EMC® ProSphere™

Version 1.7

Deployment Guide

P/N 300-999-738

REV 03

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Published February 2013

Contents

Chapter 1 Documentation map

Chapter 2 Deployment Checklist

VMware considerations 10
Network considerations 10
Storage considerations 10
Host considerations 10
Switch considerations 11

Chapter 3 Overview

ProSphere terminology 14
Deployment task reference table 16

Chapter 4 Prepare VMware Infrastructure

Base VMware infrastructure requirements checklist 20
VMware user credentials 20
Virtual hardware requirements 21
Provision thick and thin disks 22
VMware Tools on the ProSphere vApp 22
Browser requirements 22
Obtain VMware infrastructure requirements 22

Chapter 5 Configure Hosts

Avoid underscores in hostnames 26
    Characters not allowed in hostnames 26
DNS registration 26
Validate HBAs 26
EMC ProSphere/SCA Host Configuration Utility 28
Configure Windows hosts and WS-MAN 28
Configure Windows hosts and WMI 30
    Prerequisites for Windows Server 2003 and Windows Server 2008 30
    Disable UAC on Windows 2008 SP2 32
    Disable UAC on Windows 2008 R2 32
    Add a user with the necessary remote DCOM permissions 32
Configure UNIX and Linux hosts 37
    Discovery requirements 38
    Collect performance data 42

Prepare for discovery of VMware guests 43
Prepare for discovery of VMware infrastructure 43
Discovery requirements 43

Chapter 6 Configure Arrays

Configure the EMC SMI-S Provider 46
Requirements for discovery data collection 46
Requirements for performance data collection 47
Configure the provider 47

Chapter 7 Configure Switches and Fabrics

Configure Cisco switches 50
Perform preconfiguration tasks 50
Configure switches for SNMPv1/2 52
Configure switches for SNMPv3 53

Chapter 8 Deploy ProSphere

Obtain deployment files 56
Deployment time 56
Deploy ProSphere 57
Next steps 61

Chapter 9 Deploy Collectors

Collector 63
Obtain deployment files 63
Determine the Collectors required for data center 63
Collect information 64
Deploy Collectors 64
Register a Collector with the ProSphere Application 66
Load balance Collectors 66

Chapter 10 Deploy Secondary ProSphere Application

Secondary ProSphere Application 68
Limitation 68
Obtain deployment files 68
Collect information 69
Deploy a Secondary ProSphere Application 70
Register a Secondary ProSphere Application 71

Chapter 11 Post-Deployment Tasks

Synchronize time zones and system times 74
Log into ProSphere 74
Integrate ProSphere with SMAS and Unisphere for VMAX 76
Integrate ProSphere with SMAS 77
Integrate ProSphere with Unisphere for VMAX 82
Configure CMCNE 88
CMCNE 88
Location of the keytool utility on CMCNE or BNA hosts 89
Perform configuration tasks 90
Synchronize ProSphere deployments 93

Deploy trusted certificates 93
Additional information 93

Appendix A Updates and Backups

Overview 96
Supported updates 96
ProSphere update methods 96
Download an ISO file to a virtual CD-ROM 97
Install updates on ProSphere 98
Create snapshots before updating software 98
Select the EMC Update Repository as a source for updates 99
Select a virtual CDROM or web server for updates 99
Receive updates reminder at login and apply updates 100
Manually check for and apply updates 100
SMC, SPA, and SMAS 101
Create and restore snapshots or backups 102
Shut down or start up ProSphere or its virtual machines 102
Create ProSphere snapshots 103
Roll back to a snapshot 103
Back up and restore ProSphere with VMware Data Recovery 104

Preface

As part of an effort to improve and enhance the performance and capabilities of its product lines, EMC periodically releases revisions of its hardware and software. Therefore, some functions described in this document may not be supported by all versions of the software or hardware currently in use. For the most up-to-date information about product features, refer to your product release notes.

If a product does not function properly or does not function as described in this document, contact your EMC representative.

Revision history

The following table presents the revision history of this document:

Revision	Date	Description
01	December 2012	Initial version for 1.7 release.
02	February 2013	Initial version for 1.7.0.1. release.
03	April 2013	1.7.0.1 update on EMC Online Support site. Additional CMCNE configuration procedures.

Audience

This document is part of the EMC ProSphere documentation set, and is intended for use by system administrators and integrators responsible for deploying ProSphere.

Conventions used in this document

EMC uses the following conventions for special notices.

Note: A note presents information that is important, but not hazard-related.

Typographical conventions

EMC uses the following type style conventions in this document:

Normal

Used in running (nonprocedural) text for:

- Names of interface elements (such as names of windows, dialog boxes, buttons, fields, and menus)
- Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, functions, utilities
- URLs, pathnames, filenames, directory names, computer names, filenames, links, groups, service keys, file systems, notifications

Bold

Used in running (nonprocedural) text for:

- Names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system calls, man pages

	Used in procedures for: • Names of interface elements (such as names of windows, dialog boxes, buttons, fields, and menus) • What user specifically selects, clicks, presses, or types
Italic	Used in all text (including procedures) for: • Full titles of publications referenced in text • Emphasis (for example a new term) • Variables
`Courier`	Used for: • System output, such as an error message or script • URLs, complete paths, filenames, prompts, and syntax when shown outside of running text
`Courier bold`	Used for: • Specific user input (such as commands)
`Courier italic`	Used in procedures for: • Variables on command line • User input variables

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`

Documentation map

ProSphere Documentation Library

Numbers indicate suggested flow of reading

Deployment

Release notes

Information about this release you should know before proceeding

Support matrix

Software and hardware supported for deployment and discovery

Performance & scalability

Optimize performance and scalability

Determine how many Collectors you will need

Deployment guide

Configure hosts, switches, arrays, and the VMware infrastructure

Deploy ProSphere and the Collectors

Perform updates and backups

Administration

Admin guide

Manage licenses, users, and roles
Perform discovery
Manage alerts
Collect log files
Configure multiple sites
Troubleshooting

Security guide

Configure software and physical settings for a deployed ProSphere vApp

Ports usage

Configure firewalls and ports used by ProSphere

Reference

User guide

Use cases describing discovery, displaying capacity and performance data

Using alerts to analyze problems

Console help

View dedicated topics for each view and dialog

View detailed descriptions of capacity and performance metrics.

Describes all of the basic operations

Includes a topic for each error code

1 Deployment Checklist

This checklist summarizes the requirements that need to be in place before ProSphere™ is deployed. Keep this chapter and the following documents close at hand; they will guide you with detailed procedures for deploying ProSphere and setting up the SAN environment for ProSphere.

- *EMC ProSphere Support Matrix*
- *EMC ProSphere Security Configuration Guide*

Note: If your corporation requires additional ProSphere security hardening to comply with the U.S. Federal or Department of Defense mandates, the ProSphere Federal Security Hardening Guide is available to all US Federal customers. Contact your EMC® representative to obtain a copy. These procedures must be performed immediately after you deploy ProSphere.

The chapter includes the following sections:

- VMware considerations 10
- Network considerations ..... 10.
- Storage considerations 10
- Host considerations 10
- Switch considerations 11

Note: ProSphere 1.7 runs on SuSE Linux Enterprise Server 11 SP1 (64 bit) which is installed as part of the Deploy OVF Template process and is included with the ProSphere 1.7 software.

VMware considerations

- ❑ Ensure that you have at least one VMware ESX or ESXi server that is managed by a vClient server.
- ❑ Identify a VMware ESXi or vCenter server for the vApp installation. Consult your VMware administrator to ensure that all the required VMware infrastructure is in place.
- ❑ Allocate the required RAM each for the Discovery Engine, ProSphere Application, and Historical Database

Network considerations

- ❑ Collect the following network data for each of the three virtual machines and one for each Collector:
  - ❑ A valid static IP address for the virtual machine.
  - ❑ A fully qualified domain name for the virtual machine.
  - ❑ A network mask for the IP address.
  - ❑ A network gateway for the IP address.
  - ❑ Primary and optional secondary DNS server IP addresses.
- ❑ Register all IP addresses used by ProSphere in DNS, and ensure that the reverse lookup through PTR records is supported.
- ❑ Check for firewall restrictions that may interfere with normal ProSphere operation in your VMware environment, broader network, and storage resource discovery.
- ❑ Ensure that you have a license to deploy the ProSphere vApp in a DRS cluster. This requires at least an enterprise license with ESX.
- ❑ Clusters where ProSphere will be deployed must have at least two hosts and must be in DRS mode.

Storage considerations

- ❑ Download and install the EMC SMI-S Provider, used to discover EMC arrays.
- ❑ Check that the Symmetrix Management Solution (SMAS) bundle is installed on SAN attached hosts that have dedicated gatekeepers to Symmetrix arrays. SMAS contains Symmetrix Performance Analyser (SPA) and Symmetrix Management Console (SMC). VNX/Clariion arrays are discovered over TCP/IP.
- ❑ Please refer to SMC/SPA or Unisphere for VMAX release notes to determine which should be used for the site configuration being monitored by ProSphere.

Host considerations

- ❑ WMI — required to discover physical Windows hosts and collect performance data using WMI access credentials.
- ❑ WS-MAN — required to discover Windows hosts using WS-MAN access credentials.

- ❑ SSH - root and sudo — required to discover physical UNIX hosts. For the non-root user, install sudo on the host and configure the sudoer file.
- ❑ VMware Infrastructure — required to discover VMware environments. ESX server or vCenter credentials with Browse Datastore permissions are required.
- ❑ WinRM service — required to discover Windows hosts using WS-MAN access credentials (optional).
- ❑ EMC— supported HBA drivers and firmware and HBA vendor-specific SNIA libraries (required for all operating systems)
- ❑ iostat — required for performance data collection on Linux (RedHat and SuSE) and Solaris hosts.
- ❑ sar — required for performance data collection on AIX and HP-UX hosts.

Switch considerations

- ❑ HTTP or HTTPS access credentials for the SMI-S Provider to discover Brocade switches.
- ❑ Install Connectrix Manager Converged Network Edition (CMCNE) on a separate host and discover fabrics to be managed in the SMI-S Provider before discovering it from ProSphere
- ❑ SNMP v1, v2, and v3 access credentials to discover Cisco switches.
- ❑ Set up Single Sign On (SSO) for Brocade switches.
- ❑ Zoning requirements and conventions for passive discovery of hosts.

2 Overview

This chapter provides an overview of environment configuration and deployment.

The chapter includes the following sections:

- ProSphere terminology 14
- Deployment task reference table 16

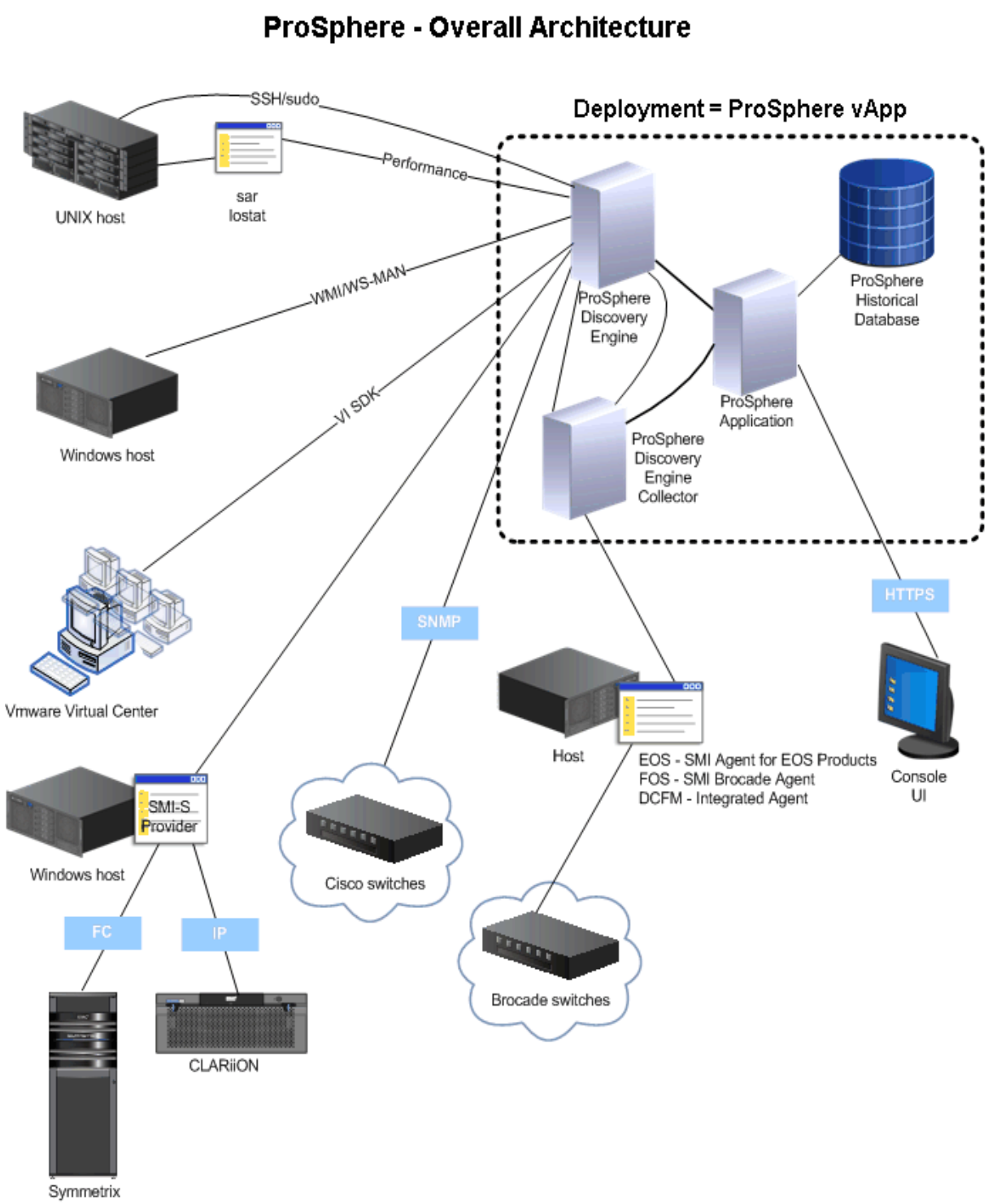
Note: If you are applying ProSphere updates, such as installing ProSphere 1.x, go directly to Appendix A, "Updates and Backups".

ProSphere terminology

The following terms related to ProSphere are used in this document:

- A "virtual machine" is a software computer that runs an operating system and applications. Multiple virtual machines can run concurrently on the same host. The virtual machines that form the core of ProSphere are: the ProSphere Application, the Discovery Engine, and the Historical Database. Some deployments include one or more instances of an additional virtual machine: the Discovery Engine (Collector). Figure 1 on page 15 illustrates these virtual machines.
- A "vApp", shown in Figure 1 on page 15, is a software solution optimized for the cloud, consisting of multiple virtual machines, packaged and maintained as a single entity in OVF format. ProSphere is deployed as a VMware vApp, configured as a collection of interdependent virtual machines.

Figure 1 ProSphere Architecture



- A "virtual appliance" is a software solution composed of one or more virtual solutions. A virtual appliance is packaged as a unit by an appliance vendor and is deployed, managed, and maintained as a unit. ProSphere is also a virtual appliance.
- A "ProSphere Application" manages ProSphere components, controlling activity with the Historical Database, the Discovery Engines, and user Consoles.

- A "Historical Database" stores attribute and performance data for all discovered objects. It receives data from the Discovery Engines and is managed by the ProSphere Application.
- A "Discovery Engine" discovers logical and physical resources in the SAN and supplies attributes and performance data to the Historical Database. It optionally controls Discovery Engine Collectors, and is managed by the ProSphere Application.
- A "Discovery Engine (Collector)" discovers logical and physical resources in the SAN and supplies attributes and performance data to the Discovery Engine. Collectors appear in scale-out deployments. While there is only one Discovery Engine, there may be many Collectors.

Deployment task reference table

Table 1 on page 16 is a guide to documentation on deployment-related tasks.

Table 1 Documentation references

To...	Refer to...
Get started...	
Learn about ProSphere architecture	Architecture chapter in the *EMC ProSphere Administrator Guide*
Decide whether and how to scale out a ProSphere deployment	*EMC ProSphere Performance and Scalability Guidelines*
Prepare the storage area network (SAN) and its components (hosts, arrays, and switches)	• See Section "Deployment Checklist" on page 9 for a list of requirements before deployment • Configuration chapters in this manual for software configuration procedures • *EMC ProSphere Support Matrix* for supported versions of hardware and software • *EMC ProSphere Release Notes* for supplemental information about a specific release
Change system passwords	*EMC ProSphere Security Configuration Guide*
Broad overview of configuration, deployment, and product use	*EMC ProSphere User Guide*
	Note: Subsequent references are to chapters in this manual.
Verify that the VMware infrastructure meets the base infrastructure requirements	
Verify that your VMware infrastructure meets the base infrastructure requirement	Chapter 3, "Prepare VMware Infrastructure"
Verify that you have the VMware credentials required for deployment	
Verify that you meet the virtual hardware requirements	
Obtain VMware information needed in the deployment process	

Table 1 Documentation references

To...	Refer to...
Configure the ProSphere environment to allow successful discoveries	
Configure third-party software used to discover hosts and related performance data	Chapter 4, “Configure Hosts”
Configure array data providers (software that exposes array management information)	Chapter 5, “Configure Arrays”, Chapter 6, “Configure Switches and Fabrics”
Configure Cisco and Brocade switches and fabrics	Chapter 6, “Configure Switches and Fabrics”
Deploy ProSphere	
Download the deployment files (.ovf file and .vmdk files) to a location accessible to the vSphere Client.	Chapter 7, “Deploy ProSphere”
Open the vSphere Client and connect to the vCenter server managing the VMware environment.	
Enter information at the Deploy OVF Template dialog box. This includes information about the resource pool for the ProSphere vApp, the datastore, and the ProSphere virtual machines.	
Use a vSphere Client to download the files and transmit them to an ESX or ESXi server.	
Deploy Collectors, if needed to scale out the deployment.	Chapter 8, “Deploy Collectors”
Perform post-deployment tasks	
Synchronize ProSphere deployments, if you have more than one deployment	Chapter 10, “Post-Deployment Tasks”
Deploy organization-trusted certificates through the ProSphere Console	

3 Prepare VMware Infrastructure

This chapter provides information about infrastructure requirements and how to prepare your VMware environment for ProSphere deployment. The following sections detail infrastructure requirements:

- Base VMware infrastructure requirements checklist 20
- VMware user credentials 20
- Virtual hardware requirements 21
- Provision thick and thin disks 22
- VMware Tools on the ProSphere vApp 22
- Obtain VMware infrastructure requirements 22

Base VMware infrastructure requirements checklist

IMPORTANT

Consult with your VMware administrator to ensure that all the required VMware infrastructure is available before you start ProSphere deployment.

The base VMware infrastructure requirements include:

- ❑ A VMware vSphere virtualized computing environment.

IMPORTANT

ProSphere does not validate hostnames. You must independently register with DNS (1) hostnames you specify for virtual machines (2) hostnames for hosts that ProSphere will discover (3) hostnames for hosts about which information will be collected in reports. Failing to register hostnames with the corresponding DNS may prevent normal operation of ProSphere.

- ❑ An installed vCenter server.
- ❑ An installed VMware ESX or ESXi server running in the vSphere environment.
- ❑ A data store with a minimum 600 GB of free space for the unzipped appliances and for the downloaded zipped appliance image files. This data store will hold the appliance images needed to run ProSphere.
- ❑ If you are deploying ProSphere in a VMware cluster setup, ESX or ESXi servers should be time-synchronized to an external Network Time Protocol (NTP) server. However, the product can be deployed on a single ESX server, if the server meets hardware requirements mentioned "Virtual hardware requirements" on page 21. If you deploy on a single ESX server, in the data center section of vCenter set the environment for a single ESX server and not a cluster.
- ❑ The clock settings of all the ESX or ESXi servers present within the cluster are synchronized. Unsynchronized ESX or ESXi servers might lead to ProSphere discovery issues.

Note: To take advantage of vSphere features that enhance availability and flexibility of a virtual infrastructure, EMC recommends that you deploy ProSphere on an ESX or ESXi server cluster.

VMware user credentials

ProSphere deployment is performed by a user logged into the VMware infrastructure. Table 2 on page 21 specifies the user credentials required by VMware for an installer.

Table 2 VMware credentials required for ProSphere deployment

VMware infrastructure resource	Required user credentials
Data store	• Allocate space • Browse data store • Low-level file operations
Host Local Operators	• Create Virtual Appliance • Delete Virtual Appliance • Reconfigure Virtual Appliance
Host Profile	View
Network	Assign Network
Resource	• Assign vApp to Resource Pool • Assign VM to resource pool • Migrate • Query VMotion
vApp	Full permissions
Virtual machine	Full permissions

Virtual hardware requirements

ProSphere administrators can use this information to make their deployment decisions based on current and expected hardware resource utilization.

Table 3 Virtual hardware requirements

Virtual Machine	Virtual Processor	RAM / Memory	Storage
Requirements for an unscaled deployment			
ProSphere Application	Four 64-bit CPUs	8 GB	230 GB
Discovery Engine	Four 64-bit CPUs	8 GB	40 GB
Historical Database	Four 64-bit CPUs	6 GB	230 GB
Requirements, for a scaled deployment with an additional Discovery Engine Collector (Collector)			
Additional Collector	Two 64-bit CPUs	6 GB	30 GB (For Thick Disk) 2.2 GB (For Thin Disk)
Requirements for a deployment with an additional (Secondary) ProSphere Application			
Secondary ProSphere Application	Two 64-bit CPUs	4 GB	230 GB

Note: No special VMware configuration procedures are required before deploying ProSphere.

