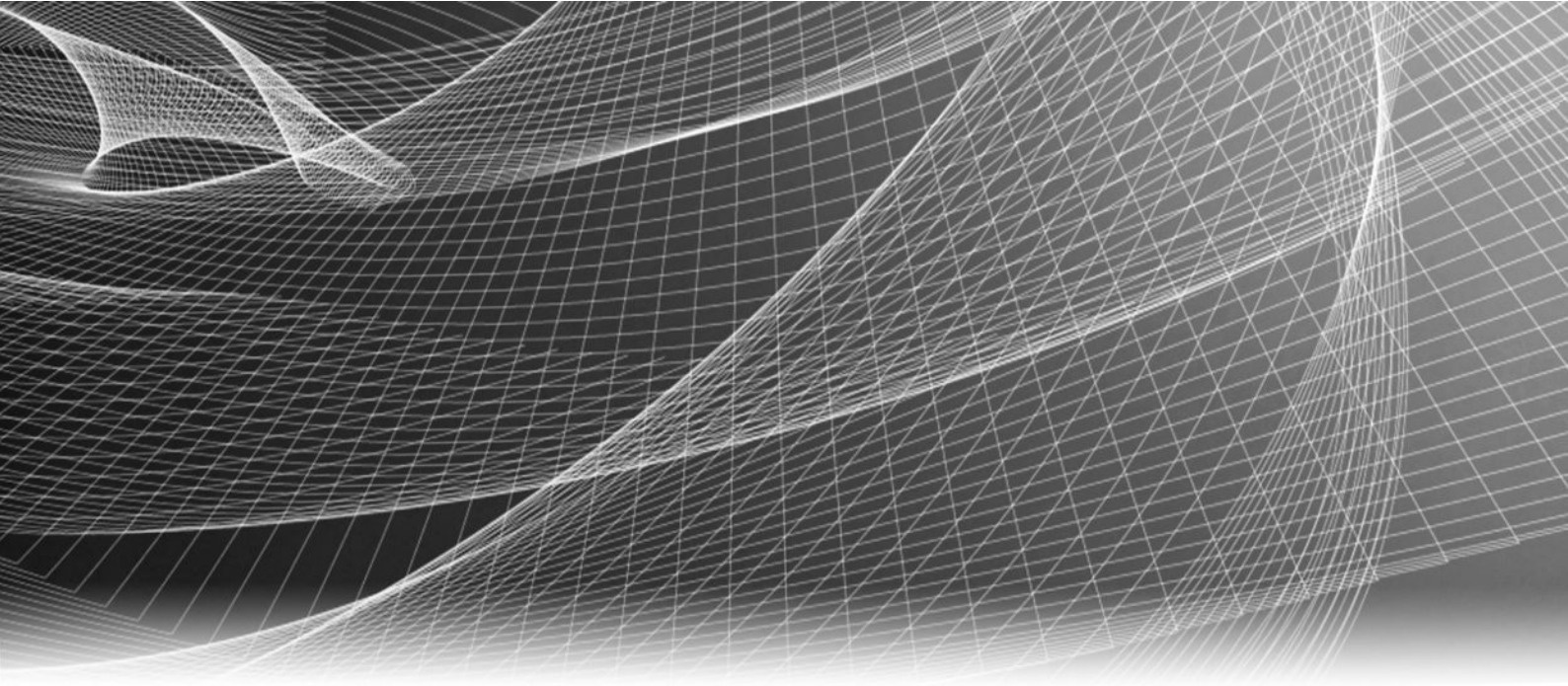


EMC®
ProSphere™

Version 2.0

Administrator Guide

P/N 300-015-290
04

EMC²

Published December, 2013

For the most up-to-date regulatory document for your product line, go to EMC Online Support (https://support.emc.com). For documentation on EMC Data Domain products, go to the EMC Data Domain Support Portal (https://my.datadomain.com).

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

TABLES

FIGURES

Preface

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function properly or does not function as described in this document.

Revision history

Revision	Date	Description
01	April 2013	Initial version for ProSphere 2.0.
02	June 2013	Initial version for ProSphere 2.0.1.0. New material in Rediscovery on page 97 and Discover file and block properties of unified storage on page 102. References to SMAS removed.
03	October 2013	Initial version for ProSphere 2.0.1.2. The following topics are modified: • Alert Model Table on page 72, includes the new OID, alertSourceCategory, and OCTET STRING instead of INTEGER OID syntaxes. • SNMP Notifications group on page 77, includes the new OID alertSourceCategory. • Alert notification examples on page 85, includes the new OID alertSourceCategory in the alert notification examples, and no longer includes"*<.id>*" in the SNMP trap example. • Important notes on the All Alerts view on page 88, includes the difference between Unisphere Remote and ProSphere alert messages.
04	December 2013	Initial version for ProSphere 2.0.1.3. The following topics are modified: • In the Overview on page 50 of the chapter on alerts, a note was added about SMC-SPA alerts. • In Alert notification examples on page 85, a table row was corrected.

Audience

This document is part of the EMC ProSphere documentation set. The document is intended for use by system administrators, security administrators, and integrators responsible for initiating discovery with ProSphere and performing standard system administration tasks.

Note

This document was accurate at publication time. Go to EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Special notice conventions used in this document

EMC uses the following conventions for special notices:

DANGER

Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

Addresses practices not related to personal injury.

Note

Presents information that is important, but not hazard-related.

Typographical conventions

EMC uses the following type style conventions in this document:

Bold	Indicates names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Indicates full titles of publications referenced in text
`Monospace`	Indicates: • System code • System output, such as an error message or script • Pathnames, filenames, prompts, and syntax • Commands and options
Monospace italic	Indicates variables
`Monospace bold`	Indicates user input
‹›	Indicates parameter or variable values supplied by the user
[ ]	Indicates optional values
|	Indicates alternate selections - the bar means “or”

Where to get help

EMC support, product, and licensing information can be obtained as follows.

Product information

For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com.

Technical support

Go to EMC Online Support and click Service Center. You will see several options for contacting EMC Technical Support. Note that to open a service request, you must

have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

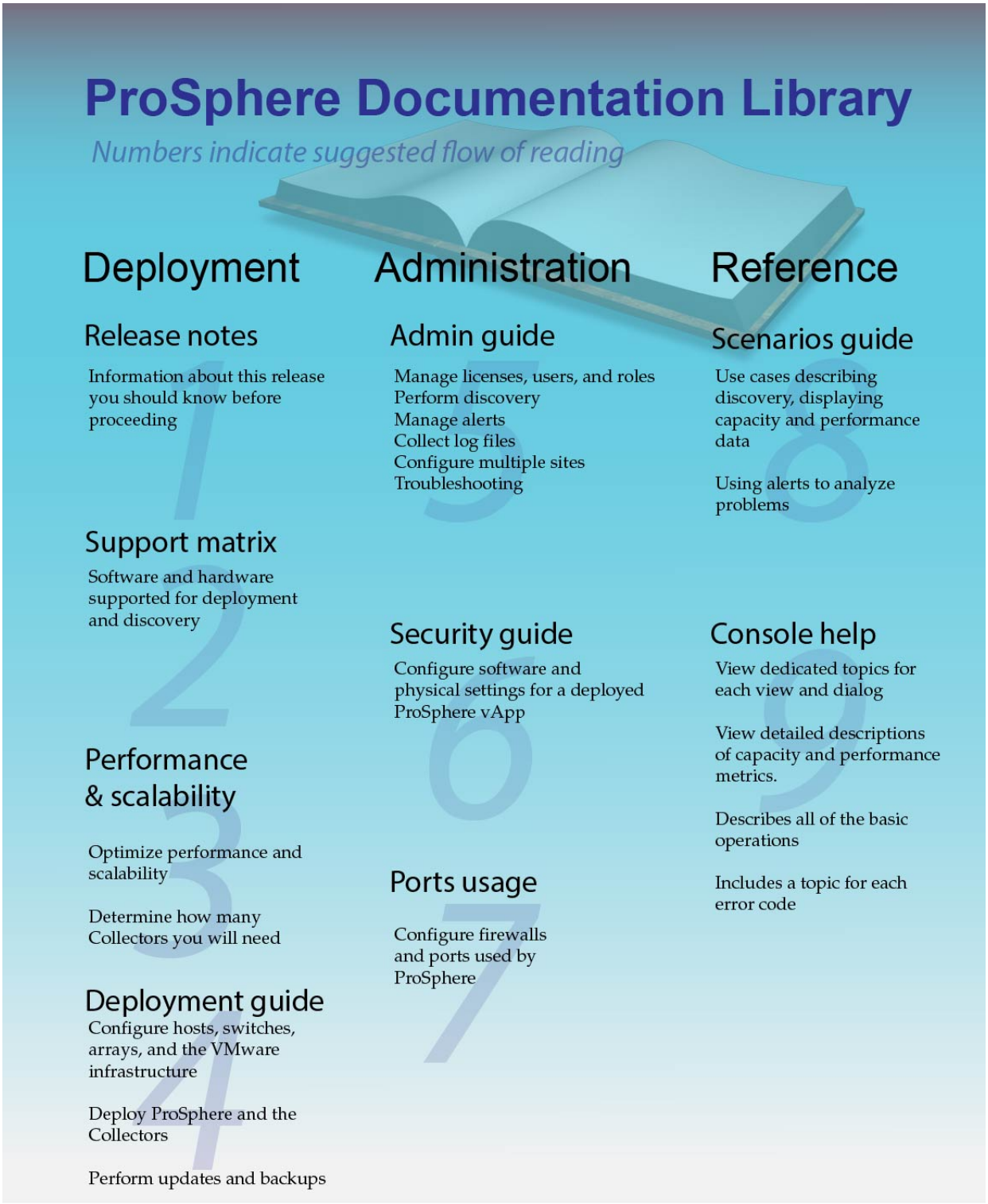
Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to techpubcomments@emc.com.

Your comments

`ProSphere_doc_comments@emc.com`

Documentation map



CHAPTER 1

ProSphere architecture

This chapter contains the following topics:

Overview

Recently, there has been an explosion in the quantity and variety of information that storage resource management applications must gather, process, and analyze. The infrastructure of a typical corporate data center has undergone profound changes due to the spread of heterogeneous environments and the commodification of storage.

Cloud computing models and virtualization technologies promise many benefits but they also create a new category of management challenges for data centers. Unfortunately, storage management products that were developed in the 1990s are struggling to meet the challenges of today's IT organizations.

EMC® ProSphere™ can handle the Web-scale challenges of a global enterprise, and it has the ability to support new hardware and emerging business models. In addition, ProSphere is easy to deploy and start up, providing fast integration into an IT environment.

Benefits of ProSphere

Some of the benefits of include:

- Ability to quickly add, move, and remove deployed instances of ProSphere as necessary
- Ability to detect, anticipate, and predict performance problems
- Ability to use policy-based data collection modes to support problem diagnosis
- Ability to view the full context of a problem to speed diagnosis
- Ability to produce summaries for operational managers, to enable efficient management of resources
- Ability to view the current status of storage infrastructure utilization
- Ability to identify current or anticipated problems in a storage infrastructure
- Ability to discover the elements in a network and view discovered inventory and object details
- Ability to view end-to-end paths of a selected object that appears on topology maps
- Ability to tag configuration items with meaningful attributes
- Ability to synchronize data between deployments of ProSphere
- Ability to dynamically scale ProSphere to meet the requirements of a data center
- Ability to share a distributed cache between virtual machines in a vApp, allowing ProSphere to scale to large environments
- Ability to avoid requiring complex firewall policies

Note

In ProSphere, virtual machines have embedded firewalls. ProSphere uses standard ports, which limits the number of required firewall changes.

ProSphere: virtualized storage management

ProSphere is deployed as a VMware vApp, a collection of interdependent virtual machines configured at the virtual machine level and at the vApp level.

virtual machine — "A software computer that, like a physical computer, runs an operating system and applications. Multiple virtual machines can operate on the same host system concurrently." [1]

These virtual machines run in one or more VMware ESX Server environments.

ProSphere is also a "virtual appliance."

virtual appliance — "A software solution composed of one or more virtual machines. A virtual appliance is packaged as a unit by an appliance vendor and is deployed, managed, and maintained as a unit."

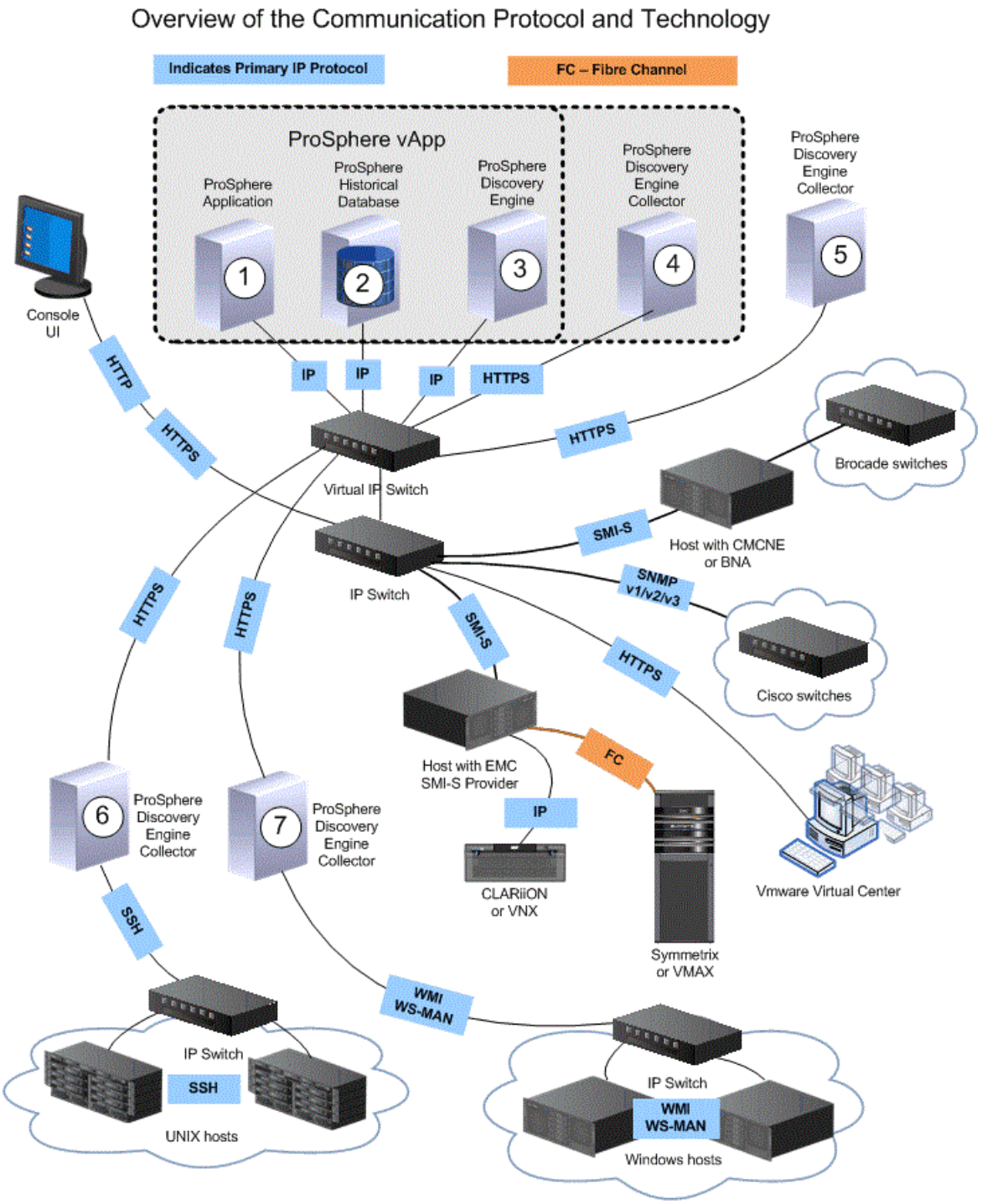
ProSphere deployment

A ProSphere deployment consists of the following VMware virtual machines: a Discovery Engine, a Historical Database, a ProSphere Application, and optionally one or more Discovery Engine Collectors.

Figure 1 on page 20 illustrates a ProSphere deployment. (The dotted line in the figure indicates the deployment.) The figure contains a sampling of the protocols and software, as well as the hosts, switches, and arrays that are associated with ProSphere deployments.

1. These definitions appear in the VMware Technical Publications Glossary at `http://www.vmware.com`.

Figure 1 ProSphere deployment



The figure shows the VMware virtual machines that constitute the core of ProSphere:

1. A *ProSphere Application* hosts the web server that provides access to the ProSphere Console and the applications running in it. A ProSphere Application houses important common services such as application security, application configuration, resource searching, and a distributed information cache for fast, distributed data access.
2. A *Historical Database* manages the storage of collected resource data, historical performance data, compliance information, configuration parameters, and other data that requires persistence.

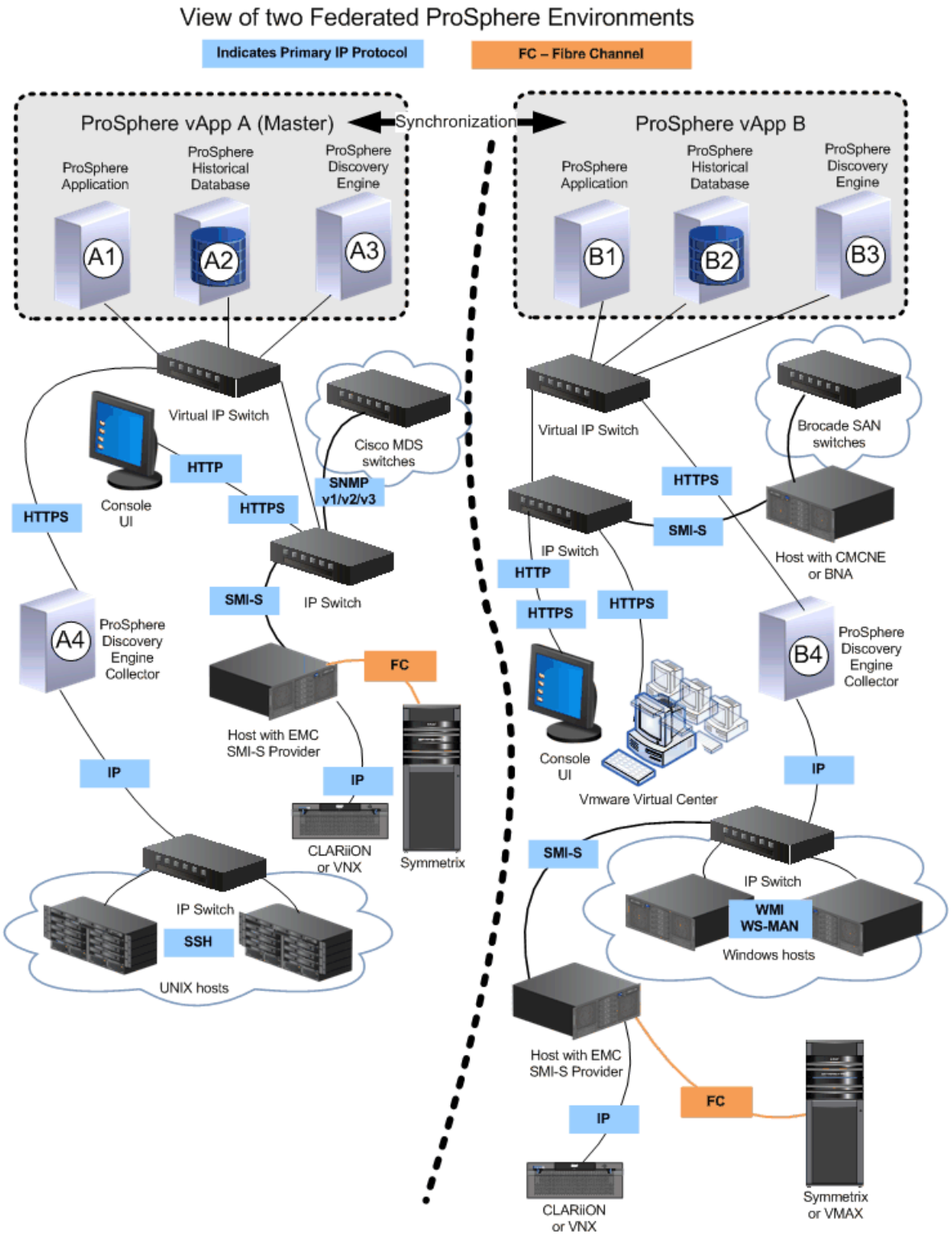
3. A *Discovery Engine* discovers managed resources in a data center and periodically refreshes data collected for these resources according to user-defined policies. Agentless discovery is supported. The Discovery Engine uses a variety of network protocols and standards-based interfaces to collect data from many network device types, such as hosts, storage arrays, and switches.

   When additional scalability is required, one or more Discovery Engine Collectors (Collectors) are added to the deployment and the Discovery Engine manages them. The figure illustrates a deployment with one Collector. A Collector focuses on collecting data from network resources. A Discovery Engine has load balancing and management capabilities that enable it to maintain multiple Collectors.
4. When additional scalability is required, one or more Discovery Engine Collectors are added to the deployment and the Discovery Engine manages them. ProSphere deployment on page 19illustrates a deployment with four Collectors (4. 5. 6. and 7 in the figure). One Collector (4) is shown protected by a firewall, and three Collectors (5, 6, and 7) are not. Each Collector focuses on collecting data from network resources. A Discovery Engine has load balancing and management capabilities that enable it to maintain multiple Collectors.

Scale out ProSphere with multiple deployments

You can deploy multiple instances of ProSphere for greater scalability or to represent logical, physical, or geographic boundaries in an enterprise. Figure 2 on page 22 illustrates an enterprise that uses two deployments of ProSphere.

Figure 2 Multiple deployments to scale ProSphere for an enterprise



Synchronize deployments

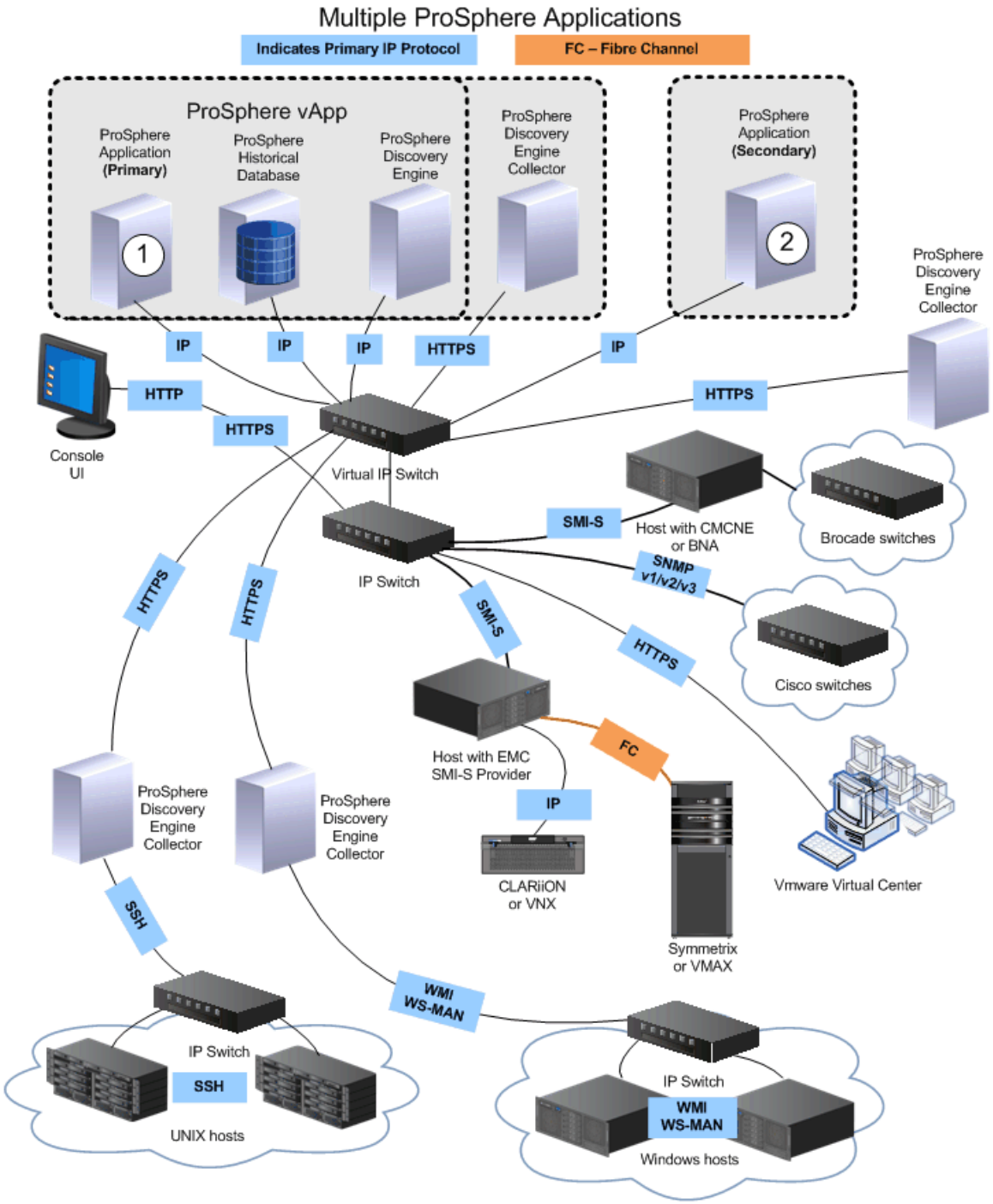
The ProSphere Applications in different deployments can be synchronized, as explained in Synchronize Data on page 137. Resource data collected by a ProSphere deployment

can be synchronized with resource data collected by other ProSphere deployments. Thus, each deployment of ProSphere in the enterprise can search data contained in other deployments. When deployments are synchronized, capacity data for all deployments is stored in one ProSphere Application selected as the Master Capacity Application.

Deploy a Secondary ProSphere Application

In rare cases, ProSphere collects an extremely large amount of performance data, large enough to degrade the performance of ProSphere. To correct this problem, you can add a Secondary ProSphere Application as shown in Figure 3 on page 24, which displays both the primary ProSphere Application (1) and the Secondary ProSphere Application (2).

Figure 3 Secondary ProSphere Application



Note

You must deploy a Secondary ProSphere Application outside of the initial vApp.

A Secondary ProSphere Application receives a share of data that is sent to the ProSphere Application. This results in increased CPU availability for the primary ProSphere Application and improved performance.

Note

The *EMC ProSphere Performance and Scaleability Guidelines* provides information about when to use a Secondary ProSphere Application.

Integration provides ease of use

Three types of integration contribute to ProSphere's ease-of-use as a storage resource management tool:

1. Single Sign-On

   Rather than require the user to establish identity with ProSphere and each of the element and fabric managers separately, the user only needs to establish identity once.

2. Launch In Context

   Symmetrix Performance Analyzer (SPA), Symmetrix Management Console (SMC), and Connectrix Manager Converged Network Edition (CMCNE) can be launched in ProSphere. These applications maintain the current context so the administrator can use them to focus on the same situation that was present in ProSphere.

3. Data integration

   Collecting data from element and fabric managers and combining it with data available through other data sources gives the user a larger view of the network and, where provided, a link to other useful products.

   Data from element and fabric managers augments alert, threshold, and performance data that is available from other data sources, including SNMP, SMI-S, and proprietary APIs.

Web-scale databases

Organizations increasingly face the need to maintain large amounts of data for long periods due to regulatory requirements. Organizations are realizing the importance of processing streams of real-time data. Given these new requirements, it is important that products that work with "Web-scale" levels of data use the right persistence and query mechanisms to deal with data of such magnitude.

The Historical Database hosts a Greenplum database, in which it stores the historical performance data collected by ProSphere. This includes data migrated from EMC ControlCenter® Performance Manager.

The integration of Greenplum technology into ProSphere adds new capabilities for the advanced analysis of performance and storage data. The main difference between Greenplum technology and other database software schemes has to do with how data is accessed. Greenplum divides data across multiple servers or segments, each of which has its own connection to a disk drive. Thus, a single database query can run against many segments of data simultaneously.

The ability to scale across machine boundaries is fundamental to achieving high levels of performance. Thus, ProSphere use the bigdata RDF store to hold all discovery and related alerting data. The bigdata RDF store is a horizontally scaled storage and computing fabric that supports optional transactions, high concurrency, and high aggregate IO rates. The bigdata RDF store was designed as a distributed database architecture running over clusters of hundreds to thousands of machines. The bigdata RDF store can also run in a high-performance single-server mode.

Discovery

The ability to track network resources and their usage is essential for data center environments. In order to do this effectively, one must be able to identify all elements in the network and monitor them. ProSphere collects key configuration information on data center assets using a variety of techniques.

After configuration information is collected, ProSphere can monitor network elements and fabrics for configuration changes, as well as monitor the performance of the elements. ProSphere collects key metrics from hosts, switches, and storage systems, making it a centralized solution for determining the likely causes of performance concerns.

The process of collecting basic information that identifies network elements is "discovery." Figure 1 on page 20 shows typical network elements, along with associated components and protocols.

Troubleshoot performance issues

ProSphere facilitates the troubleshooting of performance issues throughout a virtual network. System administrators can quickly identify where problems reside and evaluate impact at the physical and virtual layers.

After all objects in the network are discovered by ProSphere, you can switch on performance data collection for a host or for a group of hosts. This enables the collection of path performance data for all elements in the I/O paths that extend from the host or the group of hosts.

Two tiers of host data collection are available. One tier collects data from hosts at five-minute intervals; the other collects data from hosts and ESX servers at fifteen-minute intervals.

You can define alerts to trigger at specific performance threshold values. This allows ProSphere to signal problem situations before you would find evidence in a log.

You can correlate application problems with performance bottlenecks (points in the network where the flow of data is reduced) and determine how to rebalance the load among storage resources for effective use.

Charting and trending capabilities allow you to easily compare current performance data with historical performance data. Thus, you can study trends. You can use trend information to determine whether specific problems are temporary or recurring due to workload patterns.

Integration with the following element managers gives easy access to performance-related functionality:

- Symmetrix Performance Analyzer (SPA), which addresses Symmetrix array-based performance problems
- Symmetrix Management Console (SMC), which provides Symmetrix monitoring and array optimization features
- Connectrix Manager Converged Network Edition (CMCNE), which provides Brocade network management features

Note

Each day ProSphere deletes performance data that is more than 365 days old.

Display capacity data

ProSphere provides capacity information associated with discovered configuration items. The scope of collected data can be a configuration item, a local data center, or the entire enterprise. Displays contain tables and graphics including pie charts.

Capacity reports on configuration items include:

- Arrays and storage systems
- Pools
- LUNs and unbound LUNs
- Replication
- Service level and tier

You can display raw capacity, and usable capacity by trend, purpose, pool, and service level.

You can customize capacity tables by filtering, sorting, adding or removing or reordering columns. Any display in ProSphere can be customized by reformatting a display, creating a new layout, and adding attributes.

If you have more than one ProSphere deployment and decide to synchronize them, you will aggregate capacity data at a single specified Master Capacity Application. Synchronize Data on page 137 describes synchronization in detail.

Note

Capacity data that comes in daily is retained for 365 days. Capacity data that comes in weekly or monthly is retained forever.

Output reports

ProSphere provides the ability to export data for formatting into reports outside of ProSphere. You can do the following:

- Export the data from the **Explore** area to a .csv or .pdf file, then open or save the file.
- Schedule a recurring report to be sent at a specific time. This feature is available through buttons on the **Explore** area.
- Use the RestAPI to programmatically manipulate the data. For example, at a scheduled time each week you can send a report to a third-party reporting application. You can send a report to IT.
- Create smart groups based on user-created tags, which helps in creating chargeback reports

Note

At present there is no way to use the RestAPI to get bulk data with one programming call (for example, to get an entire screen of data from the **Explore** area). To do this, you would use the Export function, available in the **Explore** area.

Integrate with Watch4net

Watch4net monitors ProSphere for cross-domain performance and manages its service levels. When ProSphere is integrated with Watch4net, the transfer of ProSphere performance data can be enabled or disabled from within ProSphere. When enabled, ProSphere injects performance data into a collector of Watch4net.

In a federated ProSphere setup, Watch4net integration is performed separately in each instance of ProSphere. All ProSphere instances connect to a single instance of Watch4net.

Tag configuration items

As a ProSphere administrator you can tag a configuration item with informational attributes meaningful to your requirements. These attributes are independent of the associated configuration item and are available only in your environment for the administrators to view, manage, or share.

For example, you could tag a configuration item by its location and assign tag values to the location tag, such as city names, state names, or country names. When the configuration item is discovered, the associated tag informs administrators about the location of the discovered object.

You can use tags together with filtering and smart groups to group and display configuration items. For example, you can create a smart group based on a location tag, then user filtering to display all hosts with 5 GB capacity in a specific location.

You can use tags in smart groups and output chargeback reports for the smart groups. For example, you can create a smart group based on a location tag value **Europe**, then display a smart group that only contains hosts located in Europe. You can display chargebacks for the smart group.

You can create tags in a spreadsheet, save them to a .csv file, then import the .csv file into ProSphere. You can export tags from one deployment and input them into another.

SMTP service configuration

You can configure SMTP email settings in ProSphere. The SMTP email settings enable EMC Customer Support to receive event files and empower ProSphere administrators with alert notifications. The ConnectEMC feature uses these configured SMTP settings.

Note

Every time you configure the SMTP email settings, ensure that you open the **ConnectEMC** dialog box and click **OK**. This step will ensure that the ConnectEMC feature uses the updated SMTP email settings.

Configure the SMTP service

Procedure

1. Click **Admin** on the ProSphere Console
2. Click the **System** tab
3. Click **Configure SMTP Service**.

   The Configure SMTP Service dialog box is displayed.
4. In the **SMTP Server** field, type the name of the SMTP server to which ProSphere needs to establish a connection.

   The default value is localhost.
5. In the **Email Sender** field, type the email ID from which event files and alert notifications are to be sent.

   The default value is prosphere@localhost.domain

6. In the **Email Recipient** field, type the email ID that will receive event files through the Connect EMC service.
7. Click **OK** to save the configuration and exit out of the dialog box.

Collection of deployment information by EMC

EMC's ability to support ProSphere is enhanced by the collection and reporting of specific information about ProSphere deployment. ProSphere uses ConnectEMC, an EMC common transport module, to transfer this information securely to EMC. The following information is collected and sent to EMC support:

- Version of ProSphere deployed in the customer environment
- Summary of license compliance at the customer site
- Current ProSphere configuration including the number of installed ProSphere instances and the number of collectors for each Secondary ProSphere Application
- Number of objects such as hosts, switches, and storage systems managed by ProSphere

Collecting and reporting this information helps resolve problems and provides data for performance analysis.

If enabled, the information is collected and transferred through FTPS to EMC on a weekly basis. SMTP transport to EMC is also available. You can enable or disable the transport feature and configure the transport mechanism used through the ProSphere Console from **Admin** › **System** › **Configure ConnectEMC Service**.

Manage the ConnectEMC service on page 29 provides information on managing the ConnectEMC settings.

