

EMC Storage Integrator for Windows Suite

Version 5.0

Product Guide

302-003-290

REV 02

Copyright © 2017 Dell Inc. or its subsidiaries. All rights reserved.

Published January 2017

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners.
Published in the USA.

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

CONTENTS

Chapter 1	Introduction	7
	About this document.....	8
	Audience.....	8
	Product overview.....	8
	ESI for Windows and ESI PowerShell Toolkit	8
	ESI adapters.....	9
	ESI hypervisor support.....	9
	ESI Service and ESI Service PowerShell Toolkit.....	10
	ESI SCOM Management Packs	10
Chapter 2	Installing ESI	13
	Installation overview.....	14
	ESI system prerequisites.....	15
	ESI adapter prerequisites.....	16
	Installing ESI.....	18
	Installing the ESI GUI.....	19
	Customizing the GUI view.....	20
	Uninstalling ESI.....	21
	Reinstalling ESI.....	21
Chapter 3	Setting up connections	23
	Setting up Directory Services integration for ESI applications.....	24
	Setting up AD DS.....	24
	Setting up AD LDS.....	24
	Configuring AD DS and AD LDS for ESI Service connections.....	25
	Configuring AD DS and AD LDS for ESI, MMC, and PowerShell connections	25
Chapter 4	Configuring ESI Service	27
	Setting up ESI Service for SCOM.....	28
	Changing HTTP connection defaults.....	28
	Setting up new IP ports with the default certificate.....	29
	Setting up default IP ports with a new domain certificate.....	30
	Setting up new IP ports with a new domain certificate.....	31
	Confirming the HTTP connections.....	33
	Viewing and setting up the security policy.....	33
	Changing the system refresh interval.....	34
Chapter 5	Installing and configuring ESI SCOM Management Packs	37
	Installing ESI SCOM management packs.....	38
	Setting up ESI SCOM Management Packs.....	38
	Confirming the connection between SCOM agents and the ESI Service....	39
	Setting up the Run As profile for the EMC SI Monitoring account.....	39
	Setting up the Run As profile for the EMC SI Service Monitoring account....	39
	Setting up the SCOM agent registry.....	40
	Setting up optional ESI Service discovery overrides.....	40

	Setting up a system filter file.....	41
	Setting up the HTTP proxy.....	41
	Changing the HTTPS to HTTP override.....	41
	Setting up the required ESI Service Host override and discovery.....	42
Chapter 6	Managing storage with the PowerShell Toolkits	45
	Getting started with the ESI PowerShell toolkits.....	46
	Getting help at the Windows PowerShell command line.....	46
	Using PowerShell objects.....	46
	Adding Vblock Systems and VxBlock Systems	47
	PowerShell examples.....	48
	Provisioning a storage volume.....	48
	Removing a storage volume.....	49
	ESI PowerShell cmdlet list.....	51
	PowerShell cmdlets connection operations.....	51
	PowerShell cmdlets storage system operations.....	53
	PowerShell cmdlets host operations.....	61
	PowerShell cmdlets hypervisor operations.....	63
	PowerShell cmdlets EMC RecoverPoint replication operations.....	64
	PowerShell cmdlets SQL Server operations.....	66
	PowerShell cmdlets ESI Service operations.....	67
Chapter 7	Managing storage systems with the ESI GUI	69
	Adding storage systems.....	70
	Storage system credentials.....	70
	Removing systems from ESI.....	72
	Publishing connections.....	72
	Publishing storage systems.....	72
	Unpublishing storage systems.....	73
	Using the PowerShell scripting tool.....	74
	Managing VMAX storage systems.....	75
	Using FAST VP.....	75
	Managing metas.....	76
	Managing block storage.....	76
	Creating LUNs.....	76
	Viewing LUNs.....	77
	Expanding LUNs.....	78
	Deleting LUNs.....	78
	Viewing LUN groups.....	79
	Creating volumes.....	79
	Viewing XtremIO volumes.....	80
	Deleting volumes.....	80
	Viewing masked LUNs and volumes.....	81
	Creating snapshots.....	81
	Creating XtremIO snapshots.....	82
	Viewing snapshots.....	83
	Deleting snapshots.....	83
	Refreshing object types from an XtremIO snapshot.....	83
	Restoring a LUN from a VMAX3 snapshot.....	84
	Viewing snapshot LUNs.....	84
	Deleting snapshot LUNs.....	85
	Managing XtremIO tags.....	86
	Managing XtremIO object types with tags.....	86
	Creating consistency groups.....	86

	Managing volumes in a VPLEX consistency group.....	87
	Viewing consistency groups.....	87
	Viewing service nodes for block storage systems.....	88
	Viewing storage pools.....	88
	Viewing VPLEX storage views.....	89
	Creating VPLEX virtual volumes.....	89
	Viewing VPLEX clusters and virtual volumes.....	90
	Deleting VPLEX virtual volumes.....	90
	Viewing VPLEX initiators.....	90
	Registering and unregistering VPLEX initiators	91
	Viewing XtremIO initiator groups.....	91
	Viewing XtremIO storage controllers.....	91
	Creating and editing XtremIO schedules.....	92
	Managing file storage.....	92
	Creating shared folders.....	93
	Viewing shared folders.....	94
	Mounting shared folders.....	94
	Deleting shared folders.....	94
	Unmounting shared folders.....	94
	Creating shared folder pools.....	95
	Viewing shared folder pools.....	95
	Extending shared folder pools.....	95
	Deleting shared folder pools.....	96
	Viewing file system service nodes.....	96
Chapter 8	Managing hosts with the ESI GUI	97
	Adding hosts.....	98
	Adding Windows system hosts.....	98
	Adding Linux system hosts.....	98
	Viewing registered hosts.....	99
	Removing hosts.....	99
	Applying XtremIO host best practices.....	99
	Viewing SAN initiators.....	100
Chapter 9	Managing host disks with the ESI GUI	101
	Changing a host disk drive letter or path.....	102
	Connecting disks to a host.....	102
	Creating host disks.....	103
	Viewing host disks.....	105
	Expanding host disks.....	105
	Deleting host disks.....	106
	Disconnecting disks from a host.....	106
	Creating pass-through SCSI disks.....	107
	Connecting pass-through SCSI disks to a host.....	108
	Creating raw device mapping disks.....	109
	Connecting raw device mapping disks to a host.....	111
	Creating SCSI disks.....	113
	Connecting SCSI disks to a host.....	114
	Creating virtual disks.....	115
	Connecting virtual disks to a host.....	117
Chapter 10	Managing host clusters with the ESI GUI	119
	Adding host clusters.....	120
	Viewing host clusters and nodes.....	120

	Removing clusters from a host.....	121
	Creating cluster disks.....	121
	Connecting cluster disks to a host cluster.....	123
	Connecting cluster nodes to a host.....	123
	Disconnecting cluster disks from a host cluster.....	123
	Deleting cluster disks from a host cluster.....	124
	Changing a cluster disk drive letter or path.....	124
Chapter 11	Managing hypervisors with the ESI GUI	127
	Managing virtual machines and disks.....	128
	Creating disks for virtual machines.....	128
	Creating hypervisor SCSI LUNs.....	129
	Connecting SCSI LUNs.....	130
	Disconnecting or removing SCSI LUNs.....	130
	Managing virtual machines in ESI.....	131
	Attaching virtual disks.....	131
	Removing virtual disks from a hypervisor.....	134
	Adding, viewing, and deleting hypervisors.....	134
	Adding hypervisor servers.....	134
	Viewing hypervisor hosts.....	135
	Viewing hypervisor datastores.....	135
	Creating a hypervisor datastore.....	136
	Viewing hypervisor virtual volumes	137
	Viewing hypervisor virtual machines.....	137
	Viewing hypervisor SAN initiators and SCSI LUNs.....	137
	Deleting hypervisor servers.....	138
Chapter 12	Managing storage with Microsoft SCOM	139
	ESI Service and ESI SCOM Management Packs.....	140
	ESI Service and Management Packs best practices.....	140
	ESI Service overview.....	140
	ESI SCOM Management Pack Files.....	141
	Using the ESI Monitoring Management Pack.....	141
	Monitoring component health.....	144
	Monitoring capacity.....	146
	Viewing monitors.....	147
	Setting up monitoring maintenance mode.....	147
	Setting up optional management pack overrides.....	147
	Disabling performance data collection.....	148
	Changing discovery interval overrides.....	148
	Changing monitoring interval overrides.....	149
Chapter 13	Troubleshooting	151
	Troubleshooting EMC systems and hypervisors.....	152
	Troubleshooting the ESI VMAX Adapter.....	155
	Troubleshooting the ESI RecoverPoint Adapter.....	156
	Troubleshooting the SQL Server Adapter.....	157
	Troubleshooting the ESI Service and ESI SCOM Management Packs.....	157
	Troubleshooting Active Directory Services.....	163
	ESI logs.....	164
	EMC Sales and Customer Service contacts.....	164

CHAPTER 1

Introduction

This chapter includes the following topics:

- [About this document](#).....8
- [Product overview](#).....8

About this document

This product guide provides instructions for installing and configuring the components of EMC® Storage Integrator (ESI) for Windows Suite. It also provides information and procedures for using ESI to provision and manage storage arrays.

For the latest information about new and changed features, known issues, and environment and system requirements, refer to the *EMC Storage Integrator for Windows Suite Release Notes*. The release notes are available at [EMC Online Support](#).

Audience

ESI for Windows Suite is designed for Microsoft applications administrators who manage storage and application provisioning and monitor storage health.

This software enables administrators to view, provision, and manage block and file storage for Microsoft Windows and Microsoft SQL Server sites on supported EMC storage systems. Microsoft System Center Operations Manager (SCOM) integration with ESI provides administrators with a dashboard view of storage entities to monitor health and performance.

Administrators can manage their environment using either the ESI graphical user interface (GUI) or the PowerShell command line interface (CLI).

Product overview

ESI for Windows Suite is a set of tools for Microsoft Windows and Microsoft applications administrators.

The suite includes:

- ESI for Windows and the ESI PowerShell Toolkit
- ESI system adapters
- ESI hypervisor support
- ESI Service and the ESI Service PowerShell Toolkit
- ESI SCOM Management Packs

The toolkits are written for the PowerShell platform, which is developed by Microsoft specifically for Windows System Management automation.

ESI for Windows and ESI PowerShell Toolkit

ESI for Windows enables you to view, provision, and manage block storage for Microsoft Windows and SQL Server systems.

The ESI for Windows GUI is based on Microsoft Management Console (MMC). You can run ESI as a stand-alone tool or as part of an MMC snap-in on a Windows computer.

The ESI PowerShell Toolkit enables you to provision storage to and manage storage on Microsoft Windows hosts that use EMC storage. This toolkit includes a set of PowerShell cmdlets to manage EMC storage systems from the PowerShell command line. The ESI PowerShell Toolkit provides access to most of the provisioning functionality offered by the ESI MMC application and shares a common configuration set with the MMC application.

ESI adapters

ESI system adapters enable storage administrators to create, provision, and manage storage within the ESI GUI and to use the ESI PowerShell Toolkit.

Install system adapters for specific system support, or for SQL Server and EMC RecoverPoint™ support. The [EMC Simple Support Matrix](#) provides supported environment and software requirements. For information about adapter prerequisites, refer to [ESI adapter prerequisites](#) on page 16.

ESI supports the following storage systems and products:

- EMC ScaleIO™ software-defined storage (SDS)
- EMC Unity™ and UnityVSA™ systems
- EMC VMAX™, VMAX3™, VMAX with embedded NAS (eNAS), and VMAX All Flash families
- EMC VNX™ series
- EMC VNXe™ series
- EMC VPLEX™ systems
- EMC XtremIO™ systems

Note

The adapter enables support for managing and monitoring XtremIO clusters and arrays using IPv6.

-
- VCE™ Vblock™ Systems and VCE VxBlock™ Systems
 - EMC RecoverPoint (using PowerShell cmdlets only)
 - Microsoft SQL Server (using PowerShell cmdlets only)
 - Windows and Linux hosts
 - ESX and Microsoft Hyper-V hypervisors

Note

The VMAX adapter:

- Supports the VMAX3 service level objectives (SLO) feature.
- Cannot provision storage on host systems that are provisioned with Virtualization Domains or with the Storage Pool Manager (SPM) from previous releases of the ESI VMAX Adapter.

For information about how to add supported systems to ESI, refer to [Adding storage systems](#) on page 70 and [Adding Vblock Systems and VxBlock Systems](#) on page 47.

ESI hypervisor support

In addition to supporting physical environments, ESI supports storage provisioning and discovery for Windows virtual machines that are running on Microsoft Hyper-V or VMware vSphere.

Install the corresponding adapters for specific hypervisor support.

Storage options in ESI vary depending on the hypervisor:

- For Hyper-V virtual machines, you can create virtual hard disk (VHD and VHDX) files and pass-through SCSI disks. You can also create host disks and cluster shared volumes.
- For vSphere ESXi virtual machines, you can create virtual machine disk (VMDK) files and raw device mapping (RDM) disks without virtual compatibility mode. You can also create SCSI disks and view datastores. SCSI disks require the use of existing SCSI controllers.

ESI Service and ESI Service PowerShell Toolkit

The ESI Service is the communications link between ESI and the ESI System Center Operations Manager (SCOM) Management Packs.

Use the ESI Service to view and report on registered EMC storage systems and storage-system components that are connected to the ESI host system. SCOM pulls this data from the ESI Service. You can also use the ESI Service as a stand-alone tool without SCOM to collect, view, and report this same system data.

During the ESI installation, you can choose to install the ESI Service on the same ESI host system. When you install the ESI Service, the ESI Service PowerShell Toolkit is also installed on the ESI host system.

Use the PowerShell Toolkit to set up the ESI Service to communicate with the storage systems and ESI SCOM Management Packs.

ESI SCOM Management Packs

The ESI Service and the ESI SCOM Management Packs work with Microsoft SCOM for centralized discovery and monitoring of all supported EMC systems and storage-system components.