Provision thick and thin disks

When making a decision to use thick or thin provisioning, consider the future storage capacity requirements of all the virtual machines on the same datastore, and the disk space usage of ProSphere Application and Historical Database. *EMC ProSphere Performance and Scalability Guidelines* details the storage considerations for ProSphere deployments.

VMware Tools on the ProSphere vApp

IMPORTANT

Do not install additional VMware Tools on ProSphere vApp. VMware Tools are already installed on the ProSphere virtual machines. Additional updates to VMware Tools will be provided with the updates to ProSphere vApp.

Because ProSphere installation performs the updates to VMware Tools on ProSphere virtual machines, VMware Tools are listed as "unmanaged" when viewed in the vSphere client software. This means they are not managed by the vCenter server.

Browser requirements

ProSphere requires Adobe Flash Player version 10.2.153.1 or later, which is available for most popular browsers including Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome. If your Flash player is older than this version, upgrade to the latest available Flash player.

ProSphere is best displayed on a monitor set to a resolution of 1024x768 or higher.

Transport Layer Security (TLS) 1.0 is required as the security setting for the web browser.

Ensure that your browser accepts cookies and that pop-up blockers are disabled. For browsers in which the launching window does not automatically close (for example, Microsoft Internet Explorer), it is necessary to use a new browser instance for each ProSphere login. The browser retains cookies directing it to the previous ProSphere Application, even after you enter the URL for a new ProSphere website.

Note: A browser instance can be reused if the cookies for the appropriate ProSphere website are deleted.

Obtain VMware infrastructure requirements

Obtain the following information that you are required to specify during deployment. Space is provided below to write down these values.

IMPORTANT

Use only a vCenter to connect the vSphere Client to an ESX server. Attempts to deploy directly to an ESX server will fail.

- The IP address or hostname for the vCenter Server managing the VMWare environment. The username and password to connect the vSphere Client to the server.

  VMware Server IP address or hostname: _____

  Username: _____

  Password: _____

- The name for this deployment of ProSphere (for example, *`Local ProSphere deployment`*).

  Name for the ProSphere vApp: _____

- The following infrastructure location for the ProSphere vApp:

  Inventory Location: _____

  Host/Cluster: _____

  Disk format (Thick/Thin):_____

  Resource Pool: _____

- The name of a data store in the local vSphere environment to hold the ProSphere virtual machine images.

  Data store: _____

- The names of the vSphere network(s) in which to deploy each of the three virtual machines for the ProSphere vApp. The virtual machines may be deployed in separate subnets.

  ProSphere network: _____

  Discovery Engine network: _____

  Historical Database network: _____

  Collector network: _____

  Collector network: _____

  Collector network: _____

  Collector network: _____

- The desired secure access and network properties for the Historical Database virtual machine, including:

  DNS servers (separated by commas):

  _____

  Search domain strings (separated by spaces):

  _____

  Hostname: _____

  IP address: _____

  Netmask: _____

  Subnet gateway: _____

- The desired secure access and network properties for the Discovery Engine virtual machine, including:

  DNS servers (separated by commas):

  _____

Search domain strings (separated by spaces):

_____

Hostname: _____

IP address: _____

Netmask: _____

Subnet gateway: _____

- The desired secure access and network properties for the ProSphere Application virtual machine, including:

  DNS servers (separated by commas):

  _____

  Search domain strings (separated by spaces):

  _____

  Hostname: _____

  IP address: _____

  Netmask: _____

  Subnet gateway: _____

4

Configure Hosts

This chapter provides instructions for the installation and configuration of third-party software used to discover hosts and related performance data.

The chapter includes the following sections:

- Avoid underscores in hostnames 26
- DNS registration 26
- Validate HBAs 26
- EMC ProSphere/SCA Host Configuration Utility 28
- Configure Windows hosts and WS-MAN 28
- Configure Windows hosts and WMI 30
- Configure UNIX and Linux hosts 37
- Prepare for discovery of VMware guests 43
- Prepare for discovery of VMware infrastructure 43

Avoid underscores in hostnames

The Internet standards for protocols mandate that hostname labels can contain only the ASCII letters “a” through “z” (in a non-case-sensitive manner), the digits “0” through “9”, and the hyphen (“-”). No other symbols, punctuation characters, or white spaces are permitted.

If ProSphere encounters a host name with an underscore, users can be prevented from logging in.

You can confirm the situation by searching the log files for the following string:

```
IllegalArgumentException: Host cannot be null
```

Characters not allowed in hostnames

Do not include the following characters in hostnames:

- comma (,)
- tilde (~)
- colon (:)
- exclamation point (!)
- at sign (@)
- number sign (#)
- dollar sign ($)
- percent (%)
- caret (^)
- ampersand (&)
- apostrophe (')
- period (.)
- parentheses (())
- braces ({})
- underscore (_)
- white space (blank)

DNS registration

Make sure the hostnames are in DNS format with FQDN, and IP addresses must be registered with the appropriate domain name servers and resolve for a reverse DNS lookup. In hostnames, do not include underscores or characters listed in “Characters not allowed in hostnames” on page 26.

Validate HBAs

All host platforms require the following to discover SNIA-qualified HBA-related information:

- EMC-supported host bus adapter (HBA) drivers and firmware. The HBA driver installed must be SNIA HBA API 2.0 compliant. The *EMC ProSphere Support Matrix* provides specific details.
- The vendor-specific SNIA libraries must be installed on the target host.

Note:
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 ways:
- As part of HBA driver installation package.
- Install latest version of HBAnywhere (for Emulex installations) or SAN Surfer (for Qlogic installation).

To discover an HP-UX host with a multi-port Fibre Channel card, the package CommonIO bundle 0812(Dec 2008) or later should be present on the host to obtain the updated FC-SNIA file set.

To validate that the appropriate SNIA libraries are installed, download and run the inq application from the EMC Online Support Site using the following procedure:

1. From the EMC Online Support Site, click **Search**.
2. In the **Search** field type inq utility.
3. Select the latest version of inq.
4. Select the operating system for your host.
5. Download inq and follow the provided installation instructions.
6. Run the following command on the host after installation:

   ```
   Inq -hba
   ```

   If the command lists the HBAs, then the SNIA libraries are properly installed, which means that ProSphere can discover the HBAs.

EMC ProSphere/SCA Host Configuration Utility

The EMC Host Configuration Utility helps customers verify the settings discussed in this chapter, which enable a Windows host to be successfully discovered in ProSphere or in SCA. Optionally, the utility automatically configures the settings. The utility is available on the EMC Online Support Site (**support.emc.com)**.

Configure Windows hosts and WS-MAN

WS-MAN is the preferred discovery mechanism for Windows 2008 and later.

Note: ProSphere will not copy the INQ binary executable on Windows hosts when discovery is scheduled using the WS-MAN access profile.

This section describes how to configure WS-MAN to work with ProSphere.

Windows Remote Management (WinRM) is the Microsoft implementation of the WS-MAN protocol. Manually perform the following steps to prepare to discover configuration items (CIs) with WinRM. All of the following commands should be run from a Windows Powershell prompt.

To Configure WinRM for use with ProSphere, follow these steps on the host you wish to discover.

1. On Windows Server 2008, run **winrm quickconfig**, to enable a firewall exception for WS-MAN. Enter **y** when prompted.

   In case the command fails, ensure the Windows Remote Management service is running and the Startup Type is set to Automatic. Then run the following commands individually from a Windows Powershell prompt:

   a. **`Get-WmiObject -computer $server Win32_Service -Filter "Name='WinRM'" | Start-Service`**

      In this command, $server refers to the target Windows hostname.

   b. `winrm create winrm/config/listener?Address=*+Transport=HTTP`

   c. `netsh advfirewall firewall add rule name="Windows Remote Management(Http-In)" dir=in action=allow program="System" protocol=TCP localport="5985" profile="Domain,Public,Private" enable=yes`

Note: If you wish to configure WinRM to use HTTPS transport instead, refer to http://support.microsoft.com.

For Windows Server 2003 R2 hosts WinRM is not installed by default, but it is available as the Hardware Management feature through the Add/Remove System Components feature in the Control Panel under Management and Monitoring Tools. Complete installation and information about configuring WinRM using the Winrm command-line tool is available online in the "Hardware Management Introduction"at http://technet.microsoft.com, which describes the WinRM and the IPMI features in Windows Server 2003 R2. If you use Windows 2003 and need to install WinRM on a large number of servers, ask your Windows Administrator for assistance and direct him or her to the "Hardware Management Introduction".

2. Enable authentication on the WinRM service. The authentication scheme can be Basic or Kerberos

   a. Check the current authentication settings with the command:

      winrm get winrm/config/service/auth

   b. Enable the authentication scheme on the WinRM service with the command:

      winrm set winrm/config/service/auth @{<*authentication scheme***>="true"}**

      For example :

      To enable the Basic authentication scheme, execute the command:

      winrm set winrm/config/service/auth '@{Basic="true"}'

      To enable the Kerberos authentication scheme, execute the command:

      winrm set winrm/config/service/auth '@{Kerberos="true"}'

Note: The WinRM service supports Basic authentication only for local accounts and the Kerberos authentication for domain users in addition to users in admin groups.

3. To allow the transfer of unencrypted data on the WinRM service, run the following command:

   winrm set winrm/config/service '@{AllowUnencrypted="true"}'

4. To set the MaxEnvelopeSizekb, so that the WinRM client and server components interact with the WS-Management protocol, run the following command:

   winrm set winrm/config '@{MaxEnvelopeSizekb="1039440"}'

5. For Windows 2003, to gather details on HBA configuration, install the fcinfo file, which can be downloaded from the Microsoft website:

   `http://www.microsoft.com`

Note: You can also automatically and remotely configure the WinRM service required for WS-MAN data collection using Group Policies.

For complete details on configuring WinRM, refer to "Installation and Configuration for Windows Remote Management" at http://msdn.microsoft.com.

For WSMAN discovery through Kerberos, the Key Distributrion Center (KDC) name for user domain must be configured to discover hosts using Kerberos authentication. This can be configured in the following ways:

While deploying ProSphere:

Add the Domain Name Server (DNS) value for KDC to the DNS Server field and the domain name of KDC to the search domain field in the vApp configuration step for the ProSphere Application, Discovery Engine, Historical Database, and all the Collectors while deploying ProSphere.

After deploying ProSphere:

If the DNS value for KDC is not configured while deploying ProSphere, perform the following:

1. Power-down the vApp.
2. Right click on individual VMs and select **Edit Settings**.
3. In **Options > Properties**, add **DNS for KDC** to the **DNS Server** field and the domain name of KDC to the search domain field for Kerberos authentication.
4. Power on the vApp.

   These changes must be performed on all the ProSphere VMs and Collectors.

Note: Ensure that you can correctly resolve the hostname associated with the IP address from ProSphere.

Configure Windows hosts and WMI

ProSphere supports discovery of Windows hosts through Windows Management Instrumentation (WMI).

Note: WS-MAN is the preferred discovery mechanism for Windows 2008 and later.

ProSphere will copy the INQ binary executable on Windows hosts when discovery is scheduled using the WMI access profile.

The following sections describe how to configure WMI to work with ProSphere.

Prerequisites for Windows Server 2003 and Windows Server 2008

The following are prerequisites for Windows host discovery by ProSphere:

- Discovery must be done under the access profile of a user that is an Administrator or a member of the Administrators group. These credentials are entered as WMI credentials in ProSphere. The *EMC ProSphere Administrator Guide* explains how to create access credentials.
- The user account used for discovery must be permitted access to the host to be discovered.
- The user has WMI privileges.
- The user has write privileges to the default Temp directory.

  On Windows 2003, the path for the default Temp directory is:

  `C:\Document and Settings\<user name>\local settings\Temp`

  ProSphere tries to write data to the default Temp directory.

  If this directory does not have write privileges, ProSphere tries to write data to C:\Windows\Temp.

  If the C:\Windows\Temp directory does not have write privileges, ProSphere tries to write data to the user-configured %Temp% directory.

  If the user-configured %Temp% directory does not have write privileges, the operation fails.

  On Windows 2008, the path for the default Temp directory is:

  `C:\Users\<user name>\AppData\Local\Temp`

  ProSphere tries to write data to the default Temp directory.

If this directory does not have write privileges, ProSphere tries to write data to C:\Windows\Temp.

If the C:\Windows\Temp directory does not have write privileges, ProSphere tries to write data to the user-configured %Temp% directory.

If the user-configured %Temp% directory does not have write privileges, the operation fails.

Note: To find the exact location of the %Temp% directory:
Select **Start->Run**
Type **%Temp%**
This opens the directory.

- Ensure that the Visual C++ 2005 SP1 Redistributable Package is installed on the host.

Note: In case the windows update option is enabled and you do not find this package on your system, you can download the package from http://www.microsoft.com/

- Ensure that the WMI and Remote Registry services are running.

Note: To ensure that the services are started:
Select **Start->Run**
Type **services.msc**..
Ensure the **Windows Management Instrumentation** and **Remote Registry** services are started. If they are not, right click on the services and select **Start**.

- Make appropriate registry changes on a Windows Server 2008 R2 host. The section "Make registry changes on a Windows Server 2008 R2 host" on page 37 provides information on the required registry changes.
- For WMI, to allow access to the Root/CIMV2 namespace and all subnamespaces the following permissions must be set:
  - Execute Methods
  - Full Write
  - Partial Write
  - Enable Account
  - Remote Enable
  - Read Security

  The section "Add a user with the necessary WMI permissions" on page 33 provides information on how to set the necessary permissions.
- Microsoft Distributed Object Component Model (DCOM) communication is enabled on the server to be discovered.

  The section "Enable DCOM" on page 33 provides information on how to configure DCOM on port 135.
- The host firewall is properly configured to permit DCOM on port 135.

  The section "Add a firewall exception to open Dynamic RPC ports" on page 34 provides information on how to configure DCOM on port 135.
- ProSphere must be using Windows credentials with remote DCOM permissions and WMI permissions.

Disable UAC on Windows 2008 SP2

1. Open a command prompt and type **msconfig**.
2. Select the tools tab, scroll down select **Disable UAC**, and select **Launch**.
3. Make the desired changes in the dialog box to disable UAC.
4. Confirm the success message.
5. Reboot the host.

Disable UAC on Windows 2008 R2

1. Open a command prompt and type **msconfig**.
2. Select the tools tab, then select **Change UAC Settings**.
3. Select **Launch**.
4. Make the desired changes in the dialog box to disable UAC.
5. Reboot the host.

Add a user with the necessary remote DCOM permissions

To configure a DCOM-enabled user account on a Windows server host:

1. Log on to the server as a local or domain user who has full read/write permissions to the %Temp% directory.
2. Click the Windows **Start** button and then select **Run**.
3. Type **dcomcnfg.**
4. Expand **Component Services** in the **Console Root** tree view, and then expand **Computers**.
5. Right-click **My Computer** from the expanded **Computers** tree view, and then select **Properties**.
6. Click **Default Properties.**
7. Select **Enable Distributed COM on this computer**.
8. Click **COM Security**.
9. Click **Edit Limits** in the **Launch and Activation Permissions** area.
10. Ensure the Administrators group or the username you require is in the list of **Group and user names**.

    In case the Administrators group or the username is not present in the list:

    a. Click **Add**.

    b. Type the Administrator group or username in the **Enter the object names to select field**. The username you add must have full permissions to the %Temp% directory.

    c. Click **OK**.
11. In the **Permissions for Administrators** area, select the **Remote Launch** and **Remote Activation** boxes to provide the user with these permissions and then click **OK**.

12. Click **OK** to close the **My Computer Properties** and **Component Services** dialog boxes.

Enable DCOM

On the host to be discovered, verify that the following registry key value is set to Y:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole ->EnableDCOM
```

Add a user with the necessary WMI permissions

To set WMI privileges for a Windows user account:

1. Log on to the server as a local or domain user.
2. Click the Windows **Start** button and then select **Run**.
3. Type **WMIMGMT.MSC**.
4. Right-click on **WMI Control (Local)** and then select **Properties**.
5. Click the **Security** tab.
6. Select the **Root** > **CIMV2** namespace and then click **Security**.
7. Select the user account or group that has the DCOM permission setting required for discovery, as selected in "Add a user with the necessary remote DCOM permissions" on page 32

   In case the user account or group name is not listed, step 10 on page 32 provides instructions to add the required user account or group.
8. Ensure that all the permissions are enabled in the Permissions for Administrators area.
9. Click **Apply** and then **OK**.
10. Click **OK**.
11. Close the **Windows Management Infrastructure (WMI)** dialog box.

Configure dynamic RPC ports

Note: This procedure is applicable to both Windows Server 2003 and Windows Server 2008 and is required only when the firewall is enabled and all the dynamic RPC ports traffic is blocked in the customer environment.

To configure dynamic RPC ports:

1. Log on to the server as a local or domain user.
2. Click the Windows **Start** button, then select **Run**.
3. Type **regedt32.exe**.
4. Expand the following registry key path:

   ```
   HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc
   ```
5. Create subkeys under Rpc by right-clicking on Rpc and then selecting **New** > **Key**.
6. Set the new key name to **Internet**.
7. Right-click the **Internet** key and select **New** > **Multi-String Value**. Set the new value to **Ports**.
8. Right-click on the **Ports** key and select **Modify**.
9. Type in the dynamic RPC ports as 5000-5100.

10. Right-click the **Internet** key, select **New** > **String Value,** and assign the name **PortsInternetAvailable**.
11. Right-click **PortsInternetAvailable** and select **Modify**.
12. Type the letter **Y** in the **Value Data** field.
13. Right-click the **Internet** key, select **New** > **String Value**, and assign the name **UseInternetPorts**.
14. Right-click **UseInternetPorts** and select **Modify**.
15. Type the letter **Y** in the **Value Data** field.
16. Exit the Registry Editor.
17. Restart the host to activate these dynamic port changes.

Note: In ProSphere, if you configure a single port (for example: port 135) and try to discover hosts, multiple threads from topology and performance data collection collide on that host resulting in discovery errors. Therefore, a range of ports is required for discovery to be successful. It is recommended that you have 100 open ports to support the metrics claimed in *EMC ProSphere Performance and Scalability Guidelines*. If you have more than the typical number of applications on a host, you may need to open more ports.

Add a firewall exception to open Dynamic RPC ports

If a firewall is enabled, you need to add firewall exceptions that opens port 135 and the dynamic RPC ports.

The *EMC ProSphere Security Configuration Guide* lists ports that ProSphere requires to be open and listening, and lists port assignments.

On Windows Server 2008, if you have the default Windows 2008 firewall software then add the the following exception rules to allow the WMI traffic.

Inbound firewall exception rule for dynamic RPC ports

To create an inbound firewall exception rule ProSphere-Dynamic-RPC-ports:

1. Click **Start > Administrative tools > Windows firewall with Advanced Security**.
2. Select **Inbound Rules** in the left hand navigation tree.
3. Right-click **Inbound Rules** and click on **New Rule**.
4. Select **Rule Type** as **Custom** and click **Next**.
5. Select **This program path** in the Program section, and type **%SystemRoot%\System32\dllhost.exe** as a path for dllhost.exe
6. Ensure **Services** is set as **default (all programs and services only)** in the **Program** section, and click **Next.**
7. Select **TCP** for **Protocol Type**, **Dynamic RPC** for **Local Port**, **All Ports** for **Remote Port** in the **Protocol and Ports** section, and click **Next**.
8. Ensure the **Scope** and **Action** properties section is set as **default** and click **Next**.
9. Enable **Domain**, **Private,** and **Public** in **Profile** section, and click **Next**.
10. Set **Name** as **ProSphere-Dynamic-RPC-ports** and click **Finish.**

Note: You can also type the following command at a command prompt to create the above rule:

```
netsh advfirewall firewall add rule name="ProSphere-Dynamic-RPC-ports"
dir=in action=allow program="%SystemRoot%\System32\dllhost.exe"
protocol=TCP localport=RPC profile=public,private,domain
```

Inbound firewall exception rule for port 135

To create an inbound exception rule for the port 135 ProSphere-WMI-DCOM-in:

1. Click **Start > Administrative tools (Control Panel)> Windows firewall with Advanced Security**.
2. Select **Inbound Rules** in the left hand navigation tree.
3. Right-click **Inbound Rules** and click on **New Rule**.
4. Select **Rule Type** as **Custom** and click **Next**.
5. Select **This program path** in the **Program** section, and type **%SystemRoot%\System32\svchost.exe** as a path for svchost.exe
6. Select **Services** by clicking on **Customize** button in the **Program** section.
7. Highlight **Apply to this Service,** select **Remote Procedure Call(RPC)** as the service, click **OK** and click **Next**.
8. Select **TCP** for **Protocol Type**, **RPC Endpoint Mapper** for **Local Port**, **All Ports** for **Remote Port** in the **Protocol and Ports** section, and click **Next**.
9. Ensure the **Scope** and **Action** properties section is set as **default** and click **Next**.
10. Enable **Domain**, **Private,** and **Public** in **Profile** section, and click **Next**.
11. Set **Name** as **ProSphere-WMI-DCOM-in** and click **Finish**.

Note: You can also type the following command at a command prompt to create the above rule:

```
netsh advfirewall firewall add rule name="ProSphere-WMI-DCOM-in"
dir=in action=allow program="%SystemRoot%\System32\svchost.exe"
service=RpcSs protocol=TCP localport=RPC-EPMap
profile=public,private,domain
```

Inbound firewall exception rule to allow asynchronous WMI traffic

To create an inbound firewall exception rule ProSphere-WMI-Async-in:

1. Click **Start > Administrative Tools > Windows Firewall with Advanced Security**.
2. Select **Inbound Rules** in the left hand navigation tree.
3. Right-click **Inbound Rules** and click on **New Rule**.
4. Select **Rule Type** as **Custom** and click **Next**.
5. Select **This program path** in the Program section, and type **%SystemRoot%\System32\unsecapp.exe** as a path for unsecapp.exe
6. Ensure **Services** is set as **default (all programs and services only)** in the **Program** section, and click **Next**.
7. Select **TCP** for **Protocol Type**, **Dynamic RPC** for **Local Port**, **All Ports** for **Remote Port** in the P**rotocol and Ports** section, and click **Next**.
8. Ensure the **Scope** and **Action** properties section is set as **default** and click **Next**.

9. Select **Profile** as appropriate for the network, in the **Profile** section, and click **Next**.
10. Set **Name** as **ProSphere-WMI-Async-in** and click **Finish**.

Note: You can also type the following command at a command prompt to create the above rule: netsh advfirewall firewall add rule name="Prosphere-WMI-Async-in" dir=in action=allow program="%SystemRoot%\System32\wbem\unsecapp.exe" protocol=TCP localport=RPC profile=public,private,domain

Inbound firewall exception rule called Prosphere-WMI-in

To create an inbound firewall exception rule ProSphere-WMI-in:

1. Click **Start > Administrative Tools > Windows Firewall with Advanced Security**.
2. Select **Inbound Rules** in the left hand navigation tree.
3. Right-click **Inbound Rules** and click on **New Rule**.
4. Select **Rule Type** as **Custom** and click **Next**.
5. Select **This program path** in the Program section, and type **%SystemRoot%\System32\svchost.exe** as a path for svchost.exe
6. Select **Services** by clicking on **Customize** button in the **Program** section.
7. Highlight **Apply** to this service, select **Windows Management Instrumentation** as the service, click **OK** and click **Next**.
8. Select **TCP** for **Protocol Type**, **Dynamic RPC** for **Local Port**, and **All Ports** for **Remote Port** in the **Protocol and Ports** section, and click **Next**.
9. Ensure the **Scope** and **Action** properties section is set as **default** and click **Next**.
10. Select **Profile** as appropriate for the network, in the **Profile** section, and click **Next**.
11. Set **Name** as **ProSphere-WMI-in** and click **Finish**.

Note: You can also type the following command at a command prompt to create the above rule: netsh advfirewall firewall add rule name=" Prosphere-WMI-in" dir=in action=allow program="%SystemRoot%\System32\svchost.exe" service=Winmgmt protocol=TCP localport=RPC profile=public,private,domain

For Windows 2003, if you are using a third-party firewall software or windows firewall software, then you need to configure the firewall exceptions to allow the traffic for port 135 and the dynamic RPC ports.

The port 135 must be open to accept the incoming remote connection to the Service Control Manager (SCM), which provides RPC-based services for DCOM. The port allows the client to locate a DCOM service.

Note: This procedure is required only if the port 135 is locked in the customer environment.

To open the DCOM port:

1. Click **Start**, and then click **Control Panel**.
2. Double-click **Windows Firewall**, and then click the **Exceptions** tab.
3. Click **Add Port**.

4. Type **DCOM_TCP135** in the Name field, and **135** in the Port number field.
5. Click **TCP**, and then click **OK**.
6. Click **OK** and close the **Control Panel** window.

Note: You can also type the following command at a command prompt to open a port:
`netsh firewall add portopening protocol=tcp port=135 name=DCOM_TCP135 mode=ENABLE`

Firewall exception rule for dllhost.exe

To create a firewall exception for dllhost.exe:

1. Click **Start > Control Panel > Windows firewall**.
2. Select **Exceptions** tab and click **Add Program**.
3. Click **Browse** and select **dllhost.exe** from the path %SystemRoot%\System32\dllhost.exe.

Note: You can also type the following command at a command prompt to create the above rule:
netsh firewall add allowedprogram program="%systemRoot%\system32\dllhost.exe" name="dllhost.exe" mode=ENABLE

Make registry changes on a Windows Server 2008 R2 host

The following DCOM-related host registry changes are required to discover a Windows Server 2008 R2 host.

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. Choose the **Administrators** group and assign **Full Control**.
4. Click **Advanced**.
5. Click **Owner**, and change the owner to **Administrators** group.
6. Click **Apply** and **OK**.
7. Click **OK** and then exit the **Registry Editor**.

Configure UNIX and Linux hosts

The following sections describe how to configure Linux and UNIX hosts for ProSphere discovery and performance data collection.

Note: ProSphere will copy the INQ binary executable on Unix and Linux hosts when discovery is scheduled using the SSH access profile.

Discovery requirements

For discovery, ProSphere requires user credentials for Secure Shell (SSH) access to UNIX and Linux hosts. The user account used for discovery must be permitted access to the host to be discovered. These credentials are entered as SSH access credentials in ProSphere. The *EMC ProSphere Administrator Guide* explains how to create access credentials. Follow the special instructions later in this section.

Note: Typically a root password is not available to an installer. If a root password is available, you do not need to use sudo and or a private key. When you create SSH access credentials, enter the root password in the **Password** field of the Create Access Credentials dialog box.

Run with root privileges

One important requirement for Linux/UNIX host discovery is the ability for some discovery commands to run as root user. This can be achieved through tools or commands, such as sudo.

Use sudo for host discovery

Linux and UNIX host discovery requires use of the sudo command to elevate the discovery mechanism to root privilege for select commands. The sudo command enables you to:

- Temporarily elevate user credentials to root for specific commands that are configured in the sudoers file.
- Log on to a Linux or UNIX machine as a non-root user.
- Run SCSI commands to discover storage-related information for the host.

The following configuration must be set on the host when using sudo user for host discovery.

- The path of sudo command must be included in environment variable *$PATH* for the sudo user. The variable *$PATH* can be set either in **/etc/environment** or **/etc/default/login** or any other OS specific file.
- The paths of OS commands must be included in environment variable *$PATH* for sudo user. These paths are different for different operating systems.

  Usually, most of the command files are located at the following locations by default:

  `/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin`

  These paths should be included in *$PATH* variable.
- To test whether the path is correctly set, log in as sudo user, and run **which sudo** or **sudo**.
- The sudoers file must be available. By default, it is available in **/etc** or **/opt/sfw/etc/ or /usr/local/etc/sudoers**.
- The sudo user should have root privilege to run the following commands on a given host for resource discovery:
  - `/tmp/nl_dwd/inq`
  - `<path of fcinfo command>/fcinfo`
  - `<path of powermt command>/powermt`
  - `<path of dmidecode command>/dmidecode`

- `<path of sar command>/sar` (for collection of path performance data on AIX and HP-UX hosts)

  See the `Cmnd_Alias` section of Figure 2 on page 40.

Note: To allow a non-privileged ProSphere user to use the sar utility as root user, include the following line in the sudoers file:

```
srm ALL=(ALL) nopasswd: <path of sar command>/sar
```

For example:

```
srm ALL=(ALL) nopasswd: /usr/local/sbin/sar
```

Note: Figure 2 on page 40 provides an example of additional, required sudoers file content. It is recommended that you do not edit the sudoers file with any editor other than visudo. The permissions for a valid sudoers file must be set to 440.

```
login as: cmguser
Password:*****
#sudo
usage: sudo -h | -K | -k | -L | -V
...
#which sudo
/usr/local/bin/sudo
#ls -l /etc/sudoers
-r--r-----   1 root     root         923 Dec 13 05:36 /etc/sudoers

login as: root
Password:*****
#visudo sudoers

# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the sudoers man page for the details on how to write a sudoers file.
#
# Host alias specification
# 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,<path of fcinfo command>/fcinfo, <path of
   sar command>/sar
# Defaults specification
# User privilege specification
   root ALL=(ALL) ALL
   CMGU ALL=NOPASSWD:CMGEMC
# Uncomment to allow people in group wheel to run all commands
# %wheel ALL=(ALL) ALL
# Same thing without a password
# %wheel ALL=(ALL) NOPASSWD: ALL
# Samples
# %users ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
# %users localhost=/sbin/shutdown -h now
#cmguser ALL=(ALL) NOPASSWD: ALL

login as: cmguser
Password:*****
#sudo fcinfo hba-port
HBA Port WWN: 10000000c9702593
…
#ls /tmp/nl_dwd/inq
/tmp/nl_dwd/inq
#sudo /tmp/nl_dwd/inq -mapinfo
```

Figure 2 Sample sudoers file content for Linux/UNIX host discovery

SSH key based authentication

ProSphere uses SSH private/public key based authentication that enables you to discover UNIX hosts with a private key. A public key needs to be present on all the UNIX hosts that are to be discovered using the private key.

You can choose any key generation tool to generate a valid public/private key pair.

These steps describe the procedure to generate a public and private key pair for UNIX hosts using the ssh-keygen tool.

1. For UNIX hosts outside of ProSphere, generate a public and private key pair using the command:

   ```
   ssh-keygen -t rsa -f  <location_of_the_private_key/name_of_
   private_key_file> -N "passphrase"
   ```

   Note: Leave the passphrase blank if you do not choose to encrypt.

   For example: `ssh-keygen -t rsa -f /root/.ssh/id_rsa -N""`

2. Ensure that the public and private key pair that is generated has the following permissions:

   ```
   chmod 600 /root/.ssh/id_rsa
   chmod 644 /root/.ssh/id_rsa.pub
   ```

   Note: The private key file is id_rsa, the public key file is id_rsa.pub.

3. To make the key pair functional, append the public key to `/root/.ssh/authorized_keys` in the target UNIX host using the following command:

   ```
   cat <location_of_the_private_key/name_of_private_key_file> >>
   /root/.ssh/authorized_keys
   ```

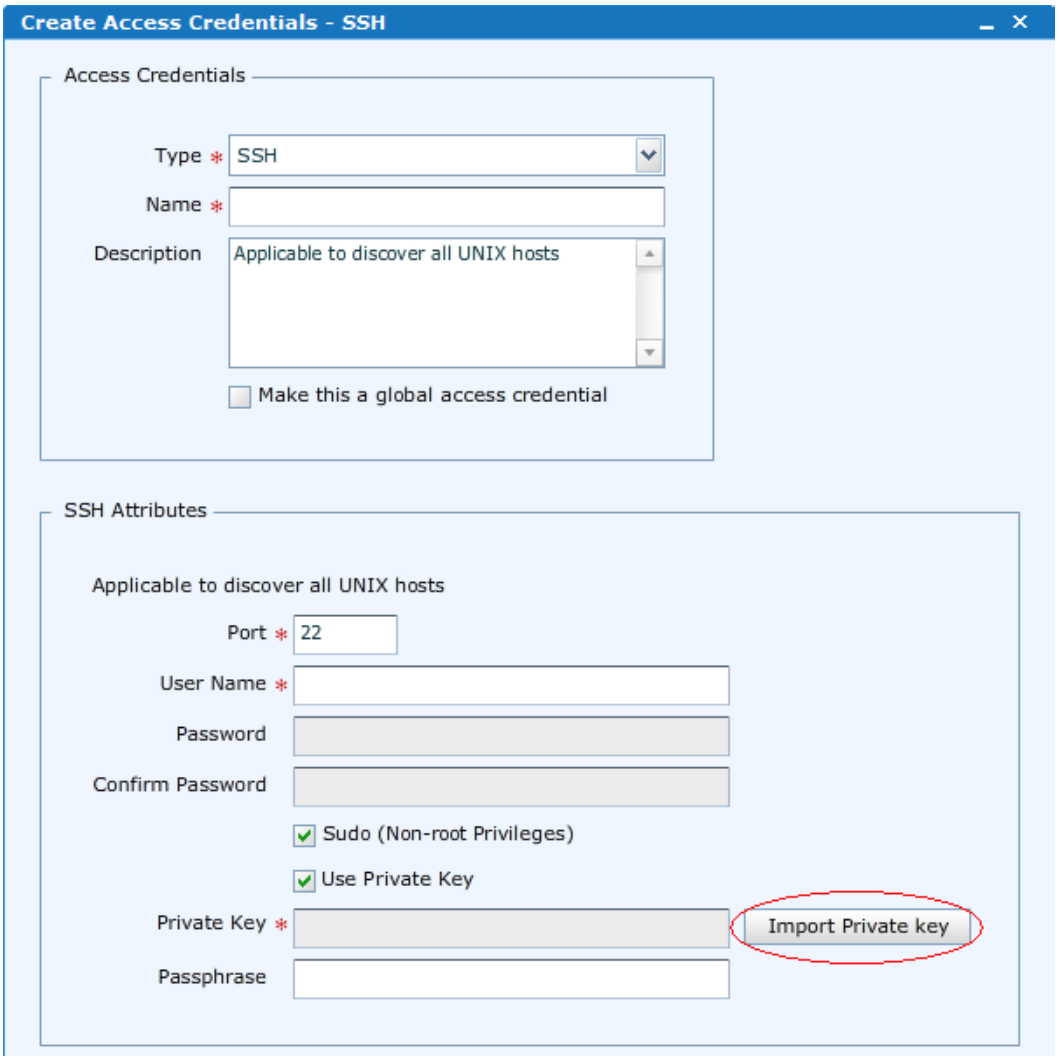
   For example:

   ```
   cat /root/.ssh/id_rsa.pub >> /root/.ssh/authorized_keys
   ```

4. Copy the private key (that is, `/root/.ssh/id_rsa`) to the ProSphere Discovery Engine:

   a. Copy the private key to any location on the machine from which ProSphere is accessed.

b. Create an SSH access credential. Leave the **Password** field blank. Use the **Import Private key** button on the **Create Access Credentials** dialog box to get the key from the machine where ProSphere is accessed and copy the key to the ProSphere Application. The following graphic illustrates the **Import Private key** button.



Collect performance data

For collection of path performance data, specific software (depending on host Operating System) must be running on the host.

- Solaris — iostat
- Linux (RedHat and SuSE) — The iostat package version 5.0.5 must be installed on the Linux host for successful path performance collection. If the package is not installed, path performance collection fails with the error "Failed to discover performance metrics."
- AIX — sar
- HP-UX — sar
- Windows 2000 and later — The Windows Management Instrumentation (WMI) service must be enabled and running.

Consult the relevant manpages and user documentation for installation and configuration instructions for these tools.

Contact your UNIX vendor for information about downloading and installing their iostat (or sar) package.

Prepare for discovery of VMware guests

A VMware guest is the operating system on a virtual machine.

For ProSphere to discover a host where a VMware guest resides (that is, discover a virtual machine rather than a physical host), VMware tools is required. Work with your VMware admin to have VMware tools installed on VMware guests.

If VMware Tools are not installed on a VMware guest, ProSphere cannot discover the virtual machine where the VMWare guest resides.

Prepare for discovery of VMware infrastructure

The virtual infrastructure of VMware environments is discovered by ProSphere from vSphere vCenter using the Virtual Infrastructure (VI) API. This Web Services API is hosted on vCenter servers and can be accessed by ProSphere for resource discovery. For more information about this service interface, refer to the VMware vSphere Web Services Documentation at:

http://www.vmware.com

Discovery requirements

For virtual infrastructure discovery, ProSphere requires:

- Assignment of individual ESX credentials or assignment of VirtualCenter credentials. In either case, Read-only permissions must be included, with the addition of Browse Datastore permissions. These credentials are entered as VMware Infrastructure credentials in ProSphere. The *EMC ProSphere Administrator Guide* provides instructions for creating discovery access credentials.
- Unblocked access to the IP address of the Web Services interface on all VMware ESX and VirtualCenter servers to discover.

5

Configure Arrays

This chapter provides configuration instructions for array data providers used by EMC ProSphere, such as SMI-S providers, to support resource discovery and data collection.

This chapter includes the following sections:

- Configure the EMC SMI-S Provider 46

Configure the EMC SMI-S Provider

The EMC SMI-S Provider provides partners and other product groups with an industry-standard SNIA interface to EMC Arrays, which produces faster solution development. Ultimately, it ensures interoperability and simplified management of customers' SAN environments. EMC SMI-S Provider supports the SNIA Storage Management Initiative (SMI), an ANSI standard for storage management.

The SMI strives to ensure consistent data by providing a unified interface to the many storage objects that must be managed in a storage environment. This enables application developers to focus on a single standard interface for the development of management tools.

The EMC SMI-S Provider has been paired with the EMC Common Object Manager (ECOM) to provide an SMI-compliant interface for EMC Symmetrix® and VNX™/CLARiiON® arrays. ProSphere can collect resource and performance data for EMC Symmetrix, VNX and CLARiiON storage arrays.

Requirements for discovery data collection

To discover supported Symmetrix, VNX, and CLARiiON storage devices and collect resource data from them in ProSphere, the following requirements must be met:

- A host that manages and monitors a Symmetrix array needs six dedicated gatekeepers from each Symmetrix array.
- A supported version of the EMC SMI-S Provider for the array must be installed on a host that has FC connectivity to Symmetrix arrays and IP connectivity to the CLARiiON/VNX arrays

Note: To be discovered, a Symmetrix array must have connectivity to the host where the SMI-S Provider is installed. Only FC connected arrays in a remote replication configuration are discovered in ProSphere, so multiple SMI-S Providers are needed to discover all the arrays. Refer to the SMI-S release notes to determine scalability limitations. Therefore, you should install SMI-S Providers on hosts in such a way that each array has connectivity from at least one SMI-S Provider host.

The EMC SMI-S Provider is available for download from the EMC Online Support site (**support.emc.com**) and may optionally be provided by EMC on CD-ROM. Installation instructions can be downloaded with the software in the *EMC SMI-S Provider Release Notes*.

Note: When installing the EMC SMI-S Provider, EMC Solutions Enabler is also installed. Any previous version of EMC Solutions Enabler will be uninstalled, and the new version of EMC Solutions Enabler will be installed. You may need to install the additional EMC Solutions Enabler daemons that are not included in the basic SMI-S Provider /EMC Solutions Enabler installation.

Note: Only one version of EMC SMI-S Provider and EMC Solutions Enabler can be installed on the same host.

- The EMC SMI-S Provider host must be accessible by ProSphere in the TCP/IP network. The host IP address, access port, username, password, and namespace for the provider must be known to enter these as access credentials in ProSphere.

These credentials are entered as SMI-S credentials. The EMC ProSphere Administrator Guide provides instructions for creating discovery access credentials.

- VNX/CLARiiON SPA IP address or FQDN, VNX/CLARiiON SPB IP address or FQDN, and VNX/CLARiiON username and password must be known.

Requirements for performance data collection

EMC Symmetrix Performance Analyzer (SPA) must be installed to display performance data for the "Array FE Directors - % busy" metric as well as handle Symmetrix Performance Analyzer alerts in ProSphere.

"Integrate ProSphere with SMAS and Unisphere for VMAX" on page 76 provides configuration details.

Configure the provider

The EMC SMI Provider must be configured to access the arrays before ProSphere can discover the arrays. The EMC SMI-S Provider release notes contain instructions for setting up the Provider.

Verify the setup of the EMC SMI-S Provider

- To verify that the EMC SMI-S Provider is correctly set up, use the TestSmiProvider tool that is installed with the Provider on the provider host.
- ProSphere array discovery requires the IP address of the EMC SMI Provider host, SMI Access Credentials that include the EMC SMI Provider user/password (default credentials are user = "admin", password = "#1Password"), SMI provider port #, and SSL Enabled setting.

Note: The EMC SMI Provider user/password is not the same as the array credentials previously mentioned for VNX/CLARiiON.

The connection to the EMC SMI-S Provider can be validated using the Discovery Job status information. Essentially, if arrays are detected then the SMI Access Credentials are correct. If arrays are not detected, then check the Discovery Job status information for errors (usually the provider is either down, the provider user/password is incorrect, the incorrect port was specified, or the SSL enabled setting is incorrect). To sanity check these settings, go to the EMC SMI Provider host, verify that the provider is running, and use the TestSmiProvider application to establish a connection to the Provider using the same information supplied in the access credentials.

- For VMAX/Symmetrix arrays, it is important to keep in mind that ProSphere only supports VMAX/Symmetrix arrays that are fibre-attached to the EMC SMI-S Provider host. This is known as a "local" connection to the provider. VMAX/Symmetrix arrays that are "remote" attached to the EMC SMI-S Provider through other intermediate arrays using RDF connections are excluded from discovery by ProSphere. The TestSmiProvider Display Version ("dv") command will show which Symmetrix and Clariion arrays are connected to the provider and whether they are local or remote.

  For VNX/CLARiiON, this means that the IP addresses for Service Processor A

and Service Processor B, as well as a "username and password of the CLARiiON or VNX array that is of administrator-level privilege with global scope" (quoted from the *EMC SMI-S Provider Release Notes*), must be specified.

- For VNX/CLARiiON that is fibre-connected to the EMC SMI-S Provider host ("local" to provider): the customer must configure the provider for in-band discovery of the VNX/CLARiiON as detailed in the *EMC SMI-S Provider Release Notes*.
- For VNX/CLARiiON that is TCP/IP connected to the EMC SMI-S Provider host ("remote" to provider): the customer must configure the provider for out-of-band discovery of the VNX/CLARiiON as detailed in the *EMC SMI-S Provider Release Notes*.

6

Configure Switches and Fabrics

This chapter provides configuration instructions for Cisco and Brocade switches and fabrics to support resource discovery and data collection in EMC ProSphere.

The chapter includes the following sections:

- Configure Cisco switches 50

Configure Cisco switches

This section applies to homogeneous fabrics that contain one or more Cisco switches.

ProSphere supports two modes of SNMP communications for Cisco switches: the less secure SNMPv1/v2 mode and more secure SNMPv3 mode.

Perform preconfiguration tasks

Before you discover a Cisco switch or a homogeneous Cisco fabric in ProSphere:

1. Ensure all hardware (including switch model) and software is listed as supported in the *EMC ProSphere Support Matrix*.
2. Verify the TCP/IP connectivity to the switches to be discovered. Test by issuing a **ping** command to these switches.

   Determine if SNMP traps are enabled. Log in to the switch and run the **show snmp trap** command, as in the following example:

```
SWDevCisco8-9216i# show snmp trap
```

Trap type		Enabled
entity	: entity_mib_change	Yes
entity	: entity_module_status_change	Yes
entity	: entity_power_status_change	Yes
entity	: entity_module_inserted	Yes
entity	: entity_module_removed	Yes
entity	: entity_unrecognised_module	Yes
entity	: entity_fan_status_change	Yes
entity	: entity_power_out_change	Yes
link	: linkDown	Yes
link	: linkUp	Yes
link	: extended-linkDown	Yes
link	: extended-linkUp	Yes
link	: cieLinkDown	Yes
link	: cieLinkUp	Yes
link	: connUnitPortStatusChange	Yes
link	: fcTrunkIfUpNotify	Yes
link	: fcTrunkIfDownNotify	Yes
link	: delayed-link-state-change	Yes
link	: fcot-inserted	Yes
link	: fcot-removed	Yes
callhome	: event-notify	No

callhome	: smtp-send-fail	No
cfs	: state-change-notif	No
cfs	: merge-failure	No
fcdomain	: dmNewPrincipalSwitchNotify	No
fcdomain	: dmDomainIdNotAssignedNotify	No
fcdomain	: dmFabricChangeNotify	No
rf	: redundancy_framework	Yes
aaa	: server-state-change	No
license	: notify-license-expiry	Yes
license	: notify-no-license-for-feature	Yes
license	: notify-licensefile-missing	Yes
license	: notify-license-expiry-warning	Yes
scsi	: scsi-disc-complete	No
fcns	: reject-reg-req	No
fcns	: local-entry-change	No
fcns	: db-full	No
fcns	: remote-entry-change	No
rscn	: rscnElsRejectReqNotify	No
rscn	: rscnIlsRejectReqNotify	No
rscn	: rscnElsRxRejectReqNotify	No
rscn	: rscnIlsRxRejectReqNotify	No
fcs	: request-reject	No
fcs	: discovery-complete	No
fctrace	: route	No
zone	: request-reject1	No
zone	: merge-success	No
zone	: merge-failure	No
zone	: default-zone-behavior-change	No
zone	: unsupp-mem	No
vni	: virtual-interface-created	No
vni	: virtual-interface-removed	No
vsan	: vsanStatusChange	No
vsan	: vsanPortMembershipChange	No
fspf	: fspfNbrStateChangeNotify	No
upgrade	: UpgradeOpNotifyOnCompletion	Yes

upgrade	: UpgradeJobStatusNotify	Yes
feature-control	: FeatureOpStatusChange	No
vrrp	: cVrrpNotificationNewMaster	No
fdmi	: cfdmiRejectRegNotify	No
snmp	: authentication	No

In this example, many of the traps are not enabled. EMC recommends enabling all traps, unless there is a compelling reason not to do so.

3. Enable SNMP traps. Run the **snmp-server enable traps** command, as in the following example:

```
SWDevCisco8-9216i# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWDevCisco8-9216i (config)# snmp-server enable traps
```

4. Display the traps that are enabled. Run the show snmp trap command. The values in the **Enabled** column should be **Yes**.

EMC recommends that all switches in the Cisco fabric have the same SNMP credentials for use with ProSphere. For example, if the SNMPv1/v2 community setting private is used, all Cisco switches in the fabric should have the SNMPv1/v2 private community name set with a role of network-admin. For an SNMPv3 user, the same SNMPv3 credentials with the role of network-admin should be set on every switch in the fabric.

Note: ProSphere displays the Cisco VSAN fabric as partially discovered if no community string was provided during its configuration.

Cisco switch discovery is initiated by pointing ProSphere discovery dialog to a seed switch. ProSphere discovers all switches in the fabric by obtaining the fabric members from the seed switch. Therefore, all Cisco switches need to have either SNMPv1/2 or SNMPv3 configuration set.

ProSphere discovers all the connected switches in a physical fabric.

ProSphere does not support discovery of Cisco switches over FCIP connections. To discover a Cisco fabric that contains FCIP connections, discover a Cisco switch on either side of the FCIP connection.

ProSphere does not support Cisco device aliases or Cisco enhanced device aliases.

Configure switches for SNMPv1/2

The SNMPv1/2 information you enter when performing discovery is necessary for ProSphere to contact the switch to obtain information. ProSphere collects data from the switch using the same SNMP community name. It uses SNMP port for communication. This is normally hard set to port 161.

1. Refer to the Cisco documentation for detailed information on configuring Cisco switches for SNMPv1/v2 management.
2. The Cisco switches must have an SNMPv1 community name that has read/write privileges set on every switch in the fabric. The SNMP community selected must have a network-admin role.

3. Log in to the switch and log in as an administrator.
4. Use the **snmp-server community** command to configure read-only privileges as shown in the next example:

```
Cisco8-9216i# config terminal

Enter configuration commands, one per line. End with CNTL/Z.

Cisco8-9216i(config)# snmp-server community eccuser ro
```

5. To determine if an SNMPv1 community user exists, log in to the switch and run the command as shown in following example:

```
Cisco8-9216i# show snmp community

Community                                Group / Access

eccuser                                  network-operator
```

6. Set the ProSphere Discovery Engine as the SNMPv1/2 trap destination.

Configure switches for SNMPv3

This section contains guidelines on creating SNMPv3 users for discovery of and management of Cisco switches in ProSphere.

The SNMPv3 information you enter when performing discovery is necessary for ProSphere to contact the switch to obtain information. ProSphere collects data from the switch using SNMPv3 secure credentials. ProSphere supports SNMPv3 only with SHA authentication and AES128 privacy. It uses the SNMP port for communication. The SNMP port is normally hard set to port 161.

Note:
ProSphere supports SNMP users that have SHA authentication and AES128 privacy only.

Refer to the *EMC ProSphere Support Matrix*.

EMC recommends creating the same SNMP v3 users with the same authentication and privacy passwords on all physical switches in the fabric.

The Cisco documentation provides information on creating SNMP v3 users on Cisco MDS switches.

For example, to create an SNMPv3 user called ECCuser with a network-operator role, SHA authorization, and AES128 authentication, do the following:

1. Run the **snmp-server user** command as shown in following example:

```
Cisco8-9216i# config terminal

Enter configuration commands, one per line. End with CNTL/Z.

Cisco8-9216i (config)#snmp-server user ECCuser network-operator
auth sha <SHA-password> priv aes-128 <AES-password>
```

2. Confirm the new user creation by running the **show snmp user** command as shown in the following example:

```
SWDevCisco8-9216i# show snmp user
```

SNMP USERS			
User	Auth	Priv(enforce)	Groups
admin	md5	no	network-admin
ECCuser	sha	aes-128(no)	network-operator

NOTIFICATION TARGET USERS (configured for sending V3 Inform)		
User	Auth	Priv