Manage the ConnectEMC service

To enable the ConnectEMC service:

1. Click **Admin** on the ProSphere Console.
2. Click the **System** tab.
3. Click **Configure ConnectEMC** Service.
4. Select the type of service.

   Note

   You can select either FTPS or EMail or you can select both options.

5. Click **OK** to save the configuration and exit the dialog box.

To disable the ConnectEMC service:

1. Click **Admin** on the ProSphere Console.
2. Click the **System** tab.
3. Click **Configure ConnectEMC Service**.
4. Disable the FTPS option and the EMail option, if it is enabled, to disable the ConnectEMC service.
5. Click **OK** to save the configuration and exit the dialog box.

CHAPTER 2

eLicensing

This chapter contains the following topics:

Overview

Licensing of the ProSphere Application is handled by providing licenses to manage storage arrays with ProSphere.

A *license* is a record of the type, version, and quantity of software a customer has purchased the right to use. If the terms of a license are not met, such as when a customer purchases new hardware that exceeds the capacity specified in a license, the customer must purchase a new license. If required, the customer must manually activate the license by uploading a new license file.

There are three types of licenses:

- EVAL (evaluation)
- IND (individual)
- ELA (enterprise licensing agreement)

Licenses are activated in one of the following ways:

- For Symmetrix VMAX (5875.150 or later) and VMAXe arrays, the ProSphere license is included in the license file for the array, and activated using the Symmetrix procedures for array activation. If the Symmetrix activation procedures for the arrays have been followed, ProSphere automatically activates the ProSphere licenses when ProSphere discovers the arrays.
- For other arrays, licenses are activated when a customer downloads a license file as described in Activate licenses on page 33.

Note

The *EMC ProSphere Support Matrix* specifies which models are supported.

License details

Table 1 on page 32 details how compliance with a license is determined for different arrays and whether activating a license requires the customer to download a license file.

Table 1 License details

Array type	Basis for compliance	Download?
Symmetrix VMAX	For Symmetrix VMAX arrays 5875 Q2-2011 SR and later (microcode version of 5875.150 and later), there is a license for each array and the raw SATA and non-SATA capacity of that array. These licenses are on the arrays and do not need to be downloaded. For Symmetrix VMAX arrays earlier than 5875 Q2-2011 SR (microcode version earlier than 5875.150), the license is for the total raw capacity of all of the arrays. This license needs to be activated and downloaded from EMC Online Support.	N
Symmetrix VMAXe	Each license is for one array. The license allows a specific amount of SATA storage capacity and a specific amount of non-SATA storage capacity.	N
CLARiiON/VNX/ Celerra	License allows a specific number of arrays for each model type licensed by the customer.	Y

Table 1 License details (continued)

Symmetrix/DMX	License allows a maximum capacity for all DMX arrays combined. This license is for DMX and pre-5875 Q2-2011 SR VMAX arrays.	Y

Upgrade from EMC ControlCenter to ProSphere

Based on your current EMC ControlCenter (ECC) maintenance status, you may be eligible for a no-cost upgrade to ProSphere. To implement the upgrade, you need a ProSphere license file.

1. From EMC Online Support (`support.emc.com`), navigate to the **License Management** page. Enter **EMC Online Support** › **Service Center** › **Get and Manage Licenses**.
2. Select **ProSphere for ControlCenter**.

This links to a portal where you register the EMC ControlCenter (ECC) product you purchased and request equivalent ProSphere entitlements.

Based on your entries in the portal, the capacity and other details for the ProSphere license file are determined. EMC Licensing (`licensing@emc.com`) will contact you about how to obtain the upgrade entitlements needed for ProSphere.

Obtain license authorization codes (LACs) and license files

When a software order is fulfilled, an administrator receives an email message. The message includes:

- One or more product IDs and license authorization codes (LAC)
- The link to use for activating purchased software and downloading a license file

ProSphere administrators should protect the LAC to prevent anyone from improperly activating the software. If a LAC is misplaced, contact the world-wide Licensing team at licensing@emc.com or call:

- North America, Latin America, Asia Pacific Japan and Korea (APJK), Australia, new Zealand: SVC4EMC (800-782-4362) and follow the voice prompts.
- EMEA: +353 (0) 21 4879862 and follow the voice prompts.

Activate licenses

EMC Online Support Licensing is an online self-service tool for activating new software licenses and managing existing licenses.

There are two methods for activating licenses:

- Lite Touch Activation - for Symmetrix VMAX and VMAXe arrays
- Normal Touch Activation - for all other arrays and ProSphere licenses

Activate new product licenses with Lite Touch

Procedure

1. Type the link specified in the email message into a browser.
2. Click **Register My Product**.

3. Type the serial number in the **Enter a Product ID/Serial Number** field.
4. Click Go.
5. Click **Download License File** for each product's license file being downloaded.

   The **File Download** dialog box appears.

   Note

   In EMC Online Support, EMC ControlCenter static keys appear along with ProSphere license information. The procedure to apply the keys is to download the license file, open them in an editor and copy the key values from the file into the key screen of EMC ControlCenter.

6. Click **Save**.

   The **Save As** dialog box appears.

7. Navigate to the folder where the license file will be stored, and click **Save**.

   When the save operation is finished, the **Download Complete** dialog box appears.

8. Click **Close**. The **EMC License Activation** page appears.
9. Optionally, in the **Email Addresses** field type the email addresses for additional license certificate recipients. Separate email addresses by commas. Click **››** to submit the email addresses.

Activate upgrade licenses with Lite Touch

Procedure

1. Type the link specified in the email message into a browser.
2. Click **Register My Upgrade**.
3. Type the product ID or serial number in the **Enter a Product ID/Serial Number** field.
4. Type the corresponding license authorization code (LAC) in the **Enter a License Authorization Code (LAC)** field.
5. Click **Search**.
6. Click the checkbox next to each product being activated or click the checkbox next to the set.
7. Optionally, enter the product ID/serial number of the license keys to be regenerated in the **Product ID/Serial Number** field. Click **Regenerate**.
8. Click **Download License File** for each type of file to download and activate.
9. Optionally, in the **Email Addresses** field, type the email addresses for additional license certificate recipients. Separate email addresses by commas. Click **››** to submit the email addresses.

Activate new products and upgrades with Normal Touch

Procedure

1. Type the link specified in the email message into a browser.
2. Click the **Log in with my password** link.
3. Type your user name in the **Login** field.

4. Type your password in the **Password** field.
5. Click **Log In**.
6. On the blue bar at the top of the screen, select **Activation › Activate Licenses** from the drop-down menu.
7. Enter an LAC in the **LAC** field.
8. Click **Search Entitlements**.
9. Click the checkbox(es) next to the entitlement(s) being activated.
10. Click **Start Activation Process**.

Note

If the correct machine name appears in the lower portion of the **Search Machines** dialog box, click **Select** to select the machine, and skip the next step.

11. Click **Add a Machine**.
    a. In the **Machine Name** field, type the name of the machine where the license files will be saved.

       You can enter any machine name, but use the same machine name each time you activate a ProSphere license.

       When the same name is used again, the new licenses are added to all the previous licenses associated with that name.
    b. Click **Save**.
12. On the **Register** page, click **Next**.
13. Click **Next**.
14. Click **Finish**.

License compliance management

The license compliance management feature of ProSphere allows a security administrator or system administrator to upload license files, and monitor, verify, and report the current software license files available in the current document.

Upload a license file

For some licenses, you must upload a license file before you can view the license information.

Procedure

1. Display the **License Management** dialog box.
2. Click **Browse** and locate the license file you downloaded from EMC Online Support.
3. Click **Import** to upload the license file.

   A new row for the license appears in the **Manage Licenses** dialog box.

Results

The new license file is a complete replacement of the existing license file used by ProSphere.

Note

ProSphere only supports LIC file format.

View license compliance information

Procedure

1. Click **Admin** in the area navigation section.
2. Click **System**.
3. Click **Manage Licenses**.

   The **Manage Licenses** dialog box opens, shown in Manage license compliance on page 36.

Manage license compliance

The **Manage Licenses** dialog box, shown in Figure 4 on page 36, displays the current status of license compliance.

Figure 4 Manage Licenses dialog box

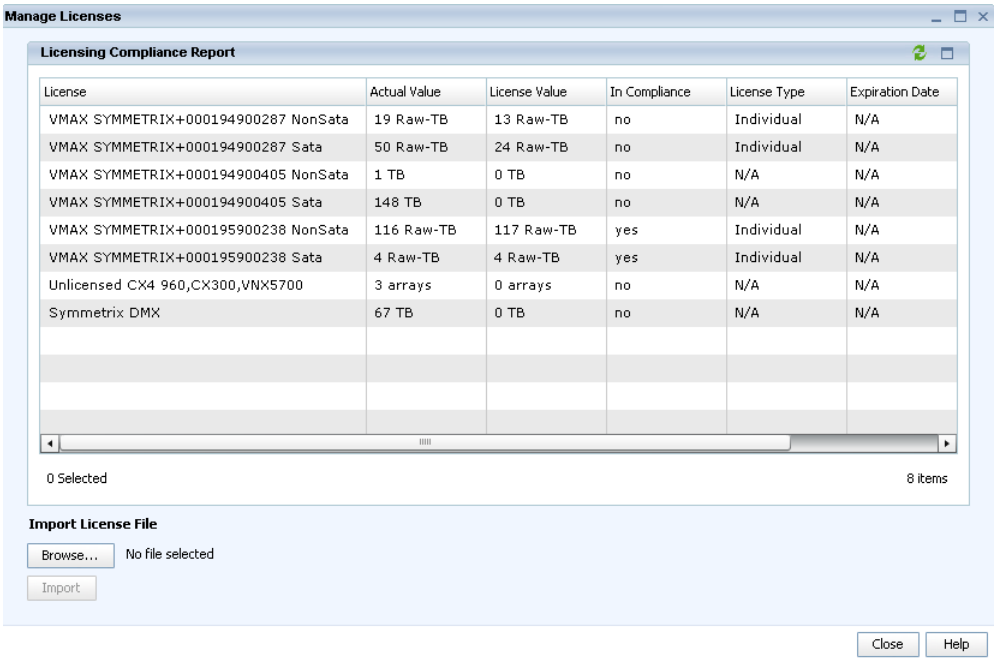


Table 2 Columns on the Manage Licenses dialog box

Column Name	Description
License	Displays the name of the license category. The name will be one of the following array licenses: • Symmetrix VMAX arrays that are 5875 Q2-2011 SR and later • CLARiiON/Unified • Symmetrix DMX arrays • VMAX pre-5875 Q2-2011 SR (microcode earlier than 5875.150)

Table 2 Columns on the Manage Licenses dialog box (continued)

Column Name	Description
Actual Value	Displays how much of the license value is currently used, followed by the units used.
License Value	Displays the maximum number of items or maximum storage capacity allowed by the license, followed by the units used.
In Compliance	Indicates if the customer is in compliance with the specific license. Yes indicates compliance. No indicates non-compliance. The software verifies compliance when a license file is uploaded for viewing in the dialog box, or when the current dialog box is refreshed.
License Type	Displays the license type. Possible values include: • EVAL — Evaluation • IND — Individual • ELA — Enterprise
Expiration Date	Displays the date of expiration of an EVAL license.

The following table describes the buttons available at the dialog box.

Table 3 Manage Licenses dialog box: buttons

Command name	Description
Browse	Click **Browse** to locate a new license file. Navigate to the location where the license file is saved on the local machine.
Import	Click **Import** to upload the license file. The license information appears in a new row in the dialog box.
Close	Click **Close** to cancel the dialog box without uploading.

CHAPTER 3

User Management

This chapter contains the following topics:

User management

User management consists of adding and removing users, selecting an authentication method, and managing user roles (predefined sets of user privileges). EMC ProSphere provides a default user and a user role. Additional users and user roles can be created by the security administrator and are managed from the ProSphere Console Administration area.

The *EMC ProSphere Online Help* provides field descriptions and definitions for user management features.

Note

A valid username and password are required not only to use the UI but to use any ProSphere back-end services.

Note

The *EMC ProSphere Security Configuration Guide* provides details on setting up, maintaining, and monitoring the secure operation of ProSphere. This includes information about logging in to or disabling logins to the root account on a ProSphere appliance, and information about the other accounts provided for logging in to ProSphere.

Manage user roles

User roles are used to group users with similar privileges and functions. Each user must be assigned a user role.

ProSphere provides three levels of users, including:

Security Administrator
A super user with administrator privileges who can manage users, user roles, user authentication, and view the audit log (similar to root in UNIX and Administrator in Windows.)

System Administrator
A super user with full administrator privileges to the entire application, with the exception of User Management.

User
A typical user with full access to the entire application, but without administrator privileges.

A user role defines the privileges for users who are assigned to the role.

The available roles are predefined. You cannot create a new role, delete a role, or modify the actions allowed for the role.

Table 4 on page 40 lists privileges allowed for each role.

Table 4 Privileges allowed by role

Privileges	Security Administrator	System Administrator	User
Create and manage users	Yes	No	No
Assign user roles	Yes	No	No

Table 4 Privileges allowed by role (continued)

Privileges	Security Administrator	System Administrator	User
Configure LDAP authentication	Yes	No	No
Modify system password	Yes	No	No
Configure synchronization passphrase	Yes	No	No
Import and Export secure certificate	Yes	No	No
Monitor system services	Yes	Yes	No
Configure and manage data sources	Yes	Yes	No
Upload licenses	Yes	Yes	No
Create a group	Yes	Yes	Yes
Create and manage discovery jobs	Yes	Yes	Yes
Search for objects	Yes	Yes	Yes
View objects in maps	Yes	Yes	Yes
View object properties	Yes	Yes	Yes
Manage and view alerts	Yes	Yes	Yes

Note

The roles mentioned here are independent of each other regardless of their privilege to access the same information within ProSphere.

Default account appadmin

The default username is appadmin, and Changeme1! is the password. The appadmin user is assigned the Security Administrator role and the System Administrator role. Therefore, the default appadmin user has all necessary privileges for user management and application administration.

You can change the password for the appadmin user.

You can delete the appadmin user only if there is another user with the Security Administrator role.

Assign a role to a user

Procedure

1. Log in with Security Administrator privileges.
2. Click **Admin** in the area navigation section.
3. Click **Users and Security** tab.

4. Click **Manage Users**.
5. Select a user you want to assign a role to.
6. Click **Edit** to open the **Edit User** dialog box.
7. Select the desired user role in the **Available Roles** box.
8. Click **Add** to move the role to the **Selected Roles** box.

   Note

   You can also use drag-and-drop to move a role between the boxes.
9. Click **OK** to save the changes nor **Cancel** to cancel the operation.

Remove a role from a user

Procedure

1. Log in with Security Administrator privileges.
2. Click **Administration** in the area navigation section.
3. Click **Users and Security**.
4. Click **Manage Users**.
5. Select a user from whom you want to remove a role.
6. Click **Edit** to open the **Edit User** dialog box.
7. Select the role in **Selected Roles** box.
8. Click **Remove** to move the role to the **Available Roles** box.

   You can also use the drag-and-drop to move a role between the boxes.
9. Click **OK** to save the changes.

Manage authentication

The Manage Authentication feature allows the Security Administrator to specify how users are authenticated when they log in. You can select either the Lightweight Directory Access Protocol (LDAP) or Local as options for types of authentication.

You set or edit user authentication options when creating or editing a user.

Configure LDAP settings

Procedure

1. Log in with Security Administrator privileges.
2. Click **Admin** in the area navigation section.
3. Click the **Users and Security** tab.
4. Click **Configure LDAP/AD Authentication**.
5. Do one of the following:
   - To create an LDAP server configuration if one does not yet exist, click **Create**.
   - To edit or change the current LDAP configuration, select the LDAP configuration in the table, and then click **Edit**.

6. Complete the fields in the **Create or Edit** dialog box. The following table describes the fields in the **Create** or **Edit** dialog box.

Field	Description
Primary Server Name	Indicates the name or IP address of the primary LDAP server. Examples: • ldap.server.com • 192.168.23.45
Secondary Server Name	Indicates the name or IP address of the secondary LDAP server. Examples: • backupldap.server.com • 192.168.23.45.
Use SSL	Select this option to use the LDAPS (secure LDAP) protocol, which is the preferred option. **Note** Selecting this option only ensures encryption of LDAP communications. To ensure that ProSphere authenticates the identity of your LDAP/AD server, paste the content of all the certificates in your LDAP/AD server's certificate chain in the **Certificate** field.
LDAP Port Override	Indicates the number of the port on which the LDAP server is listening to. If the server is listening on a non-standard port, enter that port number. Otherwise: • The default port number without SSL enabled is 389. • The default port number with SSL enabled is 636.
LDAP Timeout Override	Indicates the timeout value for the LDAP. The default value is 30000 milliseconds (30 seconds).
Bind Distinguished Name	Indicates the Distinguished Name the application uses to bind to the LDAP server in order to search for users. This Distinguished Name must have permission to search for users in the LDAP directory. Example: cn=Manager,dc=example,dc=com
Bind Password	Indicates the password the application uses to bind to the LDAP server using the Bind Distinguished Name value.
User Search Path	Indicates the Base Distinguished Name the application uses to search for users in the LDAP directory. All users will be searched for under this DN. Example: dc=example,dc=com
User ObjectClass	Indicates the value of the ObjectClass attribute for users. Examples: • For Microsoft Active Directory (AD), the typical value is user. • For SunOne and OpenLDAP, the typical value is inetOrgPerson.

Field	Description
UserId Attribute	Indicates the LDAP/AD attribute that identifies a username in a user object. • For Microsoft Active Directory (AD), the typical value is samaccountname. • For SunOne and OpenLDAP, the typical value is uid
Group Member Attribute	Indicates the LDAP/AD attribute that identifies a group member. Example: uniqueMember
Group Name Attribute	Indicates the LDAP/AD attribute that identifies a group name. Example: cn
Group ObjectClass	Indicates the value of objectclass attribute for groups. Example: group
Group Search Path	Indicates the base directory the application uses to search for groups in the LDAP directory. Example: ou=groups,dc=example,dc=com
User Search Filter	Indicates the string used to select subsets of users.
Group Search Filter	Indicates the string used to select subsets of groups.
Certificate	Paste your LDAP/AD server's Base64 Encoded X.509 formatted certificates in this field. Include the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` line for each. Paste the certificates one after the other in this field. You can paste as many certificates as required by your certificate chain.
Validate on submit	Select to validate the LDAP server data before saving the configuration. If the configuration cannot be validated, it is not saved. A message notifies you that the configuration was not saved. If not selected, the configuration is saved without validation. The following fields are validated: • Server Name • Port • Bind Distinguished Name • Bind Password

7. Click **OK** to save the changes or **Cancel** to cancel the operation.

Note

To display a tooltip that describes a field, place your cursor over the field. You can also click Help to get more information about each field.

Manage users

This section describes how to create, delete, and edit users. In addition, it describes how to change a user's password.

Create a user

Procedure

1. Log in with Security Administrator privileges.
2. Click **Admin** in the area navigation section.
3. Click **Users and Security**.
4. Click **Manage Users**.
5. Click **Create User** to open the **Create User** dialog box.
6. Complete the fields in the **Create User** dialog box to add a new user.

   The following table describes the field descriptions of the field types in the Create User dialog box.

Field	Description
Authentication method	Method to use for authenticating the user (LDAP/AD or Local).
User Name	Username of the user. • Username must be 1 to 40 characters in length. • Valid characters are alphanumeric (A-Z, a-z, 0-9), period (.), hyphen (-), and underscore (_). If you select LDAP/AD as the authentication method, click Lookup to verify that: • An LDAP server is configured • The username exists in the directory on that LDAP server
Enter Password	The password the user uses to log into the application. This field is applicable only if the authentication method is Local. The password must meet certain requirements as described in Password requirements on page 47.
Re-enter Password	The password the user uses to log into the application. This field is applicable only if the authentication method is Local.
Available Roles	Lists the roles you can assign to the user.
Selected Roles	Lists the roles selected to be assigned to the user.

7. If you select LDAP/AD as the authentication method, click **Lookup** to verify the LDAP server and the user.

Before you can use LDAP to authenticate users, you must configure an LDAP server to do the authentication.

- You can select a role, and then click **Add** or **Remove** to move that role from one box to the other.
- You can use drag-and-drop to move a role between the boxes.

8. Click **OK** to save the changes or **Cancel** to cancel the operation.

Edit a user

Procedure

1. Log in with Security Administrator privileges.
2. Click **Admin** in the area navigation section.
3. Click **Users and Security**.
4. Click **Manage Users**.
5. Select a user.
6. Click **Edit**.
7. Modify the information for the user.

   You can select a role, and then click **Add** or **Remove** to move that role from one box to the other. You can also use drag-and-drop to move a role between the boxes.

   Changes made to a user's role will not appear until the next time the user logs in.
8. If you select LDAP/AD as the authentication method, click **Lookup** to verify the LDAP server and the user.
9. Click **OK** to save the changes or **Cancel** to cancel the operation.

Delete a user

Note

You can delete the default appadmin user only if there is another user with the Security Administrator role.

Procedure

1. Log in with Security Administrator privileges.
2. Click **Admin** in the area navigation section.
3. Click **Users and Security**.
4. Click **Manage Users**.
5. Select the user you want to delete.
6. Click **Delete**.
7. Click **Yes** to delete the user or **No** to cancel the operation.

Note

When you delete a user, all discovery jobs the user created, which are assigned to the user, are automatically assigned to users with the Administrator role.

Change user password

A password is required only if the authentication method is Local. Only a Security Administrator can change the password for another user.

Procedure

1. Log in with Security Administrator privileges.
2. Click **Admin** in the area navigation section.
3. Click **Users and Security**.
4. Click **Manage Users**.
5. Select a user.
6. Click **Edit** to open the **Edit User** dialog box.
7. Modify the password information for the user.

   Note

   Password requirements on page 47 provides information on restrictions on setting a password. Click **Help** to get more information.

8. Click **OK** to save the changes or **Cancel** to cancel the operation.

Password requirements

The password must contain the following:

- A minimum of eight characters and a maximum of 40 characters
- At least one numeric character
- At least one uppercase and one lowercase character
- At least one non-alphanumeric character such as # or !

Each password must be different from the ten passwords that preceded it.

CHAPTER 4

Alerting

This chapter contains the following topics:

Overview

An alert is a propagated event generated by a configuration item in the storage environment. The alert typically includes severity, a message description, the name of the configuration item, and information about the health or performance of the configuration item.

ProSphere displays alerts for all supported switches and arrays in the storage environment. In certain instances, ProSphere also displays alerts for undiscovered configuration items or configuration items yet to be discovered.

Important notes on the All Alerts view on page 88 provides a detailed explanation for the display of undiscovered and yet to be discovered configuration items.

Note

Alerts are not synchronized across multiple deployments of ProSphere.

ProSphere supports alerts for the following configuration items:

- Brocade switches
- Cisco switches
- EMC Celerra network-attached storage (NAS)
- EMC CLARiiON
- EMC Symmetrix arrays
- EMC VNX arrays (block and file [2]).

NOTICE

Refer to the *EMC ProSphere Support Matrix* for the restrictions on alert consolidation.

Manage Alert Sources on page 53 provides more information on how ProSphere consolidates alerts for these configuration items.

Alert Severities on page 50 describes how ProSphere categorizes and displays alerts.

Table 5 Alert Severities

Alert severity	All Alerts view icon	Description
CRITICAL		Alerts requiring immediate attention. CRITICAL alert is the severest, indicating that a resource has either failed or is in a state that seriously compromises the environment. **Example:** Port is down.
ERROR		Alerts requiring attention to ensure that operations are not affected. ERROR alert indicates that the resource is approaching a state where it might soon start affecting the normal operations. **Example:** Registering 111.29.56.7 as Syslog recipient to the switch 120.77.09.11 failed.

2. NAS is also referred to as *File* in the ProSphere UI

Table 5 Alert Severities (continued)

Alert severity	All Alerts view icon	Description
WARNING		Alerts that warn of a situation that might require attention. This type of alert indicates that a resource is working, but normal operation may be affected. **Example:** The write cache on the storage system has not been configured yet or has been disabled because of a hardware component problem or software problem.
INFORMATIONAL		Alerts that contain messages about a normal event that occurred without need for any special attention or specific action to be performed. **Example:** VSAN added: Fabric_ltrcvo643VSAN70012 **Note** ProSphere assigns INFORMATIONAL severity to SMC-SPA alerts with severity -1 (unknown).

ProSphere supports the following alert management features:

Manage Alert Sources
To disable or enable alert consolidation from external sources, configure alert sources, and create access credentials for alert sources.

Performance Alert Thresholds
To set performance thresholds for usage of discovered configuration items (for example, port, director, and volume), based on which alerts are generated.

Manage Alert Notification
To create, edit and delete alert notification configurations for forwarding alerts as SNMP traps and emails.

Manage SNMP Trap Destinations
To add, edit, and delete SNMP trap destinations.

Set Alert Retention Period
To set the period for which alerts must be retained in the Alert Repository.

All Alerts
To monitor, acknowledge, unacknowledge and close alerts.
This **Operations** › **Alerts** option is documented in detail in the *EMC ProSphere Online Help*.

Set performance thresholds

Use this option to set custom threshold values for performance metrics of discovered CIs.

To help you to monitor the utilization limit and control resource performance, ProSphere enables you to set threshold metrics for discovered CIs. Alternatively, you can also use the default performance metrics (in percentage) of 85% (CLARiiON 90%) for WARNING

alerts and 90% (CLARiiON 95%) for CRITICAL alerts. You can modify these threshold values to suit the requirements of your storage environment using the **Manage Performance Alert Thresholds** option. Whenever the threshold metric set is breached, based on the performance data collection, an alert is generated and displayed in the **Operations** › **Alerts** › **All Alerts** view.

Note

Alerts are generated only for CIs which have path performance collection enabled.

Procedure

1. In the ProSphere Console, click **Admin** › **Alert Management** › **Manage Performance Alert Thresholds**.
2. Click **Set Performance Thresholds**.
3. Select **Enable** checkboxes against the metrics of your choice.

   The **Warning (%)** and **Critical (%)** fields are enabled for edit.
4. Modify the default threshold values of **Warning (%)** and **Critical (%)** as required. The permitted range is 1 to 99.
5. Click **OK**.

ProSphere performance metrics

This topic lists the various default performance metrics for CIs in ProSphere.

Note

The CLARiiON metrics are applicable to both legacy CLARiiON and VNX (block).

Table 6 Performance Metrics in ProSphere

Configuration Item Type	Affected object	Metric	Metric description	Warning % (Default)	Critical % (Default)
Switch	Port	%Port Link Utilization	Percentage of time the port is transmitting or receiving data.	85	90
Symmetrix	Port	%Port Utilization	Percentage of port performance utilization.	85	90
Symmetrix	Host Director	% Host Director Utilization	Percentage of the host director performance utilization (front-end director including Escon, fibre, or SCSI).	85	90
CLARiiON	Storage Processor (SP)	%SP Utilization	Percentage of time the SP was busy serving incoming requests.	85	90
CLARiiON	Storage Processor (SP)	% Dirty Pages	Percentage of cache pages owned by the SP that were modified	90	95

Table 6 Performance Metrics in ProSphere (continued)

Configuration Item Type	Affected object	Metric	Metric description	Warning % (Default)	Critical % (Default)
			since they were last read from or written to the SP.		

Manage Alert Sources

Use the **Manage Alert Sources** option to disable or enable as well as configure external alert sources.

Overview of alert sources

ProSphere or any of the element managers in the storage environment could be the source for alerts viewed in ProSphere. This enables you to use ProSphere to monitor and act upon (acknowledge, unacknowledge, and close) all alerts generated in your storage environment. Whenever required, you can also disable or enable alert consolidation. By default, ProSphere consolidates alerts at intervals of five minutes and is not customizable.

Note

The alert consolidation interval for only DCNM (10 minutes) differs from the default 5 minutes.

ProSphere alert consolidation requires you to set up access credentials for all alert sources, except SMC (SMI-S), and configure them. In addition to this setup, certain external conditions could also affect ProSphere's ability to consolidate alerts. Conditions that affect alert consolidation on page 69 lists these conditions and how they can be resolved.

Note

The performance threshold values set in ProSphere do not affect the external alerts.

NOTICE

Refer to the *EMC ProSphere Support Matrix* for the restrictions on alert consolidation.

What are native and external alerts?

Alerts that originate from ProSphere are called *native alerts*.

Alerts that originate outside ProSphere, from independent element managers such as SPA, are called *external alerts*. ProSphere uses distinct data gathering, processing, and mapping logic for each alert source. The syntax of the external alerts differ based on their source. ProSphere consolidates and presents the content of the external alerts in a uniform format for display in the UI, in alert notifications (email, SNMP traps), and in the REST API. As a result, the alert names, values, number of attributes, severities, and categories do not necessarily match between ProSphere and the alert source. ProSphere does not exclude any alert (except debug) from the supported source. Hence, it is possible that new and undocumented alerts from the alert source also appear in ProSphere.

ProSphere consolidates all external alerts and displays them in the **Operations › Alerts › All Alerts** view. The **Source** column in the **All Alerts** view displays `ProSphere` for native alerts and appropriate labels for external alerts as described in the next section.

How does ProSphere display external alert sources?
Table 7 on page 54 lists the external sources, ProSphere configurations (IP and access credential) for alert consolidation from each external source, and how users can identify the external sources in the **All Alerts** view.

Table 7 External Alert Sources in the **All Alerts view**

Alert source	ProSphere access Credential required	Source IP configuration required	Value in Source column	Description
Brocade Network Advisor (BNA)	Brocade Database	BNA IP	`BNA/CMCNE`	Indicates Brocade switch alerts consolidated from the CMCNE and BNA element manager instances.
EMC Connectrix Manager Converged Network Edition (CMCNE)	Brocade Database	CMCNE IP	`BNA/CMCNE`	
Cisco Prime Data Center Network Manager (DCNM)	Cisco DCNM Web Services	DCNM IP	`DCNM`	Indicates Cisco alerts consolidated from the DCNM element manager.
EMC Navisphere	EMC Navisphere	CLARiiON IP	`Navisphere`	Indicates CLARiiON alerts consolidated from EMC Navisphere element manager.
Control Station	EMC Celerra/VNX NAS XML API	Control Station IP	`Celerra`	Indicates Celerra NAS alerts consolidated from the Control Station element manager.
Symmetrix Management Console or SMC(through SMI-S Provider)	SMI-S	Solution Enabler/SMI-S IP (Preconfigured)	`SMC (SMI-S)`	Indicates SMC alerts consolidated from EMC SMI-S Provider instances. **Note** ProSphere receives SMC alerts only as indications from the SMI-S Provider. It does not receive SMC alerts directly. ProSphere converts these indications into alerts and displays them with appropriate severities. The *EMC ProSphere Deployment Guide* provides details on the use and setup of SMI-S Providers.
Symmetrix Performance Analyzer (SPA)	SMC-SPA	SPA IP (Preconfigured)	`SPA`	Indicates SPA alerts consolidated directly from SPA instances.
EMC Unisphere Remote	EMC Unisphere Remote	UniSphere Remote IP	`Unisphere Remote`	Indicates VNX alerts consolidated from the

Table 7 External Alert Sources in the **All Alerts view** (continued)

Alert source	ProSphere access Credential required	Source IP configuration required	Value in Source column	Description
				Unisphere Remote element manager.

External alerts supported

This topic lists external alert policies or categories and maps them to their ProSphere category displayed in the **All Alerts** view.

ProSphere consolidates all alerts and does its own categorization as given in List of external alerts supported in ProSphere on page 55.

Table 8 List of external alerts supported in ProSphere

CI	External alert source	Source alert policy or category	ProSphere categorization
Brocade switches	BNA or CMCNE	User Action Event	Health
		Unknown	
		Security Event	
		Product Status Event	
		Product Audit Event	
		Management Server Event	
		Link Incident Event	
Cisco switches	DCNM	FICON	Health
		Inter-VSAN	
		VSAN	
		ZONE	
		Port Alarm	
		Port Down	
		Switch Hardware	
		Switch Manageability	
		Threshold	
		Other	
Celerra	Control Station	ACLUPD	Health
		ADMIN	
		BoxMonitor	
		CAM	
		CEPP	

Table 8 List of external alerts supported in ProSphere (continued)

CI	External alert source	Source alert policy or category	ProSphere categorization
		CHAMII	
		Checkup	
		CFS	
		ConnectHome	
		DBMS	
		DEDUPE	
		DHSM	
		DLM	
		DNS	
		DRIVERS	
		DPSVC	
		EmailUser	
		EventLog	
		FCP	
		FSTOOLS	
		IP	
		JServer	
		KERNEL	
		LIB	
		LOCK	
		LocalHardwareMonitor	
		LogCollect	
		MasterControl	
		MGFS	
		NASDB	
		NaviEventMonitor	
		NDMP	
		NETLIB	
		NFS	
		PERFSTATS	
		RCPD	
		REP	

Table 8 List of external alerts supported in ProSphere (continued)

CI	External alert source	Source alert policy or category	ProSphere categorization
		SECMAP	
		SECURITY	
		SMB	
		SNAPSURE_SCHED	
		STORAGE	
		SVFS	
		SYR	
		TIMESYNC	
		UFS	
		UPSMonitor	
		USRMAP	
		VC	
		VCS	
		VMCAST	
		VRPL	
		WINS	
		XLT	
CLARiiON	EMC Navisphere	Alerts	Health
Symmetrix array	SMC (through SMI-S)	Array Events	Health
		SP Alerts	
		Device Config Change	
		Thin Device Usage	
		Device Pool Config Change	
		Port Link Status	
		HotSpare Invoked	
		CG Tripped	
		SRDF Alerts	
		SRDF Link Status	
		SRDF/A Session	
		DB Checksum Triggered	
		GK TimeOut	
		Thin Pool Rebalancing Complete Art	

Table 8 List of external alerts supported in ProSphere (continued)

CI	External alert source	Source alert policy or category	ProSphere categorization
		GK Utilization	
		Deferred Service Threshold Alert	
		Migration Complete Alert	
		Array Component Events	
		Device Status	
		Device Pool Status	
		Thin Device Allocation	
		Director Status	
		Port Status	
		Disk Status	
		SMC Environmental Alert	
		Event Lost Alert	
		Event Overflow Alert	
Symmetrix array	SPA	Array	Performance
		Cache Partition	
		Disk	
		FE Director	
		BE Director	
		BE Director (DA)	
		BE Director (DX)	
		Port Link Status	
		RDF Director	
		Device Group	
		Composite Group	
		Storage Group	
		Disk Group	
		RDF/A Group	
		Disk Group Tier	
		DSE Pool	
		External Disk	
		External Disk Group	
		RDF/A Director	

Table 8 List of external alerts supported in ProSphere (continued)

CI	External alert source	Source alert policy or category	ProSphere categorization
		RDF/S Group	
		Snap Pool	
		TP Pool	
		Virtual Pool Tier	
		System Alerts (Critical Database errors only)	
VNX (Block)	Unisphere Remote	Alerts	Health
VNX (File)	Unisphere Remote	apl	Health
		cs_core	
		cs_platform	
		dart	

Mapping of severity levels for external alerts

Table 9 on page 59 provides the mapping of severity levels for external alerts in their originating source and ProSphere.