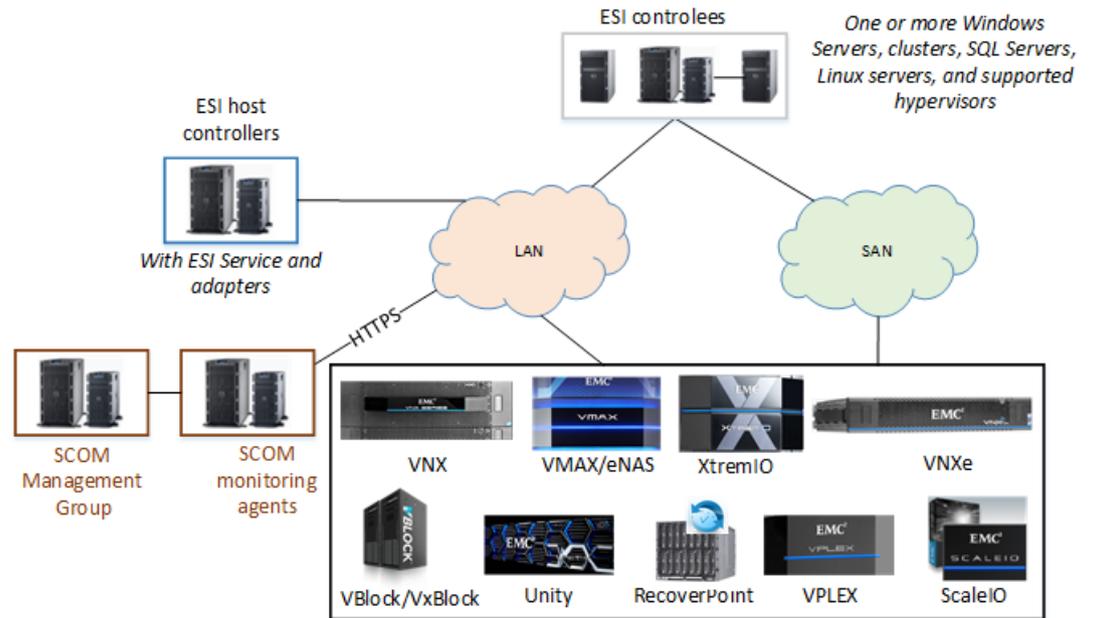
The ESI Service and ESI SCOM Management Packs support the same EMC storage systems that are supported in ESI.

Note

ESI SCOM Management Packs support EMC VNXe3200™ systems, but do not currently support EMC VNXe3100™, EMC VNXe3150™, EMC VNXe3300™, and EMC VNXe1600™ systems.

The following figure represents how one SCOM Management Group that is running the ESI SCOM Management Packs connects to multiple SCOM agents, which connect through HTTPS to one or more ESI Services.

Figure 1 ESI for Windows Suite setup with SCOM Management Group and monitoring agents



ESI host controllers: One or more ESI host servers are connected to the same Windows domain as the ESI controlees, EMC systems, EMC RecoverPoint, and SCOM monitoring agents.

For a list of supported system versions, refer to the [EMC Simple Support Matrix](#).

CHAPTER 2

Installing ESI

This chapter includes the following topics:

- [Installation overview](#) 14
- [ESI system prerequisites](#) 15
- [ESI adapter prerequisites](#) 16
- [Installing ESI](#) 18
- [Installing the ESI GUI](#) 19
- [Customizing the GUI view](#) 20
- [Uninstalling ESI](#) 21
- [Reinstalling ESI](#) 21

Installation overview

The ESI installers enable you to install ESI and select the options that you require for your ESI environment.

ESI installation files

The ESI .zip file includes:

- *EMC Storage Integrator for Windows Suite Release Notes*
- ESI Powershell installer, which provides the core ESI setup and enables you to select options, including the ESI Service
- ESI GUI installer
- ESI SCOM Management Packs installer

ESI installation options

Perform the following procedures to install and configure ESI:

1. Run the ESI PowerShell installer to install the ESI core setup on the host system and to select adapters and other options. If you choose to install the ESI Service, the installer also installs the ESI Service PowerShell Toolkit. For more information, refer to [Installing ESI](#) on page 18.

Note

Uninstall any previously installed version of ESI and then install ESI version 5.0. For more information, refer to [Uninstalling ESI](#) on page 21.

2. Optionally, when the ESI PowerShell installation is complete, add the ESI GUI to the ESI installation. For more information, refer to [Installing the ESI GUI](#) on page 19.
3. Choose to store connections settings locally, or choose to store persisting connection settings in a central store. For more information, refer to [Setting up Directory Services integration for ESI applications](#) on page 24.
4. Modify options or reinstall the same adapters and options selected during the latest ESI installation. For more information, refer to [Reinstalling ESI](#) on page 21.
5. Optionally, when the ESI PowerShell installation is complete, install the ESI SCOM Management Packs. Use the ESI Service and ESI SCOM Management Packs separately or together with ESI. For more information, refer to the following:
 - [Setting up ESI Service for SCOM](#) on page 28
 - [Installing ESI SCOM management packs](#) on page 38 and [Setting up ESI SCOM Management Packs](#) on page 38

ESI system adapter installation

All ESI system adapters, except the VMAX, VNXe, and Unity adapters, are installed by default with ESI. You must specifically choose to install the VMAX, VNXe, and Unity adapters during the ESI installation. To install the adapters at a later time, reinstall ESI and select the option to install the adapters.

For the ESI system adapters to work correctly with ESI, ensure that the system meets the following prerequisites.

- [ESI system prerequisites](#) on page 15
- [ESI adapter prerequisites](#) on page 16

ESI system prerequisites

For ESI to function correctly, your environment must meet these minimum system requirements.

- Ensure that the following are installed:
 - A supported version of .NET Framework on the ESI controller (the host on which ESI runs).
 - Windows Server on the ESI controller (Windows Server Core installations are not supported).
 - A supported version of MMC. Otherwise, the ESI installer prompts you to upgrade before installing ESI. If MMC is not installed, download and install it from the Microsoft website.
 - Microsoft PowerShell on all hosts. If PowerShell is not installed, download and install it from the Microsoft website.
 - The latest version of EMC PowerPath or Microsoft Multipath I/O (MPIO) with the Microsoft Device Specific Module (MSDSM) on the controllee host.
 - To use Microsoft Active Directory Directory Services (AD DS) with ESI, Windows Server Active Directory.
 - To use Microsoft Active Directory Lightweight Directory Services (AD LDS), an AD LDS instance on the Windows Server.
- Enable the following firewall exceptions on the ESI controllers and ESI controllees (hosts on which ESI provisions storage):
 - Remote Volume Management-Virtual Disk Service (RPC) (`vds.exe`)
 - Remote Volume Management-Virtual Disk Service Loader (RPC) (`vdsldr.exe`)
 - Remote Volume Management (RPC-EPMAP) (`svchost.exe`)
 - Windows Management Instrumentation
- Enable the remote PowerShell on ESI controllee hosts by running the `Enable-PSRemoting -force` command on the controllee host
- If you use iSCSI for SAN connectivity, use the iSCSI initiator to log in to the storage systems.
- If you use FC transport for SAN connectivity, configure zoning for the FC initiator and use that initiator to log in to the storage system.
- Ensure that ESI is installed and runs in a domain user login session with administrative privileges for the controller host. The controller and controllee hosts must be members of the same Windows domain or in trusted domains.

ESI adapter prerequisites

For ESI adapters to function correctly with ESI, ensure that your environment meets the prerequisites.

Note

You can ensure that your environment meets these prerequisites before or after you install ESI. However, they must be in place before you start the ESI application or the ESI Service.

Table 1 ESI adapter prerequisites

Adapter	Prerequisites
Unity	Install the latest version of the EMC Unisphere® Unity CLI for the specific environment on the ESI controller host. The latest versions of the Unity CLIs are available for download on EMC Online Support.
VMAX	<ul style="list-style-type: none"> • The VMAX adapter is based on the Solutions Enabler Storage Management Initiative Specification (SMI-S) provider. Download and install the latest applicable version of SMI-S that is available for your VMAX model from EMC Online Support. The EMC Simple Support Matrix lists the supported versions of EMC Enginuity™ and EMC Solutions Enabler for this release. • Install and run SMI-S on a management server that is separate from all ESI hosts and storage systems. The VMAX Adapter cannot provision storage on a server that is running SMI-S. • After installing the latest version of EMC SMI-S Provider, use VMAX to create two or more gatekeeper devices and unmask the gatekeepers to the SMI-S server that is hosting the SMI-S provider. Gatekeepers are required for accessing and issuing management commands. For more information, refer to the EMC VMAX documentation. • Install a supported version of Oracle Java SE Runtime Environment (JRE), which is required for VMAX3 systems. Refer to the EMC Simple Support Matrix.
VNX	Enable Access Logix on the storage array before connecting a host disk on a Windows host.

Table 1 ESI adapter prerequisites (continued)

Adapter	Prerequisites
VNXe	Install the latest version of the EMC Unisphere VNXe CLI for your environment on the ESI controller host. The latest versions of the VNXe CLIs are available for download on EMC Online Support.
VPLEX	<ul style="list-style-type: none"> • Ensure that a supported version of EMC GeoSynchrony™ is installed on the VPLEX systems. The EMC Simple Support Matrix lists supported software versions. • This adapter uses the standard Secure Shell (SSH) network connection to communicate with VPLEX. Confirm that the SSH port 443 is open on the ESI host. If it is not open, the connection fails.
XtremIO	<ul style="list-style-type: none"> • Requires a supported version of XtremIO. • VMware-vSphere-CLI must be installed using the default installation path.
EMC RecoverPoint	<ul style="list-style-type: none"> • Ensure that a supported version of Windows Server is installed. (Windows Server Core installations are not supported.) • Ensure that a supported version of EMC RecoverPoint/SE or EMC RecoverPoint/EX is installed. • Ensure that <code>\System.net.http.formatting</code> DLL is installed on the ESI host controller. When you select to install the ESI RecoverPoint Adapter as part of the ESI installation, this DLL is installed for you. • Ensure that the ESI RecoverPoint Adapter is installed on the ESI controller and a supported version of EMC RecoverPoint/SE or EMC RecoverPoint/EX and the applicable splitters are set up for each supported EMC storage system. <p>The <i>EMC RecoverPoint Release Notes</i>, available on EMC Online Support, provide more details about EMC RecoverPoint/SE and EMC RecoverPoint/EX.</p>
SQL Server	<ul style="list-style-type: none"> • Ensure that the Windows version supports the SQL Server version.

Table 1 ESI adapter prerequisites (continued)

Adapter	Prerequisites
	<ul style="list-style-type: none"> ESI and SQL Server must be connected to the same domain controller and you must have SQL Server Administrator login credentials.

Installing ESI

Use the ESI PowerShell installer to install the core ESI setup and other options. After the core ESI installation is complete, optionally run the installers for the ESI GUI and the ESI SCOM Management Packs.

Before you begin

- Ensure that you have met all the requirements that are listed in [ESI system prerequisites](#) on page 15 and [ESI adapter prerequisites](#) on page 16.
- If a previous version of ESI is installed in the environment, uninstall any previous ESI installer. Otherwise, the current installer does not allow you to proceed. Refer to [Uninstalling ESI](#) on page 21.

Procedure

- Locate and double-click the latest version of:
`ESI.5.*.PowerShell.Setup.msi`
- In the **ESI PowerShell Setup Wizard**, click **Next**.
- Read and accept the EMC Software License Agreement, and then click **Next**.
- In the **Prerequisites for ESI** window, confirm that the system meets the prerequisites, and then click **Next**.
- In the **Custom Setup** window, confirm or change which options to install, and then click **Next**.

Note

Some options, such as the ESI Service, are not selected by default. In the **Setup** window or for each option, click **Browse** to change the default installation paths.

- Click **Install**.

Note

If the installer detects that a later version of a redistributable file is already installed, it does not install the earlier version that is included with ESI. The installer displays an error message to indicate a failure. If you get this message, click **Yes**.

- Click **Finish**.

After you finish

When you successfully install the core ESI setup and options, you can then install:

- The ESI GUI. For more information, refer to [Installing the ESI GUI](#) on page 19.
- The ESI SCOM Management Packs. For more information, refer to [Installing ESI SCOM management packs](#) on page 38.

Installing the ESI GUI

To add the ESI GUI to the ESI deployment, run the ESI GUI installer.

Before you begin

Ensure that the core ESI setup and other options are installed before you install the ESI GUI. Otherwise, the installer does not allow you to proceed. For information about using the ESI PowerShell installer, refer to [Installing ESI](#) on page 18.

Procedure

1. Locate and double-click the latest version of `ESI.5.*.GUI.Setup.msi`.
2. In the **ESI GUI Setup Wizard**, click **Next**.
3. Read and accept the EMC Software License Agreement, and then click **Next**.
4. In the **Publish Connection Information** window, select a connection service, and then click **Next**:
 - **Active Directory**—Uses Active Directory to persist connection settings.
 - **Active Directory Lightweight Directory Service**—Persists connection settings in a central location. For this option, type the Service Name and Service Port for connecting to the AD LDS instance.
 - **Local Server**—Uses connection settings that are stored locally (same as earlier versions of ESI). For example, MMC and PowerShell use the Windows user profile folder and ESI Service uses SQLCE to persist settings locally.
5. Do one of the following:
 - If you are not using Active Directory, skip to the next step.
 - If you are using Active Directory, type the username and password of the Active Directory user account for ESI. The ESI installer uses this account to configure Windows Active Directory for ESI. The ESI username must include the domain name, as follows: `domain\username`.
6. Click **Install**.

Note

If the installer detects that a later version of a redistributable file is already installed, it does not install the earlier version that is included with ESI. The installer displays an error message to indicate a failure. If you get this message, click **Yes**.

7. Click **Finish**.
8. If you are using Active Directory Services, you must configure AD DS or AD LDS for ESI supported applications.

For more details, see [Setting up Directory Services integration for ESI applications](#) on page 24.

Note

The ESI installer tries to add a firewall exception rule to enable Remote Volume Management on the host where ESI is being installed. The installer also tries to enable the remote PowerShell (PS Remoting) on the same host. If the installer encounters a problem during these steps, ESI instructs you to perform these steps manually after the installation is complete.

Customizing the GUI view

The main ESI GUI window provides a view of the storage systems, hosts, host clusters, and applications added to ESI. You can customize the view.

The ESI interface has three panes:

- The left pane is the navigation pane.
- The center pane shows the details of the items selected in the navigation pane.
- The right pane is the **Actions** pane, which lists the possible actions based on the items selected in the navigation pane or the center pane.

Note

You can also select an item and then use the right-click menu to select an action.

Procedure

1. In the ESI GUI, select **View > Customize** from the menu bar.
2. Select or clear these check boxes from the **Customize view** dialog box.

Table 2 Customize view options

Check box	View displayed if selected
Console tree	Left navigation pane.
Standard menus (Action and View)	Top menu bar.
Standard toolbar	Icons in the second row of the menu bar. You can use the icons for navigation, and to show or hide the navigation and action panes.
Status bar	Status bar at the bottom of the Home window.
Description bar	Additional description at the top of a pane.
Taskpad navigation tabs	Not applicable.
Action pane	Right Actions pane.
Menus	Not applicable.
Toolbar	Not applicable.

3. To customize the center pane, such as to remove or add columns for a custom view, right-click a column and select actions from the menu.

By default, not all of the information is displayed for some lists due to space limitations.

4. Click the plus (+) or minus (-) symbol displayed next to a list item to expand or reduce the information displayed.
5. Use your mouse to adjust column width sizes.

Uninstalling ESI

Uninstall ESI before upgrading to a newer version of ESI or if ESI fails after an upgrade.

Procedure

1. Close all ESI applications, including ESI and the ESI PowerShell Toolkits.
2. In Windows Control Panel, open **Programs and Features**.
3. Perform one of the following and click **Uninstall**:
 - If you are upgrading from ESI version 4.1 or earlier, select the **EMC Storage Integrator** program.
 - If you are uninstalling ESI components from ESI version 5.0, perform one of the following:
 - To uninstall the ESI GUI only, select the **EMC Storage Integrator (x64) - GUI** program. The Powershell program is unaffected.
 - To uninstall the core ESI deployment, select the **EMC Storage Integrator (x64) - PowerShell** program. If the ESI GUI is installed, it is also uninstalled.