```
SWDevCisco8-9216i#
```

3. Set the ProSphere Discovery Engine as the SNMPv3 trap destination.

7

Deploy ProSphere

This chapter provides instructions for the deployment of EMC ProSphere. The following sections detail ProSphere deployment:

- Obtain deployment files 56
- Deploy ProSphere 57
- Next steps 61

Obtain deployment files

The deployment files for ProSphere include an .ovf file (small) and its related and co-located .vmdk files (large). Download these files from the EMC Online Support Site (support.emc.com) or another location specified by EMC. Place these files into a single folder in a local file share or URL location that is accessible to the vSphere Client. The vSphere Client downloads these files and transmits them to the ESX or ESXi server.

Note: A checksum error is displayed during deployment, even if one file is missing.The current and complete names of the .ovf and .vmdk files with the build numbers can be obtained from the *EMC ProSphere Release Notes*.

Deployment time

The overall deployment time can be significantly affected by:

- vSphere Client location in the network
- File transfer speeds
- Network performance in the environment

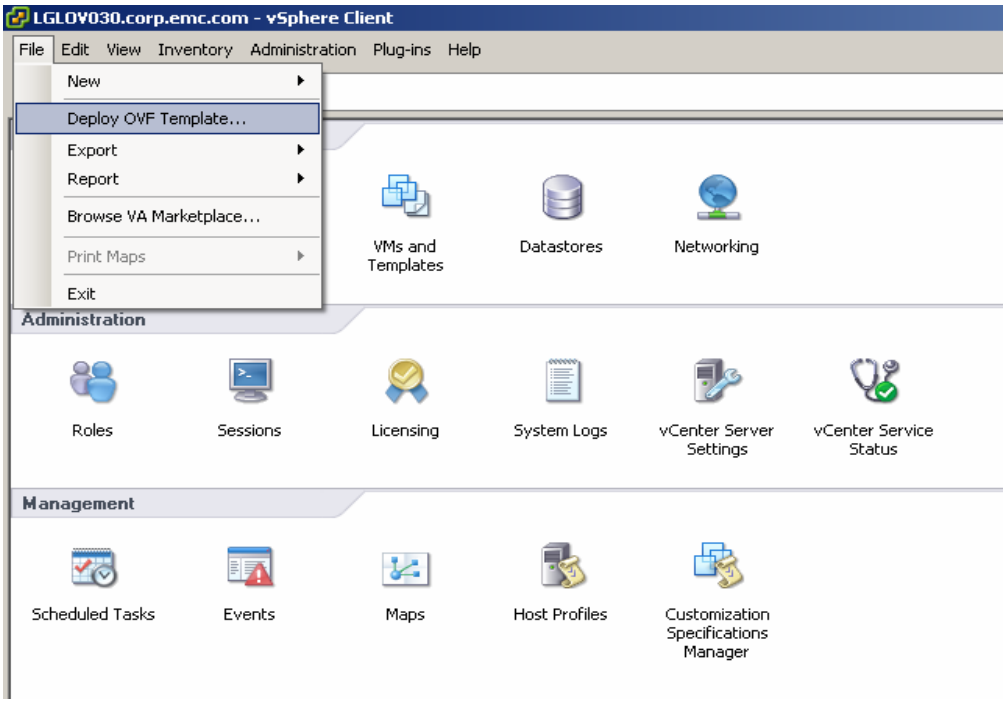
Therefore, EMC recommends that you deploy ProSphere and Collector from within a LAN shared by the VMware environment to save time. A vSphere Client running on a laptop with a small bandwidth virtual private network (VPN), may take several hours to deploy. However, a vSphere Client running in the same, fast local area network (LAN) as the VMware servers may take only a few minutes to deploy.

Deploy ProSphere

Note: Repeat this procedure for each ProSphere instance that you want to deploy.

1. Open the vSphere Client and connect to the vCenter Server managing the VMware environment.
2. Select **File** > **Deploy OVF Template**, as shown in the figure.

Note: Online help is available at each step of the **Deploy OVF Template** dialog box in the vSphere Client. But this help is not specific to ProSphere. Consult your VMware administrator if you are uncertain about any of these steps. For example, you may be uncertain about inventory location to select and so on.



3. In the **Source** step, browse to a file path or type an URL for the .ovf file. Click **Next**.
4. In the **OVF Template Details** step, review the details of the loaded .ovf file. Click **Next**.
5. In the **End User License Agreement** step, review the product license agreement, then click **Accept** followed by **Next**.
6. In the **Name and Location** step, type a unique **Name** (for example, Local ProSphere deployment) and specify an **Inventory Location** in the VMware environment for the ProSphere vApp and its virtual machines. Click **Next**.
7. In the **Host/Cluster** step, select a choice (cluster, host, or both) on which the ProSphere vApp will run. Click **Next**.
8. In the **Resource Pool** step, select a resource pool (associated with the previously selected cluster or host) in which the ProSphere vApp will run. This step is required only if a resource pool has been predefined. Click **Next**.

9. In the **data store** step, select a data store to hold the virtual machine images for ProSphere. If the Thick disk format is selected, the data store should have a minimum 600 GB of space available. Click **Next**.
10. In the **Disk Format** step, for some data stores you are required to select the storage space provisioning method for the virtual machine.

Example options include:

Thin provisioned format (expansion of available storage for the virtual machine on demand) for newer data store file systems.

Thick provisioned format (virtual machine storage is allocated and reserved as a block).

Click **Next**.

11. In the **Network Mapping** step, select a destination network for each of the virtual machines in ProSphere.

    The vSphere Client may display the warning "Multiple source networks are mapped to the host network" if multiple virtual machines are mapped to the same destination network. Ignore this message.

    Note: In the VMware environment, each selected destination network must have an IP Pool associated with it.

    Click **Next**.
12. In the **Properties** step, specify the required configuration fields. The description of property appears in red if the required value is missing or incorrect from the dialog box. The properties to set are the following.

Note: Ensure you specify only the relevant DNS and search domains.

ProSphere Setting	
Timezone setting	Server timezone to set on the Linux virtual machines deployed as part of ProSphere.
ProSphere Application Settings	
ProSphere Application Hostname	Hostname (FQDN) to assign to the ProSphere Application virtual machine (for example, **ProSphere.abc.mycompany.com**)
.ProSphere Application IP Address	IP address to assign to the ProSphere Application virtual machine. This IP address must be registered with the appropriate domain name servers and resolve for a reverse DNS lookup.
ProSphere Application Gateway	Subnet gateway for hosts in the network.
ProSphere Application DNS Servers	Comma-separated list of domain name servers (DNS) available in the network selected for the ProSphere Application and Key Distributrion Center (KDC).
ProSphere Application Netmask	Netmask applied to IP addresses in the network.

ProSphere Application Search Domain(s).	Space-delimited list of domains used in the network selected and the domain name for KDC.
Discovery Engine Settings	
Discovery Engine Hostname	Hostname to assign to the Discovery Engine (for example, **ProSphere-discovery050**).
Discovery Engine IP Address	IP address to assign to the Discovery Engine if a fixed IP address scheme is in use. This IP address must be registered with the appropriate domain name servers and resolve for a reverse DNS lookup.
Discovery Engine Netmask	Netmask applied to IP addresses in the network.
Discovery Engine Gateway	Subnet gateway for hosts in the network.
Discovery Engine DNS Servers	Comma-separated list of domain name servers (DNS) available in the network selected and the DNS for KDC.
Discovery Engine Search Domain(s)	Space-delimited list of domains used in the network selected and the domain name for KDC.
Historical Database Settings	
Historical Database Hostname	Desired network name for the virtual host on which the database will be deployed.
Historical Database IP Address	IP address to be used for access to the database virtual host if a fixed IP address scheme is in use. This IP address must be registered with the appropriate domain name servers and resolve for a reverse DNS lookup.
Historical Database Netmask	Netmask applied to IP addresses in the network.
Historical Database Gateway	Subnet gateway for hosts in the network.
Historical Database DNS Servers	Comma-separated list of domain name servers (DNS) available in the network selected and the DNS for KDC.
Historical Database Search Domain(s)	Space-delimited list of domains used in the network selected and the domain name for KDC.

Click **Next**.

13. In the **Ready to Complete** step, review the list of properties that you specified for ProSphere deployment. If you need to change a value, click **Back** to return to change the previous steps. Click **Finish** to start the deployment. A status bar is displayed in the vSphere Client, showing the deployment progress.

    Wait for the **Deployment Completed Successfully** dialog box to appear.

14. Click **Close** to close the dialog box.

15. In the vSphere Client, navigate to the **Hosts & Clusters** view.

a. Expand the tree in the left panel of this view.

b. Locate the cluster and host that you selected for ProSphere during deployment. You will see three new virtual machines:

   – Historical Database

   – Discovery Engine

   – ProSphere Application under the name of the vApp (for example, **Local ProSphere deployment**).

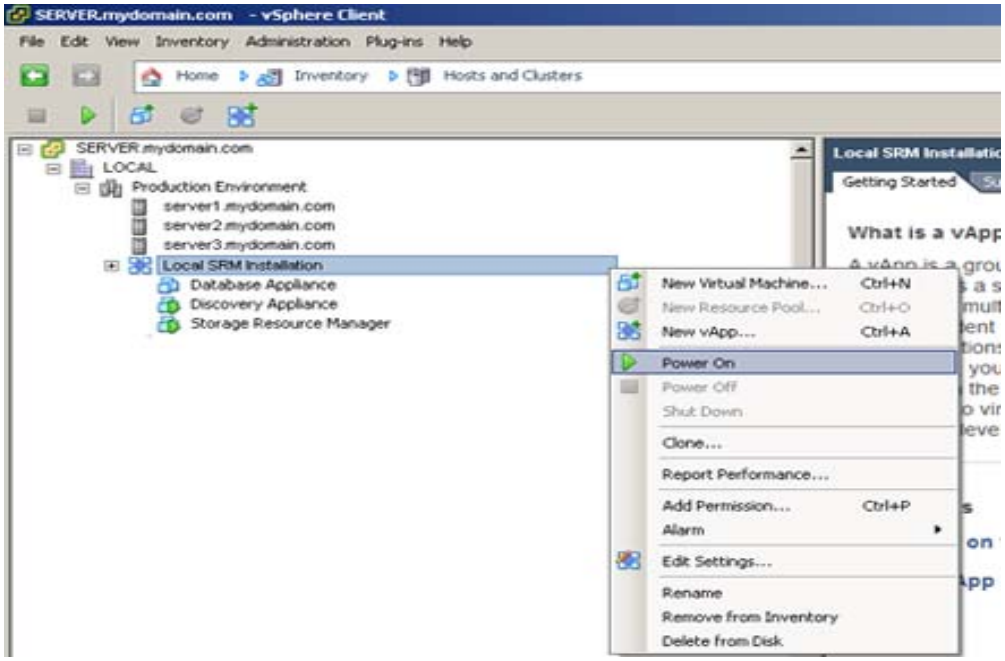
16. Start ProSphere manually after deployment. To start ProSphere in the vSphere Client:

    a. Right-click the vApp name you assigned during deployment (for example, **Local ProSphere deployment**).

    b. Select **Power On**, as shown in the figure. vSphere Client will display the power on status in the **Recent Tasks** bar at the bottom of the client.

    Wait until all virtual machines have started and the **Status** of the **Start vApp** task for the vApp name (for example, **Local ProSphere deployment**) under the **Recent Tasks** view is listed as **Completed** before proceeding.

Note: The first time the database appliance is started, it might take a while to build the required tables and perform other initialization steps.



You are now ready to start using ProSphere through its Web-based Console.

Note: If it is necessary to remove the ProSphere vApp and its dependent virtual machine from your VMware environment, follow the procedures recommended by your organization.

Next steps

Congratulations! You now have deployed ProSphere vApp. You can proceed to these next steps:

1. "Deploy Collectors" on page 63.
2. "Deploy Secondary ProSphere Application" on page 67
3. "Synchronize time zones and system times" on page 74 to verify the deployment works.
4. "Log into ProSphere" on page 74.
5. "Integrate ProSphere with SMAS and Unisphere for VMAX" on page 76.

8

Deploy Collectors

This chapter provides instructions for deploying the ProSphere Discovery Engine Collector (Collector) to scale resource discovery to meet the needs of large data centers. Collectors are VMware virtual machines that must be deployed after initial ProSphere deployment because they coordinate their activities with an existing Discovery Engine.

The following sections provide details:

- Collector 63
- Deploy Collectors 64
- Register a Collector with the ProSphere Application 66

Collector

The Collector allows you to scale ProSphere resource discovery and data collection to the size of your organization's IT environment. Consult the *EMC ProSphere Performance and Scalability Guidelines* to determine the number of Collectors to deploy.

Obtain deployment files

Ensure you downloaded files for the Collector from the EMC Online Support Site or another location specified by EMC mentioned in Table 4 on page 64. Place these files in a location accessible to the vSphere Client, such as a local file share or a URL location.

Determine the Collectors required for data center

Determine the number of Collector virtual machines required to scale ProSphere to your data center size.

Collect information

Before deploying the Collector, contact your VMware Administrator to obtain the information needed for deployment, as presented in Table 4 on page 64.

Table 4 Deployment Fact Sheet

Type	Specifics
IP address or hostname for the vCenter Server managing the VMWare environment	vCenter Server IP address or hostname
Username and password to connect the vSphere Client to the vCenter Server	Username
	Password
Name for this deployment of the Collector (for example, "ProSphere Collector 1")	Name for the Collector
Infrastructure location for the ProSphere Application. This may include a combination of Inventory Location, Host, Cluster, and Resource Pool	Inventory Location
	Host/Cluster
	Disk format (Thick/Thin)
	Resource Pool
Name of a data store in the vSphere environment to hold the Collector images	Data store
Names of the vSphere networks to deploy the Collector	Collector network
Location of downloaded deployment files	Location of OVF file

Deploy Collectors

Note: Repeat this procedure for each Collector that you want to deploy.

1. Open the vSphere Client and connect to the vCenter Server managing the VMware environment.
2. Select **File** > **Deploy OVF Template**.

Note: Online help is available at each step of the **Deploy OVF Template** dialog box in the vSphere Client. But this help is not specific to ProSphere. Consult your VMware administrator if you are uncertain about any of these steps. For example, you may be uncertain about inventory location to select and so on.

3. In the **Source** step, browse to a file path or type a URL for the .ovf file. Click **Next**.
4. In the **OVF Template Details** step, review the details of the loaded .ovf file. Click **Next**.
5. In the **End User License Agreement** step, review the product license agreement and then click **Accept** and followed by **Next**.
6. In the **Name and Location** step, type a unique **Name** (for example, ProSphere Collector 1) and specify an **Inventory Location** in the VMware environment for the Collector. Click **Next**.
7. In the **Host/Cluster** step, select a choice — cluster, host, or both — on which the ProSphere vApp will run. Click **Next**.
8. In the **Resource Pool** step, select a resource pool (associated with the previously selected cluster/host) in which the Collector will run. This step is required only if a resource pool has been predefined. If you select the same **Inventory Location** and **Host/Cluster** as the ProSphere vApp, then select the vApp as the **Resource Pool** for the Collector as well. You can manage the Collector as part of the broader ProSphere vApp. Click **Next**.
9. In the **data store** step, select a data store to hold the virtual machine image for the Collector. The data store should have a minimum 30 GB of space available for a Thick disk format and 2.2 GB for a Thin disk format. Click **Next**.
10. In the **Disk Format** step, for some data stores you are required to select the storage space provisioning method for the virtual machine.

Example options include:

- **Thin provisioned format** (on demand expansion of available storage for the virtual machine) for newer data store file systems
- **Thick provisioned format** (virtual machine storage is allocated and reserved as a block)

Click **Next**.

11. In the **Network Mapping** step, select a destination network for the Collector. Click **Next**.

Note: In the VMware environment, each selected destination network must have an IP Pool associated with it.

12. In the **Properties** step, specify the required configuration fields. The description of a property appears in red if the required value is missing or incorrect from the dialog box.

Note: Ensure you specify only the relevant DNS and search domains.

The properties to set are:

Property Group	Purpose	Property	Description
Collector Information	Configures the vApp	Collector Appliance Hostname	Hostname to assign to the Collector (for example, ProSphere Collector 1)
		Collector Appliance IP Address	IP address to assign to the Collector if a fixed IP address scheme is in use
		Collector Appliance Gateway	Subnet gateway for hosts in the network

Property Group	Purpose	Property	Description
		Collector Appliance Netmask	Netmask applied to IP addresses in the network
		Collector Appliance DNS Server(s)	Comma-separated list of DNS available in the network selected for the ProSphere Application and the DNS for KDC.
		Collector Search Domain(s)	Comma-separated list of domains used in the network selected and the domain name for KDC.
Uncategorized	Configures the Collector	Timezone setting	Server time zone to set on the virtual machines deployed as part of ProSphere

Click **Next**.

13. In the **Ready to Complete** step, review the list of properties that you specified for deployment. If you need to change a value, click **Back** to return to the previous steps and change a listed value. Click **Finish** to start the deployment. A status bar is displayed in the vSphere Client, showing the deployment progress.

    Wait for the **Deployment Completed Successfully** dialog box to appear.

14. Click **Close** to close the dialog box.

15. In the vSphere Client, navigate to the **Hosts & Clusters** view.

    a. Expand the tree in the left panel of this view.

    b. Locate the cluster and host that you selected for Collector during deployment.

Register a Collector with the ProSphere Application

You can deploy additional Collectors as required. After deploying a Collector, register it with the ProSphere Application that manages it.

To register a Collector with the ProSphere Application:

1. Type the Collector URI **https://<*collector_name*>/appliance_registration.html** in the web browser window.
2. Type the ProSphere Application hostname.
3. Type the Security Administrator credentials.
4. Click **Submit**.

   After a successful registration of the Collector with the ProSphere Application, a confirmation dialog appears.

Note: "Deploy Collectors" on page 64 provides information on deploying additional Collectors.

Load balance Collectors

The primary Discovery Engine automatically load balances the discovery requests across all available Collectors. You do not have to specify which Collector to use for each discovery job.

9

Deploy Secondary ProSphere Application

This chapter provides instructions for deploying a Secondary ProSphere Application. In rare cases ProSphere collects an extremely large amount of performance data, which might degrade the overall ProSphere performance. To meet such needs, you can add a Secondary ProSphere Application at any time after deploying ProSphere.

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

The following sections provide details:

- Secondary ProSphere Application 68
- Deploy a Secondary ProSphere Application 70
- Register a Secondary ProSphere Application 71

Secondary ProSphere Application

A Secondary ProSphere Application receives a share of data routed to the ProSphere Application. This results in an increased CPU availability and enhances ProSphere performance.

Note: A Secondary ProSphere Application does not have a functional user interface.

Limitation

During the deployment of a Secondary ProSphere Application, when performance data collection is shifted from the ProSphere Application to the Secondary ProSphere Application, most likely a data point will be dropped for any metric that is calculated using a counter/delta. This includes most metrics.

The reason is that for metrics calculated with a counter/delta, the calculation cannot occur without two collected data points. The intermediate JSON/XML data files collected on the ProSphere Application are not migrated to the Secondary ProSphere Application, so the Secondary ProSphere Application does not have the previous data locally available for calculation. By design, the Secondary ProSphere Application will not produce a data point for the interval directly after the migration. This omission is observable in the pdc-server log file. Subsequent data collection, calculation, and display should be normal, because it occurs after a second interval has passed and another set of metrics is collected for calculation against a previous set.

This observed behavior (missing data point) should not apply to metrics like Unix Host CPU %Busy that are reported directly without doing counter/delta calculations. For these metrics, the previous data is not used for calculations, and the next data point should appear as scheduled.

Obtain deployment files

Ensure you downloaded files for the Secondary ProSphere Application from the EMC Online Support Site or another location specified by EMC mentioned in Table 5 on page 69. Place these files in a location accessible to the vSphere Client, such as a local file share or a URL location.

Collect information

Before deploying a Secondary ProSphere Application, contact your VMware Administrator to obtain the information needed for deployment, as presented in Table 5 on page 69.

Table 5 Deployment Fact Sheet

Type	Specifics
IP address or hostname for the vCenter Server managing the VMWare environment	vCenter Server IP address or hostname
Username and password to connect the vSphere Client to the vCenter Server	Username
	Password
Name for this deployment of the ProSphere Application (for example, “ProSphere Application 2”)	Name for the ProSphere Application
Infrastructure location for the ProSphere Application. This may include a combination of Inventory Location, Host, Cluster, and Resource Pool	Inventory Location
	Host/Cluster
	Disk format (Thick/Thin)
	Resource Pool
Name of a data store in the vSphere environment to hold the Secondary ProSphere Application images	Data store
Names of the vSphere networks to deploy the Secondary ProSphere Application	Secondary ProSphere Application network
Desired secure access and network properties for the Secondary ProSphere Application virtual machine	DNS servers (separated by commas)