Note

During alert consolidation, ProSphere ignores any external alert of debug severity level.

Table 9 External alert severity in ProSphere

External alert source (CI)	Source alert severity	ProSphere severity
BNA or CMNE (Brocade)	Emergency	CRITICAL
	Critical	
	Alert	
	Error	ERROR
	Warning	WARNING
	Information	INFORMATIONAL
	Notice	
DCNM (Cisco)	Emergency	CRITICAL
	Critical	
	Alert	
	Error	ERROR

Table 9 External alert severity in ProSphere (continued)

External alert source (CI)	Source alert severity	ProSphere severity
	Warning	WARNING
	Notice	INFORMATIONAL
	Info	
EMC Navisphere (CLARiiON)	Critical	CRITICAL
	Warning	WARNING
	Error	ERROR
	Info	INFORMATIONAL
Control Station (Celerra)	Emergency	CRITICAL
	Alert	
	Critical	
	Error	ERROR
	Warning	WARNING
	Notice	INFORMATIONAL
	Info	
SMC (SM-S) (Symmetrix)	Fatal	CRITICAL
	Critical	
	Warning	WARNING
	Information	INFORMATIONAL
	Normal	
SPA (Symmetrix)	Fatal	CRITICAL
	Critical	
	Warning	WARNING
	Information	INFORMATIONAL
	Normal	
Unisphere Remote (VNX)	Critical	CRITICAL
	Warning	WARNING
	Error	ERROR
	Info	INFORMATIONAL

Mapping of external alert attributes

Table 10 on page 61 lists the external alert attributes and maps them to the ProSphere alert attributes which are used in the ProSphere UI, email notifications, SNMP trap notifications, and REST APIs.

Table 10 Mapping of external alert attributes

External alert source (CI)	Alert attribute	Is attribute required for valid alert? (Yes/No)	Is attribute required for new or recurring alert? (Yes/No)	ProSphere alert attribute
BNA and CMCNE (Brocade switch)	description	Yes	No	alertmessage
	contributor	Yes	No	citype
	sourcename	Yes	Yes	ciname
	eventkey	Yes	No	name
	operationalstatus	Yes	No	actualvalue
	severity	Yes	No	severity
	source	Yes	Yes	source
	ipaddress	Yes	Yes	ipaddress
	idatsource	Yes	Yes	idatsource
Control Station (Celerra NAS)	BriefDescription	Yes	N/A **Note** Uniqueness is determined by the following attributes: • MessageCode • BriefDescription message parameter key and Value pair • facility • srmbase:SerialNumber • srmbase:IPAddress • srmbase:Port	alertmessage
	Severity	Yes		severity
	facility	Yes		name
Control Station (Celerra NAS): NAS Manifest file generated by ProSphere	srmbase:originalResourceID: srmbase:PortNumber	Yes		source
	srmdiscovery:deviceType (refer type map given below)	Yes		citype
	srmbase:SerialNumber	Yes		ciname
	srmbase:IPAddress	Yes		ipaddress
DCNM (Cisco switch)	Description	Yes	No	alertmessage
	Switch	Yes	No	ciname
	Event ID	Yes	Yes	idatsource
	ipaddress	Yes	Yes	ipaddress
	Type	Yes	No	name
	Severity	Yes	No	severity
	Facility	Yes	No	source
Navisphere (CLARiiON)	alertcode	Yes	Yes	alertcode
	alerttype	Yes	Yes	alerttype
	sourceidentifier	Yes	No	ciname

Table 10 Mapping of external alert attributes (continued)

External alert source (CI)	Alert attribute	Is attribute required for valid alert? (Yes/No)	Is attribute required for new or recurring alert? (Yes/No)	ProSphere alert attribute
	eventcode	Yes	Yes	eventcode
	navifullalertdetailedmsg	Yes	No	fullalertmessage
	ipaddress	Yes	Yes	ipaddress
	navijremailmsg	Yes	No	jremailalertmessage
	classname	Yes	Yes	name
	alertlevel	Yes	No	severity
	source	Yes	No	source
SMC (Symmetrix arrays): EMC-SMC-ALERT event	UserDefined5	Yes	No	alertmessage
	InstanceName	Yes	Yes	ciname
	UserDefined10	Yes	Yes	citype
	hasassociatedpolicy	Yes	Yes	hasassociatedpolicy
	UserDefined3	Yes	Yes	resourceattribute
	UserDefined1	Yes	No	severity
	source	Yes	Yes	source
SMC (Symmetrix arrays): EMC-DISKDRIVE-OPSTATUSCHANGED event	EventText	Yes	No	alertmessage
	InstanceName	Yes	Yes	ciname
	ClassName	Yes	Yes	citype
	hasassociatedpolicy	Yes	Yes	hasassociatedpolicy
	UserDefined4	Yes	Yes	name
	UserDefined6	Yes	No	severity
	source	Yes	Yes	source
SMC (Symmetrix arrays): EMC-SPS-OPSTATUSCHANGED event	EventText	Yes	No	alertmessage
	InstanceName	Yes	Yes	ciname
	ClassName	Yes	Yes	citype
	hasassociatedpolicy	Yes	Yes	hasassociatedpolicy
	UserDefined3	Yes	Yes	name
	UserDefined4	Yes	No	severity
	source	Yes	Yes	source
SMC (Symmetrix arrays):	EventText	Yes	No	alertmessage
	InstanceName	Yes	Yes	ciname

Table 10 Mapping of external alert attributes (continued)

External alert source (CI)	Alert attribute	Is attribute required for valid alert? (Yes/No)	Is attribute required for new or recurring alert? (Yes/No)	ProSphere alert attribute
EMC-VOLUMEPOOL-xxx event	ClassName	Yes	Yes	citype
	hasassociatedpolicy	Yes	Yes	hasassociatedpolicy
	UserDefined4	Yes	Yes	name
	UserDefined6	Yes	No	severity
	source	Yes	Yes	source
SMC (Symmetrix arrays): EMC-THINPOOL-ALERT event	EventText	Yes	No	alertmessage
	InstanceName	Yes	Yes	ciname
	ClassName	Yes	Yes	citype
	hasassociatedpolicy	Yes	Yes	hasassociatedpolicy
	UserDefined5	Yes	Yes	name
	UserDefined9	Yes	No	severity
	source	Yes	Yes	source
SMC (Symmetrix arrays): EMC-VOLUME-xxx event	EventText	Yes	No	alertmessage
	InstanceName	Yes	Yes	ciname
	ClassName	Yes	Yes	citype
	hasassociatedpolicy	Yes	Yes	hasassociatedpolicy
	UserDefined6	Yes	Yes	name
	UserDefined7	Yes	No	severity
	source	Yes	Yes	source
SMC (Symmetrix arrays): EMC-FCPORT-CHANGED event	EventText	Yes	No	alertmessage
	InstanceName	Yes	Yes	ciname
	ClassName	Yes	Yes	citype
	hasassociatedpolicy	Yes	Yes	hasassociatedpolicy
	UserDefined6	Yes	Yes	name
	UserDefined7	Yes	No	severity
	source	Yes	Yes	source
SPA (Symmetrix arrays)	value	Yes	No	actualvalue
	category	Yes	No	alertcategory
	message	Yes	No	alertmessage
	symmetrixid	Yes	Yes	ciname
	citype	Yes	Yes	citype

Table 10 Mapping of external alert attributes (continued)

External alert source (CI)	Alert attribute	Is attribute required for valid alert? (Yes/No)	Is attribute required for new or recurring alert? (Yes/No)	ProSphere alert attribute
	instance	Yes	Yes	name
	metric	Yes	Yes	resourceattribute
	severity	Yes	No	severity
	source	Yes	Yes	source
Unisphere Remote (VNX)	message	No	No	alertmessage
	name	No	Yes	ciname
	idatsource	Yes	Yes	idatsource
	ipaddress	Yes	Yes	ipaddress
	component	No	No	name
	severity	No	No	severity
	source	No	No	source

ProSphere displays SMC port statuses as numeric values in the alert message as follows:

Table 11 SMC port status in ProSphere

SMC port status	ProSphere status
aborted	1
complete	3
degraded	2
dormant	2
error	1
in service	3
lost communication	0
modified error	0
no contact	0
non-recoverable error	0
ok	3
other	3
power mode	3
predictive failure	1
starting	3
stopping	3

Table 11 SMC port status in ProSphere (continued)

SMC port status	ProSphere status
stopped	3
stressed	2
supporting entity in error	1
unknown	3

Conditions that affect alert consolidation

In addition to the requisite setup in the ProSphere Console, the conditions listed here affect how ProSphere consolidates alerts from the external alert sources.

Table 12 Additional conditions that affect alert consolidation

Condition	Alert source	Description
Multiple versions of alert sources and discovery	SPA and SMC	Although the storage environment could contain different versions of SPA and SMC instances, ProSphere consolidates alerts only from the supported versions listed in the *EMC ProSphere Support Matrix*. Alert consolidation for Symmetrix arrays occurs only when ProSphere discovers SPA and SMC instances during array discovery.
	Unisphere Remote	When both legacy CLARiiON and VNX are present in your environment, the appropriate access credentials for legacy CLARiiON (**EMC Navisphere**) and VNX (**EMC Unisphere Remote**) must be used.
Synchronization of system time and time zones	Control Station, Navisphere, SPA, Unisphere Remote	The system times of ProSphere and the hosts running the following must be in sync: • Control Station • Navisphere • SPA • Unisphere Remote
	BNA and CMCNE	The time zone and system times of ProSphere and the hosts running BNA or CMCNE must be in sync.
	N/A	The system times of all ProSphere VMs must be in sync.

Prerequisites for alert consolidation

This prerequisite setup is essential for successful alert consolidation from BNA, CMCNE, Control Station, DCNM, Navisphere, SPA and Unisphere Remote.

- Create access credentials for all alert sources, except SMC, using the **Manage Access Credentials** option in the **Manage Alert Sources** view.
  Create access credentials for an alert source on page 66 for an alert source describes the procedure for adding access credentials for the alert sources.
- Configure all alert sources (except SMC and SPA) by using the **Configure** link in the **Manage Alert Sources** view.
  Create an alert source on page 67 describes the procedure for configuring the alert sources.

Create access credentials for an alert source

For successful alert consolidation from BNA, CMCNE, Control Station, DCNM, Navisphere, SPA and Unisphere Remote, you must create at least one access credential for each alert source.

Prerequisites for alert consolidation on page 66 lists the other setup required for successful alert consolidation.

Note

This topic limits itself to creation of a new access credential. If need be, you can also edit and delete access credentials using the **Manage Alert Sources** in this view. Edit and deletion of an access credential is only effective when the next round of alert consolidation is triggered.
EMC ProSphere Online Help provides the procedures for editing and deleting access credentials.

Procedure

1. In the ProSphere Console, click **Admin** › **Alert Management** › **Manage Alert Sources**.
2. Click **Manage Access Credentials**.
3. Click **Create Access Credentials**.
4. In the **Type** field, select the appropriate access credential type:
   - **Brocade Database** — For BNA and CMCNE alerts.
   - **Cisco DCNM Web Services** — For DCNM alerts.
   - **EMC Celerra / VNX NAS XML API** — For Control Station (legacy Celerra) alerts.
   - **EMC Unisphere Remote** — For all Unisphere Remote (VNX block and file) alerts.
   - **EMC Navisphere** — For Navisphere (legacy CLARiiON) alerts.

     Note

     Limit the use of Navisphere only to legacy CLARiiON arrays with Flare version lower than 28. For supported array models with Flare version above 28, use Unisphere Remote.

   - **SMC-SPA** — For SPA (Symmetrix) alerts.

5. Specify the relevant details in the rest of the fields.

   EMC ProSphere Online Help provides detailed information on the access credential of each alert source.

6. Click **OK**.

   Click **Manage Alert Sources** on the breadcrumb to navigate back to the **Manage Alert Sources** view.

Create an alert source

Use this procedure to add BNA, CMCNE, Control Station, DCNM, Navisphere, SPA, and Unisphere Remote alert sources to ProSphere.

Creating an alert source involves adding IPs of BNA, CMCNE, Control Station, DCNM, Navisphere, SPA, and Unisphere Remote to ProSphere. EMC recommends the best practice of adding the access credential before configuring the alert source in the **Manage Alert Sources** view.
Prerequisites for alert consolidation on page 66 describes the requisite setup for successful alert consolidation.

NOTICE

If the access credential for the alert source is created or changed after the source IP is specified, then you must reconfigure (or retype and save) the source IP using the **Configure** link. The ProSphere discovery process (detection and discovery) necessitates this reconfiguration.

Procedure

1. In the ProSphere Console, click **Admin** › **Alert Management** › **Manage Alert Sources**.
2. In the **Configuration** column of the alert source row, click the **Configure** link.
3. Click **Create Alert Source** to create a new source.
4. In the **IP Address** field, type a unique and valid IP address of the host where the particular alert source is installed, except for the following: .
   - SPA — The IP address is configured automatically during discovery of VMAX arrays to the host where Unisphere for VMAX is installed. The VMAX discovery job shares both **SMC - SPA** access credential is used for VMAX array discovery.
   - SMC — The IP address is configured automatically during discovery of VMAX arrays to the host where the Solutions Enabler is installed. The IP address and **SMC (SMI-S)** access credential
   - Navisphere — Configure the alert source as either SP-A or SP-B IP or both. If you choose to add both the storage processors A and B as the alert sources, ProSphere consolidates alerts from both.
     Furthermore, because Navisphere can manage multiple CLARiiON instances, ProSphere consolidates alerts from the configured SP-A, SP-B, or both. To collect alers from multiple CLARiiON instances, configure the corresponding SP-A or SP-B.

     Note

     Limit the use of Navisphere only to legacy CLARiiON arrays with Flare version lower than 28. For supported array models with Flare version above 28, use Unisphere Remote.

5. Click **OK** to save the changes in the **Configure Alert Sources** view.

6. Click **OK** to display the **Manage Alert Sources** view with the newly created alert source information.

Edit an alert source

Use this procedure to change the BNA, CMCNE, Control Station, DCNM, Navisphere, SPA, and Unisphere Remote alert sources.

Procedure

1. In the ProSphere Console, click **Admin** › **Alert Management** › **Manage Alert Sources**.
2. In the **Configuration** column of the alert source row, click **Configure**.
3. Select the required alert source and click **Edit**.
4. Change the alert source IP Address.

   If the access credential for the alert source is created or changed after the source IP was specified in **Manage Alert Sources**, then you must retype the IP.
5. Click **OK** to save the changes in the **Configure Alert Sources** view, and then click **OK** to display the **Manage Alert Sources** view with the updated alert source information.

   ProSphere uses the changed alert source IP only when the next alert consolidation is triggered.

Delete an alert source

Use this procedure to delete only BNA, CMCNE, Control Station, DCNM, Navisphere, SPA, and Unisphere Remote alert sources.

Procedure

1. In the ProSphere Console, click **Admin** › **Alert Management** › **Manage Alert Sources**.
2. In the **Configuration** column of the alert source row, click **Configure**.
3. Select the required alert source and click **Delete**.
4. Click **Yes** to confirm deletion of the selected alert source, and then click **OK** to save the changes in the **Configure Alert Sources** view.
5. Click **OK** to display the **Manage Alert Sources** view with the updated alert source information.

   ProSphere stops alert consolidation from the deleted source IP only when the next alert consolidation is triggered.

Disable or enable alert consolidation

Use this procedure disable or enable alerts from external sources.§

Even though consolidation of alerts is enabled by default, you can disable consolidation from any specific external source and enable it again, as required.

Note

The number of instances of SPA and SMC (SMI-S) displayed and enabled for alert consolidation can vary dynamically based on the most recent arrays ProSphere discovers.

Note

You cannot select multiple alert sources to enable or disable.

Procedure

1. In the ProSphere Console, click **Admin** › **Alert Management** › **Manage Alert Sources**.
2. Perform one of the following:
   - Select the alert source for which you want to disable consolidation of alerts, and click **Disable.**
     ProSphere immediately stops consolidation of alerts from all instances of the alert sources, and the `Enabled?` column is set to `Disabled` in the **Alert Sources** table.

     Note

     Although you can view individual instances of BNA, CMCNE, Control Station, DCNM, Navisphere, SPA, and Unisphere by expanding the **Source** column, you cannot enable or disable them individually. You can only enable and disable the entire alert source group.
   - Select the alert source for which you want to enable consolidation of alerts, and click **Enable**.
     The **Enabled?** column for the alert source is set to `Enabled` in the **Alert Sources** table.

   Disabling and enabling of alert consolidation do not take effect immediately. Only at the end of the preconfigured alert consolidation interval of 5 minutes, ProSphere performs the following actions:
   - If enabled, consolidates and displays new alerts in the **All Alerts** view.
   - If disabled, stops consolidation and display of new alerts in the **All Alerts** view.

Alert consolidation status

The **Status** column in the **Manage Alert Sources** view displays the status of alert consolidation from the various alert sources.

The statuses for Brocade and SPA alerts are linked to the **Log Message** dialog box. Click the **Status** link to view the complete alert consolidation status details.

Note

In the table, "Grouped instance" refers to an expandable group of individual instances of the alert sources.

Table 13 Display of Alert Consolidation Status

Alert source	Grouped or Individual instance	Consolidation status	Description
BNA, CMCNE, DCNM, Navisphere, Control Station,	Grouped	`Success`	Alert consolidation succeeded for all the configured alert source.
		`Failed`	Alert consolidation failed from one or all the configured alert source.

Table 13 Display of Alert Consolidation Status (continued)

Alert source	Grouped or Individual instance	Consolidation status	Description
Unisphere Remote			Click the status link to see the diagnosis log and follow the recommended action.
		`Expired`	Alert consolidation was disabled. Thirty minutes after disabling alert consolidation, ProSphere deletes all alert consolidation results from the Alert Repository.
		`Pending`	Alert consolidation job is yet to execute for one or more of the alert source.
		`Running`	Alert consolidation is in progress for one or more of the alert source.
BNA, CMCNE, DCNM, Navisphere, Control Station, Unisphere Remote	Individual	`Success`	Alert consolidation succeeded on this alert source.
		`Failed`	Alert consolidation failed on this alert source. `Failed` is displayed when there is no configured IP address or access credential, or when alert consolidation actually failed. Click the status link to see the diagnosis log and follow the recommended action.
		`Expired`	Alert consolidation was disabled. Thirty minutes after disabling alert consolidation, ProSphere deletes all alert consolidation results from the Alert Repository.
		`Pending`	Alert consolidation job is yet to execute.
		`Running`	Alert consolidation is in progress.
SMC (SMI-S)	Individual	`Ready`	ProSphere is ready to receive indications from EMC SMI-S Provider for SMC alerts.
		`Not Ready`	ProSphere is not ready to received indications from EMC SMI-S Provider for SMC alerts.
SPA (Grouped instance)	Grouped	`Success`	Alert consolidation succeeded for all the discovered SPA instances.
		`Failed`	Alert consolidation failed from one or all the discovered SPA instances. Click the status link to see the diagnosis log and follow the recommended action.
		`Expired`	Alert consolidation was disabled. Thirty minutes after disabling alert consolidation, ProSphere deletes all alert consolidation results from the Alert Repository.

Table 13 Display of Alert Consolidation Status (continued)

Alert source	Grouped or Individual instance	Consolidation status	Description
		`Not Run`	Initial status when ProSphere is started for the first time and noticeable only for a few minutes.
SPA	Individual	`Success`	Alert consolidation succeeded for this SPA instance.
		`Failed`	Alert consolidation failed for this SPA instance. `Failed` is displayed when there is no configured access credential or the alert consolidation actually failed. Click the status link to see the diagnosis log and follow the recommended action.
		`Expired`	Alert consolidation was disabled. Thirty minutes after disabling alert consolidation, ProSphere deletes all alert consolidation results from the Alert Repository.
		`Pending`	Alert consolidation job is yet to execute, but the SPA has been discovered in ProSphere.
		`Running`	Alert consolidation is in progress.

Manage SNMP trap destinations

Customers use third-party applications such as ticketing, emailing, or incident-tracking applications to interpret alerts. Alerts in ProSphere can be forwarded to these incident tracking applications.

The ProSphere Management Information Base (MIB), `EMC-PS-MIB<version-number>.mib`, contains the SNMP notification information model and properties of ProSphere alerts. The incident-tracking applications use the alert ID to look up information about the alert in the MIB.

ProSphere MIB Structure on page 72 provides detailed information on the `EMC-PS-MIB<version-number>.mib` file.

Set up automatic forwarding of alerts generated or updated in ProSphere to these third-party applications as SNMP traps by:

1. Adding the trap destinations in the **Manage SNMP Trap Destinations** option.
   Add an SNMP trap destination on page 78 describes the procedure for adding trap destinations to ProSphere.
2. Selecting the required trap destinations in the alert notification configurations in the **Manage Alert Notification** view.
   Manage alert notifications on page 80 provides detailed information on alert notification configurations.

Note

Alert notification trigger conditions on page 80 lists the conditions that trigger alert notifications as SNMP traps.

The Manage SNMP Trap Destinations view allows you to:

- View all the SNMP trap destinations added to ProSphere.
- Add, edit and delete SNMP trap destinations.

ProSphere MIB structure

The ProSphere MIB model includes the following:

- An SNMP Alert Model Table that:
  - Defines the alert properties as column attributes
  - Contains a Notification group that comprises a list of notifications and alert properties that ProSphere forwards as traps.
    Alert Model Table on page 72 provides detailed information on the alert OIDs in the ProSphere MIB.

    SNMP Notifications group on page 77 provides the SNMP Notification group details.
- Individual alert tag-based unique identifiers (UIDs)
- Alert object identifiers (OIDs) or attribute definitions
  ProSphere MIB OID numbering scheme on page 72 describes the OID numbering scheme.
- Alert uniform resource identifiers (URI) that uniquely identify specific alerts

ProSphere MIB OID numbering scheme

The ProSphere OID numbering scheme is in accordance with the enterprise OID defined by EMC. The enterprise OID is unique and follows the numbering scheme detailed in Table 14 on page 72.

Table 14 Enterprise OID Numbering Scheme

OID Object	Numbering Scheme
All ProSphere related objects	iso.org.dod.internet.private.enterprises.emc.prosphere = .1.3.6.1.4.1.1139.25.0
Alert Model table defined in the ProSphere MIB	iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable = .1.3.6.1.4.1.1139.25.1.1
ProSphere Notifications group	iso.org.dod.internet.private.enterprises.emc.prosphere.alert.notifications = .1.3.6.1.4.1.1139.25.1.2

Alert Model Table

This topic provides detailed information on the alert OIDs in the ProSphere MIB.

Table 15 Alert OIDs in the ProSphere MIB

OID Name	OID Numbering	OID Syntax	Description
alertIdentifier	.1.3.6.1.4.1.1139.25.1.1.1.1	OCTET STRING (SIZE(0..255))	Unique identifier of the alert. This is the key for the Alert Model Table. All the columnar object identifiers of this table are suffixed with the unique identifier value of the alert. **Example:** The unique identifier value of the alert `c0c2ce17-cd14-435c-b772-7fc9980c6a7c` is also appended with the following suffix: `.99.48.99.50.99.101.49.55.45.99.100.49.52.45.52.51.53.99.45.98.55.55.50.45.55.102.99.57.57.56.48.99.54.97.55.99`
alertURI	.1.3.6.1.4.1.1139.25.1.1.1.2	OCTET STRING (SIZE(0..255))	URI to uniquely identify the alert.
alertName	.1.3.6.1.4.1.1139.25.1.1.1.3	OCTET STRING	Affected object for which the alert is generated.
alertState	.1.3.6.1.4.1.1139.25.1.1.1.4	OCTET STRING	State of the alert: • 0 - ACTIVE • 1 - CLOSED
alertSeverity	.1.3.6.1.4.1.1139.25.1.1.1.5	OCTET STRING	Severity of the alert: • 0 - CRITICAL • 1 - ERROR • 2 - WARNING • 3 - INFORMATIONAL
alertSource	.1.3.6.1.4.1.1139.25.1.1.1.6	OCTET STRING	Source of the alert and its IP address. For example, SPA 192.10.10.1.
alertCIName	.1.3.6.1.4.1.1139.25.1.1.1.7	OCTET STRING (SIZE(0..255))	Name of the ProSphere component for which the alert is generated. For example, switch port `WWN`.
alertCIType	.1.3.6.1.4.1.1139.25.1.1.1.8	OCTET STRING (SIZE(0..255))	Type of ProSphere component for which the alert is generated. For example, "Array" or "Switch".
alertMessage	.1.3.6.1.4.1.1139.25.1.1.1.9	OCTET STRING	Alert message.
alertOccurenceCount	.1.3.6.1.4.1.1139.25.1.1.1.10	OCTET STRING	Number of times the alert occurred in ProSphere.

Table 15 Alert OIDs in the ProSphere MIB (continued)

OID Name	OID Numbering	OID Syntax	Description
alertIsAcknowledged	.1.3.6.1.4.1.1139.25.1.1.1.11	OCTET STRING	Defines if the Alert has been acknowledged or not: • 0 - true • 1 - false
alertAcknowledgeTimetTime	.1.3.6.1.4.1.1139.25.1.1.1.12	OCTET STRING (SIZE(0|29))	Time at which the alert has been acknowledged, in the format *YYYY-MM-DDThh:mm:ss.nnn ±ZZ:zz*. • *YYYY* — Year in four-digit format • *MM* — Month in two-digit format • *DD* — Day in two-digit format • - — Date field separator • *T* — Date and time delimiter • *hh* — Hour in two-digit format • *mm* — Minutes in two-digit format • *ss* — Seconds in two-digit format • *nnn* — Milliseconds in three-digit format • : — Time field separator • . — Milliseconds field separator • *±* — Time zone offset + or - GMT • *ZZ* — Time zone hour in two-digit format • *zz* — Time zone minutes in two-digit format Example: 2011-09-30T10:24:033+01:30
alertAcknowledgedBy	.1.3.6.1.4.1.1139.25.1.1.1.13	OCTET STRING	Name of the ProSphere user who acknowledged the alert. **Note** This OID is not used in the current version of ProSphere.
alertOwnerName	.1.3.6.1.4.1.1139.25.1.1.1.14	OCTET STRING (SIZE(0..255))	Name of the ProSphere user who owns the alert. **Note** This OID is not used in the current version of ProSphere.

Table 15 Alert OIDs in the ProSphere MIB (continued)

OID Name	OID Numbering	OID Syntax	Description
alertCreationTime	.1.3.6.1.4.1.1139.25.1.1.1.15	OCTET STRING (SIZE(0|29)	Time at which the alert was created, in the format *YYYY-MM-DDThh:mm:ss.nnn ±ZZ:zz*. • *YYYY* — Year in four-digit format • *MM* — Month in two-digit format • *DD* — Day in two-digit format • - — Date field separator • *T* — Date and time delimiter • *hh* — Hour in two-digit format • *mm* — Minutes in two-digit format • *ss* — Seconds in two-digit format • *nnn* — Milliseconds in three-digit format • : — Time field separator • . — Milliseconds field separator • *±* — Time zone offset + or - GMT • *ZZ* — Time zone hour in two-digit format • *zz* — Time zone minutes in two-digit format Example: 2011-09-30T10:24:033+01:30
alertModificationTime	.1.3.6.1.4.1.1139.25.1.1.1.16	OCTET STRING (SIZE(0|29))	Time at which the alert was last modified, in the format *YYYY-MM-DDThh:mm:ss.nnn ±ZZ:zz*. Where: • *YYYY* — Year in four-digit format • *MM* — Month in two-digit format • *DD* — Day in two-digit format • - — Date field separator • *T* — Date and time delimiter • *hh* — Hour in two-digit format • *mm* — Minutes in two-digit format • *ss* — Seconds in two-digit format • *nnn* — Milliseconds in three-digit format • : — Time field separator

Table 15 Alert OIDs in the ProSphere MIB (continued)

OID Name	OID Numbering	OID Syntax	Description
			• . — Milliseconds field separator • *±* — Time zone offset + or - GMT • *ZZ* — Time zone hour in two-digit format • *zz* — Time zone minutes in two-digit format Example: 2011-09-30T10:24:033+01:30
alertCategory	.1.3.6.1.4.1.1139.25.1.1.1.17	OCTET STRING	Alert category: • 1 - other (alerts not related to either performance or health of CIs) • 2 - performance (alerts created based on performance criteria or threshold for CIs) • 3 - health (alerts created based on the health state of the CI)
alertTopLevelObjectURI	.1.3.6.1.4.1.1139.25.1.1.1.18	OCTET STRING (SIZE(0..255))	URI of the top-level object.
alertActualValue	.1.3.6.1.4.1.1139.25.1.1.1.19	OCTET STRING (SIZE(0..255))	Actual utilization value of resource attribute for which the threshold alert is generated.
alertPolicyURI	.1.3.6.1.4.1.1139.25.1.1.1.20	OCTET STRING (SIZE(0..255))	URI of the policy associated with the alert. **Note** This OID is not used in the current version of ProSphere.
alertLastOccuredTime	.1.3.6.1.4.1.1139.25.1.1.1.21	OCTET STRING (SIZE(0|29))	Time at which the alert last occurred, in the format *YYYY-MM-DDThh:mm:ss.nnn ±ZZ:zz*. Where: • *YYYY* — Year in four-digit format • *MM* — Month in two-digit format • *DD* — Day in two-digit format • - — Date field separator • *T* — Date and time delimiter • *hh* — Hours in two-digit format • *mm* — Minutes in two-digit format • *ss* — Seconds in two-digit format

Table 15 Alert OIDs in the ProSphere MIB (continued)

OID Name	OID Numbering	OID Syntax	Description
			• *nnn* — Milliseconds in three-digit format • : — Time field separator • . — Millisecond field separator • ± — Time zone offset + or - GMT • *ZZ* — Time zone hours in two-digit format • *zz* — Time zone minutes in two-digit format Example: 2011-09-30T10:24:033+01:30
alertResourceAttribute	.1.3.6.1.4.1.1139.25.1.1.1.22	OCTET STRING (SIZE(0..255))	Resource attribute for which the threshold alert is generated.
alertSourceCategory	.1.3.6.1.4.1.1139.25.1.1.1.23	OCTET STRING (SIZE(0..255))	Original source category of the alert. This attribute is only applicable to new SMC-SPA, BNA and DCNM alerts. It remains blank for: • Control Station and Navisphere alerts • Recurring SMC-SPA, BNA and DCNM alerts

SNMP Notifications group

Table 16 on page 77 describes the contents of the Notification group in the ProSphere MIB.

Table 16 SNMP Notifications

Notification	Notification Identifier	Function	Variable Bindings
psEventTrap	For SNMPV1 traps: • Generic Type: 6 • Specific Type: 1 • Enterprise OID: . 1.3.6.1.4.1.1139.25. 0	Notification of a specific event that has occurred in ProSphere.	• alertIdentifier • alertURI • alertName • alertState • alertSeverity • alertSource • alertCIName • alertCIType • alertMessage • alertOccurenceCount
	TrapOID for V2C and V3 Traps: . 1.3.6.1.4.1.1139.25.1.2.1		

Table 16 SNMP Notifications (continued)

Notification	Notification Identifier	Function	Variable Bindings
			• alertIsAcknowledged • alertAcknowledgementTime • alertAcknowledgedBy • alertOwnerName • alertCreationTime • alertModificationTime • alertCategory • alertTopLevelObjectURI • alertActualValue • alertPolicyURI • alertLastOccurredTime • alertResourceAttribute • alertSourceCategory

Add an SNMP trap destination

Use this procedure to add an SNMP trap destination to ProSphere.

Procedure

1. In the ProSphere Console, click **Admin** › **Alert Management** › **Manage SNMP Trap Destinations**.
2. Click **Create Trap Destination**.
3. In the **Add Destination Details** dialog box, specify the new SNMP trap destination details:

Note

All fields in the dialog box being mandatory, **Save** is enabled only when you have specified appropriate information for them all.

Note

The combination of **SNMP Version**, **Destination IP Address/Name**, and **Port** must be unique. ProSphere does not allow duplicate entries.

Field	Description
SNMP Version	SNMP version ProSphere supports: • V1 — The default value. • V2C

Field	Description
	• V3 **Note** Once the trap destination is added, you cannot edit the SNMP version. To change it, delete the destination and add a new one.
Destination IP Address/Name	Trap destination host. This could either be an FQDN, IP address, or hostname, and can contain alphanumeric characters.
Port	Edit the default value of 162, if required. The permitted port range is between 1 and 65535.

4. Specify the SNMP version destination attributes. For a V1 or V2C destination, specify the following SNMP version destination attribute.

   For a V1 or V2C destination:

Field	Description
Community String	The default community string is public. To view the Community String text, select the **Show Text** checkbox. **Note** The SNMP community string, authentication, and privacy passphrases are encrypted to secure them in the Alert Repository.

   For a V3 destination:

Field	Description
User Name	User name that should be used at the SNMP trap destination.
Authentication Protocol	SNMP authentication protocol used: • MD5 (Message Digest 5). This is the default value. • SHA (Secure Hash Algorithm)
Authentication Passphrase Authentication	Passphrase configured for the user at the destination.
Privacy Protocol	Authentication privacy protocol used for the trap destination: • NONE — Only the SNMP username is used for authentication. If you select NONE, the Privacy Passphrase field is not enabled. • DES — Data Encryption Standard (DES) 56-bit encryption • AES — 128-bit Advanced Encryption Standard.
Privacy Passphrase	Privacy passphrase associated with the privacy protocol of the trap destination if privacy protocol is DES or AES.

5. Click **Save**. The new destination appears in the **SNMP trap destinations** table of the **Alert Management** view.

Edit an SNMP trap destination

Use this procedure to delete an SNMP trap destination.

Procedure

1. In the ProSphere Console, click **Administration** › **Alert Management** › **Manage SNMP Traps**.
2. In the **SNMP trap destinations** table, select the destination you want to modify.

   Edit is enabled.
3. Edit the relevant destination details and click **Save**.

   Note

   The **SNMP Version** field is disabled for edit.

   The modified destination details appear in the **Manage SNMP Trap Destinations** view.

Delete an SNMP trap destination

Use this procedure to delete an SNMP trap destination.

Procedure

1. In the ProSphere Console, click **Administration** › **Alert Management** › **Manage SNMP Traps**.
2. In the **SNMP trap destinations** table, select the destination you want to delete.

   Delete is enabled.
3. Click **Delete**, and then click **Yes** in the confirmation dialog box that appears.

   ProSphere deletes the trap destination deleted from any notification configuration in which it is present and stops all further forwarding of alerts to it.
   The trap destination list in the **Manage SNMP Trap Destinations** view is updated.