Note

The uninstaller does not remove either the local store file or the Active Directory user container.

Reinstalling ESI

Reinstall ESI to repair the installation or to modify the options that are currently installed.

For example, if you neglected to select ESI Service or a system adapter during the initial ESI installation, run the ESI PowerShell installer and then select the options.

If you are modifying options, reinstall the current version of ESI to the same installation path.

Procedure

1. If you plan to select either of the Active Directory options to publish connection information, remove all system connection settings before installing ESI:
 - a. Remove all systems from ESI. [Removing systems from ESI](#) on page 72 provides instructions.
 - b. Delete the following ESI settings file:

```
system drive:\Users\user name\AppData\Local\EMC\ESI\EMC
Storage Integrator.settings
```

2. Follow the instructions in [Installing ESI](#) on page 18.

Note

If the ESI GUI is installed in your deployment, run the ESI PowerShell installer first and then run the ESI GUI installer.

CHAPTER 3

Setting up connections

This chapter includes the following topics:

- [Setting up Directory Services integration for ESI applications](#)..... 24
- [Setting up AD DS](#)..... 24
- [Setting up AD LDS](#)..... 24
- [Configuring AD DS and AD LDS for ESI Service connections](#)..... 25
- [Configuring AD DS and AD LDS for ESI, MMC, and PowerShell connections](#).....25

Setting up Directory Services integration for ESI applications

ESI can store connection settings locally or persist connection settings in a central location by integrating with Microsoft Active Directory Domain Services (AD DS) or Microsoft Active Directory Lightweight Directory Services (AD LDS). The Microsoft Active Directory Services use the Lightweight Directory Access Protocol (LDAP) for both AD DS and AD LDS. You can use AD DS or AD LDS for all supported applications and systems, such as ESI, MMC, ESI Service, and SQL Server.

Microsoft TechNet provides instructions about how to install and set up [AD DS](#) and [AD LDS](#).

Setting up AD DS

Before you begin

To use AD DS with ESI, confirm that Windows Server (2016, 2012 R2, or 2012) Active Directory is installed on the Domain Controller of the AD domain.

Procedure

1. Confirm that you selected **Active Directory** in the **Publish Connection Information** window during the ESI installation.
2. Log in to the domain controller with domain administrator credentials.
3. Perform one of these procedures:
 - [Configuring AD DS and AD LDS for ESI Service connections](#) on page 25
 - [Configuring AD DS and AD LDS for ESI, MMC, and PowerShell connections](#) on page 25

Setting up AD LDS

Before you begin

To use AD LDS with ESI, confirm that Windows Server (2016, 2012 R2, or 2012) Active Directory is installed on the Domain Controller of the AD domain. Confirm that an AD LDS instance is installed on the Windows Server.

Procedure

1. Log in to the domain controller with domain administrator credentials.
2. During the AD LDS installation, set up the following application directory partition for ESI:
`DC=EMC, DC=Storage, DC=Integrator, DC-COM`
3. Confirm that you selected **AD LDS** in the **Publish Connection Information** window during the ESI installation.
4. Confirm that the AD LDS instance schema has definitions for **msDS-App-Configuration** and **msDS-Settings**. If not, extend the AD LDS schema to get them by generating an LDIF file with `ADSchemaAnalyzer.exe`. Refer to [Microsoft TechNet](#) for instructions.
5. Perform one of these procedures:

- [Configuring AD DS and AD LDS for ESI Service connections](#) on page 25
- [Configuring AD DS and AD LDS for ESI, MMC, and PowerShell connections](#) on page 25

Configuring AD DS and AD LDS for ESI Service connections

Procedure

1. Use ADSI Edit (`adsiedit.msc`) to create an ESI Service container in the ESI AD store. Use the name of the computer that is running ESI Service, such as `CN=ESIService1`.

This new container enables ESI Service to store persistence settings in the ESI AD store.

2. Perform one of these steps:
 - If ESI Service is running on a remote computer, grant full control permissions to the computer account.
 - If the directory service and ESI Service are running on the same computer, grant full control permissions to the network service account.

ESI Service runs as a network service.

Configuring AD DS and AD LDS for ESI, MMC, and PowerShell connections

Procedure

1. Use ADSI Edit (`adsiedit.msc`) to connect to the domain controller active directory and create a container for this ESI store.

For example, for `mydomain.corp.com`, create: `CN=ESI Object Connection Store, DC=mydomain, DC=corp, DC=com Distinguished Name`

`CN=ESI Object Connection Store, DC=mydomain, DC=corp, DC=com Distinguished Name`

2. Create a container in the ESI store container with the domain user name for each user.

For example, for User 1, create `CN=User1 Distinguished Name`.

3. Grant full control permissions for the users that own the ESI AD store.

CHAPTER 4

Configuring ESI Service

This chapter includes the following topics:

- [Setting up ESI Service for SCOM](#)..... 28
- [Changing HTTP connection defaults](#)..... 28
- [Viewing and setting up the security policy](#)..... 33
- [Changing the system refresh interval](#)..... 34

Setting up ESI Service for SCOM

The ESI PowerShell installer automatically enables a Windows firewall rule for the ESI Service, sets up the SSL certificate, and sets the service to listen to two IP ports on the ESI host system.

Before you begin

ESI and ESI Service must be installed. If you did not select ESI Service as an installation option, run the ESI PowerShell installer again to reinstall and select ESI Service. For more information, refer to [Reinstalling ESI](#) on page 21.

Procedure

1. If using Microsoft Active Directory services, confirm that you created an ESI Service user account within the Active Directory domain as described in [Setting up Directory Services integration for ESI applications](#) on page 24.
2. If necessary, change the HTTP connection defaults as described in [Setting up the Run As profile for the EMC SI Monitoring account](#) on page 39 and [Setting up the Run As profile for the EMC SI Service Monitoring account](#) on page 39.
3. Confirm that the correct HTTP connections are set up as described in [Changing HTTP connection defaults](#) on page 28.
4. Register or publish all applicable systems with the ESI Service as described in [Publishing storage systems](#) on page 72.
5. View and set up the security policy for the ESI Service as described in [Viewing and setting up the security policy](#) on page 33.
6. If necessary, change the security policy, which by default is set to every 30 minutes, as described in [Viewing and setting up the security policy](#) on page 33. This interval sets how often the ESI Service checks for registered systems and collects data about the registered systems and system components.

Changing HTTP connection defaults

By default, the installer sets up the HTTP port 54500 and HTTPS port 54501 connections. You can change the defaults for the ESI Service by using the following procedures:

- [Setting up new IP ports with a new domain certificate](#) on page 31
- [Setting up default IP ports with a new domain certificate](#) on page 30
- [Setting up new IP ports with a new domain certificate](#) on page 31
- [Confirming the HTTP connections](#) on page 33

Note

All of these procedures require a Windows command prompt and not a PowerShell command prompt.

Setting up new IP ports with the default certificate

Use the Windows command line to choose an available port for the default domain certificate.

Procedure

1. To delete the reserved URLs, on the ESI host computer, open a command prompt and type:

```
netsh http delete urlacl "http://+:54500/esi/"
netsh http delete urlacl "https://+:54501/esi/"
```

2. Choose new IP port numbers. To get a list of used IP ports for the ESI Service, on the ESI Service computer at a Windows command prompt, type:

```
netstat -an
```

The industry standard is to choose an available port that is between port numbers 49152 and 65535.

3. To reserve the new URLs, replace *HttpPort* and *HttpsPort* with the new port numbers by typing:

```
netsh http add urlacl url="http://+:HttpPort/esi/" user="NT
AUTHORITY\NETWORK SERVICE"

netsh http add urlacl url="https://+:HttpsPort/esi/" user="NT
AUTHORITY\NETWORK SERVICE"
```

For example:

```
netsh http add urlacl url="http://+:56560/esi/" user="NT
AUTHORITY\NETWORK SERVICE"

netsh http add urlacl url="https://+:57570/esi/" user="NT
AUTHORITY\NETWORK SERVICE"
```

4. Delete the existing firewall rule for default ports:

```
netsh advfirewall firewall delete rule name="ESI Service"
```

5. To add the new firewall rule for the new ports, type:

```
netsh advfirewall firewall add rule name="ESI Service" dir=in
action="allow" protocol="TCP" localport=HttpPort, HttpsPort
```

Replace *HttpPort* and *HttpsPort* with the new port numbers.

For example:

```
netsh advfirewall firewall add rule name="ESI Service" dir=in
action="allow" protocol="TCP" localport=<56560>,<57570>
```

6. To unbind the existing IP ports from the SSL certificate, type:

```
netsh http delete sslcert ipport=0.0.0.0:54501
```

7. To bind the ports with the new certificate, search and open **Manage computer certificates**.
8. Select **File > Add/Remove Snap-in**, select **Certificates**, and then click **Add**.
9. In the **Certificates snap-in** dialog box, select **Computer account**, click **Next**, select **Local computer**, and then click **Finish**.

10. In **Certificates (Local Computer) > Personal > Certificates**, double-click the new certificate to open it.
11. Select **Details**, select **Thumbprint**, and then highlight and copy the thumbprint.
12. At a command prompt, type:

```
netsh http add sslcert ipport=0.0.0.0:HttpsPort
certhash=Thumbprint appid="{4024FDC3-B30D-43CA-8707-
A50940B4BD14}"
```

In place of *Thumbprint*, paste the new certificate thumbprint and remove all spaces between the thumbprint numbers and letters. Replace *HttpsPort* with the applicable port number and keep **appid** the same.

For example:

```
netsh http add sslcert ipport=0.0.0.0:57570
certhash=0794721c36f00902c6b9b6cb687f7a6b2997925d
appid="{4024FDC3-B30D-43CA-8707-A50940B4BD14}"
```

13. To set the registry keys and change the ports, navigate to the **HKEY_LOCAL_MACHINE\SOFTWARE\EMC\WSI\Service** folder and change the value of the **Port** key to the new HTTP port number and the **SSLPort** value to the new HTTPS port number. For example:

```
Port: 12345    SSLPort: 23456
```

14. To restart the ESI Service, perform either step:

- Go to **Services** and restart the **ESI Service**
- Type:

```
net stop esiservice
net start esiservice
```

For details about the port setup, refer to [Confirming the HTTP connections](#) on page 33.

Setting up default IP ports with a new domain certificate

Use the Windows command line to associate ports after you create a new domain certificate.

Procedure

1. On the ESI host machine, create a new domain certificate.
Refer to your Windows documentation for more information.
2. To stop the ESI Service, open a Windows command prompt and type:

```
net stop esiservice
```
3. To unbind the existing IP ports from the ESI Service SSL certificate, type:

```
netsh http delete sslcert ipport=0.0.0.0:54501
```
4. To bind the ports with the new certificate, search and open **Manage computer certificates**.
5. Select **File > Add/Remove Snap-in**, select **Certificates**, and then click **Add**.
6. In the **Certificates snap-in** dialog box, select **Computer account**, click **Next**, select **Local computer**, and then click **Finish**.

7. In **Certificates (Local Computer) > Personal > Certificates**, double-click the new certificate.
8. Select **Details**, select **Thumbprint**, and then highlight and copy the thumbprint.
9. At a command prompt, type:

```
netsh http add sslcert ipport=0.0.0.0:54501 certhash=Thumbprint
appid="{4024FDC3-B30D-43CA-8707-A50940B4BD14}"
```

In place of *Thumbprint*, paste your new certificate thumbprint and remove all spaces between the thumbprint numbers and letters and keep **appid** the same.

For example:

```
netsh http add sslcert ipport=0.0.0.0:54501
certhash=0794721c36f00902c6b9b6cb687f7a6b2997925d
appid="{4024FDC3-B30D-43CA-8707-A50940B4BD14}"
```

10. To restart the ESI Service, at the Windows command prompt, type:

```
net start esiservice
```

For details about port setup, refer to [Confirming the HTTP connections](#) on page 33.

Setting up new IP ports with a new domain certificate

Use the Windows command line to choose an available port before you create a domain certificate.

Procedure

1. To delete the reserved URLs, on the ESI host computer, open a Windows command prompt and type:

```
netsh http delete urlacl "http://+:54500/esi/"
netsh http delete urlacl "https://+:54501/esi/"
```

2. Choose new IP port numbers. Get a list of used IP ports for the ESI Service, on the ESI Service computer at a Windows command prompt, type:

```
netstat -an
```

The industry standard is to choose an available port that is between port numbers 49152 and 65535.

3. To reserve the new URLs, type:

```
netsh http add urlacl url="http://+:HttpPort/esi/" user="NT
AUTHORITY\NETWORK SERVICE"
netsh http add urlacl url="https://+:HttpsPort/esi/" user="NT
AUTHORITY\NETWORK SERVICE"
```

Replace *HttpPort* and *HttpsPort* with the new port numbers.

For example:

```
netsh http add urlacl url="http://+:12345/esi/" user="NT
AUTHORITY\NETWORK SERVICE"
```

4. To delete the existing firewall rule for default ports, type:

```
netsh advfirewall firewall delete rule name="ESI Service"
```

5. To add the new firewall rule for the new ports, type:

```
netsh advfirewall firewall add rule name="ESI Service" dir=in
action="allow" protocol="TCP" localport=HttpPort, HttpsPort
```

Replace *HttpPort* and *HttpsPort* with the new port numbers

For example:

```
netsh advfirewall firewall add rule name="ESI Service"
dir=in action="allow" protocol="TCP" localport=56560,57570
```

6. To unbind the existing default IP ports from the SSL certificate, type:

```
netsh http delete sslcert ipport=0.0.0.0:54501
```

7. Create a domain certificate. Refer to Windows documentation for more information.
8. To bind the ports with the new certificate, search and open **Manage computer certificates**.
9. Select **File > Add/Remove Snap-in**, select **Certificates**, and then click **Add**.
10. In the **Certificates snap-in** dialog box, select **Computer account**, click **Next**, select **Local computer**, and then click **Finish**.
11. In **Certificates (Local Computer) > Personal > Certificates**, double-click the new certificate.
12. Select **Details**, select **Thumbprint**, and then highlight and copy the thumbprint.
13. At a command prompt, type:

```
netsh http add sslcert ipport=0.0.0.0:HttpsPort
certhash=Thumbprintappid="{4024FDC3-B30D-43CA-8707-
A50940B4BD14}"
```

In place of *Thumbprint*, paste the new certificate thumbprint and remove all spaces between the thumbprint numbers and letters. Also, replace *HttpsPort* with the applicable port number and keep **appid** the same

For example:

```
netsh http add sslcert ipport=0.0.0.0:57570
certhash=0794721c36f00902c6b9b6cb687f7a6b2997925d
appid="{4024FDC3-B30D-43CA-8707-A50940B4BD14}"
```

14. To set the registry keys and change the ports, navigate to the **HKEY_LOCAL_MACHINE\SOFTWARE\EMC\WSI\Service** folder and change the value of the **Port** key to the new HTTP port number and the **SSLPort** value to the new HTTPS port number. For example:

```
Port: 56560    SSLPort: 57570
```

15. To restart the ESI Service, perform one of the following steps:

- Go to **Services** and restart the **ESI Service**.
- Type:

```
net stop esiservice
net start esiservice
```

For details about the port setup, refer to [Confirming the HTTP connections](#) on page 33.