	Search domain strings (separated by spaces)
	Hostname
	IP address
	Netmask
	Subnet gateway
Location of downloaded deployment files	Location of OVF file

Deploy a Secondary ProSphere Application

1. Open the vSphere Client and connect to the vCenter Server managing the VMware environment.
2. Select **File** > **Deploy OVF Template**.

Note: Online help is available at each step of the **Deploy OVF Template** dialog box in the vSphere Client. But this help is not specific to ProSphere. Consult your VMware administrator if you are uncertain about any of these steps. For example, you may be uncertain about inventory location to select and so on.

3. In the **Source** step, browse to a file path or type a URL for the .ovf file. Click **Next**.
4. In the **OVF Template Details** step, review the details of the loaded .ovf file. Click **Next**.
5. In the **End User License Agreement** step, review the product license agreement and then click **Accept** and followed by **Next**.
6. In the **Name and Location** step, type a unique **Name** (for example, ProSphere Application 1) and specify an **Inventory Location** in the VMware environment for the Secondary ProSphere Application. Click **Next**.
7. In the **Host/Cluster** step, select a choice — cluster, host, or both — on which the ProSphere vApp will run. Click **Next**.
8. In the Resource Pool step, select a resource pool (associated with the previously selected cluster/host) in which the Secondary ProSphere Application will run. This step is required only if a resource pool has been predefined. Click **Next**.

Note: The Secondary ProSphere Application is deployed external to the ProSphere vApp (not in the same vApp as the ProSphere Application) . You cannot manage the Secondary ProSphere Application as part of the ProSphere vApp.

9. In the **data store** step, select a data store to hold the virtual machine image for the Secondary ProSphere Application. The data store should have a minimum of 230 GB space available. Click **Next**.
10. In the **Disk Format** step, for some data stores you are required to select the storage space provisioning method for the virtual machine.

Example options include:

- **Thin provisioned format** (on demand expansion of available storage for the virtual machine) for newer data store file systems
- **Thick provisioned format** (virtual machine storage is allocated and reserved as a block)

Click **Next**.

11. In the **Network Mapping** step, select a destination network for the Secondary ProSphere Application. Click **Next**.

Note: In the VMware environment, each selected destination network must have an IP Pool associated with it.

12. In the **Properties** step, specify the required configuration fields. The description of a property appears in red if the required value is missing or incorrect from the dialog box.

Note: Ensure you specify only the relevant DNS and search domains.

The properties to set are:

Property Group	Purpose	Property	Description
Secondary ProSphere Application Information	Configures the vApp	Secondary ProSphere Application Hostname	Hostname to assign to the Secondary ProSphere Application (for example, ProSphere Application 1)
		Secondary ProSphere Application IP Address	IP address to assign to the Secondary ProSphere Application if a fixed IP address scheme is in use
		Secondary ProSphere Application Gateway	Subnet gateway for hosts in the network
		Secondary ProSphere Application Netmask	Netmask applied to IP addresses in the network
		Secondary ProSphere Application DNS Server(s)	Comma-separated list of DNS available in the network selected for the Secondary ProSphere Application and the DNS for KDC.
		Secondary ProSphere Application Search Domain(s)	Comma-separated list of domains used in the network selected and the domain name for KDC.
Uncategorized	Configures the Secondary ProSphere Application	Timezone setting	Server time zone to set on the virtual machines deployed as part of ProSphere

Click **Next**.

13. In the **Ready to Complete** step, review the list of properties that you specified for deployment. If you need to change a value, click **Back** to return to the previous steps and change a listed value. Click **Finish** to start the deployment. A status bar is displayed in the vSphere Client, showing the deployment progress.

    Wait for the **Deployment Completed Successfully** dialog box to appear.

14. Click **Close** to close the dialog box.

15. In the vSphere Client, navigate to the **Hosts & Clusters** view.

    a. Expand the tree in the left panel of this view.

    b. Locate the cluster and host that you selected for the Secondary ProSphere Application during deployment.

Register a Secondary ProSphere Application

After deploying a Secondary ProSphere Application, register it with the ProSphere Application that manages it.

To register a Secondary ProSphere Application:

1. Type the Secondary ProSphere Application URI **https://<*secondary_prosphere_application_name*>/appliance_registration.html** in the web browser window.
2. Type the hostname of the managing ProSphere Application.
3. Type the Security Administrator credentials.
4. Click **Submit**.

After a successful registration of the Secondary ProSphere Application with the ProSphere Application, a confirmation dialog appears.

10 Post-Deployment Tasks

This chapter provides instructions to follow after the deployment of ProSphere. The following sections detail ProSphere post-deployment steps:

- Synchronize time zones and system times 74
- Log into ProSphere 74
- Integrate ProSphere with SMAS and Unisphere for VMAX 76
- Configure CMCNE 88
- Synchronize ProSphere deployments 93
- Deploy trusted certificates 93
- Additional information 93

Synchronize time zones and system times

After deploying ProSphere, so that SPA and Brocade path performance data collection and alert consolidation will occur as expected, ensure the following:

- Time zone and system times of ProSphere and the host running BNA or CMCNE are synchronized
- System times of ProSphere and the hosts running SPA are synchronized

Log into ProSphere

1. Open a Web browser and browse to the ProSphere Application by specifying the URL address (using the IP address or hostname) of the virtual machine where the ProSphere Application was deployed.

   Note: Ensure you enable Transport Layer Security (TLS) 1.0 in Web browser security settings.

   Note: The Web browser security settings to open ProSphere must be enabled for TLS 1.0. SSL v2 or v3 security settings are no longer supported by ProSphere.

2. Accept any security-related dialog box that may appear in the browser asking you to accept a security certificate from EMC (or allow a security exception for ProSphere) and continue.

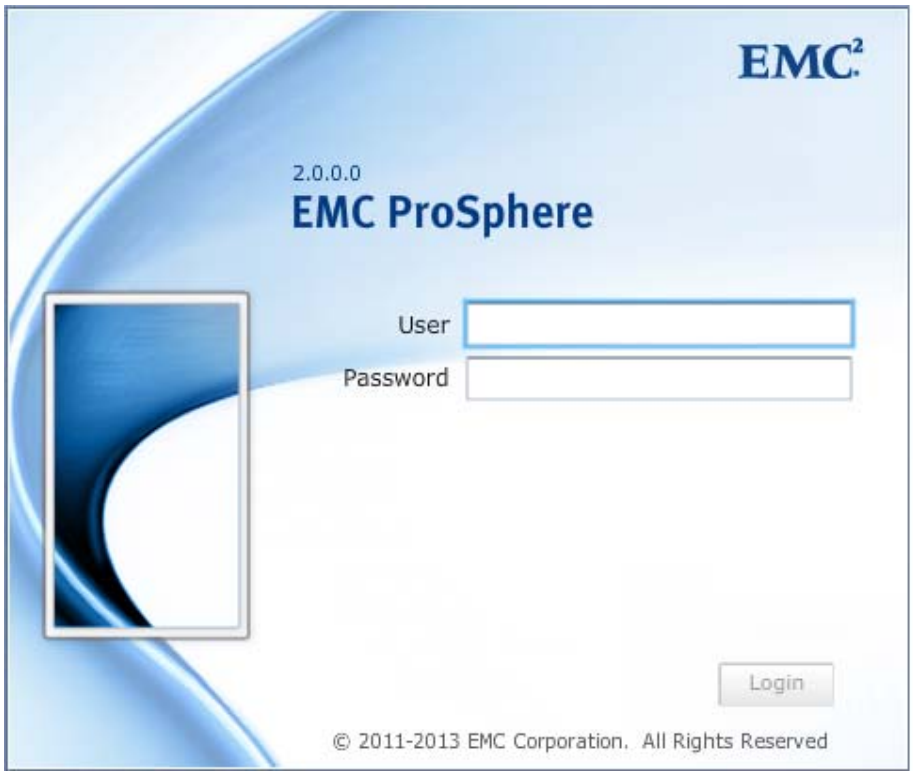
   Note: The procedure to accept the certificate varies between browsers and even between different versions of the same browsers. To prevent the dialog box from appearing at login, import the certificate from the host you have established.

3. Type the default username and password for ProSphere at the login screen (shown in the figure):

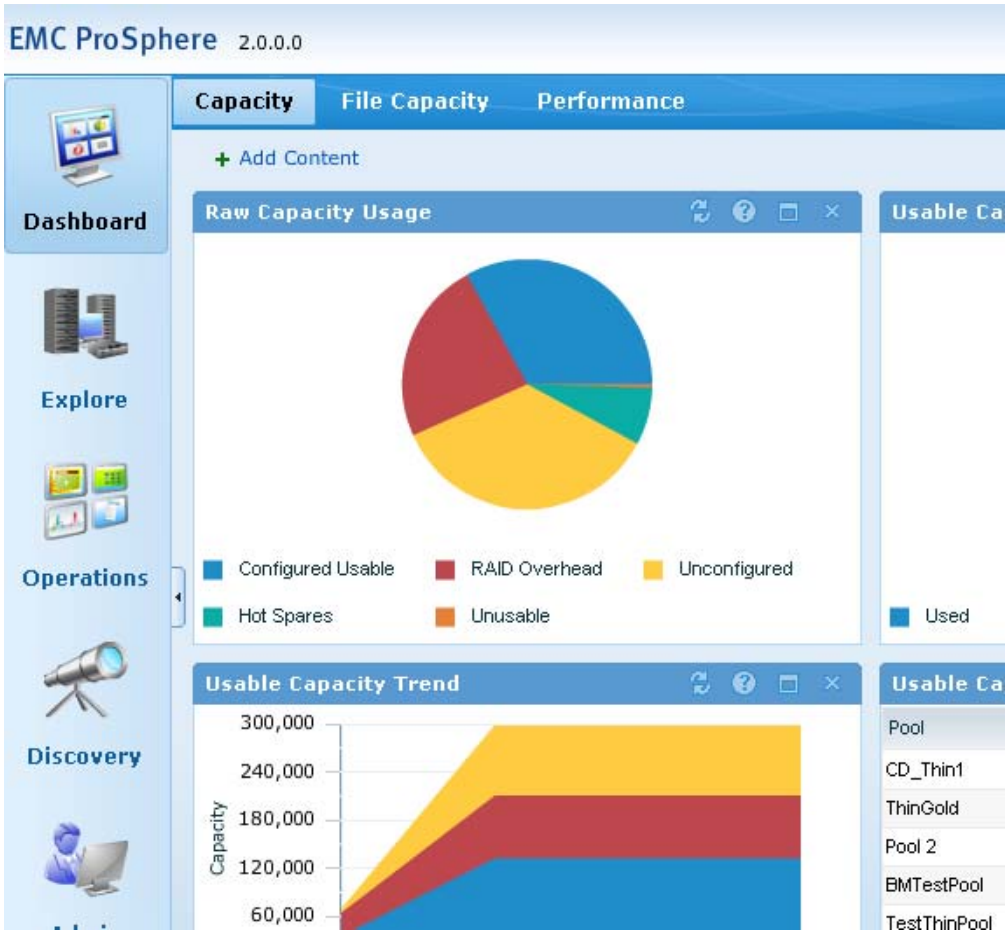
   `appadmin` in the **User** field

   `Changeme1!` in the **Password** field

   Note: The username, **appadmin**, and the password, **Changeme1!**, are predefined and assigned the roles Security Administrator, System Administrator, and User. You should change the password for this account immediately after the first login.



4. Click **Login**. The ProSphere Console is loaded and appears in the browser as shown in the figure.



Note: Be aware that after the credentials are accepted and before the ProSphere Console is visible, a quick health check is done and the user is warned about problems that might interfere with normal operation. This includes but is not limited to problems such as the ProSphere Application being unable to locate a Discovery Engine over the network.

Integrate ProSphere with SMAS and Unisphere for VMAX

Note: The *EMC ProSphere Support Matrix* provides the minimum version requirements for Symmetrix Performance Analyzer (SPA) and the Symmetrix Management Console (SMC). For requirements for installing SMAS, refer to SMAS documentation.

Note: Unisphere for VMAX is a new element manager for the VMAX arrays. Symmetrix Management Solution (SMAS) can still be used to manage many Symmetrix arrays. Please refer to SMC, SPA, and Unisphere for VMAX release notes for specific configuration support and usage.

The following are prerequisites for successful SMAS-ProSphere launch-in-context integration.

- Preferably, only one SMAS instance manages each Symmetrix array. If more than one SMAS instance manages a Symmetrix array, all instances must meet the minimum version requirement and must be the same version.
- You must have existing, supported versions of SMC and SPA in the data center on a host that can be accessed through HTTP(S) by the ProSphere virtual machines. Ensure that no firewalls block their direct communication. The *EMC Symmetrix Management Console and EMC Symmetrix Performance Analyzer Installation Guide* provides installation instructions. Installation of SPA is independent of ProSphere installation.

Note: SMC can be on a neutral host or on the service processor. SPA is installed only on neutral hosts. SMC and SPA are not installed on ProSphere virtual machines.

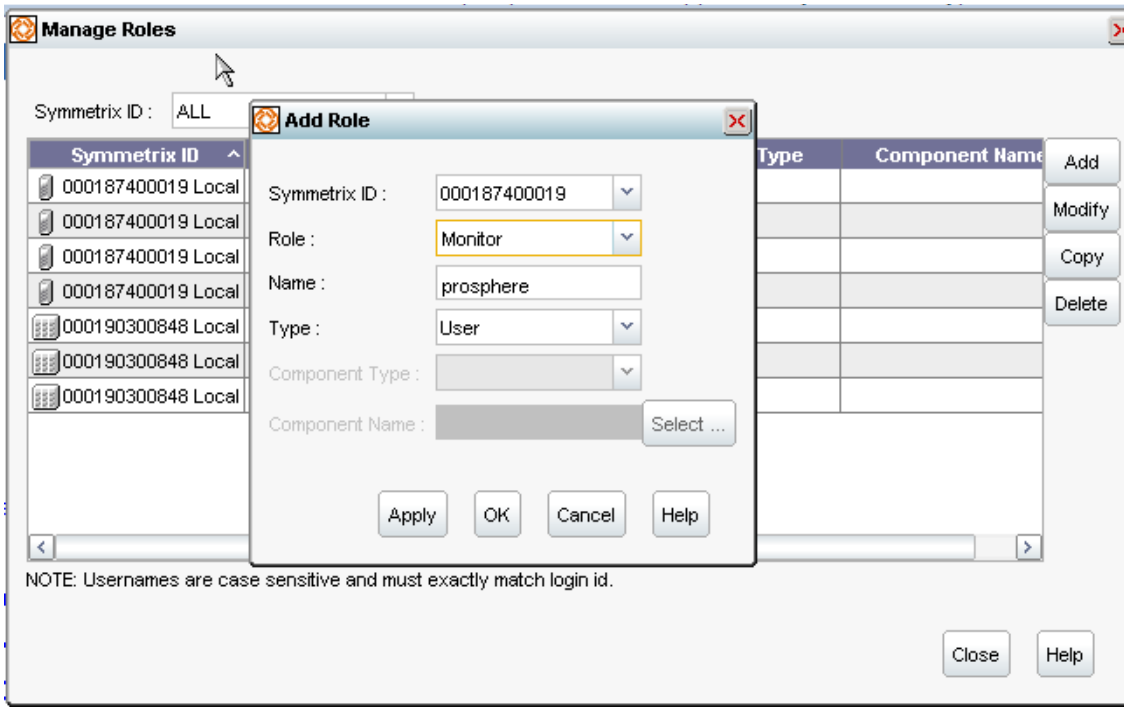
- SMC and SPA can reside on the same host. In this case, SMC and SPA together require 8 GB of RAM. Allow for additional memory required by the EMC SMI-S Providers installed on the host.
- The SPA installation must already be configured to manage the Symmetrix resources in a data center. The *EMC Symmetrix Management Console and EMC Symmetrix Performance Analyzer Installation Guide* provides configuration instructions.

Integrate ProSphere with SMAS

Perform the following steps to configure SMC and SPA:

1. Log in to **SMC** with an Administator account.
2. On each array that is managed by SMC, create an account named **prosphere**. This is required for performance data collection and alerts collection.
   a. Launch SMC and navigate to **Tasks > Manage Roles**.

b. Click **Add** and create a new user named **prosphere** for each applicable Symmetrix array. Assign the **User** type and the **Monitor** role. The **Manage**



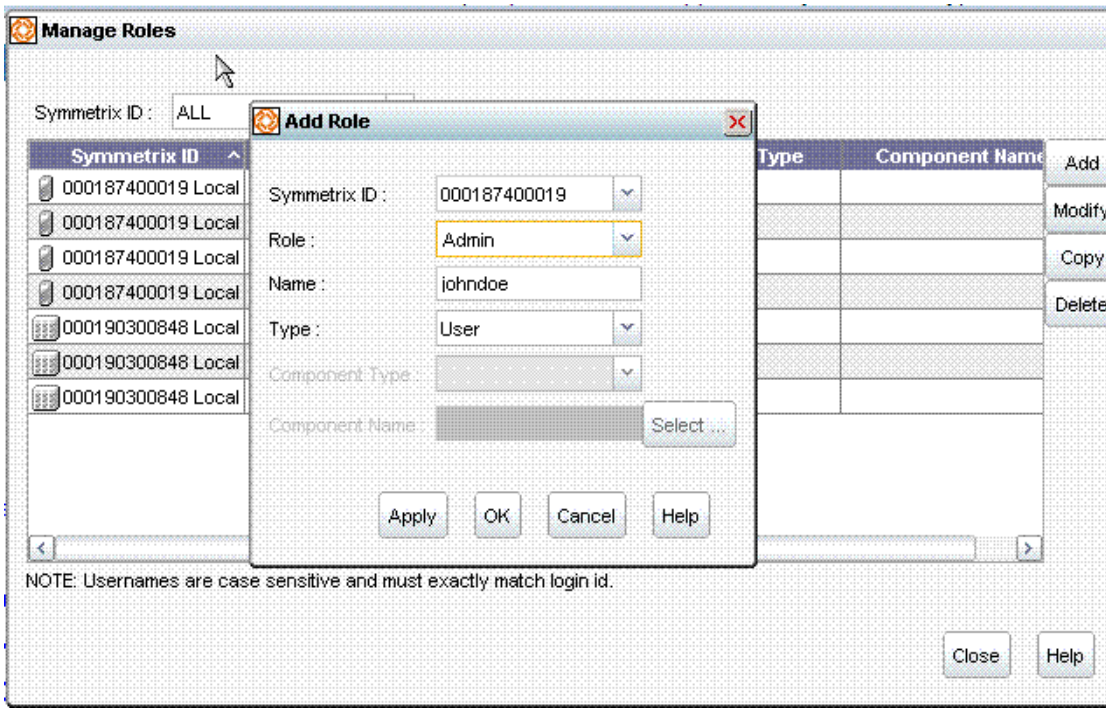
Roles dialog box displays the account name **prosphere** for each array.

3. In SMC, authorize each ProSphere user who will launch SMC/SPA and assign the role **Admin** or **Monitor** (which has fewer permissions) on each array where the user will launch SMC/SPA. This authorizes the user to launch SMC on the array specified.

   The username assigned in SMC must match the username that the user will have in ProSphere.

   For example, if John Doe will be an authorized ProSphere user who will launch SMC from ProSphere, in SMC assign the **Admin** role to the user at the **Add Role**

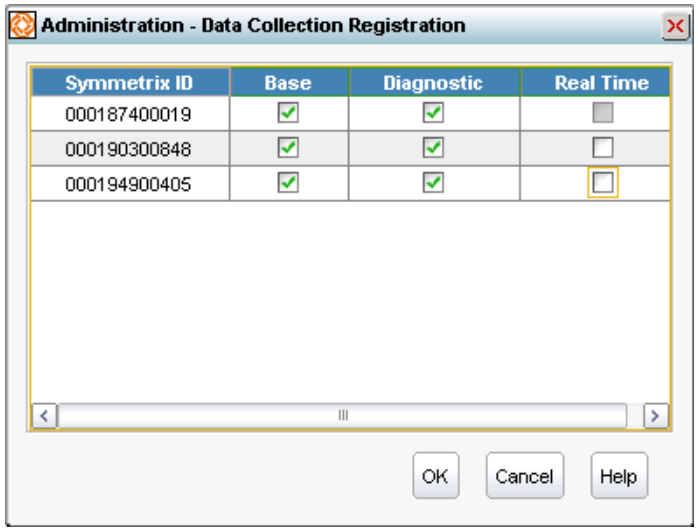
dialog box, on each array where John Doe will launch SMC.



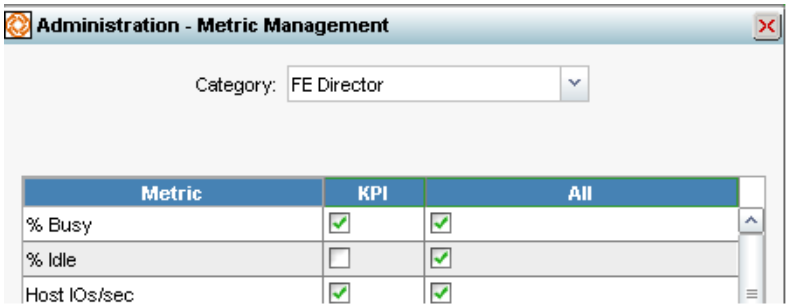
Any user account that will be created in ProSphere and used to launch SMC in context must also exist in SMC.

Note: The appadmin account exists by default in ProSphere. You can create an appadmin user account in SMC in order to use the ProSphere appadmin account to launch SMC in context fromProSphere. For the password of the appadmin account, refer to the *EMC ProSphere Security Configuration Guide*.

4. To collect **Array FE Directors - % Busy** data for a Symmetrix array, select the **Base** and **Diagnostic** collections for the array in the **Administration -> Data Collection Registration** dialog box of SPA.

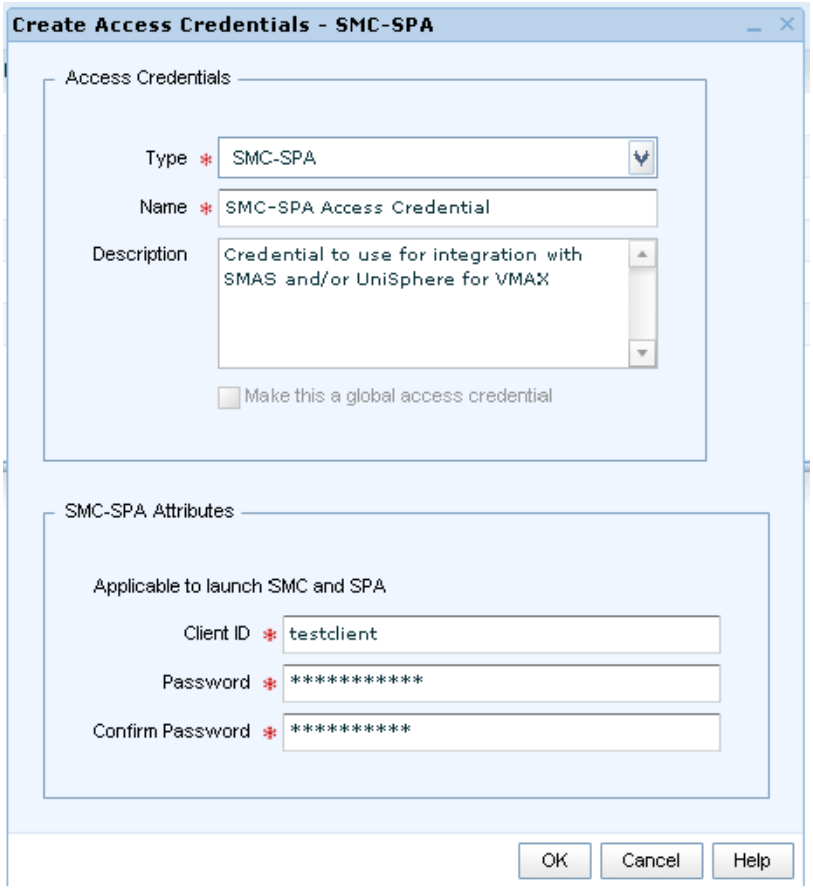


5. In addition, for the **Array FE Directors - % Busy** metric chart, select **FE Director" -> "% Busy** in the **Administration - Metric Management** dialog box. This metric is enabled by default as part of the SPA installation.



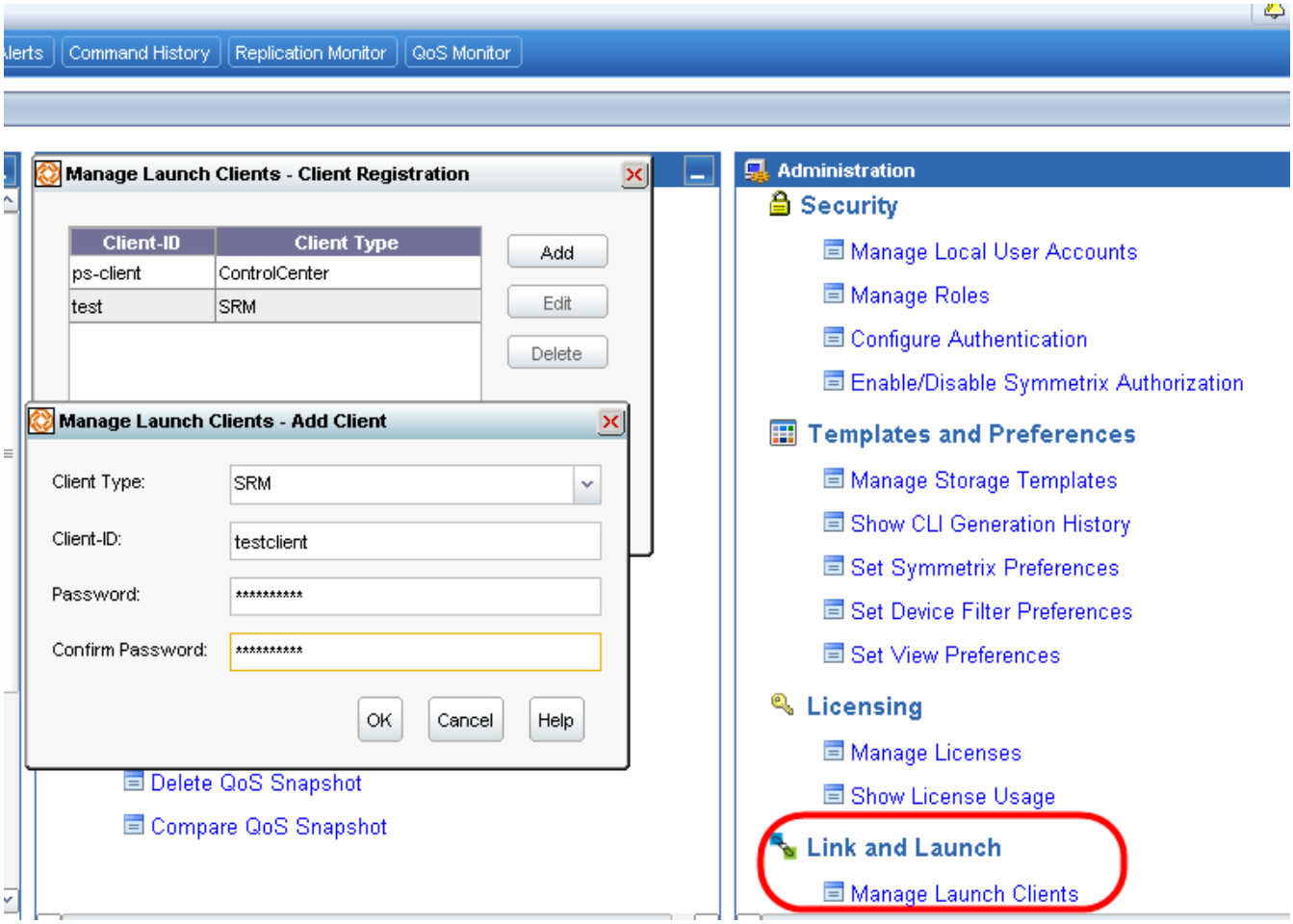
6. Create an access credential with the type **SMC-SPA** in ProSphere with **Discovery > Access Credentials > Create Access Credential.**

Note: Only one access credential with the type SMC-SPA can exist in a single deployment of ProSphere. If SMC/SPA is installed on more than one array in a deployment, use the same SMC-SPA access credential (with the same client id) for all instances of SMC/SPA in the deployment. If you have more than one deployment, assign a unique client id to the SMC-SPA access credential in each deployment.



Note: After you create an SMC - SPA access credential in a ProSphere deployment, the option of creating another will not be available in the drop-down list of the Create Access Credentials dialog box in the that deployment.

7. In each deployment, register a launch client in all SMC instances in the deployment.
   a. Go to the **Tasks** view in SMC.
   b. In **Administration**, go to **Manage Launch Clients > Link and Launch**.
   c. In the **Manage Launch Clients - Client Registration** window, click **Add**.



   d. In the **Manage Launch Clients - Add Client** window, specify **SRM** as client type, specify a client id and password, confirm the password, and select **Save**.

      All information in the SMC-SPA access credential created in ProSphere (username and password) must match the client information entered in SMC.

   e. Restart SMAS.

Note: Whenever you add a client in SMC, you must restart SMAS. If you do not, authentication fails.

8. From the Discovery view of ProSphere, re-run the discovery jobs that discovered the Symmetrix arrays. This validates the SMC-SPA access credentials for all SMC/SPA URLs discovered for the arrays.

   Both Performance Data Collection and Alerts Collection Status log message windows display appropriate error messages.

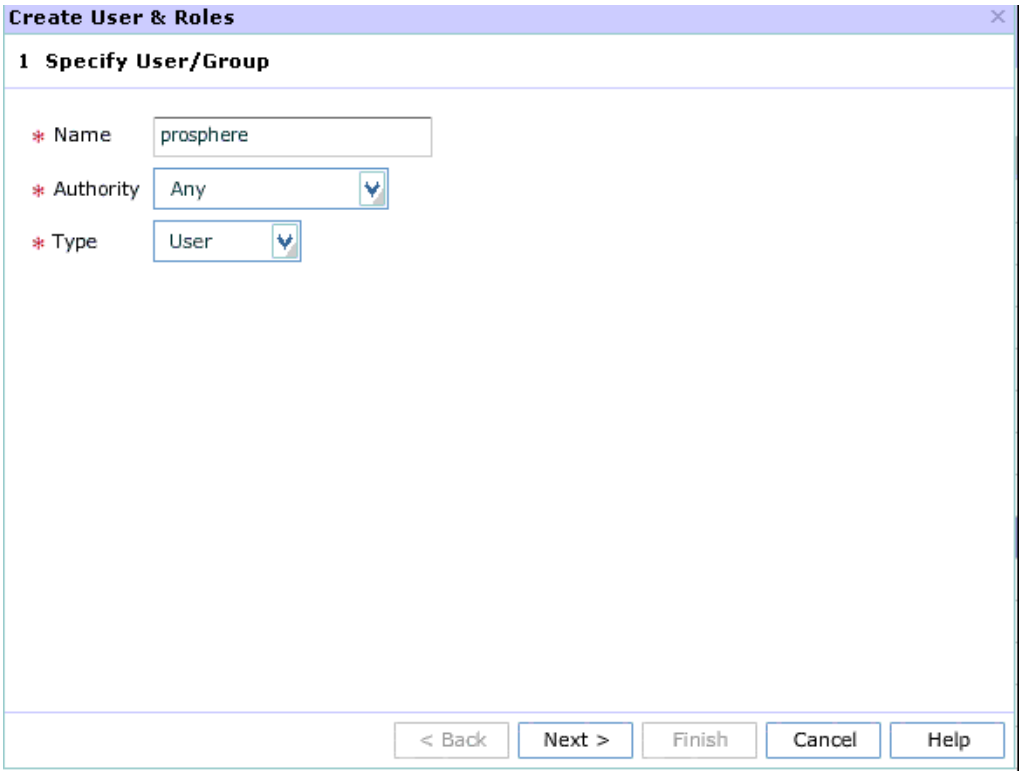
Note: When you re-run the discovery jobs, do not change any information including access credential. The discovery job uses the SMC-SPA access credential that is available in the system for performance detection.

Integrate ProSphere with Unisphere for VMAX

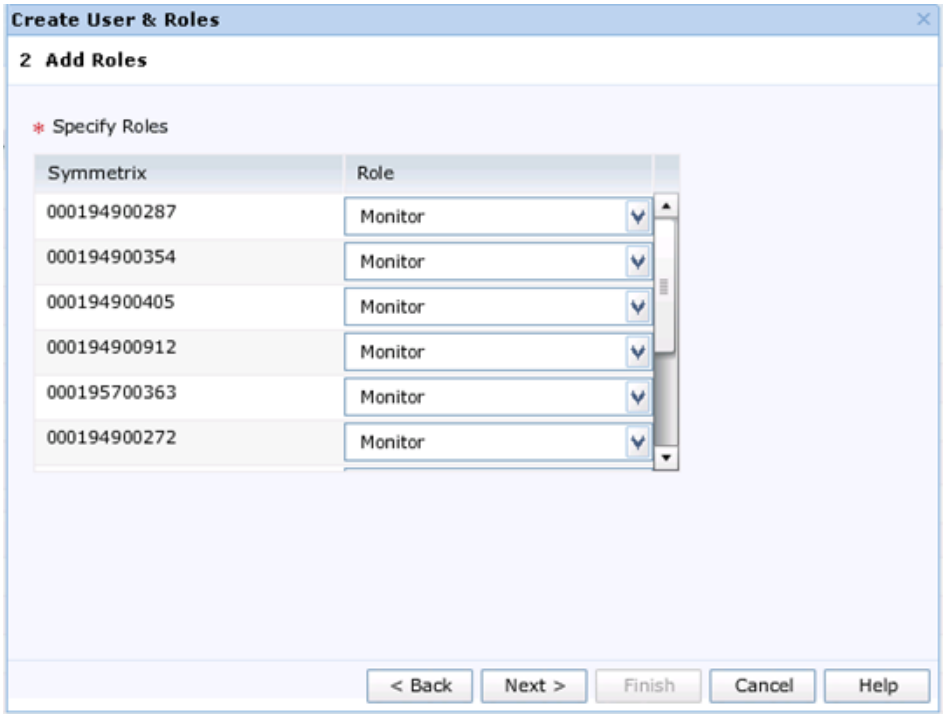
Perform the following steps to configure Unisphere for VMAX:

1. Log in to Unisphere for VMAX with an Administator account.
2. On each array that is managed by Unisphere for VMAX, create an account named **prosphere**. This is required for performance data collection and alerts collection.
   a. Navigate to **Administration**.
   b. Select **Users and Roles**.
   c. Click **Create**.

d. Create a new user named **prosphere** for each applicable Symmetrix array. Assign the type **User** and the role **Monitor**. The following example shows user input on the first authorization screen:

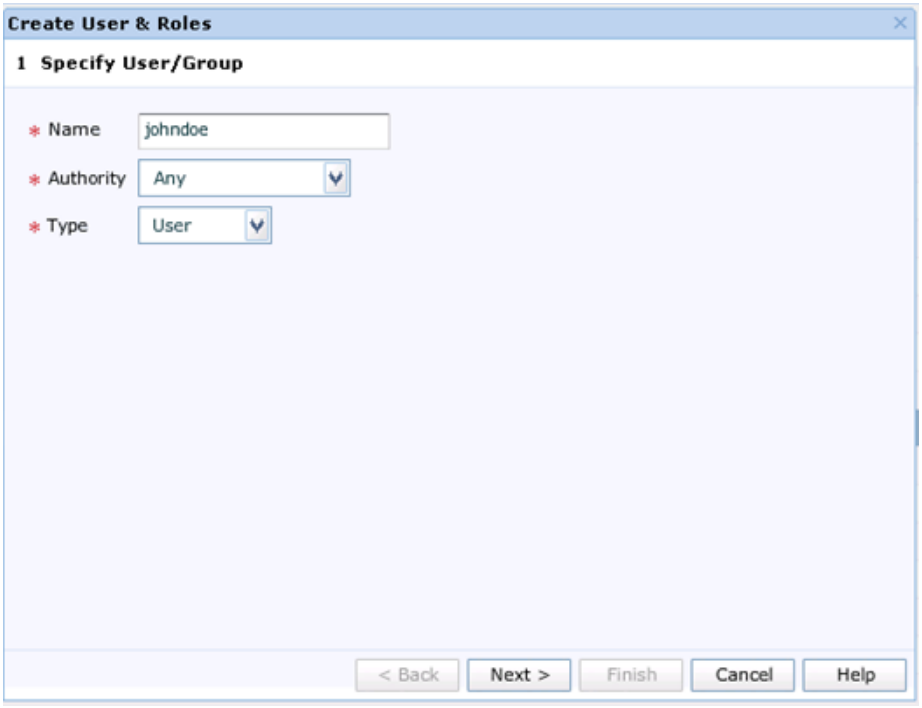


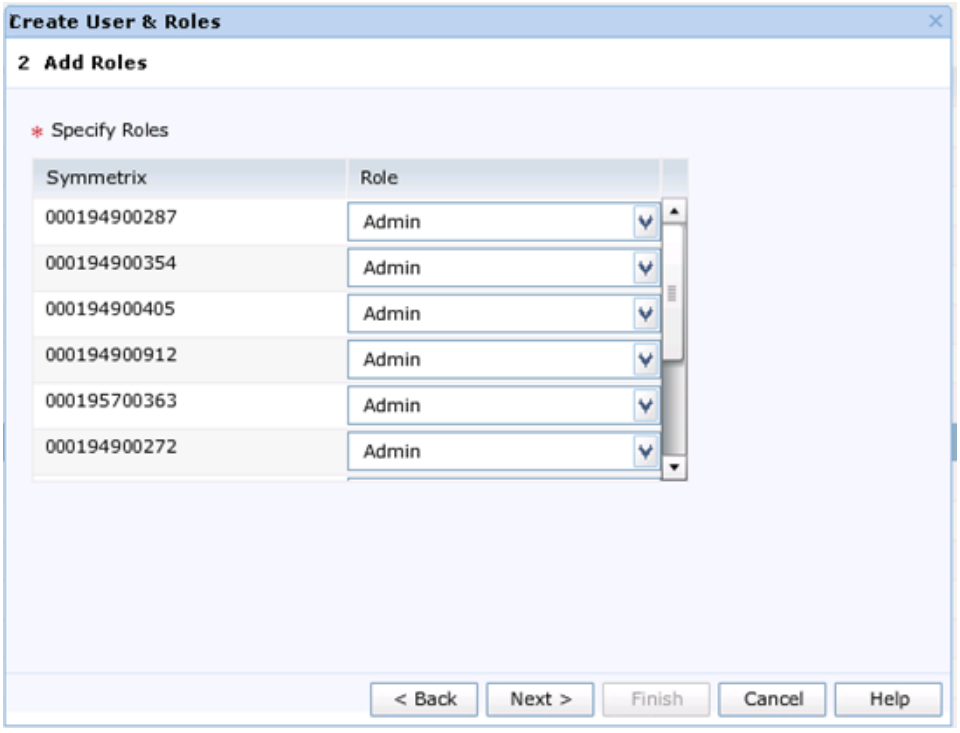
The following example shows user input on the second authorization screen.



e. Click **Next**. After reviewing your changes, click **Finish**.

3. In Unisphere for VMAX, authorize each ProSphere user who will launch SMC/SPA and assign the role **Admin** or **Monitor** (which has fewer permissions) on each array where the user will launch SMC/SPA. This authorizes the user to launch SMC on the array specified. For example, if John Doe will be an authorized ProSphere user who will launch SMC from ProSphere, in Unisphere for VMAX assign the **Admin** role to the user at the **Create User & Roles** dialog, on each array where John Doe will launch SMC.



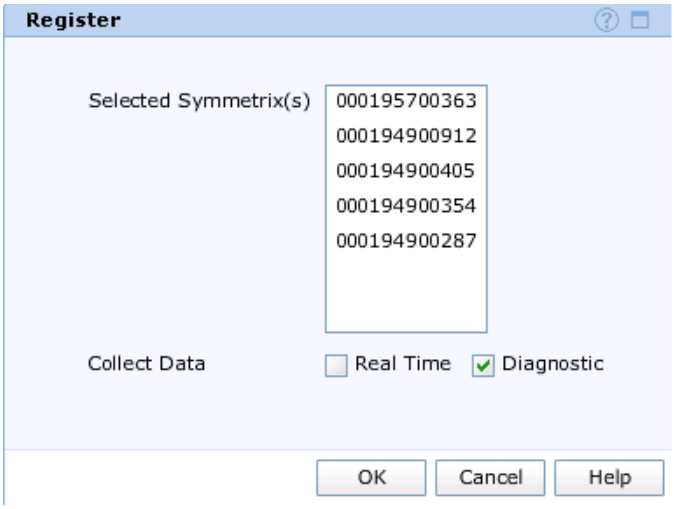


Any user account that will be created in ProSphere and used to launch SMC in

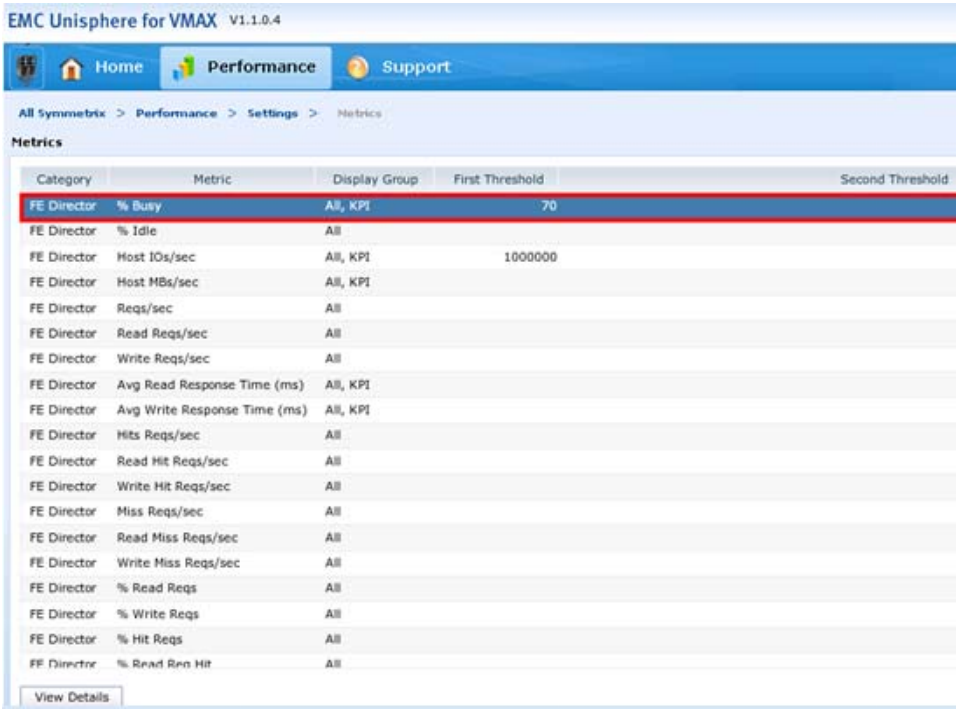
context must also exist in SMC.

Note: The appadmin account exists by default in ProSphere. You can create an appadmin user in Unisphere for VMAX in order to use the ProSphere appadmin account to launch SMC in context from ProSphere.

4. To collect **Array FE Directors - % Busy** data for a Symmetrix array, you must register it for Performance data (assuming that Unisphere for VMAX was installed with the Performance Analytics option). To do this, navigate to **Performance > Settings.**
5. Navigate to **System Registrations**.
6. Select one or more Symmetrix arrays and click **Register**. Select the **Diagnostic** collection. The **System Registrations** screen displays the array with a green indicator icon in the Diagnostic checkbox.

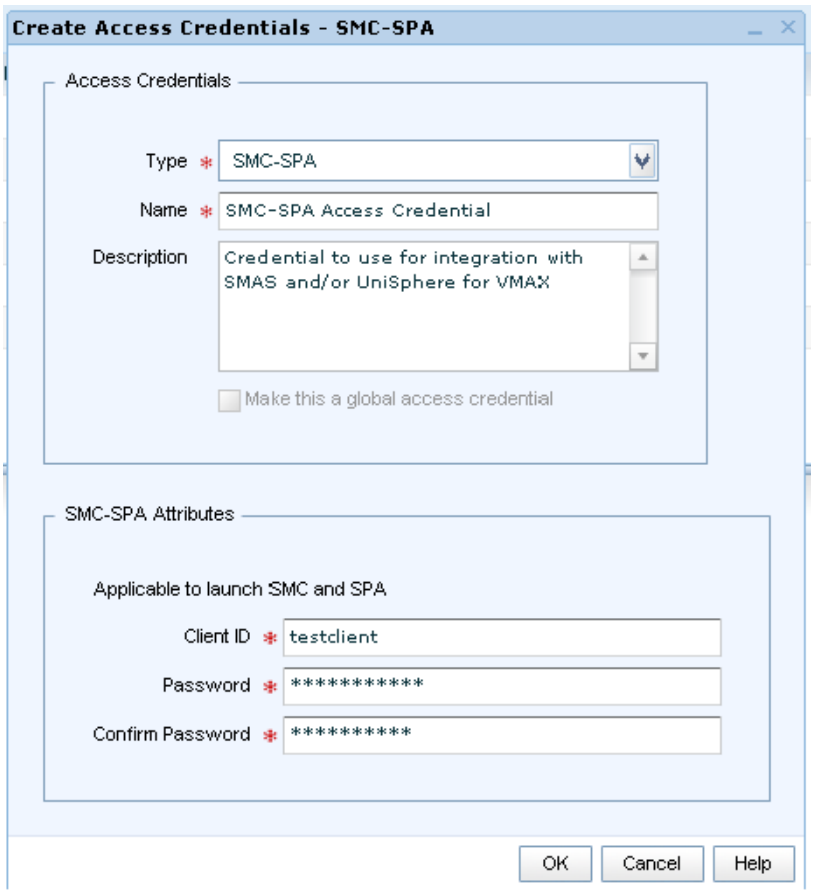


7. In addition, for the **Array FE Directors - % Busy** metric chart, ensure the metric **FE Director - % Busy** is enabled (it should be by default). To verify, navigate to **Performance > Settings > Metrics**. Click the filter button and select **FE Director**.



8. Create an access credential with the type **SMC-SPA** in ProSphere with **Discovery > Access Credentials > Create Access Credential**.

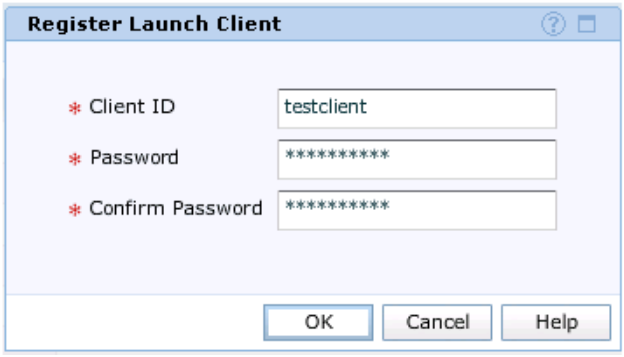
Note: Only one access credential with the type SMC-SPA can exist in a single deployment of ProSphere. If Unisphere for VMAX is installed on more than one array in a deployment, use the same SMC-SPA access credential (with the same client id) for all instances of Unisphere for VMAX in the deployment. If you have more than one ProSphere deployment, assign a unique client id to the SMC-SPA access credential in each deployment.



Note: After you create an SMC-SPA access credential in a ProSphere deployment, the option of creating another will not be available in the drop-down list of the **Create Access Credentials** dialog box in that deployment.

9. Register a launch client in all Unisphere for VMAX instances in the deployment.
   a. Navigate to **Administration > Link and Launch.**
   b. Click **Create**.

c. Enter the alphanumeric client ID and a password. All information in the SMC-SPA access credential created in ProSphere (username and password) must match the client information entered in Unisphere for VMAX.



d. Restart Unisphere for VMAX.

Note: Whenever you add a client in Unisphere for VMAX, you must restart it. If you do not, authentication fails.

10. From the **Discovery** view of ProSphere, re-run the discovery jobs that discovered the Symmetrix arrays. This validates the SMC-SPA access credentials for all SMC/SPA URLs discovered for the arrays. Both **Performance Data Collection** and **Alerts Collection Status** log message windows display appropriate error messages.

Note: When you re-run the discovery jobs, you do not need to change any information including access credential. The discovery job uses the SMC-SPA access credential that is available in the system for performance detection.

Configure CMCNE

This section applies to homogenous and mixed fabrics that contain one or more Brocade FC managed by the Connectrix Manager Converged Network Edition (CMCNE).

CMCNE

CMCNE is a unified network management solution for data, storage, application delivery, wireless, and converged networks. It provides a single interface for Brocade Fibre Channel SANs, IP networks, wireless networks, and Multiprotocol Label Switching (MPLS) networks — providing end-to-end visibility across different network types through a seamless and unified user experience.

Note: CMCNE will discover and report back on Brocade EOS switches.

In order to integrate ProSphere functions with Brocade products, you require licensed versions of one of the following: (1) BNA (2) CMCNE (Professional Plus or Enterprise Edition). The trial versions of BNA or CMCNE (Professional Plus or Enterprise Edition) can be used only for 75 days. The release notes for BNA, and the release notes for CMCNE provide detailed information on the product licensing.

You can install CMCNE with an option of either an integrated SMI Agent (SAN with SMI Agent) or just the SMI Agent only (headless installation).

Table 6 on page 89 lists the features of ProSphere supported by various versions of CMCNE or BNA.

Table 6 ProSphere features supported by CMCNE/BNA

CMCNE/BNA License type	Topology discoveries	Performance Data Collection	Alert Collection	Launch-in-Context
Headless Installation (SMI Agent only)	Yes	Yes	Yes	No
Valid Trial License	Yes	Yes	Yes	Yes
Fully Licensed	Yes	Yes	Yes	Yes

Location of the keytool utility on CMCNE or BNA hosts

The keytoolutil.bat file does not exist on CMCNE or BNA hosts. The actual file is called keytool.exe. It exists by default on CMCNE hosts at:

```
<drive>:\Program Files\CMDCE 11.2.1\jre\bin
```

On BNA hosts, the file is located at:

```
<drive>:\Program Files (x86)\Network Advisor 11.2.0\jre\bin
```

When you execute the keytool.exe.file, use the default admin password for BNA, or CMCNE, as appropriate. The following example shows how to execute the keytool.exe file on BNA:

```
D:\Program Files (x86)\Network Advisor 11.2.0\jre\bin>keytool
-importcert -v -file d:\serverCertificate.crt -alias prosphere
Enter keystore password: <default admin password>
Re-enter new password:<default admin password>
Owner: CN=aownlmsspro01.ecc.mssmgt.com
Issuer: CN=aownlmsspro01.ecc.mssmgt.com
Serial number: afddf19db0f238bb
Valid from: Thu Jun 21 13:35:51 CEST 2012 until: Tue Jun 20
13:35:51 CEST 2017
Certificate fingerprints:
         MD5:  28:EB:09:3E:DE:2C:E7:68:A4:0B:F3:56:78:80:DB:33
         SHA1:
F1:57:FF:71:77:F3:16:72:97:BA:B0:A4:DF:FD:D5:17:3B:A3:10:8A
         Signature algorithm name: SHA1withRSA
         Version: 3
```

Extensions:

```
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
```

```
KeyIdentifier [
0000: 98 79 6C 28 4B 2E 64 11   C3 A5 30 CA 91 6F 4E FB
.yl(K.d...0..oN.
0010: 85 EF 02 89                                        ....
]
]

#2: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 98 79 6C 28 4B 2E 64 11   C3 A5 30 CA 91 6F 4E FB
.yl(K.d...0..oN.
0010: 85 EF 02 89                                        ....
]