Manage alert notifications

The **Manage Alert Notification** view enables you to define notification configurations, based on which members of your organization and third-party applications (such as a ticketing or an emailing system) in your storage environment can be notified of alerts. ProSphere generates alert notifications as SNMP traps and email messages for the trigger conditions in Table 17 on page 80:

Table 17 Alert notification trigger conditions

Notification trigger condition	SNMP trap	Email message
New alert	Yes	Yes
Changed alert state (acknowledge, unacknowledge, close)	Yes	Yes
Alert recurrence	Yes	No

Note

Email notifications are limited only to the CIs that ProSphere discovers. ProSphere does not generate email notifications for system alerts (that is, alerts generated by internal components like the Monitoring Service or Array Domain Manager)

You can perform the following actions in this view:

- View a list of the alert notification configurations created
  Access the Manage Alert Notification view on page 81 explains how you can access the **Manage Alert Notification** view and describes the notification configuration details displayed in the view.
- Create alert notification configurations
  Create an alert notification configuration on page 83 explains how you can create a notification configuration.
- Edit alert configurations
  Edit an alert notification configuration on page 84 explains how you can edit a notification configuration.
- Delete alert configurations
  Delete an alert notification configuration on page 85 explains how you can delete a notification configuration.

Access the Manage Alert Notification view

Use this procedure to access the **Manage Alert Notification** view and view all alert notification configurations created in ProSphere.

Procedure

- In the ProSphere Console, click **Admin** › **Alert Management** › **Manage Alert Notification**.

  The **Manage Alert Notification** view displays the following details for the available notification configurations:

Field	Description
Group	User-defined or smart group or subgroup for which the alert notification configuration has been set. This column displays: • `Deleted` — for groups deleted after creation of the notification configuration. • `Invalid` — for a group which does not follow the recommended naming convention. This can occur when the group has been corrupted or the group filter was created incorrectly through REST APIs. • `Not Available` — for a group which has not been created in ProSphere or when ProSphere is unable to communicate with the service that manages groups. • `<Any Group>` — for any group to which the CIs might belong. • `<No Group>` — if severity is the only criteria for alert notifications.
Minimum Severity	Minimum alert severity level to send alert notifications as SNMP traps or email messages. Any alert with the selected severity level or higher triggers an alert notification.

Field	Description
	Note Based on the selected alert severity, ProSphere generates notifications for this and all higher severities. Description of the **Minimum Severity** field in Create an alert notification configuration on page 83 provides complete details.
SNMP Destinations	Simple Network Management Protocol (SNMP) trap destinations which will receive the alert notifications for the selected group. Multiple destinations are separated by commas.
Email IDs	Email IDs of the alert notification recipients for the selected group. Multiple email IDs are separated by commas.

Prerequisites for creating alert notification configurations

Use these prerequisites to set up trap destinations and SMTP details before creating alert notifications.

Procedure

1. Add trap destinations in **Admin › Alert Management › Manage SNMP Trap Destinations**.

   Add an SNMP trap destination on page 78 describes the procedure for adding SNMP trap destinations in ProSphere.

2. Specify the SMTP server and email sender for email alert notifications:

   a. In the ProSphere Console, click **Admin › System › Configure SMTP Service** field, type the name of the SMTP server which ProSphere should use to send alert email notifications.

      ProSphere uses `localhost` as the default SMTP server.

   b. In the **Email Sender** field, type the email ID to be displayed as the email sender in the email alert notifications.

      ProSphere uses `ProSphere@localhost.localdomain.com` as the default email sender.

   c. Click **OK**.

Note

The **ConnectEMC Email Recipient** field in this dialog box is not used for email alert notifications. ProSphere alerting only uses the email recipient specified in the **Create Alert Notification** dialog box. Configure SMTP Service on page 28 describes how to set up SMTP details.

Create an alert notification configuration

Use this option to provide criteria based on which ProSphere should forward alerts (internal and external) as SNMP traps and emails.

Note

Ensure that you have followed the prerequisite setup listed in Prerequisites for creating alert notification configurations on page 82.

ProSphere provides the ability to alert notifications for CIs as SNMP traps and email messages based on two criteria:

- ProSphere groups or subgroups. Any alert for a CI belonging to the selected group triggers a notification to the selected destination or email recipient. You can create only one notification configuration for a group.
- Severity level of the alerts generated. Any alert with the selected severity level or higher triggers a notification.

Each notification configuration must be unique for a group or subgroup.

Note

ProSphere does not generate alert notifications for any group that is deleted after configuration of the alert notification. Additionally, if a notification configuration contains only the deleted group, the configuration becomes inactive.

Procedure

1. In the ProSphere Console, select **Admin** › **Alert Management** › **Manage Alert Notifications**.
2. Click **Create Alert Notification**.
3. In the **Criteria** tab, displayed by default, select the appropriate values in the drop-down lists for the following fields:

Field	Description
Group	ProSphere group or subgroup for which alert notifications should be sent. In case you select a valid group or subgroup, alerts notifications are generated for the CIs only if they have been discovered. **Note** You can define only one notification configuration for a group. Use subgroups for more refined notification configurations. **Note** ProSphere sends only one alert notification (SNMP trap, email) even if the CI belongs to multiple groups. Alternatively, you can select these two values: • **‹No Group›** — Default value. ProSphere forwards alert notifications based only on the selected severity, without validating CIs (discovered and undiscovered) against any group. • **‹Any Group›** — ProSphere validates a discovered CI against all existing groups before forwarding the alert notifications.

Field	Description
Minimum Severity	Minimum alert severity for which alert notifications must be generated. **CRITICAL** is the default alert severity. **Note** Set **Minimum Severity** as the only notification criterion if you want alerts generated for both discovered and undiscovered CIs. • **CRITICAL** — Only critical alerts are forwarded. • **WARNING** — WARNING and CRITICAL alerts are forwarded. • **ERROR** — ERROR, WARNING and CRITICAL alerts are forwarded. • **INFORMATIONAL** — Alerts of all severity levels are forwarded.

4. Click the **Destinations** tab.

   Note

   Here you must specify at least one notification type — SNMP trap or email message.

   Note

   If you do not need notifications as SNMP traps, skip to step 6 on page 84.

5. In **SNMP Destinations**, select the check boxes for the required SNMP trap destinations.

   These are trap destinations configured in **Admin** › **System** › **Manage SNMP Trap Destinations** › **Create Trap Destination**.

   Note

   If you do not need email recipients for the alert notifications, skip to step 10 on page 84.

6. Click **Create Recipient** to add email recipients.

   Note

   If the email recipients you need are already available in ProSphere, skip to step 9 on page 84.

7. Type the recipients' email IDs, separating multiple IDs by commas.
8. Click **Save**.
9. In **SMTP Destinations**, select the required recipients of the email alert notifications.
10. Click **Save**.

Edit an alert notification configuration

Use this procedure to edit an alert notification configuration.

Procedure

1. In the ProSphere Console, click **Admin** › **Alert Management** › **Manage Alert Notification**.
2. In the **Alert Notification** table, select the notification configuration you want to edit.

Edit is enabled.

3. Edit the relevant details in the **Criteria** and **Destinations** tabs.

   Note

   Group criterion is disabled for edit.

4. Click **Save**.

   ProSphere updates the notification configuration list in the **Manage Alert Notification** view.

Delete an alert notification configuration

Use this procedure to delete an alert notification configuration.

Procedure

1. In the ProSphere Console, click **Admin** › **Alert Management** › **Manage Alert Notification**.
2. In the **Alert Notification** table, select the notification configuration you want to delete.

   Delete is enabled.

3. Click **Delete**, and then click **Yes** in the confirmation dialog box that appears.

   ProSphere immediately stops forwarding of alerts and updates the notification configuration list in the **Manage Alert Notification** view.

Alert notification examples

This topic provides an illustrative example each for the content of email and SNMP alert notifications that ProSphere generates.

Example 1 Email alert notification

```
An alert has been updated in ProSphere with the following attributes:

  AlertMessage       : Error: OEM_ERROR: 02/06/13 18:23:24 : FERR:
PCI Exp Port B Non-Fatal Error Bus:00H Dev:00H Fn:01H PS:61H EIP:
0000000000141640H ESP:00000000084A4C08H
  CI Name            : APM00080400345
  CI Type            : NAS Gateway
  Severity           : Error
  Source             : Celerra - 10.200.00.000
  State              : ACTIVE
  Is Acknowledged?   : Yes
  Occurrence Count   : 2
  Creation Time      : Thu Sep 12 09:56:05 IST 2013
  Last Occurred Time : Thu Sep 12 09:57:17 IST 2013
  Affected Object    : CHAMII

  This is an auto-generated email, due to notification policy from
ProSphere appliance - https://lkkkgn111.lgg.emc.com.
  To change the notification settings, please consult the site
administrator.
```

Example 2 SNMP v1 trap alert notification

OID	Value
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0.	0 millisecond

OID	Value
.1.3.6.1.6.3.1.1.4.1.0.	psEventTrap
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertIdentifier	tag:srm@emc.com,2009:srmalert:Alert::f098f71e-b449-4c5f-93a9-65905ecfec78
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertURI	tag:srm@emc.com,2009:srmalert:Alert::f098f71e-b449-4c5f-93a9-65905ecfec78
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertName	203708008804EA38
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertState	ACTIVE
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertSeverity	0
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertSource	ProSphere
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertCIName	lokkk055
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertCIType	Switch
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertMessage	Switch port Link utilization for port 203708008804EA38 is at 5%
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertOccurrenceCount	45
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertIsAcknowledged	No
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertAcknowledgementTime	
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertAcknowledgedBy	

OID	Value
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertOwnerName	
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertCreationTime	2013-09-17T06:05:59.996-04:00
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertModificationTime	2013-09-19T08:37:33.865-04:00
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertCategory	Performance
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertTopLevelObjectURI	https://lglll030.ssg.emc.com/srm/physicalswitches/100008008804EA38
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertActualValue	5
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertPolicyURI	tag:srm@emc.com,2009:srmalert:PerformancePolicy::cb68d0d5-3bed-4ae0-ab17-0a96cdae3164
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertLastOccurredTime	2013-09-19T08:37:33.864-04:00
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertResourceAttribute	ConnectivityDevicePort_percent_link_util
.iso.org.dod.internet.private.enterprises.emc.prosphere.alert.alertModelTable.alertModelEntry.alertSourceCategory	

Alert retention

The ProSphere Alert Repository retains alerts and their history for a default period of 90 days from the date of creation. You can modify it using the using the **Set Alert Retention Period** option.

At the end of the retention period, ProSphere deletes the alerts along with their history. The check for alerts that exceed the retention period starts daily at midnight (00:00:00 a.m.).

NOTICE

During upgrade, alerts older than 90 days are not migrated. If it is crucial that your organization migrate all alerts, contact EMC Customer Support. However, migrating a large number of alerts can extend the migration time by as much as four hours longer than usual. Refer to the *EMC ProSphere Performance and Scaleability Guidelines* for the operational impact of retaining alerts older than 90 days.
Additionally, the upgrade process reverts any customized alert retention period to the default value of 90 days. This value can be customized again after the upgrade is complete.

Set alert retention period

Use this procedure to modify the default retention period for alerts.

Procedure

1. In the ProSphere Console, click **Admin** › **Alert Management** › **Set Alert Period**.
2. Type the new alert retention period within the range of 1 - 365 days.
3. Click **Save**.

Important notes on the All Alerts view

This topic lists important notes about the behavior of the **Operations** › **Alerts** › **All Alerts** view.

1. The **All Alerts** view is empty when there are no alerts to display. However, occasionally, alerts appear on first launch in a new ProSphere deployment, even before ProSphere discovers CIs in the environment. This occurs for one of the following reasons:
   - The IP configurations used with the updated ProSphere deployment are the same as in the previous deployment.
   - External alerts are received from the relevant providers or element managers and not from the undiscovered or yet to be discovered CIs.
2. For the same alert, messages displayed in Control Station, Navisphere, and SMC UI may differ in the **All Alerts** view as described in the following table:

   Table 18 Alert Messages Differing in ProSphere

Alert source	Source attribute and alert message	ProSphere processing logic and alert message
Control Station	Alert message received: `CLARiiON event number 0x $navi_event_str $desc.` With: • `1 $navi_event_str =71234004` • `1 $desc = Host lglau011`	ProSphere displays: `CLARiiON event number 0x71234004 Host lglau011 Storage Array APM00120701240 SP N/A SoftwareRev 7.32.0 (4.73) BaseRev 05.32.000.5.008`

Table 18 Alert Messages Differing in ProSphere (continued)

Alert source	Source attribute and alert message	ProSphere processing logic and alert message
	Storage Array APM00120701240 SP N/A SoftwareRev 7.32.0 (4.73) BaseRev 05.32.000.5.008 Description Failed 13490 logins to 192.168.1.18 on port 2: Transport Failure (error: 0x1200505). 00 00 04 00 06 00 2c 00 d3 04 00 00 04 40 23 a1 04 40 23 a1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 71 23 40 04.	Description Failed 13490 logins to 192.168.1.18 on port 2: Transport Failure (error: 0x1200505). 00 00 04 00 06 00 2c 00 d3 04 00 00 04 40 23 a1 04 40 23 a1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 71 23 40 04.
Navisphere	navifullalertdetailedmsg: Fan ({0}) is faulted.	navifullalertdetailedmsg used by default. Fan ({0}) is faulted.
	jremailalertmessage: There are faulted fans in this system.	If navifullalertdetailedmsg is not available, jremailalertmessage is used. There are faulted fans in this system.
	Both navifullalertdetailedmsg and jremailalertmessage do not have values.	No message available.
SMC	SMC UI message: Device xxx status changed to online SMI-S indication: Device xxx is added to Symmetrix	Device xxx is added to Symmetrix

Table 18 Alert Messages Differing in ProSphere (continued)

Alert source	Source attribute and alert message	ProSphere processing logic and alert message
Unisphere Remote	Unisphere message with hexadecimal string: `The deduplication scan on system id 0x5533 has just completed.`	Unisphere message with the original hexadecimal string in parentheses preceded by the equivalent decimal string: `The deduplication scan on system id 21811 (0x5533) has just completed.`

3. The **All Alerts** view displays all alerts, including alerts received from a deleted or decommissioned CI, until the preconfigured alert retention period elapses.
4. Any action performed on alerts inside ProSphere is not propagated back to the originating sources.
5. ProSphere automatically refreshes and updates the view once every five minutes. You can also refresh the view manually, if required.

The **All Alerts** view is documented in detail in the *EMC ProSphere Online Help*.

CHAPTER 5

Initiate Resource Discovery

This chapter contains the following topics:

Resource discovery

Discovery is the process of collecting information about resources, also known as Configuration Items (CIs), from your network. The discovery process identifies your storage resources to ProSphere. Until you perform a successful discovery, most views in the ProSphere Console do not display any information.

The Discovery Engine of ProSphere can discover the following resource types in the network:

- Arrays, NAS, and unified storage
- Switches
- Fabrics
- Hosts

You can rediscover resources in the network that were previously discovered through the normal discovery process.

Note

If a single vCenter instance manages several geographically dispersed data centers and DRS/HA clusters, limit the discovery of the appropriate CIs to just the physical sites associated with a VMware data center and cluster. Create a user that has limited access to a subset of ESX servers. For example, you can create a username with access permissions to just one data center. This allows ProSphere to associate the appropriate storage with each ProSphere instance in each site.

Discover configuration items

The **Discovery** area in the ProSphere Console allows you to identify resources for discovery, view the details of the discovered resource instances, manage the discovered resources, and organize them into logical groups. The general procedure for discovering resources for use in ProSphere is:

1. Define or reuse a set of access credentials needed to connect to the resource. These credential types correspond to protocols used to access information on the remote resource. You need to provide a different set of access information for each access credential.
2. Create a discovery job to obtain data from the resource. Discovery jobs use an IP address or a range of IP addresses and a set of access credentials to remotely connect to resources on a predefined schedule and obtain data from them.
3. Run the discovery job.

Access credentials

An access credential is a set of user-specified properties that defines the way ProSphere makes a connection to objects in the network through a management interface. An access credential specifies the protocol and the required credentials for connecting to the management interface. For example, an SSH access credential contains the port number, username, and password for connecting to a Secure Shell (SSH) server on a network resource, such as a host.

You associate an access credential with a discovery job. When the discovery job runs, the protocol and credentials in the access credential are used to initiate communication with the specified object types at the IP addresses specified in the discovery job.

A discovered object is associated with the access credential used to discover it. Other management services, such as provisioning, use the object's associated access credential.

You can designate any access credential as a global access credential. You can use a global access credential with any discovery job that does not specify an access credential. When a discovery job runs using a global access credential, the system tries each global access credential until it finds one that is appropriate for the objects specified in the discovery job. The following sections describe how to create, edit, and delete an access credential.

Table 19 on page 93 lists the access credential types that ProSphere supports.

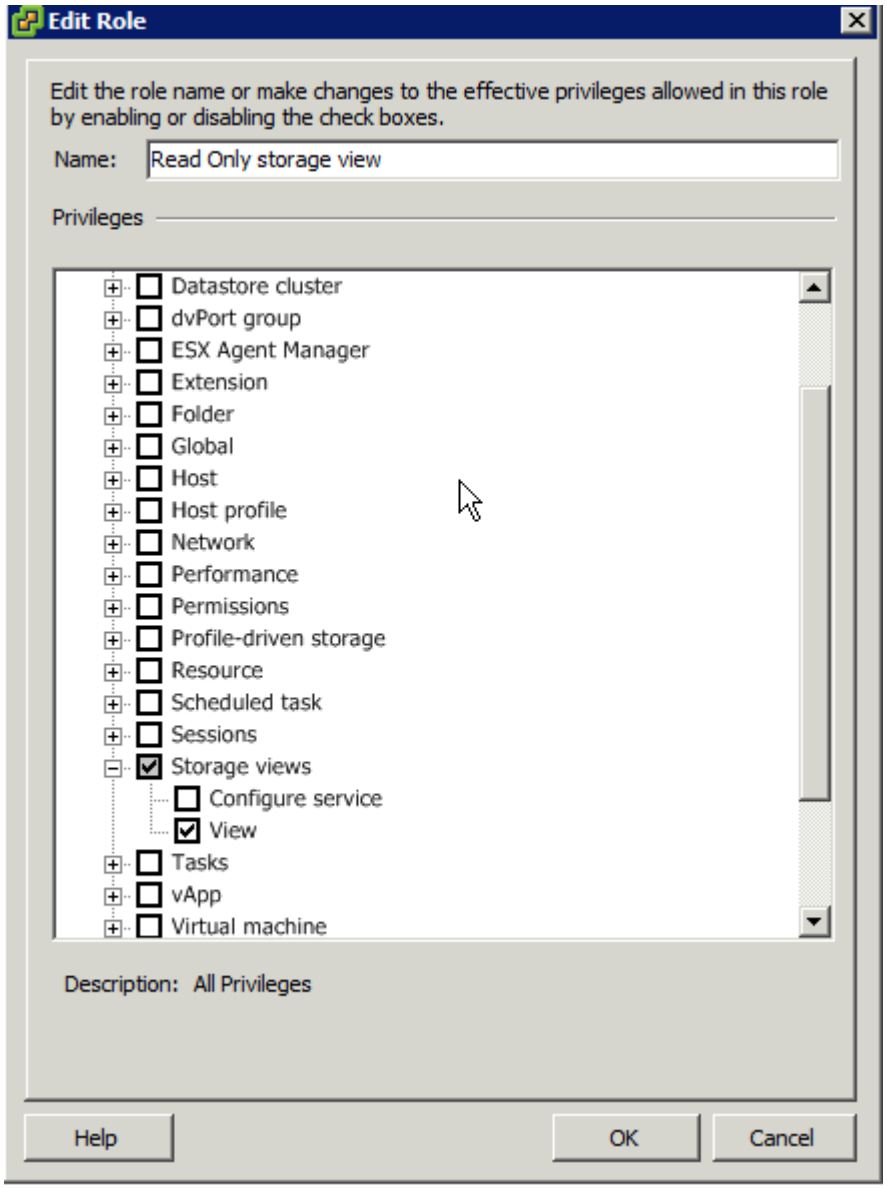
Table 19 Supported types of access credentials

Access credential types	Function
SMI-S	Discovers block storage and Brocade switches SMI-S is mandatory for both VMAX and VNX. The SMI-S provider is the primary source of performance and health status information.
SNMP V1/V2	Discovers Cisco switches
SNMP V3	Discovers Cisco switches
SSH	Discovers all UNIX hosts
WMI	Discovers Windows hosts
VMware Infrastructure	Discovers virtual hosts (VISDK)
WS-MAN	Discovers Windows hosts
SMC - SPA	Used by ProSphere internally for Performance Data Collection, and Alerts Collection from SPA server, and to launch SMC and SPA. This access credential should not be added to discovery jobs for the purpose of discovery.
Brocade Database	Serves as a single-point access for all event notifications and alerts from various element managers in the data center. This access credential should not be added to discovery jobs for the purpose of discovery.
Cisco DCNM Web Services	Consolidates Cisco switch alerts.
EMC Unisphere Remote	Discovers consolidate alerts from VNX arrays in the data center. This access credential should not be added to discovery jobs for the purpose of discovery.
EMC Navisphere	To connect to the EMC CIM (Common Information Model) Object Manager (ECOM) that runs on each of the CLARiiON service processors. It consolidates the alerts from CLARiiON system.
EMC Celerra/ VNX XML - API	Discovers file part of NAS storage.

Authorize a user in vCenter

When you create an access credential with the type **VMware Infrastructure** to discover virtual hosts vCenter, the username you specify must be a user name that has "storage view" privilege in vCenter, as shown in Figure 5 on page 94. Otherwise when you try to discover objects, you will receive a message indicating that vm capacity discovery has failed due to insufficient privileges. Discovery will be reported as partial.

Figure 5 Assign storage view privilege in vCenter



Create access credentials

Procedure

1. Click **Discovery** in the area navigation bar of the ProSphere Console.
2. Click the **Access Credentials** tab.
3. Click **Create Access Credentials**.

The **Create Access Credentials** dialog box appears.

4. Select or enter the **Type**, **Name**, and **Description**.

Note

When creating an SMI-S access credential, the name and the password cannot contain the equals (=) or pipe (|) character.

5. Type the required information in the **Attributes** area of the dialog box.
6. Click **OK**.

   The new access credentials appear in the **Access Credentials** view and can be used with a discovery job.

Edit access credentials

Procedure

1. Click **Discovery** in the area navigation bar of the ProSphere Console.
2. Click the **Access Credentials** tab.
3. Select an access credential and click **Edit**.
4. Click **OK**.

   The updated access credentials appear in the **Access Credentials** view.

Delete access credentials

Procedure

1. Click **Discovery** in the area navigation bar to navigate to the **Discovery** area of the ProSphere Console.
2. Click the **Access Credentials** tab to display the **Access Credentials** view.
3. Select the credentials you want to delete and click **Delete**.

   The **Delete Credentials** confirmation dialog box appears and displays the credentials to be deleted and any discovery jobs that rely upon them.
4. Click **Delete** to remove the credentials permanently or **Cancel** to cancel the operation. Deleted credentials no longer appear in the **Access Credentials** view.

Note

Deleting access credentials causes any dependent discovery jobs to fail.

Discovery jobs

Discovery jobs determine how and when ProSphere discovers and collects data from the resources in your network. In a discovery job, you can specify the IP addresses that you want the system to scan in order to detect undiscovered objects. The following sections describe how to create, edit, enable or disable, run, and delete discovery jobs.

Note

Following deployment of ProSphere, you must create at least one ProSphere Discovery Job to discover Brocade switches. The Discovery Job must include the IP address of the machine where the Brocade SMI Agent is running, not the IP addresses of the Brocade switches.

Create a discovery job

Before you begin

You need to create at least one access credential before you create a discovery job and discover objects.

Procedure

1. Click **Discovery** in the area navigation bar of the ProSphere Console.
2. Click the **Discovery Jobs** tab.
3. Click **Create Job**.
4. Type in a job name and description.
5. Select **Enable Job** to tell ProSphere to execute the job.

   If not enabled, the discovery job is created but not executed.
6. Click **Next**.
7. Select resource types to detect (for example, arrays, hosts, and switches) and IP addresses and address ranges to **INCLUDE** and **EXCLUDE** in the discovery process for the job.
8. Click **Next**.
9. Select **Use Global Access Credentials** to use global access credentials for the job or clear **Use Global Access Credentials** to use one or more predefined sets of access credentials. If you choose to use predefined access credentials, select each credentials set in the **Available Access Credentials** List and then click **Add** to add them to the job process.
10. Click **Next**.
11. Select a **Start on** date and time for the job.
12. Select **Make this schedule recur every** and set a recurring schedule to make this discovery job a recurring event.
13. Click **Finish**.

Note

To avoid overloading the Discovery Engine, it is recommended to schedule discovery jobs to run not more than once in 12 hours.

Edit a discovery job

Procedure

1. Click **Discovery** in the area navigation bar of the ProSphere Console.
2. Click the **Discovery Jobs** tab.
3. Select a discovery job and click **Edit**.

   The **Edit Job** wizard appears.

4. Step through the **Edit Job** wizard just as you would for the **Create Job** wizard, as described in Create a discovery job on page 96.

Delete a discovery job

Procedure

1. Click **Discovery** in the area navigation bar of the ProSphere Console.
2. Click the **Discovery Jobs** tab.
3. Select a discovery job and click **Delete**.
4. Click **Delete**.

Run a discovery job immediately

Procedure

1. Click **Discovery** in the area navigation bar of the ProSphere Console.
2. Click the **Discovery Jobs** tab.
3. Select a discovery job and click **Run**.

   The job's current status appears in the **Status** field for the job in the **Discovery Jobs** view.

Enable or disable a discovery job

Procedure

1. Click **Discovery** in the area navigation bar of the ProSphere Console.
2. Click the **Discovery Jobs** tab.
3. Select a discovery job and then click **Enable** or **Disable**.

Rediscovery

Rediscovery is the process by which the information about discovered objects is updated. Only objects in the data center that were previously discovered through the normal discovery process can be rediscovered. Rediscovery of an object depends on the discovery job that caused the object to be originally discovered. The discovery job specifies what to rediscover (the scope of the discovery process) and the conditions under which ProSphere can rediscover CIs.

Automatic rediscovery of an element occurs periodically, termed "policy-driven rediscovery," based on the polling interval for the object type. If more frequent rediscoveries of the element are desired, a separate rediscovery can be manually scheduled. Policy-driven rediscovery is full discovery--that is, discovery of all data related to the element.

In contrast to automatic and manually scheduled rediscoveries are event-based rediscoveries. Event-based rediscoveries occur automatically in response to an event an element participates in. Typically, event-based rediscovery updates specific data for an element. For instance, a storage array masking event would trigger the masking and mapping data to be rediscovered for the storage array but would exclude rediscovery of disk drives. ProSphere does not support event-based discovery for all element types.

Policy-driven rediscovery

Rediscovery of discovered objects is based on a polling interval. The polling interval is separately defined for each object type:

- Arrays: seven days

  Note

  Each day rediscovery collects limited information about arrays.

- Switches: seven days
- Hosts: one day
- NAS: seven days
- Unified storage (file-based component): one day
- Unified storage (block-based component): seven days

The smallest rediscovery interval is one day. In **Objects List** view, the **Last Updated** time indicates the most recent time an object was rediscovered.

Rediscovery is activated by default.

Event-based rediscovery

Rediscovery is triggered when a change is made to a storage system or switch. The circumstances under which an event-based rediscovery is triggered are in Table 20 on page 98.

Table 20 Event-based rediscovery

Event type	Event
Array	Add a volume
Array	Delete a volume
Array	Add a storage pool
Array	Delete a storage pool
Array	Create a masking view/record on a Symmetrix
Array	Delete a masking view/record on a Symmetrix
Array	Map a volume to a front-end port on a Symmetrix
Array	Unmap a volume from a front-end port in Symmetrix
Array	Mask a volume on a Symmetrix from a host
Array	Unmask a volume on a Symmetrix from a host
Array	Create a RAID group in CLARiiON
Array	Bind a LUN in CLARiiON
Array	Create a storage group in CLARiiON
Array	Add volumes to a storage group in CLARiiON

Table 20 Event-based rediscovery (continued)

Event type	Event
Array	Delete volumes from a storage group in CLARiiON
Array	Add a host to a storage group in CLARiiON
Array	Remove a host from a storage group in CLARiiON
Array	Delete a storage group from CLARiiON
Array	Unbind a LUN in CLARiiON
Array	Delete a RAID group in CLARiiON
Array	Create Volume replica
Array	Delete Volume replica
Array	Thin Pool threshold alert
Unified storage (block-based component)	Create a RAID group
Unified storage (block-based component)	Bind a LUN
Unified storage (block-based component)	Create a storage group
Unified storage (block-based component)	Add volumes to a storage group
Unified storage (block-based component)	Delete volumes from a storage group
Unified storage (block-based component)	Add a host to a storage group
Unified storage (block-based component)	Remove a host from a storage group
Unified storage (block-based component)	Delete a storage group
Unified storage (block-based component)	Unbind a LUN
Unified storage (block-based component)	Delete a RAID group
Switch	Enable or disable a Brocade or McDATA port
Switch	Split or merge a Brocade or McDATA fabric
Switch	Add or delete a Brocade or McDATA zone
Switch	Enable or disable a Cisco port
Switch	Split or merge a Cisco fabric
Switch	Add or delete a Cisco zone
Switch	Enable or disable a Cisco zone

Note

In ProSphere documentation, "array" refers to CLARiiON/Symmetrix and is block-based. "NAS" refers to Celerra and is file-based. "Unified storage " refers to "VNX" , which has a block-based component and a file-based component. "Storage systems" refers to arrays, NAS, and unified storage. In the file-based component of unified storage and in NAS, no events trigger rediscovery. Manual or scheduled rediscovery must be performed.

Manage discovered objects

You can manage all the objects that are discovered by ProSphere. You can perform the following operations from the **Object List** view:

- View the list of discovered objects
- View details of the discovered objects
- Delete objects

View discovered objects

You can view the configuration items discovered by ProSphere in the **Objects List** view. Click one of the tabs to display a list of the relevant discovered objects.

Procedure

1. Click **Discovery** in the area navigation bar of the ProSphere Console.
2. Click **Objects List**.
3. Click the tab for the type of discovered object (**Storage systems**, **Fabrics**, **Switches**, or **Hosts**), to view the list of the selected discovered object type in your data center.
4. Click the object in the list displayed.

   The **Configuration Item** dialog box displays details of the selected object type.

   Note

   Click **Success** or **Failure** in the **Discovery Status** column to display the discovery log.

Delete discovered object

You can delete storage systems, hosts, switches, virtual machines, and ESX hosts. Fabrics are automatically deleted when the switches that constitute the fabric are deleted. When you delete a discovered configuration item, it is removed from its local deployment. The deleted configuration item is removed from other synchronized deployments of ProSphere when either manual or scheduled synchronization of ProSphere Application occurs.

Any performance data, capacity information, and alerting history that was collected for the deleted configuration item is preserved. This data is not collected after the configuration item is deleted from the ProSphere Application.

Configuration items are associated with various system objects, such as groups. When you delete a configuration item, the associations with groups are deleted.

Procedure

1. Click **Discovery** on the ProSphere Console.

2. Select **Objects List**.
3. Select the tab for the type of configuration item you want to delete.
4. Select a configuration item.
5. Click **Delete**.
6. Click **Delete** to confirm the operation or **Cancel** to cancel the operation.

Note

Multi-delete is supported, up to 100 objects in one delete operation.

Effects of removing objects

When you physically unplug a configuration item (CI) from the network environment, you decommission it. When the discovery job that contains the IP address of the configuration item runs again either manually or at a scheduled time, it does not detect the configuration item after the configuration item is decommissioned.

If the decommissioned configuration item is reconnected, in order to see the configuration item in the Objects List you must execute the discovery job associated with the configuration item, or wait for the scheduled discovery job with the IP address of the configuration item and execute it. If you do not know which discovery job originally discovered the configuration item, create a new discovery job.

To avoid discovering a deleted configuration item that has not been decommissioned, exclude the IP address of the deleted configuration item from each discovery job associated with the configuration item, as explained in Avoid discovering a deleted configuration item (CI) on page 101.

When you delete a switch before it is decommissioned, the associated switches in the fabric, and also the fabric, are deleted. To avoid this situation, it is recommended that you only delete a switch if it is decommissioned.

When you delete an ESX host, all associated virtual machines and ESX hosts are deleted. To discover the deleted ESX host again, run the discovery job of the vCenter associated with the deleted ESX host, to discover it along with the virtual machines.

Avoid discovering a deleted configuration item (CI)

Exclude the IP address of the deleted configuration item from the associated discovery jobs:

Procedure

1. Click **Discovery Jobs**.
2. Select a discovery job.
3. Click **Edit.**
4. Click **Next**.
5. Select **Set Scope by IP addresses**.
6. Type the IP address to be scanned for discovery.
7. Select **EXCLUDE.**
8. Click **Finish**.

Discover file and block properties of unified storage

Before you begin

It is recommended to create one discovery job for both block and file discovery of a VNX array.

The following are required for creating a combined block and file discovery job:

- An SMI Provider connected to a VNX Unified array. The provider can be connected to other arrays.
- IP address of SMI Provider
- SMI Access Credential
- IP address of VNX/Celerra Control Station (this is where the VNX/Celerra XML API Server resides)
- VNX/Celerra XML API Access Credential

Procedure

1. Click **Discovery** on the ProSphere Console
2. Select **Discovery Jobs**.
3. Click **Create Job** to display the Create Job wizard.
4. Type a unique discovery job name. Click **Next.**
5. Select **Storage Systems** in the **Set Scope - by IP Address** wizard view.
6. Type the IP address of the NAS Control Station (Unified Array - VNX series or Celerra NAS Gateway), and Array SMI Provider. Click **Next**.
7. Select access credentials of type **SMI-S** and **EMC Celerra/VNX XML API** to discover the file and block properties of a unified NAS storage. You can optionally set a schedule to make the discovery job run at a specific time and at specific intervals of time in the Set Schedule step of the wizard.
8. Click **Finish.**

Resource groups

The Groups feature provides you with the ability to create a logical collection of different configuration items such as hosts, storage systems, switches, and fabrics. The logical grouping of configuration items allows you to perform operations on large sets of similar or related configuration items. Administrators have access to groups and can manage them from the Admin area of the ProSphere Application. The groups panel on the left-hand side of the **All Groups** view contains a hierarchical tree view of all groups in the system as well as groups from the synchronized ProSphere deployments. The groups from the synchronized deployments are renamed as ‹group_name›_‹hostname on which the group is present› the first time ProSphere instances are synchronized.

Note

The CI dialog for the newly discovered CIs is not available until either the next scheduled synchronization or the next manual synchronization is complete, although groups display the newly discovered CIs as their members before the operation completes.

The groups are classified into three categories, namely, system groups, simple groups, and smart groups.

System groups

System groups are groups automatically created by the system to contain all objects of a specific type. For example, All Hosts, All Arrays, All Switches, and All Fabrics, are system groups that contain all discovered objects of a specific type. The Library is also a group created by the system as a container for all system groups in the group tree. A system group cannot be deleted but the membership can be modified programmatically.