Confirming the HTTP connections

Procedure

1. Open a web browser that supports Windows Authentication and browse to the ESI Service console with the applicable IP port numbers:
 - For an HTTP connection with the default IP port numbers, go to `http://ESI Service IP:54500/esi/console`, replacing *ESI Service IP*.
 - For an HTTP connection with new port numbers, replace *ESI Service IP* and *new HTTP port*, and go to `http://ESI Service IP.new HTTP port/esi/console`, replacing *ESI Service IP*.
 - For a secured HTTPS connection with the default IP port numbers, go to `https://ESI Service IP:54501/esi/console`, replacing *ESI Service IP*.
 - For a secured HTTPS connection with new port numbers, go to `https://ESI Service IP.new HTTPS port/esi/console`, replacing *ESI Service IP* and *new HTTPS port*.
2. In the Services applet on the ESI host system, confirm that the ESI Service is installed and started as a network service.
3. On the ESI host system, confirm that the **ESIService-SSL** or **your new domain certificate** is listed in the `\Personal\Certificates` folder on the local computer. Refer to at [How to: View Certificates with the MMC Snap-in](#) for information about how to view certificates.
4. On the host, open the **Start** menu and search for **firewall** to locate the Windows firewall.
5. In the search results, select **Windows Firewall with Advanced Security**.
6. Select **Inbound rules**, and confirm that **ESI Service** is listed and enabled as the new ESI Service firewall rule for the default 54500 and 54501 ports or your new port numbers.
7. After confirming HTTP connections, publish systems to the ESI Service. See [Publishing storage systems](#) on page 72.

Viewing and setting up the security policy

The ESI Service authorizes every API call based on the Windows identity of the caller. Authorization is granted based on the caller's role membership.

The ESI Service defines the following Service roles. If these roles are changed, the ESI Service does not work.

- Administrator role group members can run configuration commands on the ESI Service and query the Entity Graph for discovered systems and system components.
- Monitor role group members can only query the Entity Graph to view discovered systems and system components and set the system refresh interval policy.
- The ESI Service Administrator can add principal names (security groups or users) to one of these ESI Service roles. Adding a security principal to a Service role enables the administrator to delegate access control to one or more users who can add or modify members of the group. After you add the group to the Monitor role, any user who belongs to this group can make an ESI Service call.

Note

As an exception to the role assignments, the ESI Service automatically grants the Administrator role to the local administrator group on the host that is running the ESI Service. Any local administrator can manage the ESI Service without being explicitly added. However, if User Account Control (UAC) is enabled, the user must be running elevated credentials.

View the security policy

You can view the security policy in one of the following ways:

- Open a web browser that supports Windows Authentication and browse to the ESI Service console. If you have changed the default port numbers, replace the following default numbers with the assigned ports:
 - For an HTTP connection, go to `http://localhost:54500/esi/console`.
 - For a secured HTTPS connection, go to `https://localhost:54501/esi/console`.
- At a PowerShell command prompt, type the following and then press Enter:


```
Get-EmcServicePolicy
```

Set the security policy for a user

At a PowerShell command prompt, type the following, using the applicable domain name and principal name that you want to add to the Monitor role, and then press Enter:

```
Add-EmcUser "domain name\principal name" Monitor
```

Note

If the principal name is invalid, the cmdlet fails. Also, if you want to add the principal name to the Administrator role, replace Monitor in the command with Administrator.

After setting up the security policy, you can change the refresh interval. See [Changing the system refresh interval](#) on page 34.

Changing the system refresh interval

The System Refresh Interval setting enables you to set how often the ESI Service polls all registered storage systems and populates the entity graph with all discovered storage systems and system components. The ESI Management Packs use this information to confirm and update to the most current data about discovered components.

By default, this interval is set to poll the storage systems every 30 minutes for new information. This setting, combined with the ESI Monitoring management pack interval number, sets the frequency for receiving monitor updates in SCOM. For example, if this interval is set to 30 minutes and the ESI Monitoring interval override is set to 10 minutes, an updated health state can take up to 40 minutes. The time intervals can affect the data performance. [Changing discovery interval overrides](#) on page 148 provides details about the Monitor interval override.

To change the system refresh interval for the ESI Service:

Procedure

1. Open a PowerShell command prompt, type this command, and then press Enter to import the ESI Service PowerShell module:

```
Import-Module ESIServicePSToolkit
```

2. Type this command and press Enter to get the current setting in minutes:

```
Get-EmcServicePolicy
```

3. Type this command, replacing 30 with the preferred number of minutes, and then press Enter:

```
Set-EmcServicePolicy -RefreshIntervalInMinutes 30
```


CHAPTER 5

Installing and configuring ESI SCOM Management Packs

This chapter includes the following topics:

- [Installing ESI SCOM management packs](#).....38
- [Setting up ESI SCOM Management Packs](#).....38
- [Confirming the connection between SCOM agents and the ESI Service](#).....39
- [Setting up the Run As profile for the EMC SI Monitoring account](#)..... 39
- [Setting up the Run As profile for the EMC SI Service Monitoring account](#).....39
- [Setting up the SCOM agent registry](#).....40
- [Setting up optional ESI Service discovery overrides](#)..... 40
- [Setting up the required ESI Service Host override and discovery](#).....42

Installing ESI SCOM management packs

Install the ESI SCOM management packs on the SCOM Management Group that is connected to the ESI SCOM monitoring agents.

The ESI SCOM agents are connected to the same Windows domain as the ESI host system that has the ESI Service installed.

Procedure

1. On the SCOM Management Group server that is connected to the ESI SCOM agents, download the ESI Zip file.
2. In the ESI Zip file, locate and double-click `ESI.SCOM.ManagementPacks.5.*.Setup.msi`.

The management pack files are installed by default to the `C:\Program Files (x86)\EMC\ESI SCOM Management Packs` folder.

3. On the **Administration** tab of the SCOM console, right-click and click **Export**.
4. Export `EMC Storage Integrator Customization.xml`.
5. Import the latest version of each ESI management pack file in SCOM.

Note

For more information about how to import the management packs, refer to [How to Import an Operations Manager Management Pack](#) on Microsoft TechNet .

6. Right-click and then click **Import**.
7. Import `EMC Storage Integrator Customization.xml`, which you exported in a previous step.

Setting up ESI SCOM Management Packs

Before you begin

Ensure that you have completed the steps in [Installing ESI SCOM management packs](#) on page 38.

Procedure

1. See [Confirming the connection between SCOM agents and the ESI Service](#) on page 39 to confirm the connection.
2. See [Setting up the Run As profile for the EMC SI Monitoring account](#) on page 39 to access the ESI Service.
3. If necessary, set up optional discovery overrides. For more information, refer to [Setting up optional ESI Service discovery overrides](#) on page 40.
4. Complete the steps in [Setting up the required ESI Service Host override and discovery](#) on page 42 to set up the host and enable discovery of the ESI Service.
5. For additional monitoring of the ESI Service, see [Setting up the Run As profile for the EMC SI Service Monitoring account](#) on page 39 to set up the monitoring account.
6. See [Using the ESI Monitoring Management Pack](#) on page 141 to set up the management packs.

After you complete these setup steps, refer to [Setting up optional management pack overrides](#) on page 147 for information about optional overrides.

Confirming the connection between SCOM agents and the ESI Service

Before setting up the SCOM agents, confirm the connection between the SCOM agents and ESI Service.

Procedure

1. On the SCOM Agent computer, open this link:

```
https://ESI Service IP:HttpsPort/esi/console/graph/Entities?
class=StorageSystem.
```

 Replace *ESI Service IP* and *HttpsPort* with the applicable values.
2. Confirm that the load time displayed at the bottom of the page is less than one second and make sure the results are consistent.

Setting up the Run As profile for the EMC SI Monitoring account

Create an EMC SI Monitoring account Run As profile for a each SCOM agent that connects to ESI Service.

Refer to [Microsoft TechNet](#) for detailed instructions.

Procedure

1. Create a Windows Run As account from the Windows account that is used in the Monitoring Role for the ESI Service.
2. In the EMC SI Monitoring account, assign the Windows Run As account to the related SCOM agent that will connect to the ESI Service.

Setting up the Run As profile for the EMC SI Service Monitoring account

Set up an EMC SI Service (ESI Service) Monitoring account Run As profile to monitor the ESI Windows Service. If you install a SCOM agent on the ESI controller host, this agent can discover and monitor the health state of the ESI Service.

The SCOM agent periodically checks if the ESI Service is running and checks the application event log for any events that are written by the ESI Service. This agent also raises alerts if the ESI Service is not running, if any events that indicate problems with the ESI Service occur, or if any expected events are not received.

Some errors are only detected and reported with a SCOM agent that is installed on the ESI host controller.

If the SCOM environment uses a Default Action account that is a local administrator, then the action account has the necessary settings.

However, if the SCOM environment uses a low privilege account as the Default Action account, you might need to use a special account to monitor the ESI Service. If you

do, work with a SCOM administrator to create the Run As account. You might also need to create a Windows account to monitor the service.

The SCOM account that monitors the ESI Service must have the **Allow log on locally** option enabled to read the Application Event log and use Windows Management Instrumentation (WMI) to query the status of the service.

Refer to SCOM documentation on Microsoft TechNet for details about agent installation considerations and instructions.

Setting up the SCOM agent registry

Before enabling the discovery of ESI Service, change Value to decimal 5120 in the following registry key for each SCOM agent that will monitor EMC systems.

Procedure

1. Open Windows Registry Editor.
2. Locate the following subkey:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
\HealthService\Parameters\Persistence Version Store Maximum
Type: REG_DWORD
Name: Persistence Version Store Maximum
Value: Number of 16-kilobyte pages
```

3. Change the value to decimal 5120.

Setting up optional ESI Service discovery overrides

Based on the specific environment, set up optional discovery overrides, such as:

- [Setting up a system filter file](#) on page 41
- [Setting up the HTTP proxy](#) on page 41
- [Changing the HTTPS to HTTP override](#) on page 41
- Setting an override to ignore the client certificate when the SCOM agent connects to the ESI Service. To set up this override, follow the steps in [Changing the HTTPS to HTTP override](#) on page 41 and set the **Ignore Certificate Error** override to **True**.
- Setting basic authentication overrides.
If one or more SCOM agents are not on the same domain or trusted domain as the ESI Service, use basic authentication. To use basic authentication, set up the User Name and Password overrides for the EMC SI Service Discovery.

Note

This override is a data security risk. Because SCOM stores the username and password as text, any user with SCOM console access or access to the file system on the agent can view and hijack the account credentials. If you set up the basic authentication overrides, secure the SCOM agents to avoid this risk.

After setting up these optional overrides, then set up the required ESI Service Host override.

Setting up a system filter file

If more than one SCOM agent connects to one or more ESI Services, set up a system filter file for each SCOM agent. The filter file tells the SCOM agent which system to monitor.

This text file must be set up on each SCOM agent with the ESI Service Registered Systems Friendly Name for all the supported systems. Confirm that each system appears in a single list.

Procedure

1. On the SCOM agent, open Notepad.
2. Type the **ESI Service Registered Systems Friendly Name** of each supported system that this agent monitors. Use one name per line in the text file.
3. Save the file to a location on the SCOM agent machine. Confirm that the Windows domain account set up in the **Run As Account** has at least read access to this file.
4. Enter the full path to this file in the **Filter File Path** override field for the ESI Service Discovery management pack.

Setting up the HTTP proxy

If the SCOM agent must connect to the ESI Service through a web proxy server, provide the following information for the Proxy Server and Bypass List overrides in the EMC SI Service Discovery for each related SCOM agent:

- **Proxy server:** proxy server string. For example:
`proxy_server:80`
- **Bypass List:** domain bypass list string. For example, the following represents that the discovery can bypass the proxy server when the host name ends with `.emc.com`:
`. *.emc.com`
- If the overrides above are not set, then the proxy settings are obtained from the registry. This assumes the proxy configuration tool, `Proxycfg.exe` has been run. If `Proxycfg.exe` has not been run, then the ESI Service can be accessed directly.

Changing the HTTPS to HTTP override

The SCOM agent always tries to connect to the ESI Service by using an HTTPS connection. By default, if the HTTPS connection fails, the SCOM agent cannot communicate with the ESI Service.

To connect with an HTTP connection instead of an HTTPS connection, set the **HTTPS to HTTP Override** to **True** for the ESI Service connection.

Note

If you set the override, secure the SCOM agents. With this override, SCOM sends the username and password as text, which can be hijacked. This option is a data security risk.

Procedure

1. Open the SCOM Operations Console and connect to the SCOM Management Group.

2. From the menu bar, select **Go > Authoring**.
3. In the left pane, select **Object Discoveries**.
4. Locate and double-click **EMC SI Service Discovery**.
5. Open the **Overrides** properties and select **Override > For a specific object of class: Windows Computer**.
6. In the **Select Object** dialog box, select the SCOM proxy agent that you want to connect to the ESI Service, and then click **OK**.
7. Select the **Override** checkbox for HTTPS to HTTP Fallback to enable the override.
8. Change the value of the **Override Value** field to **True** and then click **OK**.
9. Click **Close** to save the change.

Setting up the required ESI Service Host override and discovery

Set up the ESI Service Host override and enable the discovery of the ESI Service for each SCOM agent.

Before you begin

Perform this procedure after:

- [Setting up the SCOM agent registry](#) on page 40
- [Setting up optional management pack overrides](#) on page 147

Procedure

1. Open the SCOM Operations Console and connect to the SCOM Management Group.
2. From the menu bar, select **Go > Authoring**.
3. In the left pane, select **Object Discoveries**.
4. Locate and double-click **EMC SI Service Discovery** and the **EMC SI Service Discovery Properties** page appears.
5. Click **Overrides** and select **Override > For a specific object of class: Windows Computer**.
6. In the **Select Object** dialog box, select the SCOM proxy agent that you want to connect to the ESI Service from the list and click **OK**.
The **Override Properties** page appears.
7. Confirm the **Enabled** parameter name override is selected and that the override value is set to **True**.
8. Change the override value for the **ESI Service Host** parameter to the IP address of the computer hosting the ESI Service.
9. If the default port number of 54500 or 54501 for the ESI Service has been changed, change the port parameter default value to the correct port number.
10. In the **Select destination management pack** list box, select the **EMC Storage Integrator Customizations** management pack.
11. Click **Apply** and confirm the changed values.
12. Click **OK**.

Note

If you change the Interval or Discovery Timeout (sec) values, discovery performance might be affected.

13. After completing this setup, export and save a copy of the `EMC.SI.Customization.xml` file as a backup of your customization values. If you lose a needed customization, you can import this backup copy to recover your set customizations. This file is installed with version number 1.0.0.0. You can increment the version number when you make changes.
-

Note

For more information about creating overrides, refer to [How to Override a Rule or Monitor](#) on Microsoft TechNet .

CHAPTER 6

Managing storage with the PowerShell Toolkits

This chapter contains the following topics:

- [Getting started with the ESI PowerShell toolkits](#)..... 46
- [Getting help at the Windows PowerShell command line](#).....46
- [Using PowerShell objects](#).....46
- [Adding Vblock Systems and VxBlock Systems](#) 47
- [PowerShell examples](#)..... 48
- [ESI PowerShell cmdlet list](#)..... 51

Getting started with the ESI PowerShell toolkits

The ESI PowerShell Toolkit provides cmdlets to provision block storage and to manage:

- Microsoft SQL Server and EMC RecoverPoint
- Addition of Vblock Systems and VxBlock Systems, and ScaleIO storage systems
- Connections to host and storage systems
- Disk devices in hypervisor environments, such as VMware vSphere and Microsoft Hyper-V
- Block device snapshots for EMC VNX, VNXe, and Unity storage systems
- XtremIO snapshots and EMC RecoverPoint profiles

The ESI Service PowerShell Toolkit provides cmdlets for setting up the ESI Service for use with the ESI System Center Operations Manager (SCOM) Management Packs.

The toolkit provides cmdlets for setting up the ESI Service to:

- Get the storage system entity data and entity relationships for the entity graph
- Configure service security
- Register EMC storage systems

[ESI PowerShell cmdlet list](#) on page 51 provides links to the cmdlets based on functionality.

Getting help at the Windows PowerShell command line

Detailed cmdlet information is available at the Windows PowerShell command line.

Type the following from the Windows PowerShell command line, replacing *cmdlet name* with a specific cmdlet name:

```
get-help cmdlet name -full
```

For example, for help about the `Get-EmcLun` cmdlet, type the following at the PowerShell command line:

```
get-help Get-EmcLun -full
```

Using PowerShell objects

The ESI PowerShell toolkits accept objects as inputs, which can be standard objects, such as strings and integers. In many instances, these inputs have useful properties that can be accessed using dot notation. A full list of these objects and their properties is beyond the scope of this topic.

Defining and accessing variables

PowerShell enables you to create objects and store them in variables. For example, an ESI LUN object can be created and stored in a variable by using the `Get-EmcLun` command:

```
$lun = Get-EmcLun "My LUN"
```

This LUN object is used with the `Set-EmcLunAccess` cmdlet to present the LUN to a host:

```
Set-EmcLunAccess -LUN $lun -HostSystem $myhost -Available
```

Retrieving object information

Use the `Get-Member` cmdlet to access information about the properties and methods supported by an object. The `Get-Member` cmdlet accepts pipeline inputs. You can pipe an object returned by a cmdlet to `Get-Member` to determine the properties and methods of the object.

Standard object descriptions

The following table lists common PowerShell objects.

Object	Description
Boolean	Represents a true or false value. For true, type 1 or \$true. For false, type 1 or \$false.
Int32	Represents a 32-bit signed integer. Signed integers are either positive or negative.
Int64	Represents a 64-bit signed integer. Signed integers are either positive or negative.
SecureString	Represents an encrypted string for private data.
String	Represents a set of alphanumeric characters. A string that contains the space character must be enclosed by quotation marks. For example: <code>Get-EmcLun "My Basic LUN"</code>
UInt32	Represents a 32-bit unsigned integer. Unsigned integers cannot be negative.
UInt64	Represents a 64-bit unsigned integer. Unsigned integers cannot be negative.

Adding Vblock Systems and VxBlock Systems

Use the ESI PowerShell Toolkit to add Vblock Systems and VxBlock Systems for SCOM support.

Vblock Systems and VxBlock Systems are converged infrastructures, which are pre-configured, pre-assembled, and pre-tested with all components delivered as a single product.

Procedure

1. At the PowerShell command line, type the `Add-EmcSystem` cmdlet and provide the following parameters:

Parameters	Description
friendlyName	A short name for the system that is unique
systemType	VCESystem
Username	Username for the system
Password	Password for the system
FDQN	Fully Qualified Domain Name (FQDN) of the MSM system. For example: <code>vision234-56.vb700qa.vce.lab</code>

Parameters	Description
Port	The default port number is automatically set. If the field is empty, leave it empty to use the default port.

2. Add *IP Address FQDN SystemName* to the `etc\host` file.

For example:

```
10.1.234.56 vision234-56.vb700qa.vce.lab
vision234-56.vb700qa.vce.lab
```

PowerShell examples

Provisioning a storage volume

This example shows how to provision a new storage volume by using ESI PowerShell cmdlets.

Steps to provision the storage volume include:

- Create a new 100 GB thin LUN in a storage pool.
- Present the LUN to a Windows host and initialize the disk.
- Create an NTFS volume and mount it on an available drive letter.

The following example requires that the storage system and host are connected and available.

Example script

```
PS C:\Users\administrator.BROOKSDOM> import-module esipstoolkit
```

```
PS C:\Users\administrator.BROOKSDOM> $pool = Get-EmcStoragePool "VM
Pool"
```

```
Block storage system: [Name = APM00111102550. UserFriendlyName =
VNX5100]. Lun Pools are not initialized. Refreshing Lun Pools.
```

```
PS C:\Users\administrator.BROOKSDOM> $system = Get-EmcHostSystem NEC-
BLADE6
```

```
PS C:\Users\administrator.BROOKSDOM> $lun = New-EmcLun -Pool $pool -
CapacityInMB 102400 -Thin
```

```
TaskStatus: Started
10% : Creating the LUN...
100% : The specified LUN has been created...
TaskStatus: Completed
```

```
PS C:\Users\administrator.BROOKSDOM> Set-EmcLunAccess -Lun $lun -
HostSystem $system -Available
```

```
TaskStatus: Started
10% : Unmasking the LUN to the specified host(s)...
100% : The specified LUN has been unmasked to the specified
initiators...
TaskStatus: Completed
```

```
PS C:\Users\administrator.BROOKSDOM> $hdisk=Get-EmcHostDisk -
```

```
Host: NEC-BLADE6. Refreshing MultiPath software information.
Host: NEC-BLADE6. Retrieving disk information from Virtual Disk
Service.
WARNING: Unable to find host disk(s) with the given parameters
```

```
PS C:\Users\administrator.BROOKSDOM> $hdisk=Get-EmcHostDisk -
HostSystem $system -Lun $lun
```

```
PS C:\Users\administrator.BROOKSDOM> Initialize-EmcHostDisk -
HostSystem $system -HostDisk $hdisk -PartitionStyle GPT
```

```
TaskStatus: Started
10% : Initializing the disk...
100% : The specified disk has been initialized...
TaskStatus: Completed
```

```
PS C:\Users\administrator.BROOKSDOM> $vol =New-EmcVolume -HostSystem
$system -HostDisk $hdisk -FileSystemType NTFS -Labe
```

```
l TestVolume
TaskStatus: Started
10% : Provisioning the volume...
100% : The specified volume has been provisioned...
TaskStatus: Completed
```

```
PS C:\Users\administrator.BROOKSDOM> Get-EmcAvailableDriveLetter -
HostSystem $system
```

```
A, B, D, E, F, ... (up to Z, except for default C)
```

```
PS C:\Users\administrator.BROOKSDOM> Set-EmcVolumeMountPoint -
HostSystem $system -Volume $vol -DriveLetter Z
```

```
TaskStatus: Started
10% : Mounting the volume...
100% : The specified volume has been mounted...
TaskStatus: Completed
PS C:\Users\administrator.BROOKSDOM>
```

Removing a storage volume

Remove a volume from a host and delete the LUN where it resides.

Because the LUN identity might be unknown, map the Windows volume to the storage LUN.

Example script

```
PS C:\Users\administrator.BROOKSDOM> import-module esipstoolkit
PS C:\Users\administrator.BROOKSDOM> $system = Get-EmcHostSystem NEC-
BLADE6
```

```
PS C:\Users\administrator.BROOKSDOM> $vol = Get-EmcHostVolume -
HostSystem $system -ID TestVolume
```

```
Host: NEC-BLADE6. Refreshing MultiPath software information.
Host: NEC-BLADE6. Retrieving disk information from Virtual Disk
Service.
```

```
PS C:\Users\administrator.BROOKSDOM> $hdisk = Get-EmcHostDisk -Volume $vol
```

```
PS C:\Users\administrator.BROOKSDOM> $lun = Get-EmcLUN -HostDisk $hdisk
```

```
Associating the specified host disk with its corresponding storage system...
PS C:\Users\administrator.BROOKSDOM> Remove-EmcVolumeMountPoint -HostSystem $system -Volume $vol
TaskStatus: Started
10% : Unmounting the volume...
100% : The specified volume has been unmounted...
TaskStatus: Completed
```

```
PS C:\Users\administrator.BROOKSDOM> Set-EmcHostDiskOnlineState -HostDisk $hdisk -Offline
```

```
TaskStatus: Started
10% : Bringing the disk offline...
100% : The specified disk has been brought offline...
TaskStatus: Completed
```

```
PS C:\Users\administrator.BROOKSDOM> Set-EmcLunAccess -HostSystem $system -Lun $lun -Unavailable
```

```
TaskStatus: Started
10% : Masking the LUN from the initiators...
100% : The specified LUN has been masked from the specified initiators...
TaskStatus: Completed
```

```
PS C:\Users\administrator.BROOKSDOM> Update-EmcSystem -HostSystem $system
```

```
Refreshing disks of host system '[Name: NEC-BLADE6, IP address: 172.20.1.106.]'
Host: NEC-BLADE6. Refreshing MultiPath software information.
Host: NEC-BLADE6. Retrieving disk information from Virtual Disk Service.
```

```
PS C:\Users\administrator.BROOKSDOM> Remove-EmcLun -Lun $lun
```

```
Confirm
Are you sure you want to perform this action?
Performing operation "Remove-EmcLun" on Target "LUN 44".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):
```

y

```
TaskStatus: Started
10% : Destroying the LUN...
100% : The specified LUN has been destroyed...PS C:\Users\administrator.BROOKSDOM>
TaskStatus: Completed
```

ESI PowerShell cmdlet list

This topic lists the available ESI PowerShell cmdlets, grouped by operation type.

To get syntax, parameters, and examples for a specific cmdlets, type the following at the PowerShell command prompt:

```
get-help cmdlet name -full
```

The cmdlets support these operations:

- [Connection operations](#)
- [Storage system operations](#)
- [Host operations](#)
- [Hypervisor operations](#)
- [RecoverPoint replication operations](#)
- [ESI Service operations](#)

PowerShell cmdlets connection operations

Connect-EmcSystem

Connects or adds the host, cluster, and storage systems to ESI from the specified creation BLOB. You can use this cmdlet along with the `Get-EmcHostSystemCredential`, `Get-EmcClusterSystemCredential`, and `Get-EmcStorageSystemCredential` cmdlets to get the creation BLOB.

Disable-EmcPublisherCertificateValidation

Disables server secure channel (SSL) certificate validation when using SSL to communicate with the specified ESI service. The publish commands use SSL when connecting to the specified ESI service by specifying an HTTPS URL in the `Set-EmcPublisherEndpointUrl` cmdlet or with the `-ServiceURL` parameter. This command disables the validation of the server certificate while establishing the SSL connection. This is necessary if the specified ESI service is configured to use a self-signed certificate.

Enable-EmcPublisherCertificateValidation

Enables server `Disconnect-EmcHostSystemSSL` certificate validation when using a secured channel (SSL) to communicate with the specified ESI service. The publish commands use SSL when connecting to the specified ESI service by specifying an HTTPS URL in the `Set-EmcPublisherEndpointUrl` cmdlet or with the `-ServiceURL` parameter. This command disables the validation of the server certificate while establishing the SSL connection. This is necessary if the specified ESI service is configured to use a self-signed certificate.

Disconnect-EmcClusterSystem

Disconnects cluster systems.

Disconnect-EmcHostSystem

Disconnect host systems.

Disconnect-EmcStorageSystem

Disconnects storage systems.

Disconnect-EmcSystem

Disconnects clusters, hosts, and storage systems.

Get-EmcClusterSystemCredential

Displays the encrypted connection string or BLOB, based on the specified parameters. You can use this cmdlet with the `Connect-EmcSystem` cmdlet to connect cluster systems to ESI. The `Get-EmcClusterSystemCredential` cmdlet creates a BLOB or encrypted string that is based on the specified parameters. The cmdlet prompts you to specify the cluster name, IP address, and credentials. The cmdlet then creates a BLOB with these credentials. You can also click **Test Connection** in ESI to test the connection with the specified parameters. Current Credential is selected by default for authentication. If you are using another credential, click **Specify Credential** and type the username and password.

Get-EmcLinuxHostSystemCredential

Displays the encrypted connection string or BLOB, based on the specified connection (system object creation) parameters for a Linux system. Use the BLOB with the `Connect-EmcSystem` cmdlet to connect or add Linux host systems to ESI. This cmdlet creates a BLOB (encrypted string) from the specified connection (system object creation) parameters. It prompts for host name, IP address, and connection. Password authentication is a default selection. If you are using key-based authentication, then use the key-based username, file path, and pass phrase.

Get-EmcPublisherConnectionInfo

Displays the systems that are currently registered with the specified ESI service.

Get-EmcPublisherEndpointOptions

Displays the current options that are used to connect to the specified ESI service.

Get-EmcPublisherSupportedSystem

Displays the system types that are available for registration with the specified ESI service.

Get-EmcHostSystemCredential

Displays the encrypted connection or system object creation parameters BLOB, which you can use along with the `Connect-EmcSystem` cmdlet to connect host systems to ESI.

Get-EmcStorageIntegratorVersion

Displays ESI version details including: product name, product version, and company name.

Get-EmcStorageSystemCredential

Displays the encrypted connection or system object creation parameters BLOB, which is used along with the `Connect-EmcSystem` cmdlet to connect storage systems to ESI.

Get-EmcSupportedSystemsCreationRequirement

Displays the creational parameters that are required to add or connect to a system in ESI.

Publish-EmcPublisherConnectionInfo

Publishes the connection information of the specified system to the specified ESI service.

Publish-EmcPublisherUserConnectionInfo

Publishes the connection information for the specified system to the specified user.

Set-EmcPublisherEndpointUrl

Sets the URL to the specified ESI service on the current session.

Test-EmcSystemConnectedToBlockStorageSystem

Verifies the connectivity of a host system or replication system to a block storage system. This cmdlet only works with VNX and VMAX block storage systems. The cmdlet does not work with VNXe storage systems.

Unpublish-EmcPublisherConnectionInfo

Unpublishes the connection information for the specified system to the specified ESI service. This cmdlet unregisters the specified system from the specified ESI service.

Update-EmcSystem

Updates the specified host, storage, or cluster systems. For the host system, the cmdlet updates the host disks. For the cluster system, it updates the cluster disks. For the block storage system, it updates the LUNs.

PowerShell cmdlets storage system operations

This section lists FAST VP, Meta management, and general storage system operations.

FAST VP Operations

Add-EmcFastVpPolicy

Adds or associates the specified storage group to the specified FAST VP policy.

Add-EmcLunsToVmaxStorageGroup

Adds one or more LUNs to the specified VMAX storage group. Clears the host disk signatures and assigns new ones.

Get-EmcFastVpPolicy

Displays the FAST VP policies that are associated with the specified storage system or VMAX storage group.

Get-EmcStorageTier

Displays the storage tiers for the specified storage system or the specified FAST VP policy.

Get-EmcVmaxStorageGroup

Displays all storage groups for the specified VMAX storage system.

New-EmcVmaxSnapshot

Creates a VMAX3 snapshot.

New-EmcVmaxStorageGroup

Adds LUNs to the specified VMAX storage group.

Remove-EmcFastVpPolicy

Removes the specified FAST VP policy from the specified storage groups.

Remove-EmcLunsFromVmaxStorageGroup

Removes LUNs from a VMAX storage group.

Remove-EmcVmaxSnapshot

Removes or deletes the specified VMAX3 snapshot.

Restore-EmcVmaxSnapshot

Restores a VMAX3 snapshot back to its source.

Remove-EmcVmaxStorageGroup

Deletes the specified storage group that is not associated to any FAST VP policies.

Meta management operations

Expand-EmcCompositeLun

Expands capacity of the composite LUN.

Get-EmcAvailableCandidatesForLunComposition

Displays all the LUNs which are qualified to be a member LUN of the specified meta, meta volume, or composite LUN.

Get-EmcCompositeLun

Displays all composite LUNs from the specified storage system.

Get-EmcCompositeLunMember

Displays one or more meta or composite LUN members of the specified composite LUN head.

Get-EmcUnboundLun

Displays all the unbound LUNs that are not bound to any storage pool from the specified storage system.

New-EmcCompositeLun

Creates a meta or composite LUN from the specified LUNs. To compose or form a meta or composite LUN, at least two LUNs are required and the first LUN becomes the metahead.

Remove-EmcCompositeLun

Removes (destroys) the composite LUN from the storage system.

General storage system operations

Add-EmcUnityConsistencyGroupMember

Adds one or more members to a consistency group. A consistency group has three types of members: LUNs, hosts that have access to LUNs in the group, and hosts that have access to snapshots of LUNs in the group. This command is used to add any of these members to the consistency group. This command is applicable only for Unity systems.

Add-EmcVnxeLunGroupMember

Adds one or more members to a LUN group. A LUN group has three types of members: LUNs, hosts that have access to LUNs in the group, and hosts that have access to snapshots of LUNs in the group. This command is used to add any of these members to the LUN group. This command is applicable only for VNXe3200 systems.

Add-EmcVplexConsistencyGroupVirtualVolume

Adds a VPLEX virtual volume to a specified VPLEX consistency group.

Add-EmcXtremIOConsistencyGroupVolume

Adds XtremIO volumes to a specified XtremIO consistency group.

Add-EmcXtremIOtagEntity

Adds the specified tag to the specified consistency groups, initiators, initiator groups, snapshots, snapshot sets, and volumes.

Copy-EmcVnxAdvancedSnapshot

Copies VNX advanced snapshot to a new VNX advanced snapshot.

Dismount-EmcUnitySnapshot

Dismounts a Unity LUN or consistency group snapshot to prevent host access.

Dismount-EmcVnxAdvancedSnapshot

Dismounts or detaches the VNX advanced snapshot with its associated snapshot mount point LUN.

Dismount-EmcVnxSnapshot

Dismounts a VNXe LUN or LUN group snapshot to prevent host access.

Expand-EmcFileBasedDisk

Expands the size of a file-based disk.

Expand-EmcLun

Expands the capacity of a LUN.

Expand-EmcSharedFolderPool

Expands the capacity of a shared folder pool on VNX-File and VMAX eNAS file systems.

Get-EmcFileStoragePool

Displays VMAX eNAS and VNX-File shared folder pools.

Get-EmcLun

Displays the LUNs for the specified storage system or systems.

Get-EmcLunMaskingView

Displays LUN masking views. A LUN masking view object contains the information that a set of LUNs are unmasked to a set of initiators and the corresponding HLU (host logical unit) information of the unmasked LUNs with respect to those initiators.

Get-EmcScsiLun

Displays VMware SCSI LUNs.

Get-EmcSharedFolder

Displays shared folders available from a file storage system.

Get-EmcSnapshotLun

Displays snapshot LUNs.

Get-EmcSnapshotPool

Displays snapshot pools. This cmdlet is not supported for XtremIO systems.

Get-EmcStoragePool

Displays storage pools. For VMAX eNAS and VNX-File storage pools, use `Get-EmcFileStoragePools`.

Get-EmcStorageRegisteredHost

Displays registered hosts for a specified storage system. This cmdlet is not supported for VMAX storage systems.

Get-EmcStorageRegisteredInitiator

Displays host initiators that are registered on the storage systems. This cmdlet is not supported for VMAX storage systems.

Get-EmcStorageServiceNode

Displays storage service nodes.

Get-EmcStorageSystem

Displays storage systems.

Get-EmcSupportedSystem

Displays supported systems.

Get-EmcTargetPort

Displays target ports.

Get-EmcUnityConsistencyGroup

Displays consistency groups on the connected Unity systems. Consistency groups enable consistent snapshots of multiple LUNs and are used to grant hosts access to LUNs and to snapshots of LUNs in the group.

Get-EmcUnityConsistencyGroupMember

Displays the members of a consistency group. A consistency group has three types of members: LUNs, hosts that have access to LUNs in the group, and hosts that have access to snapshots of LUNs in the group. The `-IncludeLuns`, `-IncludeLunHosts`, and `-IncludeSnapshotHosts` parameters return only those specific types of members. If omitted, the cmdlet returns all member types.

Get-EmcUnityFileSystem

Displays the file systems on connected Unity systems. File systems contain shares which are exposed to hosts. They are allocated from pools and hosted in NAS servers. This command is for Unity systems only.

Get-EmcUnitySnapshot

Displays the snapshots on connected Unity systems. You can retrieve snapshots of a particular source LUN or consistency group with the `Source` parameter.

Get-EmcVnxAdvancedSnapshot

Displays VNX advanced snapshots.

Get-EmcVnxAdvancedSnapshotMountPoint

Displays VNX advanced snapshot mount points.

Get-EmcVnxFileSystem

Displays the file systems on connected VNXe3200 systems. File systems contain shares which are exposed to hosts. They are allocated from pools and hosted in NAS servers. This command is for VNXe3200 systems only.

Get-EmcVnxLunGroup

Displays LUN groups on the connected VNXe systems. LUN groups enable consistent snapshots of multiple LUNs and are used to grant hosts access to LUNs and to snapshots of LUNs in the group.

Get-EmcVnxelunGroupMember

Displays the members of a LUN group. A LUN group has three types of members: LUNs, hosts that have access to LUNs in the group, and hosts that have access to snapshots of LUNs in the group. The `-IncludeLuns`, `-IncludeLunHosts`, and `-IncludeSnapshotHosts` parameters return only those specific types of members. If omitted, the cmdlet returns all member types.

Get-EmcVnxesnapshot

Displays the snapshots on connected VNXe systems. You can retrieve snapshots of a particular source LUN or LUN group with the `Source` parameter.

Get-EmcVplexClusters

Displays VPLEX clusters on the connected VPLEX systems.

Get-EmcVplexConsistencyGroup

Displays VPLEX consistency groups on the connected VPLEX systems.

Get-EmcVplexInitiators

Displays VPLEX initiators on the connected VPLEX systems.

Get-EmcVplexPorts

Displays VPLEX ports on the connected VPLEX systems.

Get-EmcVplexServiceNodes

Displays VPLEX service nodes on the connected VPLEX systems.

Get-EmcVplexStorageViews

Displays VPLEX storage views on the connected VPLEX systems.

Get-EmcVplexVirtualVolume

Displays VPLEX virtual volumes on the connected VPLEX systems.

Get-EmcXtremlOXBrick

Displays X-Brick information from the XtremIO storage system.

Get-EmcXtremlIOConsistencyGroup

Displays the list of consistency groups for the specified XtremIO system.

Get-EmcXtremlIOInitiator

Displays initiators for the specified XtremIO storage system.

Get-EmcXtremlIOInitiatorGroup

Displays initiator groups for the specified XtremIO storage system.

Get-XtremlIOSnapshotScheduler

Displays all the schedulers from the XtremIO storage array

Get-EmcXtremlIOSnapshotSet

Displays snapshot sets for the specified XtremIO system.

Get-EmcXtremlIOTags

Displays all the tags from the XtremIO storage array.

Get-EmcXtremIOTagVolume

Displays all tags that are associated with the specified volume.

Mount-EmcUnitySnapshot

Mounts a Unity LUN or consistency group snapshot so it is visible to hosts in the snapshot access list for the LUN or consistency group.

Mount-EmcVnxAdvancedSnapshot

Mounts/attaches the VNX advanced snapshot with the specified snapshot mount point LUN.

Mount-EmcVnxeSnapshot

Mounts a VNXe LUN or LUN group snapshot so it is visible to hosts in the snapshot access list for the LUN or LUN group.

New-EmcLun

Creates an ESI LUN object.

New-EmcSharedFolder

Creates a file shared folder object.

New-EmcSharedFolderPool

Creates a VMAX eNAS or VNX-File shared folder pool.

New-EmcSnapshotLun

Creates a snapshot LUN. For XtremIO systems, ignore the `SnapshotPool` and `Retention` parameters.

New-EmcStorageRegisteredHost

Registers a host for a specified storage system.

New-EmcStorageRegisteredInitiator

Registers a host initiator on a specified storage system.

New-EmcUnityConsistencyGroup

Creates a consistency group on a Unity system. Consistency groups enable consistent snapshots of multiple LUNs and are used to grant hosts access to LUNs and snapshots of LUNs in the group.

New-EmcUnitySnapshot

Creates a snapshot on a Unity system. Unity allows snapshots of LUNs, consistency groups, and file systems.

New-EmcVnxAdvancedSnapshot

Creates a VNX advanced snapshot from a LUN and snapshot mount point (SMP).

New-EmcVnxAdvancedSnapshotMountPoint

Creates a VNX advanced snapshot mount LUN from a source LUN.

New-EmcVnxeLunGroup

Creates a LUN group on a VNXe system. LUN groups enable consistent snapshots of multiple LUNs and are used to grant hosts access to LUNs and snapshots of LUNs in the group.

New-EmcVnxeSnapshot

Creates a snapshot on a VNXe system. VNXe allows snapshots of LUNs, LUN groups, and file systems.

New-EmcVplexConsistencyGroup

Creates a consistency group on a VPLEX system.

New-EmcVplexDistributedVirtualVolume

Creates a VPLEX distributed virtual volume on the connected VPLEX systems.

New-EmcVplexLocalVirtualVolume

Creates a VPLEX local virtual volume on the connected VPLEX systems.

New-EmcXtremIOConsistencyGroup

Creates a consistency group on an XtremIO system.

New-EMCXtremIOSnapshotScheduler

Creates a scheduler with the specified properties.

New-EmcXtremIOSnapshotSet

Creates a snapshot set from a single volume, multiple volumes, a consistency group, or snapshot set.

New-EmcXtremIOtag

Creates a tag with the specified name.

Register-EmcVplexInitiators

Registers or unregisters a specified initiator on the connected VPLEX systems.

Register-EmcVplexVirtualVolume

Registers a specified virtual volume on the connected VPLEX systems.

Remove-EmcCifsSharedFolderMountPoint

Removes or unmounts a specified shared folder.

Remove-EmcFileBasedDisk

Deletes a file-based disk from a hypervisor.

Remove-EmcLun

Removes or destroys the LUN from the storage system.

Remove-EmcSharedFolder

Removes or destroys the shared folder from the storage system.

Remove-EmcSharedFolderPool

Delete a VMAX eNAS or VNX-File shared folder pool.

Remove-EmcSnapshotLun

Removes the snapshot LUN.

Remove-EmcStorageRegisteredHost

Removes the registered host from the storage system where it is registered.

Remove-EmcStorageRegisteredInitiator

Removes the specified host initiator from the storage system where the initiator host is registered.

Remove-EmcUnityConsistencyGroup

Deletes a consistency group from a Unity system.

Remove-EmcUnityConsistencyGroupMember

Removes one or more members from a consistency group. This command is used to remove LUNs, LUN access hosts, or snapshot access hosts from a consistency group from a Unity system.

Remove-EmcUnitySnapshot

Deletes a snapshot from a Unity system.

Remove-EmcVnxAdvancedSnapshot

Removes or deletes the specified VNX advanced snapshot.

Remove-EmcVnxLunGroup

Deletes a LUN group from a VNXe system.

Remove-EmcVnxLunGroupMember

Removes one or more members from a LUN group. This command is used to remove LUNs, LUN access hosts, or snapshot access hosts from a LUN group.