[CN=aownlmsspro01.ecc.mssmgt.com]
SerialNumber: [    afddf19d b0f238bb]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
[Storing C:\Users\nl06328\.keystore]
```

Perform configuration tasks

Perform the following steps before attempting to Launch In-Context from ProSphere to Brocade:

1. Import ProSphere Server Certificate

   Download the ProSphere Server certificate (apache certificate) from ProSphere's Export Certificate link under Admin area on the ProSphere Console and import it into the CMCNE Server. Use the keytoolutil.bat file located under <CMCNE_HOME>/bin to import the certificate. Section "Location of the keytool utility on CMCNE or BNA hosts" on page 89 explains how to access the keytool utility on CMCNE or BNA hosts.

   The alias name used can be the server shortname.

   ```
   keytoolutil.bat import path-to-server.cert-file <alias-name>
   ```

   Restart the CMCNE service after importing the server certificate.

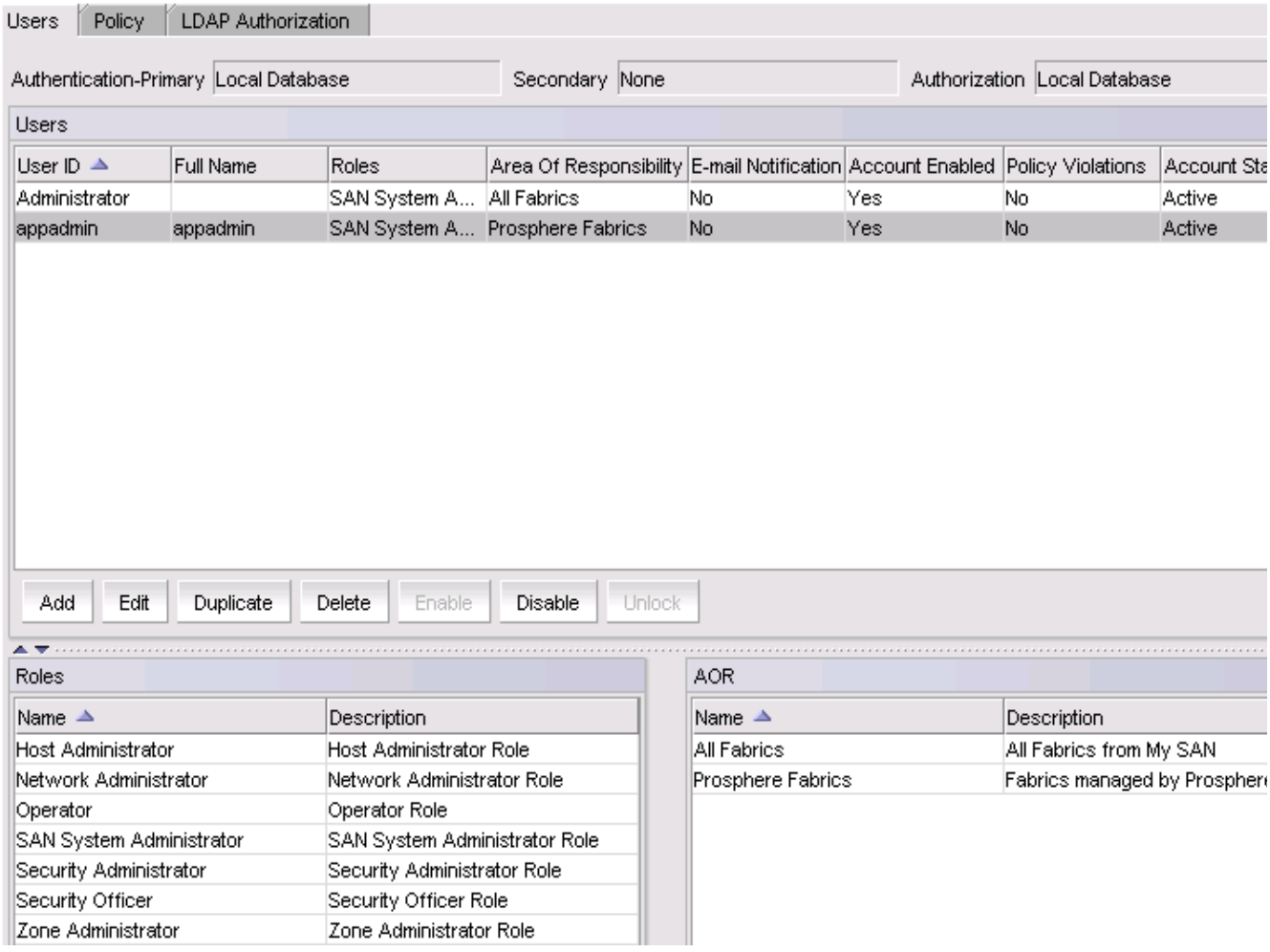
   Note: The *EMC ProSphere Security Configuration Guide* provides a detailed procedure to import the ProSphere Server certificate.

2. Create a CMCNE user whose username matches the ProSphere user credentials.

From the CMCNE user management user interface, create a local user whose name matches the ProSphere user id (for example, appadmin).

3. Add any fabrics that are discovered in ProSphere to an Area of Responsibility in CMCNE and assign them to the user account you will use to launch CMCNE, as shown in the following screen.

Note: If you will link and launch CMCNE from any discovered fabric, assign the user account to the following Responsibility: All Fabrics. It you do not want to assign permissions that allow the account to launch from any discovered fabric, create an Area of Responsibility that is a subset of the discovered fabrics and assign it to the user account.



4. ProSphere should be able to do a DNS lookup of the CMCNE host to determine the FQDN of CMCNE host. If there are firewalls between the ProSphere host and CMCNE, the firewall should be configured for the DNS lookup to work properly.
5. The Computer Name of the Windows host where CMCNE is running should be set to the FQDN of the host. For example, if the FQDN is cmcne-host.lss.emc.com, and if the Computer Name is set to cmcne-host, Launch In-Context will not work. The Computer Name should be set to cmcne-host.lss.emc.com.

Note: The *EMC ProSphere Support Matrix* lists the CMCNE version supported by ProSphere.

Authorize ProSphere users with the SMIA Configuration Tool

Note: There will be port contention if CMCNE and another SMI Cimom are installed on the same host and they both use the default ports 5988 and 5989.

On the Brocade CMCNE host do the following:

1. **Start > All Programs > CMCNE > Server Management Console**.
2. If you are not logged in as administrator, right-click on the Server Management Console and select **Run as administrator**.
3. In the CMCNE Server Console, click the **Services** tab.
4. Click **Restart**. The message "Stopping Services will cause CMCNE Clients …. " appears.
5. Click **Yes**.
6. When the restart has completed and the **Status** column displays **Started**, click **Configure SMI Agent**.
7. In the SMIA Configuration Tool Log in window, enter user ID and password.
   - Default User name: **Administrator**
   - Default Password: **password**
8. Click **Login**.
9. In the SMIA Configuration Tool under the **Home** tab, click the **Users** option.
10. In the **Users** window under the **Users** tab, click **Add**.
11. In the **Add User** window, perform the following steps for each ProSphere user:
    a. Enter the ProSphere user name.
    b. Enter the ProSphere password.
    c. Move all fabrics from **Available Roles / AOR TO Selected Roles /AOR**.
    d. Move **SAN System Administrator** from **Available Roles / AOR** to **Selected Roles /AOR**.
    e. Once all have been moved click **OK**.
12. In the **Users** window under the **Users** tab you should see the ProSphere users in the list under **Users**.

Note: ProSphere should be able to do a DNS lookup of the CMCNE host. Verify that all ports are open between ProSphere and the CMCNE server if firewalls exist between the applications. Bear in mind that host-based software firewalls can block communications and must be configured as well.

Update Licenses

On the Brocade CMCNE host perform the following steps to update licenses:

1. Launch CMCNE by selecting the **Start > All Programs > CMCNE > CMCNE** or by double-clicking the CMCNE icon on the desktop, and log in.
2. From the main (**View All**) window, select **Help > License**.
3. In the **License** window, enter the license key or use browse to locate the license key file, and click **OK**.

Synchronize ProSphere deployments

The procedure for deploying multiple ProSphere or Collector deployments is the same as for a single deployment. However, make sure you create a common Administrator credential for all the deployments and use only this credential to log into ProSphere when you intend to synchronize multiple ProSphere deployments.

The *EMC ProSphere Administrator Guide* and online help contains information about synchronizing multiple ProSphere Applications. Go to **Home > Administering ProSphere > System > Synchronize ProSphere Applications > Synchronize Multiple ProSphere Applications dialog**.

Deploy trusted certificates

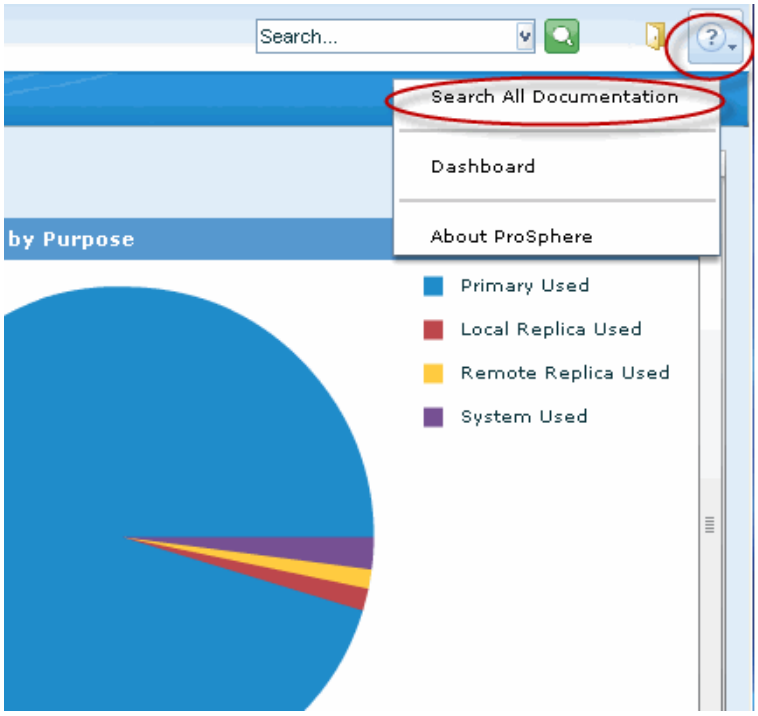
Deploy organization-specific, trusted certificates through the ProSphere Console. ProSphere is deployed with unsigned certificates. ProSphere supports only X.509 certificates. For added security, EMC recommends obtaining and deploying signed certificates specific to your organization. Certificate deployment can be performed in the ProSphere Console. The *EMC ProSphere Online Help* contains more information about importing and exporting certificates. Go to **Home > Administering ProSphere > Users and Security > Import and Export Certificates**.

Additional information

The *EMC ProSphere Documentation Library*, which is accessible from the ProSphere Console, contains additional information and assistance.

To display the library, right click the **Help** button (**?**), then select **Search All Documentation**.

Figure 3 Display the EMC ProSphere documentation library



A

Updates and Backups

Updates to EMC ProSphere are made separately to each virtual machine, from a Web browser.

This chapter explains how to deploy updates to ProSphere and includes the following sections:

- Overview 96
- Supported updates 96
- Install updates on ProSphere 98
- Create and restore snapshots or backups 102
- Back up and restore ProSphere with VMware Data Recovery 104

Overview

EMC may periodically provide you with updates to ProSphere. Updates can represent fixes, improvements, and additions to ProSphere documentation and functionality. Not all updates may affect all virtual machines in ProSphere. Consult your update documentation for specific details and instructions.

IMPORTANT

Applying updates requires first taking a snapshot or backup of all ProSphere virtual machines.

IMPORTANT

If a site has two or more ProSphere instances deployed and one or more are federated with each other, then you should perform all ProSphere updates in parallel. After updating, all instances should be rebooted at the same time. The federated groups feature supports the displaying of groups from federated sites only when master and non-master sites are running the same version of ProSphere.

Note: After an update, a few features dependent on object discovery (for example, shared LUNs view in the Explore area and the creation of VNX FAST managed service levels) may exhibit unpredictable behavior until all objects are discovered successfully.

Supported updates

The following version-to-version updates are supported:

- 1.5.0.x > 1.7.0.x
- 1.6.0.x > 1.7.0.x

ProSphere update methods

The virtual machines in ProSphere include the following:

- ProSphere Application
- Discovery Engine and any Collectors
- Historical Database

Table 7 on page 97 details the ways perform updates on ProSphere virtual machines.

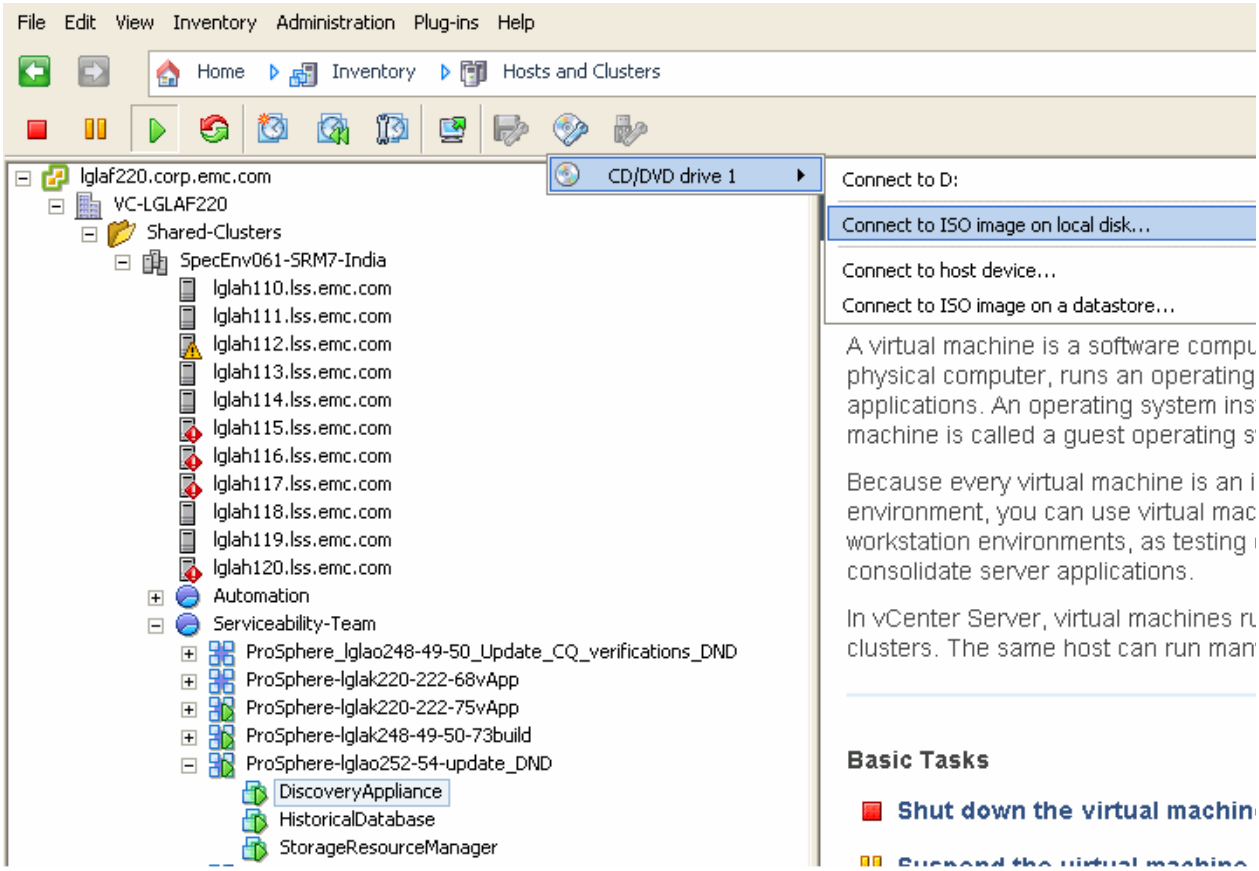
Table 7 Update Details

Source	Extension	Action	Method
EMC Update Repository	n/a	"Select a virtual CDROM or web server for updates" on page 99 explains how to configure the ProSphere update interface to use one of the URLs of the EMC Update Repository to obtain updates from the web. A different URL has the updates for each ProSphere virtual machine. Apply updates.	Specified Repository
Customer-installed web server	zip	Create a web server for updates and configure a location where the web server will access the zip files. Go to EMC Online Support site URL provided by EMC. Download and unzip the zip files to the configured location. "Select a virtual CDROM or web server for updates" on page 99 explains how to configure the ProSphere update interface to use the URL of the web server to obtain updates. Apply updates. There is a separate zip file for each ProSphere virtual machine. Each zip file contains two folders, Manifest and Packages. The Manifest folder contains xml metadata files, and the Package folder contains the rpm packages that need to be updated.	Specified Repository
CD-ROM	iso	Go to an EMC Online Support site URL. Download an ISO file to a virtual CD-ROM as explained in "Download an ISO file to a virtual CD-ROM" on page 97. "Select a virtual CDROM or web server for updates" on page 99 explains how to configure the ProSphere update interface to obtain updates from a virtual CD-ROM. Apply updates.	Virtual CD-ROM Updates

Download an ISO file to a virtual CD-ROM

1. In vSphere, display the vSphere client.
2. Select each of the three ProSphere virtual machines and connect the ISO file to the virtual machine with the **Connect to ISO image on local disk option**, as shown in the following figure**.** The three virtual machines are:
   - DiscoveryAppliance
   - HistoricalDatabase

- StorageResourceManager.



After the ISO file is attached, the identification of updates can take a few minutes, unless the update check is forced.

Install updates on ProSphere

The following sections explain how to update ProSphere.

Note: After applying updates, some features of ProSphere may not work correctly until after arrays are rediscovered.

Create snapshots before updating software

Before applying an update, you should create a snapshot or backup of each of the ProSphere virtual machines. "Create and restore snapshots or backups" on page 102 provides more information about creating virtual machine snapshots and backups for ProSphere.

After applying updates to a ProSphere virtual machine, shutdown and restart the vApp. Follow the instructions in "Shut down or start up ProSphere or its virtual machines" on page 102.

Note: ProSphere does not create rollback or backup points before applying updates.

Consult your VMware documentation for more information about creating backups and snapshots than what is presented here. VMware also provides documentation at http://www.vmware.com.

Select the EMC Update Repository as a source for updates

This section explains how to configure the source of manual updates as the EMC Update Repository on the web.

After logging in to ProSphere, perform the following:

1. Click **Admin** on the ProSphere Console.
2. Click the **System** tab.
3. Click **Manage Application Software**.
4. Select a system component.
5. Click **Specify Repository** to open the **Specify Repository** dialog box.
6. Select **Use EMC repository.**
7. Type the URL from Table 8 on page 99.
8. Enter username and password.

Note: A valid EMC Online Support username and password is required to access the EMC Update Repository.

Table 8 Update URL for ProSphere virtual machines

Virtual machine	Update URL
ProSphere Application	`https://vupdate.emc.com/StorageResourceManager`
Discovery Engine	`https://vupdate.emc.com/DiscoveryAppliance`
Historical Database	`https://vupdate.emc.com/HistoricalDatabase`
Collector	`https://vupdate.emc.com/CollectorAppliance`

Select a virtual CDROM or web server for updates

This section explains how to configure the source of manual updates as one of the following values:

- Use CD-ROM updates (if applying updates from an iso file)
- Use specified repository (if using a zip file)

After logging in to ProSphere, perform the following:

1. Click **Admin** on the ProSphere Console.
2. Click the **System** tab.
3. Click **Manage Application Software**.
4. Select a system component.
5. Click **Specify Repository** to open the **Specify Repository** dialog box.
   a. If you select **Use CDROM updates**, you will download the ISO file to a virtual CD-ROM as explained in Table 7 on page 97.

b. If you select **Use specified repository,** type the URL of the customer-installed web server where your virtual machine will look for updates. If the URL requires authentication, provide a valid username and password.

Receive updates reminder at login and apply updates

The system periodically checks for updates.

If updates are available when you log in to ProSphere, the **Software Updates Available** dialog box is displayed to remind you.

Table 9 on page 100 describes the buttons available on the dialog box.

Table 9 Software Updates Available dialog box: buttons

Button	Description
Update Software	Displays the **Update Software** dialog box. To apply updates, click the checkbox next to each update to apply, then click **Install Updates**. After installing updates, if you have the Discovery Engine Collector deployed, click the Help button for the mandatory procedure. Otherwise, in the vSphere client, power off and reboot the ProSphere vApp. Follow the instructions in "Create and restore snapshots or backups" on page 102. **Note:** Updates to ProSphere are available only in a new browser session. Therefore, after updates are applied, a message appears and prompts you to close the browser and reopen it. During the restart, a journal migration operation is in progress, which will take up to ten minutes. After ten minutes, log in to the ProSphere Console. If no message is displayed, assume the journal migration operation was successful. If a failure message is displayed, contact Customer Support.
Remind Me Later	Postpones the reminder.
No Reminder	Prevents the reminder from reappearing.
Help	Displays online help.

If the **Software Updates Available** dialog box is not displayed, you can disable the updates reminder with the following procedure:

1. Click **Admin** on the ProSphere Console.
2. Click the **System** tab.
3. Click **Manage Application Software.**
4. At the **Manage Application Software** dialog box, click **Update Options**.
5. Select **No automatic check for updates**.
6. Click **OK,** or click **Close** to close the dialog box without making changes.

Manually check for and apply updates

To manually check for updates:

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

3. Click **Manage Application Software**.

If updates are available, the **Health Details** area on the **Manage Application Software** dialog box displays a message indicating that updates are available. If the attempt to check for updates did not succeed, details of the failed operation appear.

"Manage Application Software dialog box: buttons" on page 101 discusses the buttons available on the **Manage Application Software** dialog box.

Table 10 Manage Application Software dialog box: buttons

Button	Description
Update Software	Displays the **Update Software** dialog box. To ensure that the most recent available updates are listed, click **Check for New Updates**. To apply updates, click the checkbox next to each update to apply, then click **Install Updates**. After installing updates, if you have the Discovery Engine Collector deployed, click the Help button for the mandatory procedure. Otherwise, in the vSphere client, power off and reboot the ProSphere vApp. Follow the instructions in "Create and restore snapshots or backups" on page 102. **Note:** Updates to ProSphere are available only in a new browser session. Therefore, after updates are applied, a message appears and prompts you to close the browser and reopen it. During the restart, a journal migration operation is in progress, which will take up to ten minutes. After ten minutes, log in to the ProSphere Console. If no message is displayed, assume the journal migration operation was successful. If a failure message is displayed, contact Customer Support.
Specify Repository	Selects a source for updates. "Select the EMC Update Repository as a source for updates" on page 99 describes this button.
Update Options	"Receive updates reminder at login and apply updates" on page 100 describes this button.
Close	Closes the **Manage Application Software** dialog box without applying updates.
Help	Displays online help.

SMC, SPA, and SMAS

The upgrade impacts the currently running performance data collection and alert collection jobs, causing them to fail.

To avoid discovery failure, create an SMC-SPA access credential in ProSphere to represent all SMC/SPA instances in the SAN. An SMC-SPA access credential allows ProSphere to be represented as a launch client in SMC. The launch client needs to be registered in all SMC/SPA instances.

Upgrading ProSphere from 1.5 to 1.6 or later can have the following results:

- Performance data collection may fail
- Alert collection jobs may fail
- Discovery jobs configured with default credentials are dissociated.

If array detection fails, the status of the array is displayed on the Performance Detection Failures link in Discovery Job Execution Results.

The reasons for failure can be:

- The SMC-SPA access credential was not created.
- The SMC-SPA access credential attributes do not match the information in the corresponding launch client in an SMC/SPA instance.

Follow the steps in "Integrate ProSphere with SMAS and Unisphere for VMAX" on page 76.

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. "Back up and restore ProSphere with VMware Data Recovery" on page 104 explains how to create backups with VMware Data Recovery.

IMPORTANT

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

IMPORTANT

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.

Table 11 on page 102 explains how to perform shutdowns and startups with right-click options from the vSphere Console.

Table 11 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

IMPORTANT

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.

IMPORTANT

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:

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 the architecture chapter of the *EMC ProSphere Administrator Guide*. Shut down Collectors, then shut down the vApp. Shut down 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**.

IMPORTANT

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, enter 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:

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. The synchronization chapter of the *EMC ProSphere Administrator Guide* discusses this situation in detail.

Back up and restore ProSphere with VMware Data Recovery

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

If VMware Data Recovery 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.

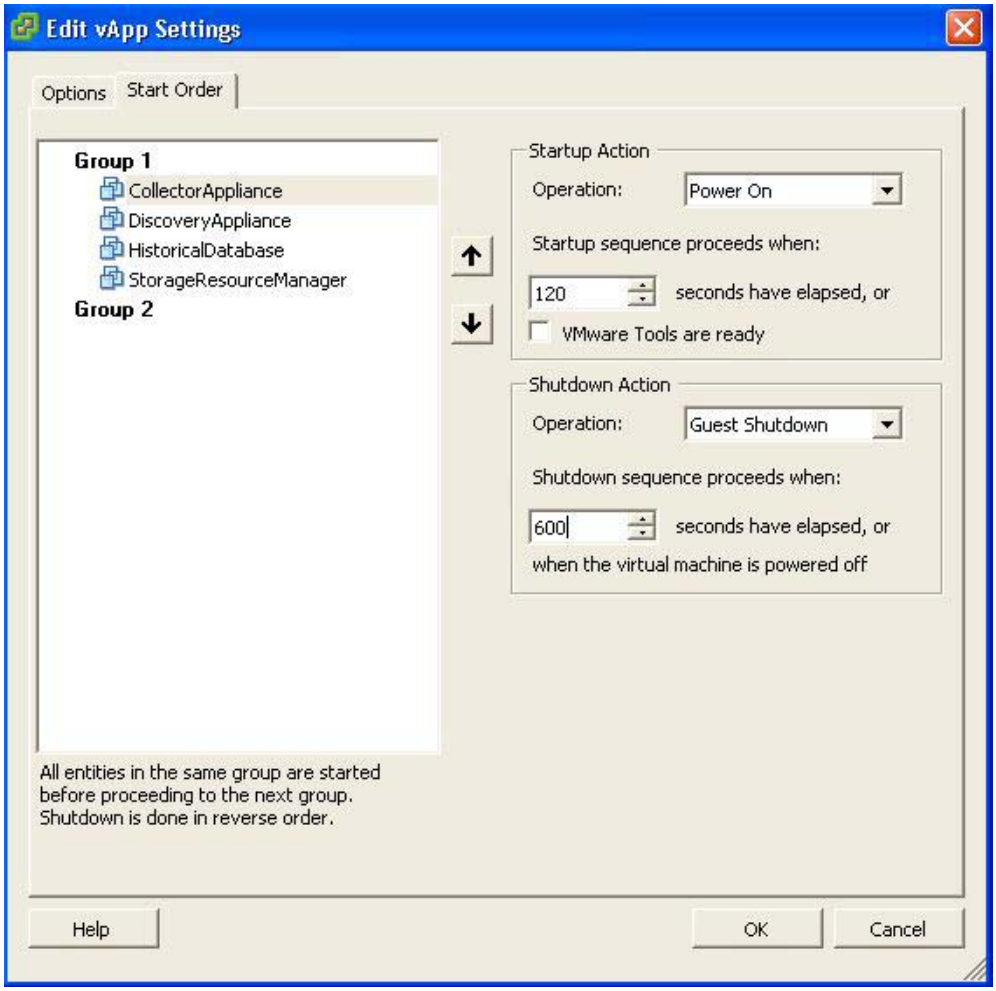
In a scale-out deployment, additional virtual machines of the Collector type exist, as described in the architecture chapter of the *EMC ProSphere Administrator Guide*. Schedule separate backup jobs for the vApp and for the Collector. Schedule these backups to occur at the same time. When restoring the virtual machines from backups, disable automatic power on 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 into Group1, along with other ProSphere machines. 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.

Perform the following step to allow the Collector to gracefully shut down:

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

4. Set **Shutdown sequence proceeds when** to **600**.



5. Click **OK**.