Simple groups

A simple group can contain configuration items, groups, and smart groups as its subgroups. A simple group changes only when you explicitly add or remove members and subgroups. An object can be a member of more than one simple group. Simple groups are intended for collections of configuration items that rarely change.

Smart groups

A smart group contains objects that meet user-defined criteria based on the object attributes. At regular intervals (either the default interval of 15 minutes or any other user-specified interval), the system scans your repository for discovered objects that meet the smart group criteria and automatically adds or removes the objects.

Subgroups

Simple groups and smart groups can be subgroups of a simple group. A subgroup can have only one parent.

A smart group cannot have a simple group as its subgroup.

Create a simple group

Procedure

1. Click **Admin** in the area navigation bar of the ProSphere Console.
2. Click the **Groups** tab.
3. In the left tree table, expand a group under which you plan to create a new group.
4. Click **Create Group**.
5. Type a unique name for the newly created group.

Create a smart group

Procedure

1. Click **Admin** in the area navigation bar of the ProSphere Console.
2. Click **System**.
3. Select **Manage Groups**.
4. In the tree on the **All Groups** tab, expand a group under which you plan to create a new smart group.
5. Click **Create Smart Group**.

Alternatively, you can use the right-click option on a parent group in the left tree table.

6. Type a unique name for the new smart group.
7. Select the **CI Type** (**Host**, **Storage System**, or **Switch**), along with the attributes, operators, and specific values associated with each selected CI type.
8. Click **ADD** to add a few more conditions on the basis of which items will be filtered into the smart group you create.
9. Select one of the options:
   - **AND** to select objects that match all specified criteria. By default, the chosen conditional operator is **AND**.

     When you perform an **AND** operation, you cannot use a combination of CI types.
   - **OR** to select objects that match only a subset of specified criteria.

     When you perform an **OR** operation, you can use a combination of other CI types when you add subsequent rows.

   By default, the chosen conditional operator is **AND**. When you perform an **AND** operation, you cannot use a combination of CI types. When you perform an OR operation, you can use a combination of other CI types when you add subsequent rows.

   Note

   When you select **AND** or **OR**, the selected conditional operator is applicable to all rows of criteria that are added in the smart group.
10. Select **Matching is case sensitive**. This makes the matching of field values to be case-sensitive.
11. Click **Save & Close**.

Edit a simple group

Procedure

1. Click **Admin** in the area navigation bar to navigate to the Admin area of the ProSphere Console.
2. Click **System.**
3. Click the **All Groups** tab to display logically grouped resources.
4. In the tree, expand the group in which you plan to edit the group.
5. Select the group you want to edit.
6. Click **Edit** to edit a simple group.

Edit a smart group

Procedure

1. Click **Admin** in the area navigation bar of the ProSphere Console.
2. Click **System.**
3. Select **All Groups** .
4. In the tree, expand the group in which you plan to edit the smart group.

5. Select a group.
6. Click **Edit**.

   Alternatively, you can use the right-click option on a parent group in the tree.
7. Step through the "edit smart group procedure" just as you would the "create smart group procedure" presented in Create a smart group on page 103.

Delete a group

Procedure

1. Click **Admin** in the area navigation bar of the ProSphere Console.
2. Click **System.**
3. Select **All Groups**.
4. In the tree, select **Groups**.
5. In the table, select the group to delete.
6. Click **Delete**.

Tags for discovered configuration items

As a ProSphere administrator you can tag a configuration item with informational attributes meaningful to your requirements. These attributes are independent of the associated configuration item and are available only in your environment for the administrators to view, manage, or share.

For example, you could tag a configuration item by its location. The name of the tag could be "Location" and a value for the tag could be "New York". When the configuration item is discovered, the associated tag informs administrators of the discovered object's location.

Tagging a configuration item allows you to:

- Associate tags to configuration items in ProSphere
- Export tag data to an output file
- Import tag data from an input file into the system
- Manage the tag values through the ProSphere Console
- Create smart groups based on tags

Create a tag

You can create a tag from the **Admin › System › Manage Tags** view or alternately from the CI dialog **Attributes › Manage tags** view.
To create a tag from the Admin area in the area navigation section:

Procedure

1. Log in with Security Administrator privileges.
2. Click **Admin** in the area navigation section.
3. Click **System**.
4. Click **Manage Tags**.
5. Click **Create Tag** to open the **Create Tag** dialog box.

6. Type a name for the tag in the **Tag** field.
7. Type in the values for that tag in the **Values** field. Separate values with a comma.
8. Click **OK**.

Edit a tag

You can edit a tag from the **Admin › System › Manage Tags** view or alternately from the CI dialog **Attributes › Manage tags** view.

Procedure

1. Log in with Security Administrator privileges.
2. Click **Admin** in the area navigation section.
3. Click **System**.
4. Click **Manage Tags**.
5. Select a tag from the tags list.
6. Click **Edit**.

   The values under the **Values** column is highlighted
7. Click to view the edit options in a drop-down list.
8. Remove an existing tag value or add a new tag value from the drop-down list.

   If you are adding more than one values, separate each of them with a comma.
9. Click outside of the menu to assign the modified values for the tag and save the changes.

Associate a CI with a tag

You can associate a discovered configuration item with a tag for the purpose of adding additional information about the item, easily identifying the item, creating a smart group, or searching for the item. When you associate a tag, you can use a previously created tag or create a new tag.

Use an existing tag to associate

1. Click **Discovery** on the ProSphere Console, and select **Object List**.
2. Select the relevant tab where the discovered configuration item is listed.
3. Click the discovered configuration item. The configuration item panel is displayed.
4. Click **Manage Tags**. The **Manage Tags** dialog box appears.
5. From the list of tags shown, select the tag, and click **OK**. The association is completed.

Create a new tag to associate

1. Click **Discovery** on the ProSphere Console, and select **Object List**.
2. Select the relevant tab where the discovered configuration item is listed.
3. Click the discovered configuration item. The configuration item panel is displayed.
4. Click **Manage Tags**. The **Manage Tags** dialog box appears.

5. Click **New Tag**.
6. Enter name of the tag in the text field, and press **Enter**. The created tag is listed under **Tag.**
7. Along the listed tag, click under the **Values** column. A drop-down list appears.
8. Select the check box, and enter the relevant value for the tag. You can separate multiple values with a comma (,).
9. Click **OK**. The association is completed.

Note

When you create a tag, do not enter the unsupported special characters in the **Tag Name** and **Values** fields. The unsupported special characters are backward slash (\), forward slash (/), quotation marks (" or '), angle brackets (› or ‹), pipe symbol (|), colon symbol (:), hash symbol (#), and comma (,).

Export a tag

A tag record consists of the name of that tag, its assigned values, and URI of the Configuration Item to which the tag is associated. You can export the tag data in the CSV format onto a location of your preference. The stored tag record can be viewed in a spreadsheet or be imported onto a ProSphere appliance as a .CSV file.

Procedure

1. Log in with Security Administrator privileges.
2. Click **Admin** in the area navigation section.
3. Click **System**.
4. Click **Manage Tags**.
5. Select a tag.
6. Click **Export**.

   A **Save as** dialog box appears.
7. Select the location where you want to store the tag file, and then click **Save**.

   The tag file is stored in the CSV format.

Import a tag

You can import the tag data in the CSV format onto ProSphere. The .csv file contains combination of tag names, and tag values associated with Configuration items. The column header of the .csv file contains Tag Name, Tag Value, Object Name. The object name can be an IP Address of the CI, a Full Qualified Domain Name of the CI or the Host Name.

The imported tag record would be shown along with other tag records. A tag record consists of the name of that tag, its assigned values, and URI of the Configuration Item to which the tag is associated.

Procedure

1. Log in with Security Administrator privileges.
2. Click **Admin** in the area navigation section.
3. Click the **System** tab and then click **Manage Tags**.

4. Click **Import**.

   A dialog box to select the tag data file is displayed.

5. Select the tag data file that needs to be imported, and then click **Save**.

Path performance collection

Path performance collection is a process by which you collect performance data for a selected host or group of hosts and for switches and storage systems on the input and output paths of the host.

After you enable path performance collection, the process starts automatically for any new switches or storage systems discovered on the input and output paths of selected hosts. When discovery is successful for a newly added host in a group, smart group or subgroup for which path performance collection is turned on, the process of path performance collection starts automatically.

Note

For any current restrictions on storage systems for which performance data is collected, refer to the *EMC ProSphere Support Matrix*.

Collection intervals

The default collection interval for path performance collection is 15 minutes. You can change the collection interval to 5 minutes or 60 minutes for discovered hosts or for a specific group. A new collection interval set for a group is applicable to all its subgroups and discovered hosts.

For a discovered host or subgroup, path performance data is collected using the shortest interval defined for any group that contains the host or subgroup.

Restrictions

- If you switch on path performance collection for a group, you cannot switch it off for individual hosts and subgroups contained in the group.
- The collection interval for individual hosts and subgroups cannot be longer than the collection interval set for the entire group.

Limitation

In case of a user-defined, mixed group that contains hosts, storage systems, and switches, the collection of path performance data is based on hosts. For example, suppose that group A contains members host H1, switch S1, and array A1. Group A contains objects that are not connected to a host—switch S2 and array A2. Group A contains a host that is not connected to a switch or array—H3.

If you enable performance data collection on group A, performance data collection selects all hosts in group A, and for each selected host it looks for an end-to-end path containing the host. Performance data is collected for all discovered hosts, and for any discovered storage system or switch that is contained in an end-to-end path that contains a host.

If H1->S1->A1 is an end-to-end path, performance data is collected for H1, S1, and A1.

If S2 and A2 have no associated host, thus no available end-to-end path, no performance data is collected for them.

Performance data is collected for H3, because it is a discovered host.

Switch on performance data collection for discovered hosts

You can switch on path performance collection for discovered hosts and groups.

Procedure

1. Click **Discovery** in the area navigation bar on the ProSphere Console.
2. Click **Objects List**.
3. Select **Hosts**.
4. Switch on the toggle button in the **Path Performance Collection** column.

Start path performance collection for groups

Procedure

1. Click **Admin** in the area navigation bar on ProSphere Console.
2. Click **System**.
3. Select **Manage Groups**
4. Click **Groups** in the left hand panel. This displays all the members.
5. Switch on the toggle button in the Path Performance Collection column for the desired member

Stop path performance collection for discovered hosts

You can switch off path performance collection for discovered hosts and groups.

Procedure

1. Click **Discovery** in the area navigation bar on the ProSphere Console.
2. Click **Objects List**.
3. Select **Hosts**.
4. Switch off the toggle button in the **Path Performance Collection** column.

Stop path performance collection for groups

Procedure

1. Click **Admin** in the area navigation bar on ProSphere Console.
2. Click **System.**
3. Select **Manage Groups**.
4. Click **Groups** in the left hand panel. This displays all the members.
5. Switch off the toggle button in the **Path Performance Collection** column for the desired member.

Change the collection interval for discovered hosts

Before you begin

Before you change the collection interval for a host, you must turn on performance collection for at least one discovered host.

Procedure

1. Click **Discovery** in the area navigation bar on the ProSphere Console.

2. Click **Objects List**.
3. Select **Hosts**.
4. Click Settings in the **Path Performance Collection** column.
5. Select a collection interval from the available list.

Change the collection interval for groups

Before you begin

Before you change the collection interval for a group, you must turn on performance collection for at least one group of discovered hosts.

The collection interval for a group must be larger than the largest value of a single discovered host contained in that group.

Procedure

1. Click **Admin.**
2. Click **System.**
3. Click **Manage Groups**.
4. Click **Groups** in the left hand panel in the All Groups tab.
5. Click **Settings** in the Path Performance column. (This is available only when the path performance is on.)
6. Select a collection interval from the available list.

Capacity utilization of discovered arrays

The capacity utilization for discovered storage systems is reported using service level. At deployment, ProSphere has a set of predefined service levels and associated predefined definitions. Service levels are used to associate the LUNs and report the capacity of utilization by a service level for storage groups and different configuration items.

Note

A single service level can have multiple definitions associated with it.

Service level definitions

Definitions are either FAST managed or non-FAST managed.

- The FAST managed definitions are characterized by the Policy Name associated with the discovered storage unit. Each policy has predefined tiers associated with it. The predefined tiers have definitions made up of disk characteristics, which are created when the policy is defined on the Symmetrix.
- The non-FAST managed definitions are characterized by array type, disk technology, disk speed, and RAID protection.

There are four predefined service levels, namely, Platinum, Gold, Silver, and Bronze. The predefined service levels can be modified to other types of definitions. Table 21 on page 111 lists predefined service levels and their predefined definitions.

Table 21 Predefined service levels and their predefined definitions

Service level	FAST managed	Definition type
Platinum	Yes	Policy name
	No	Array type - Any Array Name - NA Disk Technology - Enterprise Flash Drive Disk Capacity - Any Protection - Any
Gold	Yes	Policy name
	No	Array type - Any Array Name - NA Disk Technology - Fibre Channel; RAID 1 Disk Capacity - Any Protection - RAID 1
Silver	Yes	Policy name
	No	Array type - Any Array Name - NA Disk Technology - Fibre Channel; RAID 5 Disk Capacity - Any Protection - RAID 1
Bronze	Yes	Policy name
	No	Array type - Any Array Name - NA Disk Technology - SATA Disk Capacity - Any Protection - Any

If the definitions are not FAST managed, the criteria for a definition consist of a set of rules you create. The rules filter a specific array based on parameters such as disk technology, disk size, and RAID protection type for a specific service level. Table 22 on page 111

Table 22 Definition attributes

Array type	Disk technology	Disk capacity (GB)	Available RAID protection type
CLARiiON	ATA	0 - 200	RAID 0
	Fibre Channel	200 - 500	RAID 1
	SAS	500+	RAID 10
	SATA		RAID 3

Table 22 Definition attributes (continued)

Array type	Disk technology	Disk capacity (GB)	Available RAID protection type
	SATA II	Custom	RAID 5 RAID 6
Symmetrix	Any Enterprise Flash Drive FC 10K FC 15K Fibre Channel SATA	0 - 200 200 - 500 500+ Custom	RAID 1 RAID 5 RAID 5 3+1 RAID 5 7+1 RAID 6 RAID 6 14+2 RAID 6 6+2

Create a service level

Procedure

1. Click **Explore** on the ProSphere Console.
2. Select the **Service Levels** tab.
3. Select **Manage Service Levels**.
4. Click **Create Service Level**.
5. Type a service level name in the **Service Level Name** field.
6. Click **Create Definition**.
7. Select one of the following:
   - **Yes** if the definition is FAST managed. Select the appropriate **Array Type**, **Definition Type**, and **Policy Name**.
   - **No** if the definition is not FAST managed. Select the appropriate **Array Type**, **Disk Technology**, **Disk Capacity**, and **Protection**.

   Note

   If you select the custom option for **Disk capacity**, type a disk size in the field that is next to the custom option.
8. Click **OK** to create a service level.

Edit a service level

Procedure

1. Click **Explore** on the ProSphere Console.
2. Select the **Service Levels** tab.
3. Select **Manage Service Levels**.
4. Select a service level.

5. Click **Edit**.
6. Modify the service level name in the **Service Level Name** field.
7. Click one of the following:
   - **Create Definition** to add a new definition to the selected service level.
   - **Edit** to edit the definition.
8. Make the required modifications to the selected definition.

   Note

   You can change a non-FAST managed definition to a FAST-managed definition.

   Note

   In a non-FAST managed definition, if you select the **Custom** option for **Disk Capacity**, you can type in the specific range for disk size in the field next to the **Custom** option. If you do not select the **Custom** option you can select the other available options: Any, 0-200 GB, 200-500GB or 500+GB. The Custom option is available only for the non-FAST managed definition.
9. Click **OK** to save the changes.

Reorder service levels

Procedure

1. Click **Explore** on the ProSphere Console.
2. Select the **Service Levels** tab.
3. Select **Manage Service Levels**.
4. Select a service level from the list of service levels.
5. Click:
   - The arrow pointing up, on the left side of the table, to shift the selected service level up by one row.
   - The arrow pointing down, on the left side of the table, to shift the selected service level down by one row.

Host resolution

The host resolution feature collects information about a host without using discovery. Hosts identified by host resolution are termed "system created hosts."

In some instances, you may not want to share access credentials for a host. At times, ProSphere cannot access a host. In these situations, ProSphere cannot discover a host, but attempts to use a zone name to identify the host and collect information with host resolution. Thus, you can still display graphical representations of network topology. You can display performance data about CIs connected to a system created host.

Note

The host resolution feature does not enable ProSphere to collect performance data for a host. To collect performance data, ProSphere must use discovery to collect information about the host.

For accurate host resolution, follow consistent zone naming conventions. For example, you can configure zoning in a fabric by creating one zone per server and including a host name in the zone name.

The **Created By** field on the **Discovered Hosts** view indicates how ProSphere identified a host, as described in Table 23 on page 114.

Table 23 Host identification methods

Created By field displays...	Method used to identify host
System	Host resolution
Discovery	Discovery

Note

When a host is passively discovered, or when there is a zoning misconfiguration between the host and the array, the host LUN name may be displayed as `Unknown`.

Configure host resolution

Procedure

1. Click **Discovery** in the area navigation bar of the ProSphere Console
2. Click **Discovery Jobs**.
3. Select an access credential.
4. Select **Configure Host Resolution**.

   Note

   Configuring host resolution requires administrator privileges. The **Configure Host Resolution** button is hidden for the User role.

5. Select **Resolve hosts**.

   By default, **Resolve hosts** is selected. If **Resolve hosts** is not selected, host resolution does not occur in future discoveries.

6. Specify DNS usage, as described in the following table.

Setting	Means
Upon successful validation by DNS	If DNS validation fails, do not attempt to resolve the host. This is the default.
Independent of validation by DNS	Even if DNS validation fails, attempt to resolve the host.
Without using DNS	Do not use DNS to validate that the host name exists.

Note

If DNS validation succeeds, host resolution collects additional host attributes, including the IP address of the host and the name of the host's domain.

7. Type one or more strings to specify the zone naming conventions in your fabric.

   Click the plus (+) button on the last displayed line if you need an additional input line. Click the minus (-) button to remove an input line.

   Use *%h%* to specify where the host name occurs in a zone name. Use the wildcard character (*) to indicate that any characters can occur at a location in a zone name.

   For example, if the zone name is *z_host1_iwa_lab*, the following zone convention strings allow ProSphere to identify the host name as *host1*:

   *z_%h%_*_**

   *z_%h%_**

   _%h%_iwa_

   NOTICE

   Be careful to type correct strings. If you type an incorrect string, ProSphere can create invalid hosts. For example, if a zone name is *z_host1_abc_lab*, the zone naming convention *z_%h%* yields a host name of *host1_abc_lab*, instead of *host1*.

8. Select one of the following:

Button	Action
OK	Saves values and closes the dialog box. If **Resolve hosts** is selected, host resolution is performed at the next discovery.
Resolve Now	Saves values and immediately performs host resolution on previously discovered zones.
Cancel	Cancels the dialog box.

CHAPTER 6

Log Files

This chapter contains the following topics:

Logs overview

ProSphere supports logging of events by services associated with its components. All components along with their logging services are available in the **Manage Logs** dialog box accessed from the **Administration** › **System** › **Manage Logs** option.

A single service may have multiple log files that are maintained in text files with a .log extension. When you download them, ProSphere creates a single compressed .zip file for all the log files of the selected service.

Use the **Manage Logs** dialog box to perform the following tasks:

- Edit the log levels set for the service logs on page 118
- View ProSphere components and services related to them on page 121
- Download logs for selected components to provide to EMC Customer Support on page 122

The downloaded logs are useful for sharing with EMC Customer Support when their intervention is required to resolve operational issues for which no documented resolution is available.

Note

If you encounter problems while performing any operational, maintenance, or setup tasks, before contacting EMC Customer Support, check Troubleshooting on page 153, and online help topics on troubleshooting, for possible resolutions or workarounds.

Log levels

The log level controls the detail at which information about a component is written to a log file. ProSphere supports five log levels.

The log levels are listed here in the descending order of detail available in the logs:

- TRACE — Provides the most detailed information.
- DEBUG — Provides information on events that may be relevant for debugging.
- INFO — Provides information relevant to the overall progress of the application. INFO is the default log level.
- WARN — Provides information on potentially harmful conditions that merit attention to ensure that critical application operations are not affected.
- ERROR — Provides information on events that may or may not be fatal to ProSphere and merit investigation.

As you move up the list, log levels are cumulative. Each log level causes the logger to write messages of that log level and levels below it to a log. For example, if log level is set to INFO for a service, the logger writes messages of the types INFO, WARN, and ERROR for that service to the log.

NOTICE

To conserve disk space, log levels should not be set to the DEBUG or TRACE levels for more than one or two hours. After collecting log files, reset the log level back to INFO.

Edit log levels for ProSphere components

Few components have multiple logging services. Such component services are grouped as parent logging categories containing subcategories. For grouped logging categories,

you can only edit the log levels for the parent category and not the log level set for the subcategories. This means that subcategories log at the log level set for the parent category.

Note

You cannot edit the log level for a few of the components. Components that do not allow changing the log level on page 119 lists the components for which you cannot edit the log level.

Procedure

1. Click **Administration** on the ProSphere Console.
2. Click the **System** tab and then click **Manage Logs**.
3. In the **Manage Logs** dialog box, select the service log category for which you want to edit the log level.
4. Click **Edit Log Level**.

   The **Edit Log Level** dialog box appears with the log level as Info.
5. Select the log level you want to set for the selected service.
6. Do one of the following:
   - Click **Update** to save the selected log level and close the **Edit Log Level** dialog box.

     Note

     All services associated with the parent category begin logging at the new log level.
   - Click **Cancel** to close the **Edit Log Level** dialog box without making any changes to the log level and return to the **Manage Logs** dialog box.

Components that do not allow changing the log level

The following table lists the components for which ProSphere does not support editing of the log level along with the associated services and log files. Editing of the log level for these components is not possible due to a variety of technical limitations. The default log level for these components is INFO.

Table 24 Components with uneditable log levels

Component	Service name	Log file
Database	Database	• All logs in the directory `/var/lib/gpsql/gpAdminLogs`. • All logs in the data directory for the database master (`/data/master/gpsrm-1/pg_log`). • All logs in the data directory for the segment instances (for example, `/data/gpdata4/gpsrm3/pg_log`).
Array Discovery	Discovery	`array1.log`
Broker Service		`brstart.log`

Table 24 Components with uneditable log levels (continued)

Component	Service name	Log file
Path Domain Manager		path.log
Host Domain Manager		host1.log
Indication Domain Manager		indications.log
Service Daemon		sm_serviced.log
SAN Domain Manager		san1.log
Trap Daemon		sm_trapd.log
VMware Domain Manager		vminframon.log
Discovery Configuration Service		• AMSDataManager.log • TaskManager.log • Scheduler.log • TaskScheduler.log • discovery-service.log • translator.log, path_java.log
ConnectEMC Service	Infrastructure	• ConnectEMC.log • ConnectEMC_*Transfer Method*.log Example: ConnectEMC_FTP.log • *Transfer Method*-cURL.log Example: FTP-cURL.log
Monitoring Service	Monitoring	srm_mon_svc_down.log
Apache Web Server Service	Others	• access_log, ssl_request_log • error_log, mod_jk.log • rcapache2.out
Firewall service		firewall-ProSphere_Application.log
VAMI		vami_set_hostname.log
XML Database Service		xdb_err.log, xdb_out.log
Historical Service	Performance	spi-historicalserver.log

Logs that do not allow change of log level

The following table lists the log files for which ProSphere does not support change in log level although users can edit the associated component log level in the **Manage Logs** UI. The default log level is INFO.

Table 25 Log files with uneditable log levels

Service name	Unchangeable level in...	Editable log level for...
Infrastructure	`data_export_out.log` Location: `/var/log/`	Log Management Service
	• `srmConfigInitError.out` Location: `/var/log/` • `SRMConfiguration.log` Location: `/var/log/tomcat6/`	Configuration Service
Others	`ntp.log` Location: `/var/log/`	Time Service
Performance	• `srm-ActiveProbe.log` Location: `/var/log/` • `/var/log/srm-datacollectionservice-service.log` Location: `/var/log/`	Active Discovery Probe Service
	`srm-collectorregistry-service.log` Location: `/var/log/`	Data Collection Registry service
	`srm-threadmanager-service.log` Location: `/var/log/`	Data Collection Thread Manager Service
	`srm-dsrestlet-service.log` Location: `/var/log/`	Discovery Service RESTlet Service
Web server	• `catalina.out` • `sda-datasource-app/litewave.trc` Location: `/var/log/tomcat6/`	Tomcat Service

View ProSphere components and services

Procedure

1. Click **Administration** on the ProSphere Console.
2. Click the **System** tab and then click **Manage Logs**.

   The **Manage Logs** view appears with the following details:
   - Service Log

The ProSphere logging component and its services supporting logs. Click the expand button (**+**) to view the individual services.

- Description

  A description of service logs available for the specific component. For a component service, this column provides a description of the log entries users can find in the logs.

- Log Level

  The log level set for the component and its services. The log level indicates the type and quantity of log messages currently output for a specific component.

3. Click **Close** to close the **Manage Logs** dialog box and return to the **System** view.

Download service logs of selected ProSphere components

When you need help diagnosing problem, you may need to send debug logs to EMC Customer Support. The **Download** option in the **Manage Logs** dialog box enables you to download select service logs of ProSphere components in a .zip file format.

Procedure

1. Click **Administration** on the ProSphere Console.
2. Click the **System** tab and then click **Manage Logs**.
3. In the **Manage Logs** dialog box, select the service (parent category or subcategory) for which you want to download the logs.

   Note

   You can select multiple parent categories or subcategories.

4. Click **Download**.

   The **Download Logs** dialog box appears.

5. In **Download to:** type the name with which you want to save the downloaded log files in a .zip file format.
6. Click **Open** and browse to the location on your local system where you want to save the downloaded service logs.
7. Do one of the following:

   - Click **OK**.
   - Click **Cancel** to return to the **Manage Logs** dialog box without downloading the selected service logs.

Sample log

This topic contains a sample log file.

Each *message* in the file has the following format:

- Header line, which contains information, most of which specifies where and when the message was output:

  `<yyyy-mm-dd hh-mm-ss>,<thread-id> <log level> <module-name>`

  where:

  - *‹yyyy-mm-dd hh-mm-ss›* is the time specified in the format year-month-day hour-minute-second

- *‹thread-id›* is the id of the thread
- *‹log level›* is the log level in effect
- *‹module-name›* is the name of the module

- Message line, having the following format:

  com.emc.srm.*<application-name>*.*<component-name[.<subcomponent-name>...]* <message>

  where:
  - *‹application-name›* is the application that output the message
  - *‹component-name›* is the component that output the message
  - *‹subcomponent-name›* is the subcomponent that output the message

The following is an example of log entries available in an INFO log:

```
2011-01-28 17:10:53,045 ERROR [main]
com.emc.srm.sda.sdarestdataserver.SrmAtomClientFeedProcessor Error in
processing the response received for the GET query.
2011-01-28 17:10:53,045 ERROR [main]
com.emc.srm.sda.sdarestdataserver.SrmAtomClientFeedProcessor Error in
processing the response received for the current page request.
2011-01-28 17:10:53,054 INFO [main]
com.emc.srm.sda.sdarestdataserver.SrmAtomClientFeedProcessor Sending
the POST query through Java client.
2011-01-28 17:10:53,057 INFO [main]
com.emc.srm.sda.sdarestdataserver.SrmAtomClientFeedProcessor Content
Type set to application/atom+xml
2011-01-28 17:11:03,059 INFO [main]
com.emc.srm.sda.sdarestdataserver ............polling the config
service....2011/01/28 17:11:03
2011-01-28 17:11:03,421 INFO [main] com.emc.srm.sda.sdarestdataserver
2011-01-28 17:11:03,422 INFO [main] com.emc.srm.sda.sdarestdataserver
End fetching configuration data
2011-01-28 17:11:03,513 INFO [main] com.emc.srm.sda.sdarestdataserver
SDADataServer successfully started on port number: 9877
2011-01-28 17:11:03,513 INFO [main] com.emc.srm.sda.sdarestdataserver
SDADataServer started on port 9877
2011-01-28 17:15:21,449 INFO [main] com.emc.srm.sda.sdarestdataserver
Started fetching configuration data
2011-01-28 17:15:27,812 ERROR [main]
com.emc.srm.sda.sdarestdataserver.SrmAtomClientFeedProcessor Error in
processing the response received for the GET query.
2011-01-28 17:15:27,813 ERROR [main]
com.emc.srm.sda.sdarestdataserver.SrmAtomClientFeedProcessor Error in
processing the response received for the current page request.
2011-01-28 17:15:27,848 INFO [main]
com.emc.srm.sda.sdarestdataserver.SrmAtomClientFeedProcessor Sending
the POST query through Java client.
```

Log retention

ProSphere retains logs in the database, depending on two predefined retention parameters for each service:

- Maximum file size of the log file

  When an active log reaches the defined maximum file size, ProSphere archives the file and creates a new log for subsequent entries.

- Maximum number of archived files

  When the number of archived files for a service reaches the maximum number defined for it, the archived files are removed from the database to make space for new log files. This can vary for each ProSphere component.

Note

If you need to customize the log retention parameters to your specific needs, contact EMC Customer Service.

This table lists the maximum log file size and maximum number of archived files allowed for all services that generate logs into the `/etc/srm/logconfig` directory.

Table 26 Log retention parameters for services

Service name	Maximum file size	Maximum number of archived files
Admin Rest Server	15MB	10
Alert Indication Client	15MB	10
Alerting Service	15MB	10
Cache Server (0)	15MB	10
Cache Server (1)	15MB	10
Capacity Input Server	15MB	10
Capacity UI Server	15MB	10
Coherence JMX Service	15MB	10
Configuration Service	15MB	10
Discovery Data Service	15MB	10
Discovery Rest Service	15MB	10
Event Manager Service	15MB	10
Event Rest Service	15MB	10
Launch In-Context Service	15MB	10
Licensing UI Service	15MB	10
Log Management Service	15MB	10
Maps Service	15MB	10
MSA Configuration Proxy Service	15MB	10
MSA Configuration Service	15MB	10
Performance Data Collection Server	300MB	12
Service Level Service	15MB	10
Time Service	15MB	10
Tomcat Service	15MB	10
Topology Service	30MB	12
Topology Transformer Service	30MB	12

Table 26 Log retention parameters for services (continued)

Service name	Maximum file size	Maximum number of archived files
Topology Change Notification Service	15MB	12

CHAPTER 7

Migration from EMC Control Center

This chapter contains the following topics:

Comparison of ProSphere with EMC ControlCenter

Table 27 on page 128 lists several advantages that ProSphere has over EMC ControlCenter.

Table 27 Comparison: EMC ControlCenter and ProSphere

Feature	ControlCenter	ProSphere
Main components	EMC ControlCenter server EMC ControlCenter store API server StorageScope server	Functions are performed by the ProSphere Application.
Deployment procedure	Installer deployed each component separately with InstallShield.	Only one vApp to deploy. A wizard automatically deploys all components.
Discovery	Discovery required that agents be deployed on managed elements (for example, on each host, on Symmetrix® arrays, and on CLARiiON® arrays). An agent pushed data to EMC ControlCenter. Many Symmetrix agents were required.	ProSphere is agentless. In ProSphere's agentless discovery, a small number of customer-installed software components called "providers" surface information that conforms to standard profiles, such as SNIA an DMTF, to gather information about elements. Using providers requires less software to be installed and managed than using agents. ProSphere collects data from the network objects that have providers installed.
Protocols	Numerous protocols Some agents have more than one protocol.	SMI-S SNMP SSH WMI WS-MAN
Database	Traditional database management system. Different query processing jobs generally share access to the same hard-drive disks, which can slow individual queries.	A single database query can run against many segments of data simultaneously.

Overview of WLA data import

ProSphere uses agentless performance data collection for discovered configuration items. Both EMC ControlCenter 6.1 and ProSphere recognize a similar set of configuration items, called "managed objects" in EMC ControlCenter. This makes it possible to import historical performance data collected and stored in EMC ControlCenter's Workload Analyzer (WLA) Archiver to add to ProSphere's performance data for trending.

The advantage of the WLA data import feature is that it enables you to view EMC ControlCenter performance data in ProSphere without logging into EMC ControlCenter. You can reimport the EMC ControlCenter performance data any number of times to obtain the latest performance data for discovered configuration items or import data for newly added EMC ControlCenter configuration items.

Note

ProSphere performance data collection influences the running of WLA data import. Impact of path performance collection on page 135 discusses this in detail.

Only users with administrator privileges can view, set up, and run import jobs in ProSphere.

Data import assumptions on page 130 explains why EMC ControlCenter agent management permission is required.

The import job imports 30 days of daily performance data (.btp files) for discovered configuration items from the EMC ControlCenter WLA Archiver data source. The import operation excludes the performance data for the day the import job starts running. So, if the import job is started on May 6th, the import job imports performance data from April 6th to May 5th into ProSphere from the EMC ControlCenter data source. The imported performance data can be viewed in the Configuration Item dialog box.

If there are multiple instances of EMC ControlCenter in your enterprise setup, you can import performance data from all EMC ControlCenter WLA Archivers in the deployments to ProSphere.

Note

While migration is running it utilizes available CPU. If VMware alerts are triggered due to increased CPU utilization, we recommend that the user refer to the VMware documentation to configure the user's system to prevent the alerts.

Working with data sources

You can access the EMC ControlCenter performance data import feature by selecting **Administration** › **System** › **Import Performance Data**. The **Import Performance Data from ControlCenter** dialog box is displayed.

The **Import Performance Data from ControlCenter** dialog box allows you to perform the following activities:

- View a list of all added WLA Archiver data sources along with import status and details. Access details about import jobs on page 132 provides detailed information on import jobs.
- Add WLA Archiver data sources. Add a WLA archiver data source on page 130 describes how to add a WLA Archiver data source to ProSphere.
- Edit WLA Archiver data sources. Edit details of a WLA archiver data source on page 131 describes how you can edit details of existing WLA Archiver data sources in ProSphere.
- Reimport daily performance data from WLA Archivers. Import performance data on page 131 describes reimport functionality and provides instructions on how to reimport performance data from EMC ControlCenter.

Prerequisites for data import

To import performance data successfully from EMC ControlCenter WLA Archivers, ensure that the following prerequisites are met:

- EMC ControlCenter 6.1 UB5 release or higher is available.
- EMC ControlCenter infrastructure and WLA Archivers must be running.
- The Historical Database and the Performance Metric Integration Server services are running. Monitor services on page 154 explains how to display the status of services.
- CIs corresponding to the EMC ControlCenter "managed objects" must be discovered in ProSphere.

Data import assumptions

WLA data import makes the following assumptions about data import:

- Deployments of ProSphere and EMC ControlCenter will run in parallel for a certain period of time.
- Only one import job can be run at any time for a single instance of EMC ControlCenter. When an import job is initiated, it runs first. All other jobs are placed in a queue in chronological order.
- If you need to import data from EMC ControlCenter, you should be aware that WLA Agents must be running for the data to be transmitted. If the data fails to be imported into ProSphere, contact the EMC ControlCenter administrator and request that they check and restart the agents.