Remove-EmcVnxSnapshot

Deletes a snapshot from a VNXe system.

Remove-EmcVplexConsistencyGroup

Deletes a consistency group from a VPLEX system.

Remove-EmcVplexConsistencyGroupVirtualVolume

Deletes specified virtual volumes from a VPLEX consistency group.

Remove-EmcVplexVirtualVolume

Deletes specified virtual volumes from a VPLEX system.

Remove-EmcXtremIOConsistencyGroup

Deletes a consistency group from a specified XtremIO array.

Remove-EmcXtremIOConsistencyGroupVolume

Removes an XtremIO volume from an existing consistency group.

Remove-EMCXtremIOSnapshotScheduler

Removes the scheduler from the list of schedulers on the XtremIO array.

Remove-EmcXtremIOSnapshotSet

Removes a snapshot set from a specified XtremIO system. Removing a snapshot set deletes all the snapshot volumes that are associated with the snapshot set.

Remove-EmcXtremIOtag

Removes the specified tag from the list of tags.

Remove-EmcXtremIOtagVolume

Removes the specified tag from the specified volume.

Restore-EmcSnapshotLun

Restores a snapshot LUN.

Restore-EmcUnitySnapshot

Restores a Unity snapshot back to its source.

Restore-EmcVnxAdvancedSnapshot

Restores the VNX advanced snapshot to source LUN.

Restore-EmcVnxeSnapshot

Restores a VNXe snapshot back to its source.

Restore-EmcXtremlOSnapshots

If required, reassigns or restores a snapshot, volume, consistency group, or snapshot set, and to create a backup of snapshots.

Restore-EmcXtremlOSnapshotSet

Refreshes a snapshot set based on selected snapshot set tags.

Set-EmcCIFSSharedFolderMountPoint

Mounts a shared folder onto a host system.

Set-EmcLun

Sets the storage service node for the specified LUN. For VNX storage systems only, it sets the storage tiering policy and LUN compression and compression rate for the specified LUN.

Set-EmcLunAccess

Masks or unmask a LUN to a host, cluster, FC, or iSCSI initiator.

Set-EmcVNXLunAllocationPolicy

Modifies the VNX Allocation Policy of a LUN.

Set-EmcVplexUnmaskLun

Unmasks a LUN to the specified VPLEX host.

Set-EMCXtremlOSnapshotScheduler

Updates the scheduler with the specified properties.

Set-EmcXtremlOTag

Renames the specified tag.

Update-EmcVnxAdvancedSnapshot

Updates the VNX advanced snapshot.

PowerShell cmdlets host operations**Add-EmcHostDiskToCluster**

Adds a disk to a cluster.

Clear-EmcHostDiskSignature

Clears the host disk signatures and assigns new ones.

Expand-EmcHostVolume

Expands the volume of a host.

Find-EmcHostDisk

Finds the ESI host disk that is associated with an ESI LUN, host LUN identifier, or VM disk configuration on a host or cluster system.

Get-EmcAvailableDriveLetter

Displays the available drive letters on a host system or cluster system.

Get-EmcCifsNetworkShare

Displays network shares that are used by a specified host.

Get-EmcClusterDisk

Displays cluster disks.

Get-EmcClusterGroup

Displays cluster groups.

Get-EmcClusterNode

Displays cluster nodes.

Get-EmcClusterSystem

Displays connected cluster systems. A cluster system can be added to ESI using the `Get-EmcClusterSystemCredential` and `Connect-EmcSystem` cmdlets.

Get-EmcHostBusAdapter

Displays the host bus adapters for the specified hosts.

Get-EmcHostDisk

Displays host disk objects.

Get-EmcHostLunIdentifier

Displays the host LUN identifier.

Get-EmcHostSystem

Displays connected host systems.

Get-EmcHostVolume

Displays host volumes.

Initialize-EmcHostDisk

Initializes a host disk by bringing the disk online and setting a specified partition style in a host or cluster system.

New-EmcVolume

Creates a volume.

Remove-EmcHostDiskFromCluster

Removes a disk from a cluster.

Remove-EmcVolumeMountPoint

Removes or unmounts the specified volume.

Set-EmcHostDiskOnlineState

Changes the online state of the specified disk.

Set-EmcHostDiskReadOnlyState

Changes the read-only state for the specified disk.

Set-EmcVolumeMountPoint

Sets the drive letter or mount path for the volume.

PowerShell cmdlets hypervisor operations

Add-EmcFileBasedDiskToVirtualMachine

Adds or attaches a file-based disk to a virtual machine.

Add-EmcPassthroughDiskToVirtualMachine

Adds or attaches a pass-through disk to a virtual machine.

Get-EmcAvailablePassthroughDiskCandidate

Displays available pass-through disk candidates to attach or add to a virtual machine for a specified hypervisor.

Get-EmcAvailableScsiControllerLocation

Displays available SCSI controllers for a virtual machine that you can use to attach file-based or pass-through disks.

Get-EmcDatastore

Displays VMware datastores.

Get-EmcESXCluster

Displays VMware ESX clusters.

Get-EmcESXHost

Displays VMware ESX hosts.

Get-EmcHyperVSystem

Displays connected Hyper-V systems.

Get-EmcHyperVSystemCredential

Displays the credentials for Microsoft Hyper-V to connect ESI.

Get-EmcVcenterSystem

Displays vCenter systems.

Get-EmcVirtualMachineScsiController

Displays the SCSI controllers from the virtual machine configurations.

Get-EmcVirtualVolume

Displays the virtual volumes for an ESX Hypervisor or a vCenter system.

Get-EmcVMwareSystemCredential

Displays the encrypted connection parameters BLOB or the system object creation parameters for VMware systems. Use this cmdlet and the `Connect-EmcSystem` cmdlet to add or connect storage systems to ESI. It creates a BLOB or encrypted string by using the specified connection or system object creation parameters. ESI prompts you for the server IP address and credentials and then uses these parameters to create a BLOB. You can use the BLOB to connect or add VMware systems to ESI by using the `Connect-EmcSystem` cmdlet. To test the connection with the specified parameters, click **Test Connection** in ESI.

Get-EmcVirtualDiskConfiguration

Displays the virtual disk configuration for the specified host disk of a virtual machine, which can be either a file-based or pass-through disk.

Get-EmcVirtualMachineConfiguration

Displays the virtual machine configuration.

Get-EmcVirtualMachineHypervisor

Displays the virtual machine hypervisor.

New-EmcFileBasedDisk

Creates a file-based disk for a specified hypervisor.

New-EmcDatastore

Creates a datastore.

Remove-EmcDatastore

Deletes the specified datastore.

Remove-EmcVirtualDiskFromVm

Removes a file-based or pass-through disk from the virtual machine.

PowerShell cmdlets EMC RecoverPoint replication operations

Disable-EmcReplicaCopy

Disables a replica copy to stop the replication of that copy.

Disable-EmcReplicaCopyImageAccess

Disables a replica copy image access so that it is not available for mounting. Replication changes are again propagated to the copy.

Disconnect-EmcReplicationService

Disconnects replication services.

Enable-EmcReplicaCopy

Enables a replica copy to start replication on that copy.

Enable-EmcReplicaCopyImageAccess

Enables a replica copy image access so that it can be available for mounting. Replication changes are not propagated to the copy while image access is enabled. When image access is enabled for replica snapshots, ESI automatically uses the RecoverPoint Image Access mode of Logged Access. This mode ensures that the snapshot resides on the replica LUN and not the journal.

Get-EmcConsistencyGroup

Displays consistency groups that are used to protect LUNs.

Get-EmcReplicaCopy

Displays the list of replica copies that specify the copies within a consistency group.

Get-EmcReplicaCopySnapshots

Displays the list of snapshots for the specified replica copy.

Get-EmcReplicaLink

Displays the list of replica links that specify the replication connection and direction between two replica copies within a consistency group.

Get-EmcReplicaLun

Displays the replica LUNs for replication.

Get-EmcReplicaSet

Displays replica sets that contain the LUNs for the replication of source LUNs.

Get-EmcReplicationService

Displays the list of replication services. The replication service is the primary object for managing replication clusters, sites, and systems.

Get-EmcReplicationServiceCluster

Displays the list of replication clusters, which contains all the replication sites and systems in a replication service. A replication cluster is a group of EMC RecoverPoint sites and appliances working together to replicate storage and applications that are managed in ESI.

Get-EmcReplicationServiceCredential

Displays the encrypted connection string or BLOB. You can use this cmdlet along with the Connect-EmcSystem cmdlet to connect or add replication services to ESI.

Get-EmcReplicationServiceSite

Displays the list of replication sites, which contains all of the replication systems in the site.

Get-EmcReplicationSystem

Displays the list of replication systems. A replication system is an individual replication appliance that performs and facilitates replication.

Move-EmcProductionReplicaCopy

Performs a permanent failover to the specified replica copy, after which the copy becomes the new production copy.

New-EmcBookmark

Creates an EMC RecoverPoint bookmark for the specified consistency group. An EMC RecoverPoint bookmark is a text label that you can apply to a snapshot to uniquely identify it at any point in time. For multiple consistency groups, you must apply a parallel bookmark. Bookmarks are useful to mark specific events, such as an application update or for a failover. All bookmarks are listed in the copy journal. You can only bookmark a snapshot for a consistency group that is enabled and actively transferring.

New-EmcConsistencyGroup

Creates a consistency group, which is a group of one or more replica sets that can be backed up together and recovered together as a unit or a set. Consistency groups can include both local and remote replica copies, and usually include as many replication sets as there are volumes in the production storage to replicate.

New-EmcParallelBookmark

Creates a parallel bookmark for multiple consistency groups.

New-EmcReplicaCopy

Creates a replica copy, which can be either local or remote copies of a LUN, for a consistency group.

New-EmcReplicaLink

Creates a replica link between two replica copies.

New-EmcReplicaSet

Creates a replica set for a consistency group. A replica set is a source LUN and the local and remote copies that a replication cluster manages, and that performs continuous backup for the source LUN.

Remove-EmcConsistencyGroup

Deletes a consistency group and removes all associated resources for that consistency group.

Remove-EmcReplicaCopy

Deletes a replica copy from a consistency group and removes and masks LUNs for that replica copy.

Remove-EmcReplicaSet

Deletes a replica set from a consistency group and removes and masks LUNs for that replica set.

Set-EmcRecoverProductionCopy

Recovers the production copy by using the specified replica copy. This recovers the production to correct file or logical corruption by rolling the production back to a previous point-in-time.

PowerShell cmdlets SQL Server operations

This section lists the cmdlets available for Microsoft SQL Server.

Add-EmcDatabaseToAvailabilityGroup

Adds one or more SQL Server databases to an AlwaysOn Availability Group.

Add-EmcReplicaToAvailabilityGroup

Adds a secondary replica to an AlwaysOn Availability Group. An Availability Group can have up to four secondary replica.

Get-EmcDatabaseAvailabilityGroup

Displays the configuration settings, status, and other information about a database availability group (DAG).

Get-EmcSqlServerAvailabilityGroup

Adds a secondary replica to an AlwaysOn Availability Group. An Availability Group can have up to four secondary replica.

Get-EmcSqlServerDatabase

Displays the databases that are present in a SQL Server. Lists databases in a SQL Server Instance. For each database, details, including the data file path and log file path, are shown.

Get-EmcSqlServer

Displays the details of a SQL Server.

Get-EmcSqlServerCredential

Displays connection information. Prompts the user for the connection details and the credentials that are required to connect to the SQL Server.

New-EmcSqlServerAvailabilityGroup

Creates a SQL Server AlwaysOn Availability Group with specified details of Primary and Secondary Replica along with databases to be added.

New-EmcSqlServerDatabase

Creates a SQL Server database with specified details such as name of the database, file paths for data file, and log file.

Remove-EmcDatabaseFromAvailabilityGroup

Removes one or more SQL Server databases from an AlwaysOn Availability Group.

Remove-EmcReplicaFromAvailabilityGroup

Removes a secondary replica from an AlwaysOn Availability Group. An Availability Group can have up to four secondary replica.

Remove-EmcSqlServerAvailabilityGroup

Removes an AlwaysOn Availability Group from a SQL Server.

Remove-EmcSqlServerDatabase

Removes one or more databases from a SQL Server.

PowerShell cmdlets ESI Service operations

Add-EmcSystem

Registers storage systems with the ESI Service.

Add-EmcUser

Adds an authorized user to the ESI Service. Only authorized users can access the ESI Service. This command adds a Windows user or security group with the specified role to the ESI Service.

Disable-EMCServerCertificateValidation

Disables the server certificate validation when using SSL to communicate with the ESI Service.

Enable-EMCServerCertificateValidation

Enables the server certificate validation when using SSL to communicate with the ESI Service.

Get-EmcEntity

Displays one or more Entity objects from the Entity Graph of an ESI Service instance.

Get-EmcEntityClass

Displays the class names of entity objects in the Entity Graph of an ESI Service instance.

Get-EmcEntityRelationship

Displays one or more Entity relationship objects from the Entity Graph of an ESI Service instance. An Entity relationship represents a directional link between two Entity objects in an Entity Graph, where one Entity is the source and the other a target. This command returns entity relationship objects that satisfy the specified parameters.

Get-EmcSecurityRole

Displays the security roles for the ESI Service.

Get-EmcServiceConnectionOptions

Displays the current options for connecting to the ESI Service. Returns the current Service URL and other options for the ESI Service connection.

Get-EmcSystem

Displays all of the registered storage systems for the ESI Service.

Get-EmcSystemType

Displays all system types that are available for registration with the ESI Service.

Get-EmcUser

Displays the authorized users of the ESI Service.

Remove-EmcSystem

Unregisters (removes the registration of) a specified storage system with the ESI Service.

Remove-EmcUser

Removes an authorized user from the ESI Service. This command removes a Windows user or security group that has been granted one or more roles in the ESI Service. It can remove a single role or all roles for a user.

Set-EmcServicePolicy

Sets the system refresh interval service policy for the ESI Service.

Set-EmcServiceUrl

Sets the URL to the ESI Service for the current session. By default, the commands in the ESI Service PowerShell Toolkit connect to an instance of the ESI Service running on the local host. This command allows you to specify a URL to another ESI Service instance.

CHAPTER 7

Managing storage systems with the ESI GUI

This chapter contains the following topics:

- [Adding storage systems](#)..... 70
- [Removing systems from ESI](#)..... 72
- [Publishing connections](#)..... 72
- [Using the PowerShell scripting tool](#)..... 74
- [Managing VMAX storage systems](#)..... 75
- [Managing block storage](#)..... 76
- [Managing file storage](#)..... 92

Adding storage systems

Use the **Add System** action to add supported storage systems to ESI.

Note

To add ScaleIO systems to ESI, use the ESI Service Powershell Toolkit cmdlets.

Procedure

1. In the left pane of the ESI window, select **EMC Storage Integrator > Storage Systems**.
2. In the **Actions** pane, click **Add Storage System**.
3. In the **Add System** dialog box, specify the following for the storage system.

Option	Description
System Type	Type of storage system to add Note The VMAX selection represents the group of VMAX storage systems supported with this release of ESI. Supported VMAX systems are listed in the EMC Simple Support Matrix .
Friendly Name	Short name for the storage system that is unique across different storage systems

4. In the **Add System** dialog box, specify the connection information and then click **Add**.

Refer to [Storage system credentials](#) on page 70 for a description of the credentials for each type of storage system.
5. Click **Test Connection** to test the connection before adding it.
6. Click **Add**.

The storage system appears under **Available Systems** in the center pane.
7. For VPLEX systems only, select the VPLEX system, and in the **Actions** pane click **Connect**.

The **VplexClusters** tab appears and shows the VPLEX cluster. Expand the VPLEX node under **Storage Systems** and select a cluster to show information for that particular VPLEX cluster.

Storage system credentials

When you add a storage system, the required credentials are different for each storage system. Fields that are marked with an asterisk (*) in the ESI UI are required.

The following table lists the storage system options for supported ESI storage systems.

Option	Description
Username	Username for the storage system. Not used for VMAX systems and can be omitted.
Password	Password for the storage system. Not used for VMAX systems and can be omitted.
Management Server IP Address (Unity, VNXe, and VPLEX)	IP address for the storage system management server.
SPA's IP Address (VNX-F and VNX-Block)	IP address of storage processor (SP) A.
SPB's IP Address (VNX-F and VNX-Block)	IP address of SP B.
IP address (VMAX eNAS)	IP address of the management server.
XMS IP Address (XtremIO)	IP address of the management server.
Array serial number (VMAX and optionally XtremIO)	Serial number of the array. For XtremIO systems: <ul style="list-style-type: none"> To add a specific cluster, specify the array serial number. Leave blank to add all clusters that belong to the XtremIO Management Server.