Import performance data

This section explains how to import performance data from EMC ControlCenter:

Procedure

1. Add a ControlCenter WLA Archiver data source on page 130
2. Import the data on page 131

Add a ControlCenter WLA Archiver data source

Specify the EMC ControlCenter WLA Archiver data sources from which you will import performance data.

To add an EMC ControlCenter WLA Archiver data source:

Procedure

1. In the **Import Performance Data from ControlCenter** dialog box, click **Add**.
2. Provide the following WLA Archiver data source details:

Field	Description
WLA Archiver Host Name	FQDN or a valid host name or IP address. For example, Test123.abc.xyz.com, CCWLAMigrationHost1, or 192.168.0.0.

Field	Description
	Note An error is displayed only if you add the FQDN or IP address first and then attempt a duplicate entry with the hostname. ProSphere allows you to add a data source hostname and then a duplicate entry for the same data source with either its FQDN or IP address. The duplicate entry is not recognized as an error. The application treats duplicate entries as separate import jobs without overwriting any imported performance data.
Archiver Port	Valid IP address to access the WLA host. The default port is 30103. Only numeric values are valid and the range is from 0 to 65535.
SSL Enabled	Check box is selected by default. You can clear the checkbox if SSL is not applicable to your EMC ControlCenter deployment.

3. Click **OK** to save the details and create the new EMC ControlCenter WLA Archiver data source.

Edit an EMC ControlCenter WLA Archiver data source

You can edit the details of EMC ControlCenter WLA Archiver data sources listed in the **Import Performance Data from ControlCenter** dialog box.

Procedure

1. In the **Import Performance Data from ControlCenter** dialog box, click **Edit**.
2. Edit the data source details and click **OK**.
3. Click **OK** to save the modified details and return to the **Import Performance Data from ControlCenter** dialog box.

Import the data

When you run an import job, ProSphere processes the performance data (.btp) files contained in the EMC ControlCenter hosts you specified in the **Import Performance Data from ControlCenter** dialog box.

Procedure

1. In the **Import Performance Data from ControlCenter** dialog box, click the WLA Archiver data import job you want to run.
2. Click **Import** in the **Import Performance Data from ControlCenter** dialog box.

   If another import job is already running, the import job is placed in chronological order in the Pending queue.

Results

When the import job has successfully finished importing performance data for the selected data sources (**Status** column displays Success), you can view the performance data in the **Performance** charts for a specific host, switch, or storage system.

Reimport performance data on page 132 describes when and how you can rerun an import job and how this rerun or reimport is handled in ProSphere.

Reimport performance data

Reimportation of performance data uses the same procedure explained in Import the data on page 131.

ProSphere allows you to rerun any import job whether or not the previous run was successful. In the reimport process the import job performs the following operations:

- Checks existing configuration items and imports performance data to ProSphere without overwriting the existing data
- Collects performance data for new configuration items

Access details about import jobs

Procedure

1. Click **Import Performance Data**.

   The **Import Performance Data from ControlCenter** dialog box opens. Import performance data from ControlCenter dialog box on page 132 provides detailed information.

2. Click **Close** to close the **Import Performance Data from ControlCenter** dialog box and return to the **System** tab.

Import Performance Data from ControlCenter dialog box

The **Import Performance Data from ControlCenter** dialog box provides details of the import jobs for the EMC ControlCenter WLA Archivers listed.

Note

Import details in the dialog box are not updated in real time. Use the **Refresh** button to view the latest details.

The default listing order in the view is from the WLA Archiver data source. However, if you choose to sort the data sources by any of the columns in the dialog box, the sorting order last used is retained when you next access the **Import Performance Data from ControlCenter** dialog box.

The **Import Performance Data from ControlCenter** dialog box provides the information in Table 28 on page 132

Table 28 Import Performance Data from ControlCenter dialog box

Field	Description
WLA Archiver Data Source	Fully qualified domain name (FQDN), host name, or IP for the WLA Archiver. This is the EMC ControlCenter source host where the performance data is available for importing. **Note** Import job states on page 134 lists all possible statuses and messages corresponding to each of these import data job states.
State	State of the most recent import job for the WLA Archiver. This could be:

Table 28 Import Performance Data from ControlCenter dialog box (continued)

Field	Description
	• Never Run — Indicates the import job has not been initiated. This is the initial state for a newly added import job. • Running — Indicates the import job is active and daily performance data is being imported from the selected WLA Archiver. All other import jobs initiated reside in the job queue in the Pending state. Jobs are picked up from the Pending queue in chronological order of initiation. • Pending — Indicates the import job has been initiated but is waiting in the job queue, because another job is currently active. Any number jobs can be Pending, in chronological order. • Completed — Indicates the import job was successfully executed with data either imported successfully or with failures. A corresponding **Status** message appears when the job is completed.
Status	Provides more information on the import job state — In Progress, Success or Failure. • Success — Indicates the import job was completed with all performance data imported from the data sources. • Failed — Indicates the import job failed to import all performance data from the data sources. An import job could fail for a number of reasons (for example, a network error, or incorrect configuration settings). **Note** This column is blank for Never Run state. **Note** You can verify the status of the import job using URIs. This can be especially useful when troubleshooting issues that might arise in WLA data import. The *EMC ProSphere RestAPI Online Help* help provides detailed information on the WLA data import URIs.
Message	Provides a description of the In Progress, Successful, Failure import statuses. The *EMC ProSphere RestAPI Online Help* provides detailed information on the messages displayed in this column.
Last Started	Date and timestamp when data import was last done.
Duration	Duration of the last data import job in the format *hh*hr(s).*mm*min(s) *ss*sec(s) (for example, 3hrs 1min 3secs).
CI Count	Total number of configuration items processed by the import job. This count appears only when the import job has completed. **Note** The CI Count does not necessarily indicate successful import of data to ProSphere for all processed configuration items. Check the **Status** and **Message** columns to verify if the data has been imported successfully for all processed configuration items.

Table 28 Import Performance Data from ControlCenter dialog box (continued)

Field	Description
	Note The CI Count is 0, the import job completed successfully, but no performance data is available to be imported to ProSphere for the discovered CI.

Import job states

The following table lists messages for the different states and statuses.

Table 29 Import job states, corresponding statuses and messages

State	Status	Message
Never Run	Not applicable, the Status and Message columns are blank.	N/A
Pending	Not applicable, the Status and Message columns are blank.	N/A

Running	In Progress	`<n> of <N> btp files processed`
		Example:
		`2000 of 3000 btp files processed`
		Note
		<n> is the actual number of files successfully processed out of the total number <N>.

Running	In Progess	`<n> of <N> btp files processed. Refreshing Performance Data.` Example: Message appears when the Status is in progress. Indicates the import job has successfully imported the performance data, but the data is being loaded into the ProSphere performance table.

Completed	Success	`<n> of <N> btp files processed. Performance data imported for all ProSphere CIs`
		Example:
		`500 of 500 btp files processed`

		`<n> out of <N> btp files processed. Performance data not available for ProSphere CIs.`

Table 29 Import job states, corresponding statuses and messages (continued)

State	Status	Message
		Example: `500 of 500 btp files processed. Performance data not available for ProSphere CIs.` **Note** If there are no btp files available for import, then only the message “Performance data not available for ProSphere CIs" is displayed **Note** The CI count column displays 0 (zero).

Completed	Failure	`<n> of <N> btp files processed. Reason: <Reason for failure to import all btp files>.`
		Example:
		`231 of 367 btp files processed. Reason: Unable to connect to WLA Agent.`

		`Host name cannot be resolved.`
		`Handshake failure <n> out of <N> btp files processed. Unexpected error.`

Impact of path performance collection

When you turn on path performance collection for a CI in **Discovery** › **Objects List** › **Hosts** (for arrays and switches) or **Admin** › **System** › **Manage Groups** › **Groups**, WLA data import is affected as follows:

- To avoid overlap between historical and performance data, ProSphere only imports historical data that was collected for a configuration item before path performance collection is turned on.
  Any import job that is running when path performance collection is turned on, or is started while path performance collection is running, excludes data for the configuration item.
- The contents of data that ProSphere imports for a configuration item depends on when the WLA data collection policy was enabled in EMC ControlCenter. EMC ControlCenter performance data is collected at hourly intervals.

  Note

  For configuration items not affected by path performance collection, ProSphere imports historical data for the full 30 days.

Example: Assume an import job for a configuration item was started on June 30th and EMC ControlCenter collects performance data at 15 minutes past each hour. Because 30 days of data are imported, not including the day of the import job, we would expect the import job to import all historical data from May 31st to June 29th (30 days).

Example: Assume path performance collection is turned on at 17:12 (HH:MM) on June 18th. As a result, WLA data import is limited to historical data collected until 16:15 of June 18th. No historical data is imported in an hourly collection at 17:15 because path performance collection was turned on at 17:12.

- For the time during which WLA data import and path performance collection are not running, ProSphere does not have any EMC ControlCenter performance data to display for a configuration item.
  This can happen if an import job stops because path performance collection is turned on and then, at a later time before WLA data import is again turned on, path performance collection is turned off. Until path performance collection runs again, and after it stops running an import job collects the newly collected performance data, there is a gap in the display of EMC Control Center performance data for the configuration item.

Example: An import job for a configuration item was started on June 30. Path performance collection was then turned on at 17:12 (HH:MM) of June 18, so WLA data import stops and the contents of the data import operation end at 17:00 (HH:MM) on June 18. Path performance collection is then turned off on June 23 at 10:20.
Assume that path performance collection is not run from June 23 10:20 to July 10 and during this time no import job is started. For the period when neither WLA data import nor path performance collection is running, ProSphere does not have any performance data for the configuration item.

CHAPTER 8

Synchronize Data

This chapter contains the following topics:

Overview

Synchronization is the combining of data about configuration items that are discovered in more than one deployment. Synchronization operates on deployments regardless of their physical location and creates a synchronized data set. The synchronized data set is updated every four hours and is available across all deployments. Without synchronization, the data in each deployment would be available only in that deployment.

Note

You can create separate deployments of EMC ProSphere to separate geographic areas or to scale the product. An environment can include multiple instances of ProSphere deployed in different portions of a lab, or in multiple labs in a data center, or in multiple data centers.

After synchronization, you can perform search operations and then display data about configuration items in the synchronized deployments. Synchronization enables you to do a search on a partial string for a configuration item and display a list of configuration items with the partial string in their names. If you click on a configuration item in the list, data is displayed from the ProSphere Application where the data resides.

Note

The data synchronization feature does not provide a single view into the database. It allows you to search for a configuration item and locate data stored in a different deployment of ProSphere.

When you synchronize deployments, you select one deployment to be the Master Capacity Application (MCA). The MCA stores all of the capacity data for the synchronized deployments.

NOTICE

Ensure that the Administrator logged into a ProSphere Application to add one or more ProSphere Applications for synchronization has identical user credentials on all ProSphere Applications that will be synchronized.

Data loss during synchronization

The ability to create an MCA allows you to store the capacity data for multiple synchronized deployments in just one location. The data is available for output in reports.

When you designate one ProSphere Application as an MCA, the full range of capacity data at remote applications is lost. However, as soon as the next rediscovery operation completes, the master application again has full knowledge of configuration items at the remote applications.

The only exception to this “full knowledge” is in historical data, which is to say, data that reflects changes over time, including any data that reflects historical trends. Examples include data that reflects the renaming of an array, or the declining state of available storage. All of this data about past events is lost, and for the new data collected by rediscovery, the clock restarts at the moment of rediscovery.

NOTICE

EMC recommends that you synchronize applications as soon as possible because the longer you wait, the larger the body of lost data can be. If you synchronize an application when it is deployed, the application does not contain any capacity data, so none is lost.

Note

In synchronization, no alerting data is lost.

Prepare deployments for synchronization

Keep in mind the following:

- If only one deployment is rolled back, it lacks information about other synchronized deployments and about discovered objects; but the other deployments (not rolled back) have the information. In other words, the previously synchronized deployments will no longer be "in sync," which can cause errors.

  To avoid errors, when rolling back the virtual machines in deployment X to snapshots, all deployments synchronized to deployment X must be rolled back to snapshots. Roll back to a snapshot on page 145 explains how to roll back virtual machines.

  Note

  If you synchronized deployments at a time later than the time of the state you are rolling back to, after the rollback you must resynchronize the deployments.

- To avoid errors, EMC advises customers to use policies that are clear as to which deployment manages which object.

  If two deployments manage the same object, the object appears twice in the synchronized data set, which can lead to errors.

Synchronization process

- Configure synchronization passphrase on page 139
- Add ProSphere Application for synchronization on page 140
- Synchronize resource data on page 140

Configure a synchronization passphrase

To synchronize discovered data in multiple ProSphere deployments, the ProSphere Applications in these deployments must be configured to communicate with each other. To enable communication between the ProSphere Applications, a ProSphere security administrator must configure the same synchronization passphrase on all ProSphere deployments that will be synchronized.

Procedure

1. Click **Admin** on the ProSphere Console.
2. Click the **Users and Security** tab.
3. Click **Configure Synchronization Passphrase**.
4. Type in the synchronization passphrase.

   The passphrase must be 6-10 words, not characters, long. The passphrase must not be the same passphrase as the one used in the last ten times it has been changed.

Any extra space leading or trailing the passphrase is truncated. Extra space in between words is changed to a single space.

5. Click **OK** to submit and save the synchronization passphrase.

Identify and add ProSphere Applications for synchronization

The **Synchronize Multiple ProSphere Applications** dialog box is the starting point for data synchronization. To access the **Synchronize Multiple ProSphere Applications** dialog box:

Procedure

1. Click **Admin** on the ProSphere Console.
2. Click the **System** tab.
3. Click **Synchronize ProSphere Applications**.

   The **Synchronize Multiple ProSphere Applications** dialog box appears.

   Note

   To synchronize discovered resource data with previous deployments of EMC ProSphere, you must identify the ProSphere Applications in the other deployments.

4. Identify other ProSphere Applications.
5. Click **Add**.
6. Enter a Fully Qualified Host Name for another ProSphere Application in the **Add Application** dialog box. Your current ProSphere Application must be able to resolve and contact this hostname for it to be successfully added.

   Note

   If the hostname cannot be resolved or the remote ProSphere Application does not respond, an error dialog box appears. If you add a new, unsynchronized site in error, you can click **Cancel** in the **Synchronize Multiple ProSphere Applications** dialog box and then reopen the dialog box to get a fresh table without the unwanted entry. After synchronization, a ProSphere Application entry cannot be removed.

7. Click **OK** to save the hostname of the external ProSphere Application.

   The new entry appears in the table in the **Synchronize Multiple ProSphere Applications** dialog box.

8. If an MCA is not yet established, select the radio button for the ProSphere Application that is to be set as the MCA.

Synchronize resource data

Synchronization is the combining of data about configuration items that are discovered in more than one deployment. Without synchronization, the data in each deployment would be available only in that deployment.

Click **Synchronize** in the **Synchronize Multiple ProSphere Applications** dialog box. This saves the selection of an MCA.

The **Last Synchronization Status for Applications** table appears. The information about synchronization progress can be monitored in this view.

Synchronization behavior and limitations

The following behaviors and limitations apply to synchronization of data between ProSphere Applications:

- If you synchronize with a ProSphere Application that is already synchronized with one or more other ProSphere Applications, the fully qualified hostnames of the other ProSphere Applications also appear in the list in the **Synchronize Multiple ProSphere Applications** dialog box. When synchronization starts, the data from these ProSphere Applications is included in the synchronized data set.
- If two or more ProSphere Applications share knowledge of the same discovered resource, search results in ProSphere display one entry of the resource for each instance of ProSphere that finds it.
- Relationships between discovered resources in ProSphere do not cross ProSphere Application boundaries (are not synchronized), and topology maps in ProSphere only show relationships between resources discovered by the same ProSphere Application.
- Once added and synchronized, a remote ProSphere Application cannot be removed from the list of synchronized applications displayed in the **Synchronize Multiple ProSphere Applications** dialog box.
- If a remote, previously synchronized ProSphere Application is not accessible during a future synchronization attempt, the entire synchronization process fails. Some identified ProSphere Applications are synchronized and some are left unsynchronized. Details of these successes and failures appear in the Last Synchronization Status for Applications table.

Synchronization status

The Last Synchronization Status for Applications table allows you to view status information for an ongoing synchronization attempt. This table is only visible in the **Synchronize Multiple ProSphere Applications** dialog box after the **Synchronize** button has been clicked.

The Last Synchronization Status for Applications table includes the following fields:

Field	Description
Synchronized Application With	Application for which a synchronization attempt was made with this application.
Last Successful Start Time	Last time a successful synchronization attempt was started between this application and the identified remote application.
Last Successful End Time	Last time a successful synchronization attempt was ended between this application and the identified remote application.
Last Start Time	Last time a synchronization attempt (successful or unsuccessful) was started between this application and the identified remote application.
Last End Time	Last time a synchronization attempt (successful or unsuccessful) was ended between this application and the identified remote application.
Status	Success or failure status of the synchronization attempt.
Failure Reason	If a synchronization attempt failed, this field provides information related to the failure.

CHAPTER 9

Backups

This chapter contains the following topics:

Create and restore snapshots or backups

Snapshots or backups of the ProSphere virtual machines ensure that you can return to the complete, previous working state of ProSphere in the event of a failed update.

Instead of using snapshots, your data center may use VMware Data Recovery as a backup solution for your virtual environment. ProSphere backup and restore using VMware data recovery on page 146 explains how to create backups with VMware Data Recovery.

NOTICE

If more than one deployment is synchronized, we recommend that you schedule backups of synchronized sites so they start at the same time. This minimizes errors that result from sites being “out-of-sync.”

Note

Your VMware environment may have predefined policies related to the creation of snapshots and backups. Consult your VMware administrator before creating snapshots or backups of ProSphere virtual machines. The procedures presented here are only examples.

Shut down or start up ProSphere or its virtual machines

NOTICE

If a ProSphere vApp or virtual machine is improperly shut down, network configuration data may be lost, and the ProSphere virtual machine will be isolated from the network after powering on. This is a known problem with VMware.

Shut down or start up ProSphere or its virtual machines on page 144 explains how to perform shutdowns and startups with right-click options from the vSphere Console.

Table 30 Shutdown and Startup Procedures

Item	To shut down use...	To start up use...
ProSphere virtual machine	Shutdown Guest	Power On
ProSphere vApp	Power Off	Power On

NOTICE

Do not execute reboot from the command line or use **Restart Guest** from VMware tools. This may render the appliance unusable and result in an empty `ovfEnv.xml` which corrupts the `/etc/hosts` file with incorrect entries.

NOTICE

If a Collector is powered off directly without first properly shutting down the system, the ProSphere Console can hang. The recommended practice is to use the **Shutdown Guest** command in vCenter before powering off.

Create ProSphere snapshots

To create a snapshot of each of the ProSphere virtual machines in the VMware vSphere Client:

Procedure

1. Open the vSphere Client and connect to the vCenter Server managing the VMware environment in which ProSphere is running.
2. Navigate to the ProSphere vApp.

   You can find the vApp by entering a name in the **Search Inventory** search field. You can also navigate to the vApp in the **Inventory Panel**.

   Note

   In a scale-out deployment, additional virtual machines of the Collector type exist, as described in ProSphere deployment with additonal collector on page 21. Shut down the Collectors, then shut down the vApp. Shut down the Collectors by first right-clicking each in the VSphere Console and then selecting **Shutdown Guest**.
3. Shut down the vApp by right-clicking it and then selecting **Power Off**.

   NOTICE

   Snapshots should not be taken if ProSphere is running.
4. Right-click the first virtual machine and select **Snapshot** › **Take snapshot**.
5. In the **Take Virtual Machine Snapshot** dialog box, type a **Name** and **Description** for the snapshot.
6. Click **OK** to create the snapshot.

   The snapshot creation status is displayed in the **Recent Tasks** status bar.
7. Repeat steps 4 through 6 for each virtual machine in the ProSphere vApp.
8. When each snapshot displays a status of Completed, power on the ProSphere vApp. Right-click the ProSphere vApp and select **Power On**.
9. Restart any Collectors. Restart each Collector by right-clicking it in the VSphere Console and selecting **Power On**.

Roll back to a snapshot

To roll back to a snapshot of a ProSphere virtual machine in the VMware vSphere Client:

Procedure

1. Open the vSphere Client and connect to the vCenter Server managing the VMware environment in which ProSphere is running.
2. Navigate to the ProSphere vApp and select one of its virtual machines.

   You can find the vApp by entering a name in the **Search Inventory** search field. You can also navigate to the vApp in the **Inventory Panel**.
3. Right-click the virtual machine and select **Snapshot** › **Snapshot Manager**.
4. In the **Snapshot Manager** dialog box, select the name of the snapshot to roll back to and then click **Go to**.

5. Click **Yes** in the **Confirm** dialog box to proceed with the rollback.

Note

If rolling back a ProSphere virtual machine due to a failed update, EMC recommends rolling back each of the ProSphere virtual machines to a corresponding snapshot.

Note

If multiple instances of ProSphere are synchronized and one is rolled back to a snapshot, attempts to access details of objects discovered after the rollback occurred will return errors. Synchronize data on page 137 discusses this situation in detail.

Backup and restore ProSphere using VMware Data Recovery

The *VMWare Data Recovery Administration Guide* explains how to back up and restore virtual machines.

If VMware Data Recovery (VDR) is used for backups, each virtual machine must have a name that differentiates it from all virtual machines in all deployments by a customer in a vCenter.

In a scale-out deployment, additional virtual machines of the Collector type exist, as described in ProSphere deployment with additonal collector on page 21. Schedule separate backup jobs for the vApp and for the Collector. Schedule these backups to occur at the same time. When restoring the virtual machines from backups, disable automatic power on of the Collector so you can manually power it on after you power on and restore the Discovery Engine.

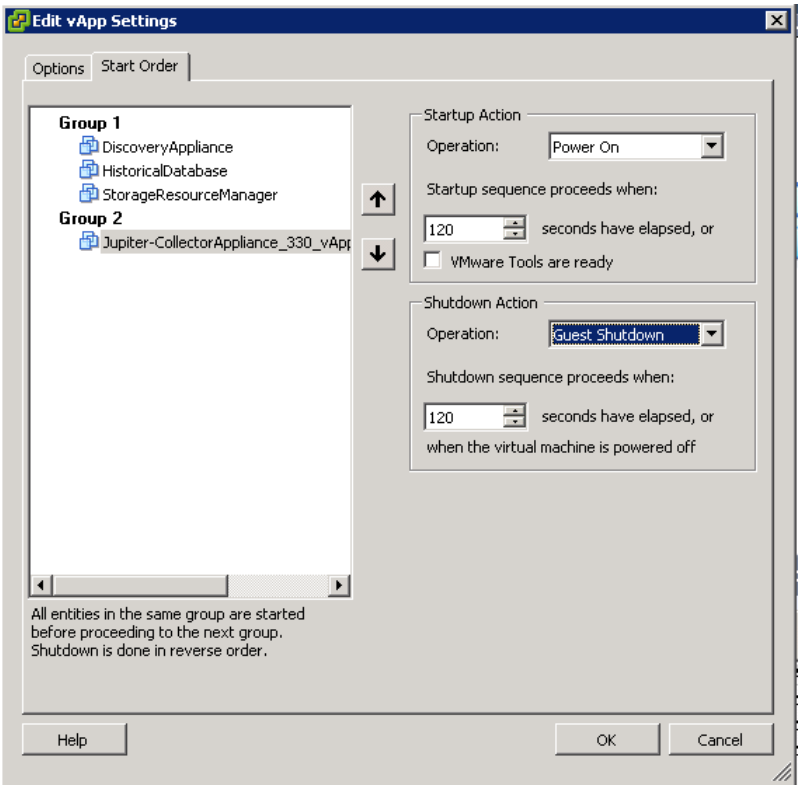
When backing up with VDR, move the Collectors inside the vApp container. When you do this, by default the **Shutdown Operation** will be set to **Power Off**. This value does not permit a graceful shutdown of the Collector.

Shutdown ProSphere Collector in VDR

Perform this procedure to allow the Collector to gracefully shut down.

Procedure

1. Select **Edit Settings**.
2. Select the **Start Order** tab.
3. Under **Shutdown Action**, set the **Operation** to **Guest Shutdown**.



4. Click **OK**.

Disaster recovery

For disaster recovery (DR) and high availability (HA), ProSphere supports VMware High Availability (HA), VMware vMotion, and VMware Distributed Resource Scheduler (DRS). Currently, the supported disaster recovery solution is confined to an ESX cluster where an ESX server fails. Virtual machines on the failed server are brought up on other ESX servers in the same cluster.

Export a customer environment for backup or troubleshooting

The following procedure exports persistent data from ProSphere to serve as a backup, or for use in recreating a customer environment. Recreating a ProSphere environment allows Technical Support to troubleshoot the issues at a customer site by reproducing the customer environment at EMC. When Technical Support asks you to export data from ProSphere, use this procedure.

Note

Reproducing the customer environment is limited to post-discovery scenarios.

To export data from a ProSphere environment, use a REST client application. Many available tools can be used including RESTClient, which is a browser add-on for Firefox, Chrome, or Safari; Poster, which is an add-on for Firefox; and HTTPAnalyzer, which is an Internet Explorer add-on.

These instructions explain the procedure using the RESTClient (`http://restclient.net`) add-on for Firefox:

Procedure

1. Launch Firefox.
2. Install the RESTClient add-on
   a. Select **Add-ons**.
   b. Click **Get Add-ons**.
   c. Type **restclient** in the **Search** dialog box.
   d. Click the **Install** button next to latest version of RESTClient available.
   e. Click **Restart** now to restart Firefox.
3. Log in to ProSphere .
4. Open a new tab and start the RESTClient add-on.
5. In the RESTClient URL field enter `https://<prosphere-hostname|IP-address>/srm/admin/system/data/exportjob?location=<databasespecifier>`

   The following table defines the values for `<database-specifier>`. The most common option is `vapp`, which initiates the export for all of the ProSphere virtual machines. The `vapp` option is what you should use if you are making a backup of ProSphere persistent data.

Option	Description
vapp	Specifies all databases
discovery	Discovery Engine database
srm	ProSphere database
db	Historical Database

6. Change the **Method** field to **POST**.
7. Click **SEND** to start the export job.

Check the status of an export job

Procedure

1. In the RESTClient URL field enter `https://<prosphere-hostname|IP-address>/srm/admin/system/data/exportjob?location=<databasespecifier>`

   Export a customer environment for backup or troubleshooting on page 147 defines the values of `<databasespecifier>`.
2. Change the **Method** field to **GET**.
3. Click **SEND** to check the status of the export job.
4. On the **RESTClient Response Body** tabs you will receive an XML feed with details about the export job. When the export job is finished, an `EXPORT PROCESS COMPLETED` message will be displayed in the feed. For example:

```
<entry>
    <title>Appliance:ProSphere Application</title>
    <link rel="related" href="https://<prospherehostname/IP>/cgi-
bin/export-tar.cgi" />
    <updated>2012-11-30T13:58:31Z</updated>
    <content type="application/xml">Executed script output:EXPORT
```

```
PROCESS COMPLETED</content>
  </entry>
```

Note

You may also make the **GET** request using a new browser tab, instead of using RESTClient.

Download the exported environment

This procedure explains how to download the compressed tar file containing the export data.

Procedure

1. Open a new browser tab.
2. Type the URL `https://<hostname/IP>/cgi-bin/export-tar.cgi` for the virtual machine for which you need the export.
3. You will be prompted to save the `export.tgz` file to your local host.
4. Repeat steps 1–3 for each of the ProSphere virtual machines to obtain an export of the entire environment.

Cancel a running export job

Procedure

1. In the RESTClient URL field enter `https://<prosphere-hostname|IP-address>/srm/admin/system/data/exportjob?location=<databasespecifier>`

   Export a customer environment for backup or troubleshooting on page 147 defines the values of `<databasespecifier>`.
2. Change the **Method** field to **`DELETE`**.
3. Click **SEND** to cancel the export job.

Delete exported data

If exported data is no longer needed, perform the following procedure to delete it from the ProSphere virtual machine:

Procedure

1. In the RESTClient URL field enter `https://<prosphere-hostname|IP-address>/ srm/admin/system/data/exportjob?location=<databasespecifier>`. Export a customer environment for backup or troubleshooting on page 147 defines the values of `<databasespecifier>`.
2. Change the **Method** field to **`DELETE`**.
3. Click **SEND** to delete the exported data saved on the ProSphere virtual machines.

APPENDIX A

Appliance Maintenance

This appendix contains the following topics:

Expand the storage space for a virtual machine

The ProSphere Application has two associated virtual machine disks, and the Historical Database has two associated virtual machine disks. One virtual disk houses the system files. The other virtual disk houses application data. During the life of a virtual machine you may need to expand the storage space allocated for application data by adding a virtual machine disk.

The following procedure adds a virtual machine disk to a running system for use by the ProSphere Application or the Historical Database:

Procedure

1. Add a new disk to the virtual machine from the vSphere Console.
2. Select **Edit Settings** on the virtual machine.
3. Click **Add**.
4. Select **Hard Disk**, then click **Next**.
5. Select **Create a new virtual disk**, then click **Next**.
6. Specify the disk size, the provisioning type, and the location of the disk, then click **Next**.
7. Specify the virtual device node (the default value should be **OK**), then click **Next**.
8. Review the options, and then click **Finish**.
9. Access a Linux login prompt.

Note

You can access a login prompt through the vSphere Console or using an SSH tool such as PuTTY.

---

10. Log in to Linux with the account name **`svcuser`** and the password **`Changeme1!`**.
11. At the system prompt, type the command **`expand_disk`**.

APPENDIX B

Troubleshooting

This appendix contains the following sections:

Contacting Customer Support

Where to get help
EMC support, product, and licensing information can be obtained as follows.

Product information
For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to the EMC Online Support Site (registration required) at:

`http://support.emc.com`

Technical support
For technical support, go to the EMC Online Support site and choose Support by Product. Enter ProSphere. On the Support page, you will see several options, including one for making a service request. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments
Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your general opinions of EMC documentation to:

`techpubcomments@emc.com`

Send your opinions of EMC ProSphere documentation to:

`ProSphere_doc_comments@emc.com`

Submit log files to Customer Support

If you receive an error message, a link takes you to a dedicated help topic, which may suggest a solution. If the problem cannot be addressed immediately, online help directs you to contact Customer Support. Customer Support may ask you to submit log files.

Procedure

1. Download and zip log files.
2. Go to EMC Online Support and open a service request.
3. Attach the log files to the service request.

Monitor services

You can monitor services on the following virtual machines: ProSphere Application, Discovery Engine and Historical Database.

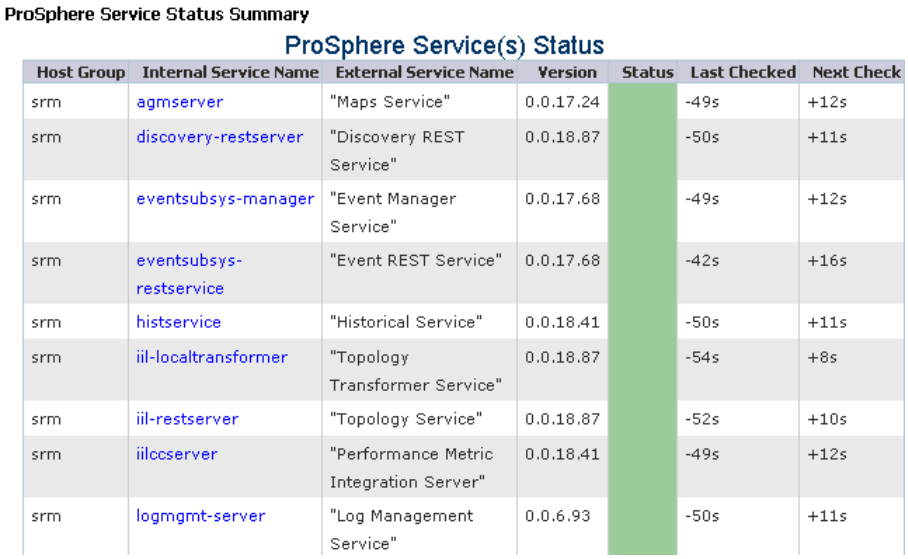
Procedure

1. To view all running services, type the following URL in a browser: **`https://<host-name|ip-address>/cgi-bin/mon.cgi?`**

   where *‹host-name›* or *‹ip-address›* identifies the ProSphere Application, Discovery Engine, Historical Database.

2. To view only failed services, type the following URL in a browser: **`https://<host-name|ip-address>/cgi-bin/mon.cgi? command= query_opstatus_failures`**

   where *‹host-name›* or *‹ip-address›* identifies the ProSphere Application, Discovery Engine, Historical Database.
   The following figure shows a sample from the Monitoring Service display of all running services.



ProSphere Service Status Summary

ProSphere Service(s) Status

Host Group	Internal Service Name	External Service Name	Version	Status	Last Checked	Next Check
srm	agmserver	"Maps Service"	0.0.17.24		-49s	+12s
srm	discovery-restserver	"Discovery REST Service"	0.0.18.87		-50s	+11s
srm	eventsubsys-manager	"Event Manager Service"	0.0.17.68		-49s	+12s
srm	eventsubsys-restservice	"Event REST Service"	0.0.17.68		-42s	+16s
srm	histservice	"Historical Service"	0.0.18.41		-50s	+11s
srm	iil-localtransformer	"Topology Transformer Service"	0.0.18.87		-54s	+8s
srm	iil-restserver	"Topology Service"	0.0.18.87		-52s	+10s
srm	iilccserver	"Performance Metric Integration Server"	0.0.18.41		-49s	+12s
srm	logmgmt-server	"Log Management Service"	0.0.6.93		-50s	+11s

Information about services

This table describes the information that appears in the **Monitoring Service** display.

Table 31 on page 155 describes the information that appears in the Monitoring Service display.

Table 31 Information about service

Type	Description
Host Group	Group to which the service belongs. ProSphere Application services belong to the srm group. Third-party services belong to the system group.
Internal Service Name	Internal name for the service
External Service Name	Customer-facing name for the service.
Version	Version of the service. For services in the srm group, the version number is for internal use only. For services in the system group, the version number is the version number of third-party software.
Status	The value in the Status column is a color indicating a specific status. Possible values are: • Unchecked (blue) - ProSphere is aware of the component but does not check the functional status of the component. • Failed dependency (orange) - Service on which this service depends failed the most recent status check • Good (green)- Component passed the most recent status check. • Failed (pink) - Component failed the most recent status check. • Disabled (yellow)- Component is currently disabled.

Table 31 Information about service (continued)

Type	Description
Last Checked	Most recent time the application service was monitored.
Next Check	Next time the service will be monitored.

To display information about a service, click the service.

Figure 6 on page 156 shows a partial display of information about a service.

Figure 6 Information about a service

Downtime Summary For Hostgroup "srm" and Service "srm-coherence"

Log begins at:	Tuesday, Mar 1, 2011 at 12:11:21
Total observed service failures:	0
Mean time between service failures:	0 seconds
Mean observed service failure time:	0 seconds
Median observed service failure time:	0 seconds
Standard deviation of observed service failure times:	0 seconds
Minimum observed service failure time:	0 seconds
Maximum observed service failure time:	0 seconds
Approximate percentage of time in failure-free operation:	100.00%

Test detail for FAILED service "srm-coherence"

Variable Description	Value
Service Description	"Cache node that will connect to the SRM components"
Time remaining until this service is next checked	31 seconds
Service being checked	srm-coherence
Current status of this service (0=error, 1=OK, 7=unchecked)	0

Detailed information about a service

Detailed information about a service.

Table 32 on page 157 describes the detailed information that appears for a service.

Table 32 Information about a service

Type	Description
Downtime Summary for Hostgroup *hostgroup-name* and Service *application-service*	
Login begins at	Specifies when the Monitoring Service was last started. **Note** This value, along with the current time, provides a time frame for events in the table.
Total observed service failures	Number of service failures by a component in the time frame.
Mean time between service failures	Calculated mean time between service failures by the component in the time frame.
Mean observed service failure time	Calculated mean time of service failures by the component in the time frame.
Standard deviation of observed service failure times	Calculated standard deviation of service failure times in the time frame. Standard deviation indicates whether the number of failures is abnormally high.
Minimum observed service failure time	Smallest time between observed service failures in the time frame.
Maximum observed service failure time	Largest time between observed service failures in the time frame.
Approximate percentage of time in failure-free operation	Approximate percentage of the time the service has run without failure in the time frame.
Success detail for group *hostgroup-name* and service *application-service*	
Service description	Name of the service.
Time remaining until this service is next checked	Time until the service is checked again.
Service being checked	Name of the service.
Current status of this service (0=error, 1=OK, 7=unchecked)	Current status of the service.
Is the monitor running right now	Whether the Monitoring Service is running.
Monitor used to test this service	Parameters passed by the Monitoring Service to the command line tool that starts the checking operation.
Last time a trap was received on this service	Most recent time that the Monitoring Service responded to an asynchronous system notification.
Summary output from most recent failure of this service	Summary of output returned by the services's most recent failure.
Last time this service returned an OK result	Date and time stamp indicating the most recent time success status was returned when monitoring the service.

Table 32 Information about a service (continued)

Type	Description
Previous opstatus for this service (0=error, 1=OK, 7=unchecked)	Status of the service on the most recent monitoring before the current monitoring.
Detail output from the most recent failure of this service	Detailed output returned on the services's most recent failure.
Time this service was last checked	Time of the previous monitoring of the service.
Test interval	Interval between checks of the service (set internally).
Host group	Group to which the service belongs. Table 17 on page 105 provides further detail.
Last exit value of monitor for this service (0=OK, anything else indicates failure)	Status returned by the Monitoring Service the last time it monitored the service. This value reports on the operation of the Monitoring Service.
Dependency status (1=dependencies OK, 0=dependencies not OK or no dependencies)	If 1 is returned, services on which this service depends are returning success status. For example, if service X can only succeed if the ping service can reach a specific host, dependency status refers to the status of the ping service. If 0 is returned, services on which this service depends are not returning success status, or the service has no dependencies.
Hostgroups/services on which this service depends	Host groups or services that must return success status for this service to return a success status.
Number of corrective actions taken	Number of attempts to correct a problem.

What to do if a service fails

If a service fails, use the Monitoring Service display to confirm which services are down.

If after several minutes the service is still unavailable, this indicates a more serious problem. Collect the log files for the impacted service(s) and contact Customer Support.

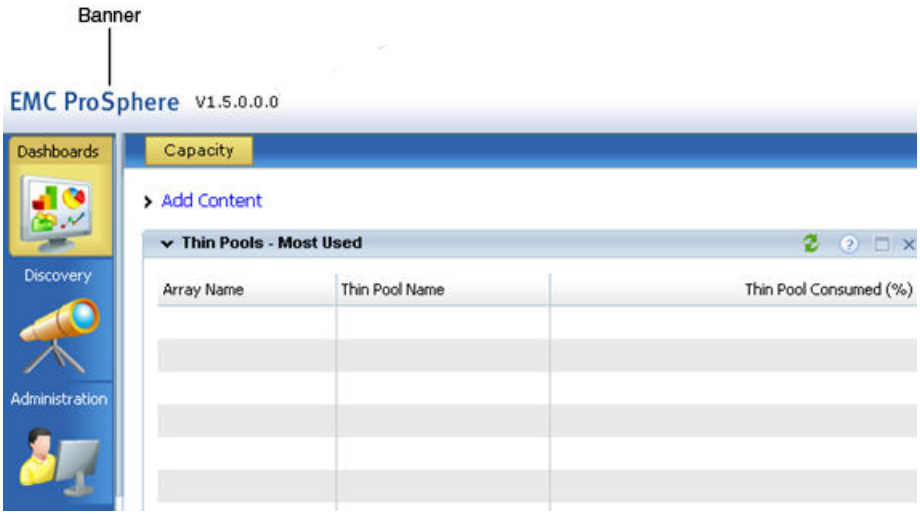
ProSphere services are designed to automatically restart after a failure. If a transient condition has caused the service to shut down, the service should restart on its own once the system detects that the service has stopped.

View UI trace information

UI actions and internal messages are tracked and trace information can be displayed during a session. The messages can be sorted by Class, Level, Message, or Timestamp. They are also filterable by Class, Level, or Message contents.

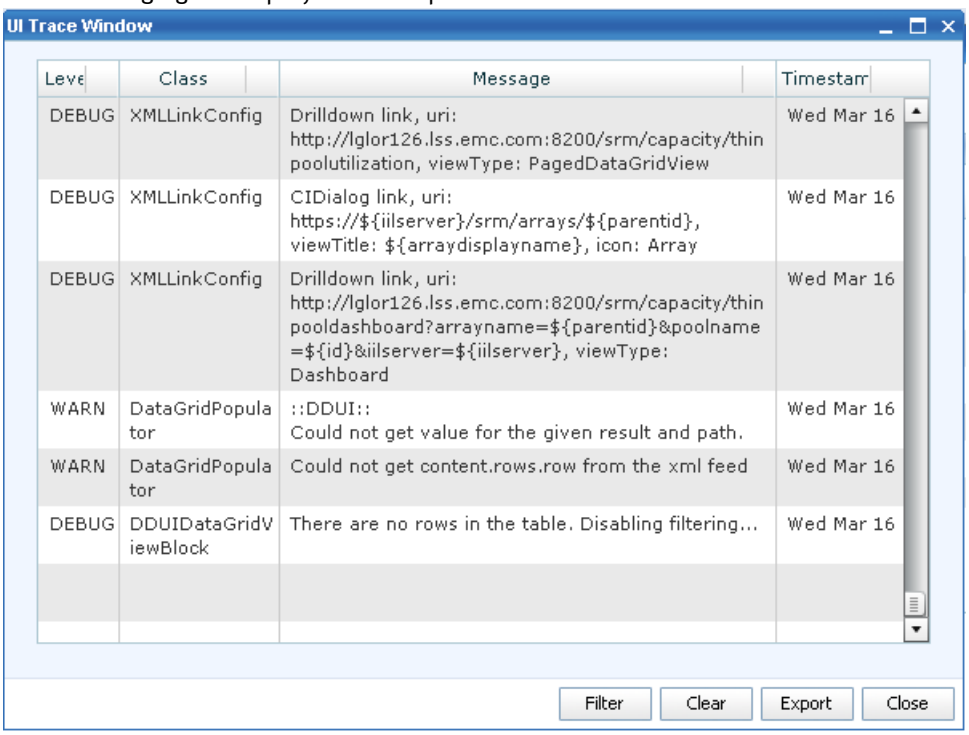
Procedure

1. On a screen in the ProSphere Console, put the pointer on a banner.



2. Hold down **Shift-Ctrl** and click.

   The **UI Trace** window displays information about user interface events.
   The following figure displays an example of UI trace information.



Note

Click the column label to sort a table by those values. Click a second time to invert the sort order. To sort by two columns, click the first column, then **CTRL**-click the second column; the sorting is performed in that order.

Information displayed in the UI Trace window

Table 33 on page 160 describes the types of information displayed in the **UI Trace** window.

Table 33 UI trace information

Type	Description
Level	Level of severity of the event.
Class	Internal class that was the source of the message.
Message	Detailed information about the reported event.
Timestamp	Timestamp identifying the time of the reported event.

Table 34 on page 160 explains the function of the buttons on the **UI Trace** window.

Table 34 UI trace buttons

Button	Action
Filter	Display the **Trace Filters** dialog box.
Clear	Clear the **UI Trace** window.
Export	Copy all highlighted rows in the **UI Trace** window to the paste buffer.
Close	Close the **UI Trace** window.

Filter UI trace messages

You can filter the messages displayed in the **UI Trace** window.

Procedure

1. Click **Filter** at the **UI Trace** window.
2. In the **Trace Filters** dialog box, select criteria, then click **Filter** to filter the message display.

   The following table explains how to filter UI trace messages.

Option	Description
Levels	Filter messages by severity level.
Trace Message	Filter messages by a string contained in the message.

Option	Description
Class Names	Filter messages by internal class. **Note** This functionality usually assumes an understanding of the underlying software architecture. Click **None** to clear all class names. Click **All** to select all class names. To reselect severity levels and class names, click **Default**. This selects all severity levels and all class names and clears the **Trace Message** field.

3. Click **Close** to close the **UI Trace** window.

   No settings are saved.

Collect Adobe Flex logs

Adobe Flex logs contain UI trace messages, and may contain additional trace messages. Customer Support may ask you to configure Adobe Flex logs to be sent to your local PC, so you can send the logs to Customer Support.

Note

The following procedure requires that the debug version of the Adobe Flash Player be installed.

To configure logs to go to a local PC:

Procedure

1. On a Windows system, create the file: `C:/Documents and Settings/<username>/mm.cfg`
2. On a Linux system, create the file: `/home/<username>/mm.cfg`
3. In the file, add the lines:

   ```
   ErrorReportingEnable=1
   TraceOutputFileEnable=1
   ```

   On a Windows system, the log file is saved to:`C:\Documents and Settings\username\Application Data\Macromedia\Flash Player\Logs\flashlog.txt` On a Linux system, the log file is saved to:`/home/username/.macromedia/Flash_Player/Logs/`

Export a customer environment

Recreating a customer environment allows Technical Support to troubleshoot the issues at a customer site by reproducing the customer environment at EMC. When Technical Support asks you to export data from the customer environment, follow the procedure Export a customer environment for backup or troubleshooting on page 147.

Deployment issues

This section describes deployment issues.

Allow time for file download and deployment

The download time for the OVF files and the associated VMDK files can vary from minutes to many hours, depending upon the network bandwidth and the location of the files. If necessary, schedule the file downloads for time periods when critical personnel are not required to be present.

In addition, actual deployment time depends on the location of the downloaded OVF files relative to the vCenter/ESX where the vApps are going to be created. In other words, to reduce the deployment time, the host containing the OVF files should be on the same subnet as the ESX server on which the vApps are created.

Uppercase characters cause log service to fail

If you deploy ProSphere using any uppercase characters for the host names, the error ADM-0003 is displayed and the log management service fails to run. The solution is to use only lowercase characters in the host names when deploying ProSphere.

Corrupted or missing VMDK file causes error

If a .vmdk file is missing or corrupted, ProSphere will fail to boot.

Check the MD5 checksum code of the deployment files with a MD5 tool to verify that the code is the same as in the files available for downloading at EMC Online Support.

Migrating a ProSphere vApp to a different vCenter

If you try to migrate a ProSphere vApp from one vCenter to another vCenter implementation, you lose the ProSphere vApp. This happens because VMware migration tools do not support the moving of a vApp folder.

Deploy a new ProSphere instance into the new vCenter using the same ProSphere host information. Migrate the ProSphere virtual machines from the old vCenter to the new vCenter and put them in the vApp folder.

Changed properties are not recognized by ProSphere

After deployment, if you change a property set in deployment, perform this procedure so that ProSphere recognizes the new value.

Procedure

1. Log in to the vSphere Client.
2. Right-click the ProSphere vApp and choose **Shut down** or **Power Off**. The vApp should take several minutes to shutdown.
3. Right click one of the ProSphere virtual machines and select **Edit Settings**.
4. Select the **Options** tab.
5. Under vApp Options, select **Properties**.
6. Complete the fields on this page using the same values originally used to deploy ProSphere.
7. Change the DNS IP address.

Note

Do not change the hostname.

8. Repeat the steps above for the remaining two virtual machines.
9. Right click the ProSphere vApp and choose **Power On**.

CMCNE installation: error in default path

If "(x86)" is contained in the default path for CMCNE installation (such as `C:\Program Files (x86)\CMCNE 11.1.4 & C:\Program Files (x86)\`), an error occurs, and the keytool utility does not work correctly. The installation procedure cannot process a closing bracket in a default path.

The workaround is to specify a different installation path.

Updates issue: "Software updates available" message

Even after ISOs are unmounted, the "Software Updates available" popup appears.

Procedure

1. Unmount the ISO from the vSphere client.
2. Log in to ProSphere
3. Change the repository from CD-ROM to a different repository.
4. Log out from ProSphere.
5. Log in to ProSphere and change the repository back to CD-ROM.

Synchronization issues

This section describes issues affecting synchronization of deployments.

ProSphere Application credentials

ProSphere Applications cannot enter into a synchronized relationship if the login credentials of the Administrator establishing the synchronization are not valid on the various ProSphere Applications being synchronized.

Ensure that the Administrator logged into a ProSphere Application to add another ProSphere Application for synchronization has identical user credentials on both ProSphere Applications. The same would also apply if the Administrator were adding more than one ProSphere Application for synchronization.

Time window for discoveries

Delay initiating discoveries on newly synchronized ProSphere Applications for at least 10 minutes after the initial synchronization has successfully completed. This applies to the Master Capacity Application as well as other ProSphere Applications.

Because of limitations in the way discovered data propagates through the system, all ProSphere Applications in your synchronized deployment should not have any discovered data at the time when they are first synchronized.

Data across multiple data centers may be incomplete

The goal of ProSphere is to discover and report the network objects and their relationships across your entire enterprise, without regard to what items are physically located in a given data center.

ProSphere can discover objects across the enterprise, such as a host in Site A, and switches and arrays in Site B. However, ProSphere does not currently report on the relationships between these disparate, synchronized objects. So, the relationship data in maps and tables where relationships cross instances of ProSphere may be incomplete. All relationships within a single instance of ProSphere will be accurately reported, regardless of which ProSphere instance you are using.

Synchronization of hosts

Hosts, once added to the **Synchronize Multiple ProSphere Applications** dialog box, cannot be removed. Consequently, if you uninstall the ProSphere vApp from a host that is added to the dialog box, the application continues to attempt synchronization with the host without success.

Unresolved FQHNs

When you synchronize ProSphere Applications, each ProSphere Application in the group to be synchronized must be able to resolve the Fully Qualified Host Names (FQHNs) of the others into IP addresses via DNS lookup.

The *EMC ProSphere Deployment Guide* describes the steps to take in deployment to ensure that Fully Qualified Host Names are resolved.

Failure to resolve FQHNs can be an issue specifically when ProSphere Application are in separate domains that normally cannot resolve each other's addresses.

If hosts to be synchronized cannot resolve FQHNs of the other hosts to be synchronized, edit vApp properties in vSphere. Include the appropriate name servers and search domains, before synchronizing the ProSphere instances.

Login issues

On logging into ProSphere, the vApp checks for the availability and health of its component virtual machines to ensure proper application operation. If problems are encountered during these checks, additional information in the form of application status is displayed.

If no problems are encountered during these checks, no additional information is displayed, and login proceeds normally.

Note

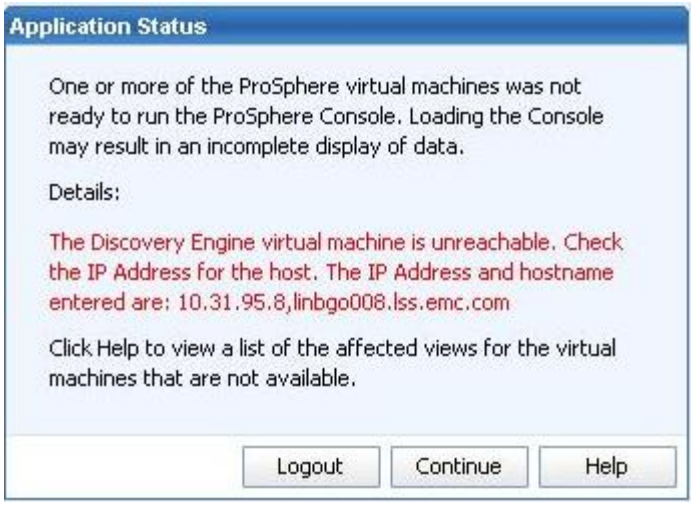
At login, usernames are case-sensitive.

Virtual machine unreachable

The status `Virtual machine unreachable` appears when the status check for either the Discovery Engine virtual machine or the Historical Database indicates that the virtual machine is unreachable.

Figure 7 on page 165 shows the dialog box that appears.

Figure 7 Application Status - Virtual machine unreachable for Discovery Engine



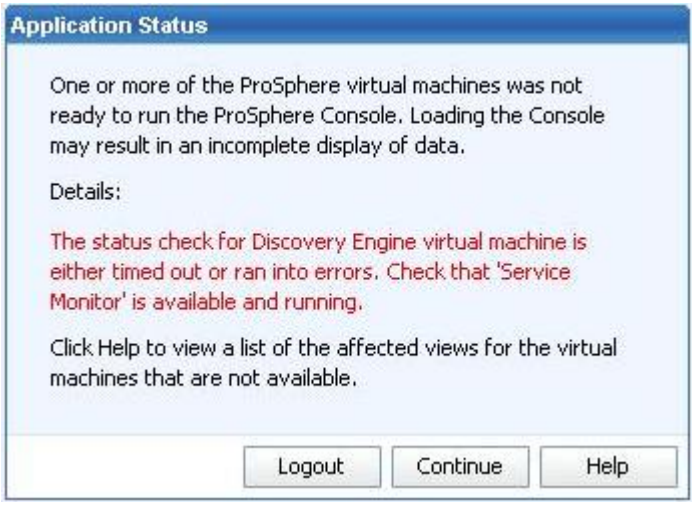
The virtual machine could not be contacted. You should check the virtual machine status in the vSphere Client and ensure that it is properly powered on. If the interruption in communication between the ProSphere Application and the virtual machine is only temporary, after a short time you can try refreshing your browser to see if a connection has been restored. This situation can also be caused by a misconfiguration of the Historical Database hostname, the Discovery Engine hostname, or the IP address during the deployment of the ProSphere vApp.

Status check of virtual machine timed out or ran into errors

The status `Status check of virtual machine timed out or ran into errors` appears when the status check for any of the virtual machines (ProSphere Application, Discovery Engine, Historical Database) does not successfully complete.

Figure 7 on page 165 shows the dialog box that appears.

Figure 8 Application Status - Status check timed out or ran into errors for Discovery Engine



ProSphere could not verify the state of services on the virtual machine. Monitor services on page 154 provides more information.

Virtual machine not ready

The status “Virtual machine not ready” appears when one or more of the services on any of the virtual machines (ProSphere Application, Discovery Engine Historical Database) is not ready.

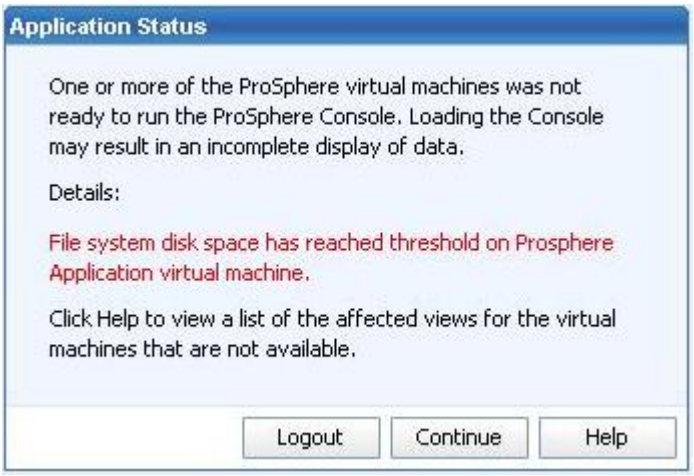
You can wait and then refresh your browser to check if the situation has been resolved. If it has not, you can check the status of the services to identify the problem. Monitor services on page 154 provides more information.

Disk Space threshold reached

The Disk space alert for ProSphere Application status appears when the file system disk space for any of the virtual machines (ProSphere Application, Discovery Engine, Historical Database) reaches a threshold value.

Figure 9 on page 166 shows the dialog box that appears.

Figure 9 Application Status - Disk space alert for ProSphere Application



The system administrator must extend storage space by adding a disk to a logical volume. Expand the storage space for a virtual machine on page 152 provides more information.

Hostname underscores cause login failure

If you receive a login error and you are certain the username and password you entered are correct, verify that the hostnames entered during deployment of ProSphere do not contain underscores.

Browser issue: ProSphere Console page can be stale

The ProSphere Console page can be stale because Internet Explorer is retrieving stored pages rather than getting fresh content.

The ProSphere Console page is displayed within a browser, and some browsers default to retrieving older cached pages rather than the current page.

To avoid displaying a stale pages, specify that newer versions of the pages should be used rather than stored versions.

Note

Internet Explorer 9 does not appear to recognize the configuration change in steps 1 and 2, so you may have to use Internet Explorer 8 or another browser.

For Internet Explorer 8, use the following procedure:

Procedure

1. Go to **Tools › Internet Options › Browsing History › Settings**.
2. In the **Temporary Internet Files** section, select "Every time I visit the webpage" for when to check for newer versions of stored pages. Click **OK**.
3. Go to **Tools** › **Internet Options** › **Browsing History** › **Delete**.
4. Select **Check** › **Temporary Internet files**.
5. Clear **Preserve Favorites website data**. Click **Delete.**
6. Restart Internet Explorer.

ProSphere Console issue: network latency causes timeouts

Depending on network latency or machine load, occasional messages during normal operation report failures relating to Apache Error code 502. These errors do not always imply the underlying operation failed, but may refer to post-operation communication of status. EMC recommends checking the status of such an operation through the ProSphere Application before restarting it.

Capacity issue: CLARiiON in Equalizing state

When a CLARiiON disk that had failed and was being replaced with a hot spare is replaced with a good new drive, the disk is put into the Equalizing state, and the data on the hot spare is copied back to the new drive.

While the CLARiiON array status does not show as degraded when the disk is in an Equalizing state, the EMC SMI-S Provider may return inaccurate numbers, including negative values.

When all the disks are in a Ready state, the next discovery of the array will resolve the invalid metrics.

Historical Database issues

If you receive an error message indicating that the Historical Database is unavailable and you cannot correct the problem on your own, contact Customer Service.

If the database is corrupted, Customer Service will explain how you can access the most recent automatic backup of the Historical Database and how to obtain backed up performance data.

Note

An automatic backup occurs each night. If you created a more recent snapshot, instead of using the backup you can roll back the Historical Database to the most recent snapshot.

NOTICE

A power loss can corrupt the Historical Database. To protect against corruption, ensure that the ESX servers on which the Historical Database is running are protected from power outages. VDR backups provide resilience to ESX server outages. If VDR backups are not being maintained, the ESX server should be setup with battery backups. If this precaution is not observed, you may need to rediscover all configuration items (CIs).

CMCNE launch-in-context does not work

If CMCNE launch-in-context does not work, perform the following steps:

Procedure

1. Discover the switch through the SMI provider where the element manager is installed (as opposed to the default SMI provider for the switch).
2. Export the certificate for the ProSphere Application where you are logged in.
3. Install the certificate into the element manager using the keytool.
4. Restart the element manager.
5. Search for the switch of interest, then invoke the CI dialog, which will display the topology map from a switch perspective.
6. Click the **Attributes tab**.

   If Management IP has a value, the CMCNE launch **Top Talkers** will be enabled.

EMC SMI Provider for Symmetrix and CLARiiON

This topic lists problems that can arise while using EMC SMI provider for Symmetrix and CLARiiON.

Identify EMC SMI-S Provider version numbers

If the provider version is not qualified, array discovery can fail or partial discovery can occur.

Note

The *EMC ProSphere Support Matrix* provides information on supported EMC SMI-S Provider/Solutions Enabler kit versions.

To verify the versions of the Solutions Enabler and the SMI-S provider, do the following:

Procedure

1. Start the EMC SMI-S Provider TestSmiProvider utility.

   For details on how to start the utility refer to Start the TestSmiProvider utility on page 171.
2. At the command prompt, type the following:`dv`

   This command displays version information for the ECOM CIMOM, SMI-S Provider, Solutions Enabler, and all the attached Symmetrix and CLARiiON systems.

Change an EMC SMI-S Provider password

Procedure

1. Open a web browser and type the following URL to bring up the ECOM Administration utility:`https://<provider-host>:5989/ecomconfig`
2. Log in using the administrator username and password for the EMC SMI-S Provider.

   The default credentials are:
   Username = admin

   Password = #1Password
3. Select **Change Password** and type **`admin`** as the username.
4. Type the provider's current admin password, and the provider's new password.

Obtain EMC SMI-S Provider log files

In the event of an array discovery problem involving the EMC SMI-S Provider, Product Support requires the EMC SMI-S Provider log files to diagnose the problem.

Procedure

1. Open a web browser and type the following URL to bring up the ECOM Administration utility:`https://<provider-host>:5989/ecomconfig`
2. Log in using the EMC SMI-S Provider administrator username and password.

   The default credentials are:
   Username = admin

   password = #1Password
3. Click **Display Log File**.
4. Use the web browser to save the web page as a file.
5. Click **Back to Main Menu** located at the bottom of the displayed log.
6. Click **Display Security Log File**.
7. Use the web browser to save the web page as a file.

Modify EMC SMI-S Provider log severity

Procedure

1. Open a web browser and type the following URL to bring up the ECOM Administration utility:`https://<provider-host>:5989/ecomconfig`
2. Log in using the EMC SMI-S Provider administrator username and password.

   The default credentials are:
   Username = admin

   password = #1Password
3. Click **Logging Options**.
4. Select the requested **Log File and Log Severity** from the drop-down list.
5. Click **Save Log Level**.

Restart the EMC SMI-S Provider

Procedure

1. On Windows you can restart the EMC SMI-S Provider using the Services wizard to restart the ECOM service, or you can perform the following steps in the CMD shell:
   a. Stop the provider using following commands.
      - From the `ECIM/ECOM/bin` directory: `sm_service stop ecom.exe`
      - From the `ECIM/Slp/lib` directory: `slpd -stop`
   b. Restart the provider using the following commands.
      - From the `ECIM/ECOM/bin` directory: `sm_service start ecom.exe`
      - From the `ECIM/Slp/lib` directory: `slpd -start`
2. On Linux you can restart the EMC SMI-S Provider by performing the following steps in a shell:
   a. Stop the provider using following commands.
      - From the `ECIM/ECOM/bin` directory, find the PID of the running ECOM daemon: `ps -ef | grep "ECOM -d"`
      - Kill the ECOM daemon: `kill -s TERM <ecom-pid>`
      - Find the PID of the running SLP daemon: `ps -ef | grep slpd`
      - Kill the SLP daemon: `kill -s TERM <slpd-pid>`
   b. Restart the provider using the following command from the SYMCLI directory.
      - From the `ECIM/ECOM/bin` directory: `./ECOM -d`
      - From the `ECIM/Slp/lib` directory: `slpd`

Remove subscriptions to EMC SMI Provider indications

Indications are notifications sent by a CIM Object Manager in response to an event monitored by an SMI-S Provider. Indications are only sent to subscribers that wish to receive the notification. In this case, the subscribers are components in the Discovery Engine (specifically, the Discovery Engine's Indication RM) that trigger rediscoveries of a discovered element. For example, the addition, deletion, or modification of an array's StoragePool, StorageVolume, or masking record triggers a partial rediscovery of the array.

For optimal provider performance, no more than two or three appliances should access the same EMC SMI-S Provider. If more appliances subscribe to the same SMI-S Provider, the provider may not perform as expected. For example, if array indications received arrive much later (over 15 minutes later) than an array modification that should have triggered them, this may indicate that the provider is not performing optimally.

The TestSmiProvider application may be used to remove some or all indication subscriptions from the SMI-S Provider. Indication subscriptions are made again the next time the SMI-S Provider is used in an initial array discovery or rediscovery. If you do not want the appliance to resubscribe for indications, then you must delete the associated discovery/rediscovery policy.

Clean up indication subscriptions from an EMC SMI Provider

Procedure

1. To clean up all indication subscriptions from an EMC SMI-S Discovery Engine Provider:
   a. Start the EMC SMI-S Discovery Engine Provider TestSmiProvider utility. Refer to Start the TestSmiProvider utility on page 171.
   b. Type **ind** to go to the **Indications** menu.
   c. Type **del** to execute Delete all subscriptions and accept all defaults.
   d. Type **q** to quit the utility.
2. To clean up indication subscriptions for a selected Discovery Engine:
   a. Start the EMC SMI-S Provider TestSmiProvider utility. Refer to Start the TestSmiProvider utility on page 171.
   b. Type **ind** to go to the **Indications** menu.
   c. Type **del** to execute Delete all subscriptions and accept all defaults.
   d. Note the destination property displayed (for example, http://1.2.3.4:6012) that includes the Discovery Engine IP address for which you would like to remove indication subscriptions.
   e. Type **dsd** to delete indication subscriptions for a selected destination and accept all default values. Enter the destination for the desired Discovery Engine.
   f. Type **q** to quit the utility.

```
localhost:5988) ? ind
##########################################################################
##
Indications menu
##########################################################################
##
sub - Subscribe
uns - Unsubscribe
ls - List all subscriptions
lf - List all filters
ld - List all listener destinations
del - Delete all subscriptions
dsd - Delete all subscriptions for the destination
scql - Subscribe to all CQL filters
swql - Subscribe to all WQL filters
b - Back
q - Quit
##########################################################################
##
(localhost:5988) ? dsd
Namespace[interop]:
Destination []: http://1.2.3.4:6012
Deleted all subscriptions for the destination: http://1.2.3.4:6012
Please press enter key to continue...
```

Start the TestSmiProvider utility

Procedure

1. Start the TestSmiProvider application by going to the appropriate directory and entering TestSmiProvider.

   The TestSmiProvider for EMC SMI-S Provider is located at:`C:\Program Files\EMC\ECIM\ECOM\bin\TestSmiProvider.exe or /opt/emc/ECIM/ECOM/bin/TestSmiProvider`

2. Connect to a running EMC SMI-S Provider by entering the requested information when prompted (defaults are listed in brackets and may be accepted by pressing ENTER).

Powering off Discovery Engine degrades provider performance

EMC ProSphere Discovery Engines that are powered off and have array indication subscriptions with an EMC SMI-S Provider cause the Provider to repeatedly attempt to deliver indications, thus impacting the provider's performance and stability.

A Discovery Engine creates indication subscriptions as part of an initial discovery or rediscovery of an array. Once the indication subscriptions are created, the provider attempts to deliver an indication to the discovery engine whenever the specific array event that triggers the indication occurs.

To prevent the provider from making repeated attempts to deliver new indications, Discovery Engines should remain powered on if they have indication subscriptions with a provider.

For optimal EMC SMI-S Provider indication delivery performance, no more than three EMC ProSphereDiscovery Engines should access the same EMC SMI-S Provider.

If a Discovery Engine must be powered off permanently or for several days and the provider continues to be used, then refer to Configuration issues on page 172 for information on removing the indication subscriptions.

Configuration issues

The following sections describe configuration issues involving the EMC SMI-S Provider that can prevent successful discovery.

EMC SMI-S Provider configuration issue

Symmetrix masking and mapping data is not discovered when new access pools have been created and contain devices.

Solution
Set up the proper Access Control Lists and permissions on the EMC SMI-S Provider host.

How to configure Symmetrix ACL
If Symmetrix Access Control is being used to protect Symmetrix devices, the host from which you run the device masking commands must be configured in an access control group with an ACL (Access Control List) granting VLOGIX rights to ALL_DEVS.

If Solutions Enabler Access Control is enabled on the Symmetrix array, then the host on which the SMI-S Provider is running must have sufficient privileges to perform the necessary operations. At a minimum, the host on which the SMI-S Provider is running must be in a group that has access to ALL_DEVS with BASE and VLOGIX privileges.

VLOGIX behavior
During initial setup of the system, the access group UnknwGrp !INPOOLS ALL is present. In this scenario, the VLOGIX privilege returns as True since you are granted access to all devices in the Symmetrix array. Initially, because no pools are present, the VLOGIX privilege is associated implicitly with all devices by this ACL.

Once you create an access pool and add a device to it, the VLOGIX privilege is no longer implicitly associated with all devices and, therefore, a check for the VLOGIX privilege would now fail. For the UnknwGrp to still have VLOGIX privilege, that privilege must be explicitly granted to the UnknwGrp and associated with ALL_DEVS.

How to determine if the EMC SMI-S Provider is configured properly

1. Determine if Access Control Lists are enabled on the Provider host.

Note

Do not confuse an Access Control of N/A with access control being disabled. N/A simply means that the host where this command is being run does not have the ADMIN privileges to view the ACLs and Groups.

2. Verify Access Control List configuration allows the EMC SMI Provider to access the masking database.

The following section contains an expanded discussion of these points.

SYMCLI examples

1. Determine if Access Control Lists are enabled on the Provider host.
   Example of Access Control being OFF (Disabled):

```
>symacl list -v -sid 000187400019
S Y M M E T R I X A C C E S S C O N T R O L S T A T U S
Symmetrix ID: 000187400019
Access Control : Disabled
Session Locked : N/A
Time Held in Seconds : 0
134 EMC ProSphere Administrators Guide
Troubleshooting
Lock Identifier : N/A
Time Enabled : N/A
Time Disabled : N/A
Time Updated : N/A
ADMIN priv : N/A
ADMINRD priv : N/A
>symacl list -acl -sid 019
Symmetrix ID: 000187400019
Symmetrix access control is disabled for this Symmetrix
```

Note

Do not confuse an Access Control of N/A with access control being Disabled. N/A simply means that the host where this command is being run does not have the ADMIN privileges to view the ACLs and Groups.

Example of Access Control being enabled when EMC SMI-S Provider host does not have ADMIN privileges:

```
>symacl list -v -sid 854
S Y M M E T R I X A C C E S S C O N T R O L S T A T U S
Symmetrix ID: 000194900854
Access Control : N/A
Session Locked : N/A
Time Held in Seconds : 0
Lock Identifier : N/A
Time Enabled : N/A
Time Disabled : N/A
Time Updated : N/A
ADMIN priv : No
ADMINRD priv : No
```

2. Verify Access Control List configuration allows the EMC SMI-S Provider to access the masking database.
   a. If Access Control is disabled then there is no need to do anything and the EMC SMI-S Provider should be able to access the masking database.
   b. If Access Control is enabled and there are no other access pools other than ALL_DEVS and !INPOOLS, then the EMC SMI-S Provider should be able to access the masking database.

c. If Access Control is enabled and there are additional access pools with devices allocated to them, then verify that the EMC SMI-S Provider host belongs to a group that has VLOGIX access to the ALL_DEVS access pool.

NOTICE

If volumes were never added to an access pool then the Provider may appear to have the correct privileges since it will return masking information. However, as soon as an access pool is created and a volume assigned to it then the EMC SMI-S Provider will no longer be able to access the array's masking and mapping database until the Provider host is added to an access group that has VLOGIX access to the ALL_DEVS access pool.

Example of when an EMC SMI-S Provider host has Access Control enabled but does not have any other access pools:

In this case, the Provider host belongs to UnknwGrp which does not have the VLOGIX access listed under Access Type. But, as long as there are no access pools that have devices added, then this Provider would be able to access the masking database since the !INPOOLS pool exists with access type ALL. However, as soon as an access pool is created and a device added (!INPOOLS pool access type changes to BASE) then this same Provider would no longer have access to the masking database.

```
>symacl list -acl -sid 854
Symmetrix ID: 000194900854
Group Name Pool Name Access Type
-------------------------------------------
UnknwGrp ALL_DEVS BASE
UnknwGrp!INPOOLSALL
```

The following command checks for additional access pools that contain devices which, if found, would cause a change in the !INPOOLS default behavior:

```
>symacl list -accpool -sid 407
Symmetrix ID: 000194900407
Number of Number of
Pool Name Devices ACLs
-------------------------------- --------- ---------
TestPool 10 0
>symacl list -acl -sid 407
Symmetrix ID: 000194900407
Group Name Pool Name Access Type
---------------- ---------------- -----------
TestGRPTestPool BASE
```

Mapping and masking profile

Clariion and VNX arrays must be added to the provider with a user that has administrator-level access with global scope.

Occasionally, clients of CLARiiON arrays are unable to traverse the Masking and Mapping profile because they are unable to obtain instances of the Clar_LunMaskingSCSIProtocolController class. This results in the following error being generated in the Solutions Enabler symapi log file:

```
STOR_C_MASK_DB_INCONSISTENT_STATE
```

The internal database is in an inconsistent state, and must be fully synchronized before performing this operation.

The symapi log file is located in the following directories:

- Windows:
  `c:\program files\emc\symapi\log`
- Linux:
  `/var/symapi/log`

The following EMC SMI-S Provider error is present in Discovery Engine Array1.log and in the provider's symapi log file: "The internal database is in an inconsistent state, and must be fully synchronized before performing this operation."

The following two EMC Knowledgebase solutions are associated with this error message:

- emc386086 — This is for duplicate HBA records. The fix is to restart the CLARiiON CIMOM.
- emc241018: — This is for duplicate HBA records information with different data. One record has SG information and the other one does not. The fix is to delete the initiator records.

Out-of-band discovery method

SMI-S Provider has a programmatic interface that provides management applications integrated with the provider the ability to discover CLARiiON or VNX storage arrays out of band. This discovery method does not require that a CLARiiON or VNX LUN be visible to the host on which the SMI-S Provider is running. Only the IP connection to the storage array is required.

If your management application uses this programmatic interface, you must provide the following information:

- IP address of SPA and SPB of the CLARiiON or VNX array to be managed.
- Username and password of the CLARiiON or VNX array that is of administrator-level privilege with global scope.

Solutions Enabler access control limitation

Symmetrix arrays that have Access Control enabled must give the EMC SMI-S Provider host full access to the array so that all Storage Pool, Storage Volume, and Masking and Mapping data can be discovered. The host must have sufficient privileges to perform the necessary operations.

Discovery username must have array access

Perform the following:

- Verify that the username to be used for discovery of the CLARiiON/VNX Block array is authorized for array access. **`Symcfg auth list`**
- Verify the username associated with SPA and SPB.
- If the desired user is not listed in the output of the command above, then execute the following command for both SPA and SPB for the arrays to be discovered.

  ```
  symcfg auth add -host <SPA Address> -username <username> -password
  <password>
  ```

  This command is documented in more detail in the *SMI-S Provider Release Note*s.

Consult the *EMC ProSphere Support Matrix* for supported versions of these arrays.

Groups issue: no special characters in Smart Group criteria

The **Value** field in **Create Smart Group** and **Edit Smart Group** dialog boxes cannot have special characters such as comma (,), pound (#), and colon (:). If a Smart group is created using these special characters, the **Value** field is blank when you edit the smart group.

Mapping issue: incomplete map from HP-UX 11.31 to array

Some arrays connected to HP-UX 11.31 hosts are not displayed in the **Map** view of the **Configuration Item** dialog box, although the hosts and connected switches are displayed

correctly. This issue occurs because ProSphere and INQ do not support native multipathing for HP-UX 11.31. However, if you use Veritas DMP, ProSphere does discover the relationship to arrays.

Common reasons for discovery failure

The following topics describe common reasons for discovery failure.

Prerequisites for host discovery are missing

Host discovery fails if the host does not have supported HBAs, drivers, firmware, and SNIA-approved API libraries.

SNIA library is an industry-standard library used to manage the Fibre Channel HBAs. This library is supported by HBA vendors like Qlogic, Emulex, and is typically bundled with the Fibre Channel Device driver. If an HBA is running with the supported firmware and driver, this does not mean that the SNIA API libraries are installed. In some cases, the HBA or host OS vendors provide SNIA API libraries installed separately from the HBA drivers.

The E-Lab support tool specifies the requirements for connectivity only. Because HBA SNIA libraries are not required for connectivity, SNIA information is not provided in E-Lab.

For ProSphere to discover SNIA qualified HBAs:

- The HBA driver installed must be SNIA HBA API 2.0 compliant.
- The vendor specific SNIA libraries must be installed on the target host.

The HBA model number and part number should be verified before updating the hosts with SNIA libraries for HBA.

You can install the SNIA library in one of the following methods:

- As part of HBA or HBA driver installation.
- Manually as per vendor specification.
- Automatically using HBAnywhere (for Emulex installations) or SANSurfer (for Qlogic installation.

To validate whether the SNIA libraries are installed:

Procedure

1. Download inq from EMC Online Support:`Home > Support > Product and Diagnostic Tools > INQ Utility`
2. Select the latest version.
3. Select the operating system.
4. Run the following command on the host.`Inq -hba`

   If the command lists HBAs, the SNIA libraries are installed.

Location of HBA API libaries

The HBA API is implemented as a common library which depends on vendor-specific libraries for specific HBA model support.

On Windows systems:

- The common library HBAAPI.DLL is installed in `%SYSTEMROOT%/SYSTEM32`.
- The location of the vendor-specific libraries can be found by searching the key SNIA in the registry entries in HKEY_LOCAL_MACHINE.

On Unix systems:

- The common library libHBAAPI.so is installed in `/usr/lib` for 32-bit systems, and the appropriate 64-bit library locations depending on operating system.
- The location of the vendor-specific libraries can be found in `/etc/hba.conf`.
- HP-UX (32-bit) links`/opt/snia/api/lib/libHBAAPI.sl` to `/usr/lib`.
- HP-UX (64-bit) links `/opt/snia/api/lib/pa20_64/libHBAAPI.sl` to `/usr/lib`.

SMI Indication Destination cannot be obtained

Array discovery may fail and the following errors may appear in the discovery job results:

```
Indication destination has not been configured. Indications cannot be received and will not trigger rediscoveries.
```

```
Invalid subscription destination. Check network settings. Event rediscovery may be affected
```

The Broker temporarily loses contact with SMI Indication Adapter and cannot pass its location to the array discovery so the indication destination can be determined. When the array discovery attempts to subscribe to indications it must pass this indication destination and ultimately fails because no destination is available.

Run the array discovery job again since the broker may have reestablished communications with the SMI Indication Adapter.

Failure to open WMI sessions

Non-availability of prerequisites might result in failure to open WMI sessions.

The following prerequisites are required for successful Windows host discovery:

- The user (defined in the access credentials) through which the discovery is done must be an administrator, or should be part of an administrator group.
- The Windows Management Instrumentation (WMI) service must be running on the target host.
- Firewall and WMI must be properly configured.
- DCOM communication must be enabled between the target host and ProSphere. On the target host, make sure the following registry key is set to Y:`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole ->EnableDCOM`

  Note

  Only NTLM v2 authentication security is supported for WMI discovery.

In addition to the WMI configuration, for Windows 2008 R2 Releases, configure DCOM as described in Configure DCOM for Windows 2008 on page 177.

Configure DCOM for Windows 2008

Procedure

1. Run the regedit command to open the Registry Editor and navigate to the key`HKEY_CLASSES_ROOT\CLSID\76a64158-cb41-11d1-8b02-00600806d9b6` (which is for the WBEM Scripting Locator).
2. Right-click and select **Permissions**.

3. Select the **Administrators** group in the **Security** tab and click **Advanced**.
4. Select the **Owner** tab and change the owner to **Administrators** group.
5. Click **OK**.

   It navigates you to the **Permissions for** dialog box.
6. Ensure that the Administrators group has the **Allow** checkbox selected next to **Full Control**.
7. Click **OK** and then exit the **Registry Editor**.

Prerequisites for UNIX host discovery

SSH is used to discover UNIX and Linux servers. For UNIX, there are no prerequisites other than file access permissions that are available through the root user.

Prerequisites for HP-UX host discovery

To discover an HP-UX host with multi-port Fibre Channel card, the package CommonIO bundle 0812(Dec 2008) or later should be present on the host to get the updated FC-SNIA file set.

Note

When the HBA has multiple ports, the earlier version of FC-SNIA file set does not retrieve the HBA Port WWN and Target Port WWN information. Hence, the HBA Port WWN and Target Port WWN fields display a value of NA.

Discovery of HBA information

Active Probe (APE) uses the inq utility to discover HBA information:

- The probe checks if it has the necessary permission to write into the folders. This is checked by pushing some javascript files (.js) into:
  (Windows 2003)

  `C:\Documents and Settings\<username>\Local Settings\Temp`

  (Windows 2008)

  `C:\Users\<username>\appdata\local\temp`
- The probe tries to run the javascript files using the Cscript command. In case there are no exceptions, the probe has the necessary permissions to access the file system.
- If file system permissions are available, inq is pushed into:
  (Windows 2003)

  `C:\Documents and Settings\<username>\Local Settings\Temp\nl_dwd\`

  (Windows 2008)

  `C:\Users\<username>\appdata\local\temp\nl_dwd`
- Based on inq output, the probe takes the discovered information to the UI.
- These actions are followed by actions of other probes in other discovery processes.

For UNIX hosts, inq is located in:`/tmp/nl_dwd`

If inq does not exist, the SCP command is used in UNIX to copy inq. In Windows, WMI calls are used.

The following commands require root privileges to run on a given host and are used for storage resource discovery:

- `/tmp/nl_dwd/inq`
- `<path of powermt command>/powermt`
- `<path of dmidecode command>/dmidecode`

Note

If you have logged in as a sudo user, type the following to run inq: `sudo /tmp/nl_dwd/inq -mapinfo`

Credentials are incorrect

Verify that all WMI access credentials are correct. If they are not, the `host1.log` file displays the following error message:

```
Credentials/Authentication Failure
```

Note

In the Manage Logs dialog box, described in Chapter 6, “Log Files”, the Host Domain Manager selection outputs the host1.log file.

If the wrong credentials were passed for discovery from the access credentials, the host1.log file displays the following message for the IP with the credentials of the target host:

```
03-02-08 11:03:23 AM==>
HostDetection.DiscoveryTaskToTomcatSubmitter.createTasksForIPsAndAddTo
Tomcat:
172.23.147.219-Got an unsuccessful result from ActiveProbe
03-02-08 11:03:23 AM==>
HostDetection.DiscoveryTaskToTomcatSubmitter.createTasksForIPsAndAddTo
Tomcat:
172.23.147.219-The message is Authentication failed
03-02-08 11:03:23 AM==>
HostDetection.DiscoveryTaskToTomcatSubmitter.createTasksForIPsAndAddTo
Tomcat:
172.23.147.219-The resolution is CHANGE_USER_OR_CREDENTIALS
03-02-08 11:03:23 AM==>
HostDetection.setDetectionResults: detection result added
is [, Host, SSH, 0, , , , , , 219 discovery1209740538880, , , ]
```

If an unreachable IP was tried for detection or discovery or if there were network issues, the following message appears in the host1.log for the targeted IP address that was tried and unsuccessful:

```
19-02-08 11:19:34 AM==>
HostDetection.DiscoveryTaskToTomcatSubmitter.createTasksForIPsAndAddTo
Tomcat:
192.168.101.101-The resolution is CHECK_NETWORK
19-02-08 11:19:34 AM==>
HostDetection.setDetectionResults: detection result added
is [, Host, SSH, 0, , , , , , invalid discovery1209741352567, , , ]
```

Use sudo to run commands at root level

Sudo allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root user, while logging all commands and arguments. Sudo operates on a per-command basis. Sudo is not a replacement for the shell. Sudo enables you to:

- Temporarily elevate user credentials to root for specific commands that are configured in the sudoers file.
- Log on to a UNIX machine as a non-root user.
- Run SCSI commands to discover storage related information for the host.

Platform support for sudo
Sudo is supported for all flavors of Linux and UNIX.

The following topics provide additional details:

- Configure sudo on page 180
- sudoers file example on page 180
- Discover a host with sudo on page 181
- Error symptoms for a host with partial sudo prerequisites on page 181
- Verify sudo feature prerequisites on page 181
- Improper account configuration on UNIX hosts on page 182

Configure sudo

Sudo is configured using the sudoers file located in the /etc folder. Edit this file using visudo. Additional information about visudo is available at the following URL: `http://www.gratisoft.us`

Note

It is not recommended to edit the sudoers file using any editor other than visudo.

Edit the sudoers file located in the `/etc` folder file using visudo.

Additional information about visudo is available at the following URL: `http://www.gratisoft.us/sudo/man/visudo.html`

sudoers file example

1. Define both the User alias specification and Cmnd alias specification and use both in the definition of the User Privilege specification. The following is an example snippet of the `/etc/sudoers` file for the mentioned configuration:

```
# User alias specification
User_Alias CMGU=cmguser
# Cmnd alias specification
Cmnd_Alias CMGEMC=/tmp/nl_dwd/inq,<path of powermt command>/
powermt,<path of dmidecode command>/dmidecode
# User privilege specification
root ALL=(ALL) ALL
CMGU ALL=NOPASSWD:CMGEMC
```

2. Define either the User alias or Cmnd alias specification and use the defined alias in the User Privilege specification. The following is an example snippet of `/etc/sudoers` file for the mentioned configuration:

```
# User alias specification
# Cmnd alias specification
```

```
Cmnd_Alias CMGEMC=/tmp/nl_dwd/inq,<path of powermt command>/
powermt,<path of dmidecode command>/dmidecode
# User privilege specification
root ALL=(ALL) ALL
cmguser ALL=NOPASSWD:CMGEMC
```

3. Define the User Privilege specification using neither the User alias nor Cmnd alias specification. The following is an example snippet of `/etc/sudoers` file for the mentioned configuration:

```
# User alias specification
# Cmnd alias specification
# User privilege specification
root ALL=(ALL) SETENV: ALL
cmguser ALL=NOPASSWD::/tmp/nl_dwd/inq,<path of powermt
command>/powermt,<path of dmidecode command>/dmidecode
```

Note

A sudo user should be provided permission to run only inq, powermt, and fcinfo commands. The powermt command is added in the file only if PowerPath is installed on the host. A sudo user should not have permission to run all commands (to run as root user). For example:

```
cmguser ALL=(ALL) NOPASSWD: ALL
```

This is not a valid configuration, because it allows the sudo user cmguser to run all commands on all hosts without any password. Take care not to define multiple user privilege specifications for the same sudo user. After adding the sudo user to the host, set the path variable for the sudo user:

```
PATH=/usr/bin:/etc:/usr/ucb:/usr/bin/X11:/sbin:/usr/java14/jre/
bin:/usr/java14/bin:/usr/local/bin/:
```

Discover a host with sudo

To discover the host, use the created sudo username and password in the access credentials.

Error symptoms for a host with partial sudo prerequisites

- If the target host does not have the sudo account, but the sudo feature is installed, then the policy fails because the account to log in to the host is not available.
- If the target host has a valid sudo account (without the sudo feature installed), then there is a partial discovery due to limited credentials.
- If the target host has a valid account with the sudo feature installed, but the credentials provided for the sudo account are invalid, the discovery fails due to authentication failure.

Verify sudo feature prerequisites

- Log in to the respective host using sudo credentials. If login credentials do not work, resolve this with your local IT group.
- Set default to the `/tmp/nl_dwd` folder, if it is present, and execute the command `sudo /tmp/nl_dwd/inq –mapinfo`. If sudo is installed, all HBAs and the respective host devices are visible. Otherwise, the following message appears: **Sudo is not available.**
- If the `/tmp/nl_dwd` folder is not present, type sudo. If you see the message **sudo: not found** or **Sudo is not available**, have your local IT technician install sudo.

- Using the administrative (root) account, check the settings for the host to be discovered in the sudoers file. The UNIX sudoers file is typically located at `/etc/sudoers` or `/usr/local/etc/sudoers`. On some UNIX hosts, the sudoers file can be edited using visudo. Otherwise, use locally available editors (vi, and so on).

Improper account configuration on UNIX hosts

On all UNIX hosts with sudo accounts, the sudo messages repeatedly appear.

This issue is observed only when the discovery command fails, and a line is added to the console. Because the application is designed to retry the same command at an interval of x seconds for two hours, the message repeatedly appears. It is the absence of the sudoers file that causes the problem.

Improperly configured sudo accounts could result from the following scenarios:

- The credentials given to ProSphere do not include the `/etc/sudoers` file. The following message is displayed on the UNIX console:

  ```
  user NOT in sudoers ; TTY=pts/4 ; PWD=/ ; USER=root ;
  COMMAND=/tmp/nl_dwd/inq -mapinfo
  ```

- `/etc/sudoers` file was never setup. Sudo accounts are not used. The following message is displayed on the UNIX console:

  ```
  can't stat /etc/sudoers: No such file or directory; s/2 ; PWD=/ ;
  USER=root ; COMMAND=/tmp/nl_dwd/inq
  ```

VM host was powered down or deleted

The initial discovery of VM host fails occasionally with an error: `Querying VMware web service for previously found VM <VM DNS name> failed for unknown reason. Aborting VM/IP/OS discovery.`

The VM host which was detected initially, changed its state during discovery or just before discovery. It was either powered down or deleted resulting in discovery failure.

The UI may show inconsistent failure results and empty Object Name for this VM host.

Rerun the initial discovery policy to fix this issue.

Inaccurate data in the Inventory view

Discovering ESX and VM guests without a DNS name will result in an inaccurate Inventory view for these objects.

Assign DNS names to ESX and VM guests before discovery of the vCenter by ProSphere.

Proper credentials required for ESX discovery

If you use the ESX host credentials for discovery of an ESX server, both the ESX host and the VM are discovered. However, in the ESX object details view the tabs labeled VMs and Path Details are missing.

To avoid this problem, perform ESX discovery through the VMware Virtual Center.

Discovery job progress delayed

In the **Discovery Jobs** › **Log tab** › **Run Date** column, when you click on the run date for a job that is discovering a very large number of objects, the Job Execution Results dialog box does not show job progress for several minutes.

Click the discovery job values in the # Failed Detections, # Partially Discovered Objects, and # Fully Discovered Objects to display the job status.

Job Execution Results: Object name missing

For discovery jobs that involve VMware discovery, the Job Execution Results dialog box could contain an empty object name. This happens when the virtual machine object corresponding to that result is deleted from the system due to a DNS change event, or when a user deletes the host after it is discovered. The second case is possible with any physical host other than the ESX server.

There is no workaround.

Job Execution Results shows object name after discovery failure

When viewing **Discovery Jobs** › **Details** › **Run Date** › **Job Execution Results - Job Run Date table**, the Object Name column cells will be populated with an object even when there has been a detection failure. In these cases, the cells should be empty.

Launch the **Failed Detections** and **Fully Discovered Objects** dialogs using the individual links in the cells of the # Failed Detections and the # Fully Discovered Objects columns.

ProSphere fails to discover remote Symmetrix arrays

A Symmetrix array is considered local to the EMC SMI-S Provider when it is directly accessible over Fibre Channel through Symmetrix gatekeepers. Symmetrix arrays that are remote to the EMC SMI-S Provider are indirectly accessed through another Symmetrix by way of a Symmetrix Remote Data Facility (SRDF) connection. These remote Symmetrix arrays are not discovered by ProSphere because masking and mapping data cannot be obtained. A detection failure is present for each remote Symmetrix array found during an initial discovery to alert the user.

Two EMC SMI-S Providers are necessary for ProSphere to discover both Symmetrix arrays connected in an SRDF configuration. In this case, each EMC SMI-S Provider will have a Fibre Channel connection to one of the Symmetrix arrays which represents one end of the SRDF connection.

For example, EMC SMI Provider on host AtoB will see Symmetrix A through a fibre connection and Symmetrix B through an SRDF connection. In contrast, EMC SMI Provider on host BtoA will see Symmetrix B through a fibre connection and Symmetrix A through an SRDF connection.

Therefore, ProSphere requires array discovery policies that include both EMC SMI-S Providers so that both Symmetrix A and B are discovered. As expected, each array discovery policy will report a detection failure for each remote Symmetrix.

Insufficient number of Symmetrix Gatekeepers

An insufficient number of Symmetrix gatekeepers results in slow Provider performance and contributes to discovery failures due to timeouts.

For optimal EMC SMI-S Provider performance and stability, ensure that there are at least six gatekeepers per Symmetrix that is fibre-connected to an EMC SMI-S Provider host. Adding more than six gatekeepers for larger Symmetrix arrays marginally improves performance.

CPU and OS version are not reported for virtual guest

In the Attributes tab for Virtual Guest, the CPU and OS version information is not reported.

The Operating System attribute provides information on the OS version.

Partial discovery information appears for Cisco switches

ProSphere displays the Cisco VSAN fabric as partially discovered if no community string was provided during its configuration.

NAS licenses not enabled

Upon successful discovery, if you receive one or more of the following error messages, verify that corresponding licenses for NAS components (CIFS/NFS/SnapSure) are enabled:

- `[CifsShareQueryOperation] Failed. Please Check if the license is enabled for CIFS component on the NAS Control Station. Refer the log file for further details.`
- `[NfsShareQueryOperation] Failed. Please Check if the license is enabled for NFS component on the NAX Control Station. Refer the log file for further details.`
- `[FileSystemCheckPoint] Failed. Please Check if the license is enabled for Snapsure component on the NAS Control Station. Refer the log file for further details.`

To enable licenses on the NAS, use the commands in Table 35 on page 184

Table 35 NAS license commands

Command	Function
`nas_license -list`	Displays enabled NAS licenses
`nas_license -create nfs` (or **`cifs`**, or **`snapsure`**)	Enables a specific NAS license

For more information refer to the "Configure Storage Systems" chapter of the *EMC ProSphere Deployment Guide*.

Rediscovery issue: Daylight Savings Time

Scheduled or unscheduled rediscovery should not be run when the physical servers or VMware virtual machines are operating at the same time as Daylight Saving Time (DST) changes.

Performance data issues

This section describes issues related to performance data collection.

Limitations to path performance collection for virtual machines

If you discover a virtual machine using ESX Server, you will be able to turn on Path Performance Collection with the following limitations.

The following VMware Guest Performance Charts are not supported:

- Host Devices - Response Time
- Host Devices - Queue Length

You can rediscover VM-Guest using WMI/SSH to collect details for the missing charts.

Performance data can be interrupted by new discoveries

Once initial discovery of an environment is complete, performance data collection may fail for subsequent discoveries of additional objects. This failure occurs for the polling period (typically 5 minutes). The initial discovery establishes entry points in the database for performance data; if subsequent passes collect data for new objects, these passes are treated as failed data collections.

The situation is self-correcting. Data collection passes that happen after the failed one are processed correctly if there are no further changes relative to the failed time interval.

Response time chart is empty for Windows 2008 hosts

There is an anomaly in Queue Length within Windows 2008 where the queue length is actually N-1. Therefore, if the queue depth is reported as 1, the queue will actually be reported as idle. This has the potential to skew the response time within the Host Summary Performance view.

There is no workaround at this point.

Host Device Response Time versus Array LUN Response Time

The host device response time, in comparison to the array LUN response time, might have a deviation such that the corresponding numbers do not match one to one. This is because the following formulas are used to compute the values:

Host Device Response Time = Queue Length / IOs per second

Array Device Response Time = (Sample Average Read Time + Sample Average Write Time) / (Sample Average Reads + Sample Average Writes)

Naming of devices is mixed

There are device naming inconsistencies in the Host Devices - Chart Details dialog box that cause devices to appear with two different name formats, depending on whether or not the device is associated with a known array LUN.

There is no workaround.

Array FE Directors - % Busy graph blank for Symmetrix

The Array FE Directors - % Busy graph may be blank for some Symmetrix arrays even though the arrays are successfully discovered. This happens when more than six Symmetrix arrays are managed by a host.

The reason for this is that, for optimal performance in our recommended configuration, Solutions Enabler sets the default to six Symmetrix arrays for performance data collection.

Note

This default setting does not affect collection of performance data for VNX and CLARiiON arrays.

Follow these steps to modify the default setting for performance data collection of Symmetrix arrays.

1. On your host, open the `daemon_options` file.
   For a Windows host:
   `symapi\config\daemon_options`
   For a Linux host:
   `symapi/config/daemon_options`
2. Uncomment the `storstpd: DMN_MAX_ARRAYS` parameter and set it to desired value.
3. Restart the Solutions Enabler performance collector service (storstpd daemon).

Follow the Solutions Enabler documentation for the maximum number of arrays allowed, based on the available memory and CPU on the host.

Log file issues

This section describes issues related to log files.

Downloading log files

When you download a set of selected log files, its status appears at the bottom of the browser. Log file downloads can take a very long time depending upon their size. You can minimize the window and work with other modules of ProSphere. However, there is no option to terminate the download.

Once you click Download for a set of selected files, the Download Logs button in the user interface (UI) is disabled, thus disabling concurrent downloads of log files. However, another set of log files can be downloaded from another open instance of the same ProSphere appliance.

Editing log levels

The log levels for a few components cannot be edited through the Manage Logs dialog box.

Components that do not allow changing the log level on page 119 provides a list of components that do not support editing of log levels.

NOTICE

Log levels should not be set to the Debug or Trace levels for more than one or two hours. After collecting your log files, you should reset the log level back to Info.

Error unzipping database log ZIP file on Windows hosts

If you unzip the database logs downloaded from **Admin** › **System** › **Manage Logs**, the following error occurs:

```
gpsegstop..py_svthistapp:gpadmin_20120216-
Historical_Database.log
```

This error is caused by the semicolon in the filename of the downloaded ZIP file. A semicolon is not a valid character for filenames on Windows hosts.

The workaround is to use WinRAR instead of WinZip to unzip the database logs.

Alerting issues

This section describes issues related to alerts.

Unisphere for VMAX alerts not displayed

When Unisphere for VMAX alerts are not displayed in the ProSphere Console, verify that the time set on the Discovery Engine and the installed server host are synchronized.

SPA and ProSphere metric names may differ

The names for alert metrics reported in SPA and the ProSphere UI may differ. For example:

- SPA uses the term `IOs/sec`, but ProSphere uses the term `IO_RATE`
- SPA uses the term `Avg Read Response Time (ms)`, but ProSphere uses the term `RESPONSE_TIME_READ`

Table 36 on page 187 provides a complete list of the differences in names of the alert metrics between SPA and ProSphere

Table 36 Differences in alert metrics names in ProSphere and SPA

Metric category	SPA metric name	ProSphere metric name
Array metrics	Host IOs/sec	ARRAY_IO_RATE
	% Cache WP	ARRAY_TOTAL_CACHE_UTILIZATION
	% Hit	ARRAY_PERCENT_HIT
	Device WP Events/sec	ARRAY_DEV_WRITE_PENDING_EVENT_PER_SEC
	System WP Events/sec	ARRAY_SYS_WRITE_PENDING_EVENT_PER_SEC
Device Group (DG)Metrics	Read Response Time (ms)	DG_SAMPLED_AVG_READ_TIME
	Write Response Time (ms)	DG_SAMPLED_AVG_WRITE_TIME
	% Write Miss	DG_PERCENT_WRITE_MISS
	% Read Hit	DG_PERCENT_READ_HIT
	Response Time (ms)	DG_RESPONSE_TIME
	Host IOs/sec	DG_IO_RATE
Disk (DISK) Metrics	Avg Response Time	DISK_RESPONSE_TIME
Front End Director (FE_DIR) Metrics	Host IOs/sec	FE_DIR_IO_RATE

Table 36 Differences in alert metrics names in ProSphere and SPA (continued)

Metric category	SPA metric name	ProSphere metric name
Back End Director (BE_DIR) Metrics	IOs/sec	BE_DIR_IO_RATE
RDFA Group Metrics	Avg Cycle Time	RDFAGROUP_AVG_CYCLE_TIME
	Active Cycle Size	RDFAGROUP_ACTIVE_CYCLE_SIZE
Disk Group (DISKGROUP) Metrics	Avg Read Response Time (ms)	DISKGROUP_RESPONSE_TIME_READ
	Avg Response Time	DISKGROUP_RESPONSE_TIME
	Avg Write Response Time (ms)	DISKGROUP_RESPONSE_TIME_WRITE
RDF DIR (RDF_DIR) Metrics	MBs Sent and Received/sec	RDF_DIR_MB_RATE

Downgrading to ProSphere 1.0, then upgrading to ProSphere 1.5

When you deploy ProSphere 1.5, ProSphere subscribes to SMC events through the EMC SMI-S Provider, which converts the SMC events to indications. Even if you remove ProSphere 1.5, the subscription to the SMI-S Provider indications for SMC events persists. Suppose you deploy ProSphere 1.0, which does not support consolidation of SMC alerts, on the same ESX or ESXi cluster, and later you upgrade to ProSphere 1.5. ProSphere 1.5 now displays all SMC alerts received before the downgrade to ProSphere 1.0, along with the new ones received after the upgrade to ProSphere 1.5.

Until you unsubscribe from SMC events, the SMI-S Provider continues to send indications to ProSphere. To unsubscribe from SMC events in the SMI-S Provider, you need to execute an SMI-S script that removes the ProSphere 1.5 subscription. SMI-S documentation provides information on how to unsubscribe from SMC events.

SMC (SMI-S) alerts appear when SMC is not installed

You may see certain external alerts displayed as SMC (SMI-S) alerts in ProSphere even when no instances of SMC are installed in your environment. This is because the source of the alerts is the Solutions Enabler. The SMI-S Provider receives the alerts from the Solutions Enabler and sends them to ProSphere. Because these alerts are identical to SMC alerts, ProSphere displays them as SMC (SMI-S).

The Solutions Enabler is also responsible for displaying SMC (SMI-S) alerts which have been disabled in SMC.

Alert notifications do not appear for Cisco DCFM alerts

Alerts from Cisco DCFM are collected even before Cisco switches are discovered. Later the Cisco switches are discovered in ProSphere. When a user action such as acknowledge, unacknowledge, or close is performed on an alert consolidated from a Cisco DCNM alert source for a switch is not yet discovered, alert notification does not occur.

To receive alert notifications for alerts for which the CI is not discovered, create a notification policy and use the criteria No Group.

WS-MAN certificate import issues

This section describes errors that occur while importing a WS-MAN certificate.

Enhanced Key Usage field is not set to Server Authentication

The following error message is displayed when you are creating HTTPS Listener with a third-party certificate:

```
The winRM command cannot process the request. The Enhanced Key
Usage field of the certificate is not set to Server
Authentication.
```

To troubleshoot the error, follow these steps:

Procedure

1. Launch and run mmc (**Start** › **Run** › **mmc** › **OK**).

   The mmc console appears.
2. Select **File** › **Add/Remove Snap-in...**. The **Add/Remove Snap-in** window appears.
3. Click **Add**. The **Add Standalone Snap-in** window appears.
4. Select **Certificates**. The **Certificates Snap-in** window appears.
5. Select **Computer account** and click **Next**.
6. Select **Local computer** if you want the snap-in to manage the same machine or **Another computer** if you want the snap-in to manage any other machine.
7. Click **Finish**.
8. Close all the open windows and select **OK** to close the **Add/Remove Snap-in** window. The **Certificates** store is populated in the **Console** window.
9. Click **Certificates** › **Personal**. The **Certificates** folder appears.
10. Double click the certificate. The **Certificate** window appears.
11. Select **Details tab** › **Edit Properties**. The **Certificate Properties** window appears.
12. Select **General tab** › **Enable only following purposes**. Select the **Server Authentication** check box and clear all the other check boxes.
13. Click OK to close all the open windows.

Certificate CN and hostname do not match

The following error message is displayed when the hostname does not match CN name in the certificate:

```
The winRM client cannot process the request. The certificate CN
and hostname that were provided do not match
```

To troubleshoot the error, follow these steps:

Procedure

1. Double click the certificate (CER) file.
2. Navigate to the **Details** tab and select the **Subject** field.

3. Get the CN name and ensure that the same CN name is used in the **winrm** command.

Resource already exists

The following error message is displayed when you try adding a certificate after one was added:

```
The WS-Management service cannot create the resource because it
already exists.
```

To troubleshoot the error, follow these steps:

1. Delete the existing thumbprint executing the command: c:\> **winrm delete winrm/config/listener?Address=*+Transport=HTTPS**
2. Navigate to the **Details** tab and select the **Thumbprint** field.
3. Add the new thumbprint to the listener.

Cannot find the certificate that was requested

The following error message is displayed when you try to add to the listener a certificate that is not imported:

```
The WS-Management service cannot find the certificate that was
requested
```

To troubleshoot the error, follow these steps to import the certificate before adding it to the listener:

Procedure

1. Navigate to the directory on the host where the PFX file is copied.
2. Execute the following command to import the certificate to the Personal Store: **certutil -importpfx -p <password> <PFX Filename>**

Note

If certutil is not available, use **mmc** › **Add/remove snap in** › **Certificate** › **Personal**. Import the PFX certificate under the Personal store.

Certificate structure was incomplete

The following error mesage is displayed when you try to add a certificate that has incomplete structure:

```
The WinRM client cannot process the request. The certificate
structure was incomplete. Change the certificate structure and
try the request again.
```

To troubleshoot the error, follow these steps:

- Navigate to the **Details** tab and select the **Thumbprint** field.
- Verify the thumbprint to the listener.

HttpSetServiceConfiguration failure

While adding the certificate to the listener, you might encounter the following error:

```
WSManFault
    Message
```

```
        ProviderFault
            WSManFault
                Message = The function: "HttpSetServiceConfiguration"
failed unexpectedly.
                          Error=1312.
Error number: -2147023584 0x80070520
A specified logon session does not exist. It may already have been
terminated.
```

This error is generally seen when the certificate is inappropriate or has been tampered with.

To troubleshoot the error, import the certificate again. Then, try to create the listener again with the thumbprint of the certificate.