SMI provider host (VMAX)	Hostname or IP address of the SMI-S provider.
SMI provider port (VMAX)	IP port of the SMI-S provider. You can accept the default port 5988 for HTTP or 5989 for HTTPS.
Use secured connection (VMAX)	Use a secure connection to the SMI-S provider.
Use Windows Authentication (VMAX)	Use Microsoft Windows authentication.
Connection timeout (seconds) (VMAX)	Time limit for a connection to connect to the SMI-S provider.
Operation timeout (seconds) (VMAX)	Time limit for an operation to be completed.
Ignore server certificate name validation (VMAX)	Bypass security certificate name validation.
Add Host Key If Missing (VMAX eNAS)	Include a host key.
Replace Host Key If Changed (VMAX eNAS)	Replace the existing host key.
Port number (VNX-F, VNX-Block, VPLEX, and XtremIO)	The default port number is automatically set. If the field is empty, leave it empty to use the default port.

Option	Description
	<p data-bbox="844 275 895 298">Note</p> <p data-bbox="844 317 1406 375">For VNX-Block, this option is the control station port number.</p>

Removing systems from ESI

Use the **Remove System** action to remove storage systems, applications, appliances, and other supported systems from ESI.

Procedure

1. In the left pane of the ESI window, select **EMC Storage Integrator** or **Storage Systems**.
2. In the center pane, select the storage system.
3. In the **Actions** pane, click **Remove System**.
4. Click **Yes**.

Publishing connections

Use the **Publish Connection** action to reuse the parameters required to add storage systems. This option enters the parameters automatically.

You can choose to publish storage system creation information to the following locations:

- **Another User:** Give a storage administrator or ESI user access to a specific set of supported EMC storage systems and related EMC RecoverPoint replication systems. Publish systems to a remote storage administrator.
- **The ESI Service:** Publish or register the supported storage systems so that the ESI Service and the ESI SCOM Management Packs can discover and monitor them.

Note

Because the ESI Service does not monitor replication systems, they cannot be published to the ESI Service.

Note

You can also use the `Add-EmcSystem` cmdlet in the ESI Service PowerShell Toolkit to publish supported storage systems.

Publishing storage systems

Publish one or more systems to a specified ESI user or to the ESI Service.

Before you begin

If you are publishing a storage system to the ESI Service, ensure that the ESI Service is installed.

Procedure

1. In the left pane of the ESI window on the ESI host controller system, select **EMC Storage Integrator**.
2. In the **Actions** pane, click **Publish Connection**.
3. In the **Publish Connection Information** dialog box, set the following parameters.

Option	Description
Publish To Target	Select Another User or ESI Service .
User	If you selected Another User , type the username for access to the published systems.
Password	If you selected Another User , type a password for the specified user.
Target Host	If you selected ESI Service , type the IP address or name of the host system that is running the extension or service.
Default Port	If you selected ESI Service , clear to specify a different port number.
Port	If you selected ESI Service and cleared the Default Port checkbox, type a new port number.

4. Click **Refresh** for a list of available systems.
5. In the **Local – Storage and Replication Systems** pane, select the systems that you want to publish, and then click **Add**.
6. To accept the list of systems to publish in the **Target – Storage and Replication Systems** pane, click **Publish**.

Note

This pane also lists systems that were previously published or registered with the ESI Service by using the ESI Service PowerShell Toolkit, the ESI PowerShell Toolkit, or this procedure.

After you finish

If you published storage systems to the ESI service, set up the security policy. See [Viewing and setting up the security policy](#) on page 33

Unpublishing storage systems

Unpublish or remove the connection information for selected systems from the ESI Service.

Before upgrading ESI, you must unpublish all systems from the ESI Service. You can use either:

- The Publish Connection action in the ESI GUI

- The `Get-EmcSystem` and `Remove-EmcSystem` cmdlets, which are part of the ESI Service PowerShell Toolkit

Note

You cannot unpublish a system from another user after publishing it. However, you can remove a system by running ESI under the user's session and removing the system with the ESI **Remove System** action or the ESI PowerShell Toolkit.

Procedure

1. In the left pane of the ESI window, select **EMC Storage Integrator** or **Storage Systems**.
2. In the **Actions** pane, click **Publish Connection**.
3. In the **Publish Connection Information** dialog box, set the following for the ESI Service.

Option	Description
IP Address/Name	Type the IP address or name of the host system that is running the service.
Publish To	Select ESI Service as the connection information for the systems.
Default Port	Accept the default port or clear the checkbox to specify a different port number.
Port	If you clear the Default Port checkbox, type the port number for the service.

4. Click **Refresh** for a list of published systems.
5. In the **Target – Storage and Replication Systems** pane, select the systems that you want to unpublish, and then click **Remove**.
6. Click **Publish** to accept the list of systems to unpublish.

Note

This pane also lists systems that were previously published or registered with the ESI Service by using the ESI Service PowerShell Toolkit or this procedure.

7. Click **Close**.

Using the PowerShell scripting tool

The PowerShell scripting tool enables you to create a partial PowerShell script that you can modify to repeat an action using different parameters.

Use the PowerShell scripting tool to manage these block and file systems:

- VMAX
- VNX
- VNXe
- Unity

- XtremIO

Procedure

1. In the left pane of the ESI window, select the storage system or host and then select an action.
 - For storage systems, select one of the following:
 - **Create Shared Folder**
 - **Create Shared Folder Pool**
 - For hosts, select one of the following
 - **Create Shared Folder**
 - **Create Disk** (for an online disk only)
 - **Disconnect Disk**
 - **Delete Disk**
 - **Connect Disk** (Unity and XtremIO systems)
2. Continue through the wizard selecting the required parameters until the **Review input parameters** screen appears.
3. Do one of the following:
 - Select **Script to clipboard** to copy the partial script for pasting into PowerShell.
 - Select **Script to file** to create a PowerShell file that you can save and modify.
4. Click **Cancel** to exit the wizard.
5. Paste the script into PowerShell and run the script.

Managing VMAX storage systems

Creating thin pools

With the VMAX Adapter, ESI only supports provisioning disks from thin pools for VMAX systems. Before creating, provisioning, and managing disks in ESI, you must create the thin pools with other EMC tools, such as the EMC Solutions Enabler SYMCLI or Unisphere for VMAX.

Creating and connecting disks

The VMAX Adapter enables you to use ESI to create disks for a VMAX host or cluster. You can change the drive letter and the path after the disk is created. To provision a LUN for a VMAX host or cluster, the VMAX system must be either locally connected to the host or to the cluster member nodes.

[Adding hosts](#) provides instructions for creating and connecting VMAX host disks with ESI.

Using FAST VP

The ESI VMAX Adapter supports EMC Fully Automated Storage Tiering for Virtual Pool (FAST® VP) policies for the VMAX family. FAST VP is a VMAX feature that combines virtual provisioning of thin pools with automated data movement between tiers, which is based on performance measurements and user-defined policies.

Each FAST VP policy can contain different tiers, including FC tiers, SATA tiers, and so on. A storage group represents a set of LUNs, storage volumes, or devices that you can apply to a FAST VP policy.

Use the ESI PowerShell FAST VP cmdlets to perform the following tasks:

- Add and remove FAST VP policies to storage groups.
- Manage and remove storage groups.
- Add LUNs to and remove LUNs from storage groups.

ESI limitations for FAST VP and VMAX systems include:

- You must create storage pools, FAST VP policies, and tiers with other EMC tools, such as the EMC Solutions Enabler SYMCLI or Unisphere for VMAX.
- If LUNs in a storage group are not bound to at least one pool that is part of the policy tier, you cannot associate a FAST VP policy to the storage group.
- You cannot rebind LUNs to different storage pools for FAST VP.

Managing metas

The VMAX Adapter enables you to use ESI to expand and extend existing LUNs into metas and create new metas or meta volumes for a VMAX host or cluster. Metas are combined storage devices that can be grouped together to create a larger meta.

Metas represent meta volumes, composite LUNs, metadevices, meta LUNs, composite volumes, and metaheads. Meta members represent meta volume members, constituent LUNs, and composite LUN members.

To create and manage metas, use the ESI PowerShell Toolkit meta cmdlets.

ESI limitations for expanding LUNs into metas and for creating and managing metas include:

- Expanding a bound stripe meta volume results in a Business Continuity Volume (BCV), which has the same meta configuration to preserve data. During the expansion, the system creates a mirror relationship between the meta and the BCV, which means the meta and the BCV contain the same data. After the expansion, the storage system detaches the BCV from the meta and by default, ESI does not delete the device. You can manually delete the devices with EMC tools, such as EMC Solutions Enabler SYMCLI or Unisphere for VMAX, to manage disk space.
- The `Expand-EmcLun` cmdlet expands meta volumes, but does not expand thin meta LUNs.
- You cannot expand meta volumes that involve a clone, remote data facility (RDF), or snap session. However, you can expand existing bound LUNs by forming new metas with the `New-EmcCompositeLun` cmdlet.
- You cannot compress or shrink meta volumes.

Managing block storage

Creating LUNs

Use the **Create LUN** wizard to create a LUN.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. In the **Actions** pane, click **Create LUN**.

The **Create LUN** wizard appears.

3. Select a storage pool, and then click **Next**.
4. On the **New LUN** page, set details for the new LUN or LUNs, and then click **Next**.

Option	Description
LUN Count	Number of LUNs to be created
Sequence Number	<p>First number to append to the name for the first LUN.</p> <hr/> <p>Note</p> <p>For example, to create three LUNs with the appended numbers 15, 16, and 17, type 3 in the LUN Count field and type 15 in the Sequence Number field.</p>
Name	Name of the LUN or LUNs
Description	Description of the LUN or LUNs
Size	Size and unit of measurement for each LUN
Service Node	Storage processor that hosts the LUN or LUNs
Provision Type	Select either Thick or Thin
Stop provisioning new LUNs when error occurs	Stop creating new LUNs if an error occurs during the process

5. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Results

The new LUN or LUNs appear in the LUNs list for the specific storage system.

Viewing LUNs

View LUNs or the initiators to which each LUN is unmasked.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. Click **LUNs** in the center pane.
3. Select the LUN from the list.
4. Click the plus (+) symbol to expand the LUN and view the initiators to which the LUN is unmasked.

Expanding LUNs

For VMAX3 and VNX block systems, expand both thin and thick pool LUNs with the ESI GUI. ESI supports expanding LUNs connected to a RAID group with the managing metas cmdlets in the ESI PowerShell Toolkit.

Note

You cannot expand LUNs (volumes) for XtremIO storage systems in ESI.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. Click **LUNs** in the center pane.
3. Select the LUN that you want to expand.
4. In the **Actions** pane, click **Expand LUN**.
The **Expand LUN** wizard appears.
5. On the **New LUN Capacity** page, type an increased capacity for the LUN and select a unit of measurement.
6. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Results

The expanded storage capacity is listed for the LUN in the **LUNs** tab.

Deleting LUNs

Procedure

1. In the left pane of the ESI window, select the storage system.
2. Click **LUNs** in the center pane, and then select one or more LUNs to delete from the list.

Note

Hold down the Ctrl key to select multiple LUNs.

3. In the **Actions** pane, click **Delete LUN**.
The Delete LUN wizard appears.
4. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Viewing LUN groups

View LUN groups for VNXe3200 systems only.

For each LUN group, you can view total capacity, total current allocation, thin provisioning setting, member LUNs, snapshots, hosts with LUN access, and hosts with snapshot access.

Procedure

1. In the left pane of the ESI window, select a VNXe3200 system.
2. Click **LUN Groups** in the center pane.
3. Select a LUN group from the list.
4. Click the plus (+) symbol to expand and view group details.

Creating volumes

In ESI, volumes are LUNs. The **Create LUN** wizard enables you to create the new volumes as LUNs.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. In the **Actions** pane, click **Create Volume**.

The **Create LUN** wizard appears.

3. Select a storage pool, and then click **Next**.
4. On the **New LUN** page, set details for the new volume or volumes, and then click **Next**.

Option	Description
LUN Count	Number of LUNs (volumes) to be created
Sequence Number	<p>First number to append to the name for the first LUN (XtremIO volume).</p> <hr/> <p>Note</p> <p>For example, to create three LUNs with the appended numbers 15, 16, and 17, type 3 in the LUN Count field and type 15 in the Sequence Number field.</p> <hr/>
Name	Name of the volume or volumes
Description	Description of the volume or volume group or select Not Applicable if no description is required

Option	Description
Size	Size and unit of measurement for each volume
Service Node (grayed out)	Not applicable for XtremIO volumes

- Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

The new volume or volumes appear in the **Volumes** tab for the selected XtremIO storage system.

Viewing XtremIO volumes

View volume storage information for XtremIO systems.

For XtremIO entities, ESI manages XtremIO volumes as LUNs and manages volume mappings as masking views.

Procedure

- In the left pane of the ESI window, select the XtremIO storage system.
- Click **Volumes** in the center pane.
- Select a volume from the list.
- To expand the volume and view the initiators to which the volume is unmasked, click the plus (+) symbol.

Deleting volumes

Procedure

- In the left pane of the ESI window, select the XtremIO storage system.
- Click **Volumes** in the center pane, and then select one or more volumes to delete from the list.

Note

Hold down the Ctrl key to select multiple volumes.

- In the **Actions** pane, click **Delete Volume**.
The **Delete LUN** wizard appears.
- Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Viewing masked LUNs and volumes

Masked LUNs and masked XtremIO volumes are provisioned and managed as logical storage system components in ESI. How you view masked LUNs depends on the type of storage system.

Note

For XtremIO entities, ESI manages XtremIO volumes as LUNs and manages volume mappings as masking views.

Use the ESI PowerShell Toolkit to mask and unmask LUNs with ESI. Refer to `Set-EmcLunAccess` in [PowerShell cmdlets storage system operations](#) on page 53 for more information.

Note

You can also view masked LUNs with the `Get-EmcLunMaskingView` cmdlet. Refer to [PowerShell cmdlets storage system operations](#) on page 53 for more information.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. In the center pane, select the applicable tab for the storage system:

Option	Description
VNX-Block	Use the Storage Groups tab.
VMAX and VNXe3200	Use the LUN Masking Views tab.
XtremIO	Use the Masking Views tab.

The masked LUNs or volumes are displayed.

Creating snapshots

Use the **Create Snapshot** wizard to create snapshots for VMAX3, VNXe, Unity, and UnityVSA storage systems.

To create a snapshots on XtremIO storage systems, refer to [Creating XtremIO snapshots](#) on page 82.

Procedure

1. In the left pane of the ESI window, select a storage system.
2. Click **LUNs** in the center pane.
3. Select the LUN for which you want to create a snapshot.

4. Under **Actions**, click **Create Snapshot**.
The **Create Snapshot** wizard appears.
5. In the **New Snapshot** page, type a name for the new snapshot.
6. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

The snapshot is visible in the **Snapshots** tab.

7. (Optional) For VMAX systems, create a child snapshot from a snapshot that you created from the LUN.
 - a. Click the **Snapshots** tab and select the snapshot.
 - b. Go to step 4 and repeat the procedure.

Creating XtremIO snapshots

Create snapshots of XtremIO volumes, XtremIO consistency groups, and other XtremIO snapshots.

Procedure

1. In the left pane of the ESI window, select an XtremIO storage system.
2. Click **Volumes**, **Snapshots** or **Consistency Groups** in the center pane.
3. Under **Actions**, click **Create Snapshot**.
4. From the wizard, do one of the following:
 - If you selected **Volumes**, type a snapshot suffix.
 - If you selected **Snapshots** or **Consistency Groups**, type a snapshot name and snapshot suffix.
5. Select **Read only** or **Writable** for the snapshot type and then click **Next**.
6. On the **View Tags** page, from the list of available tags, select tags to associate with the snapshot and then click **Next**.
7. Click **Next** to continue through the wizard, and then click **Finish**.

Note

Click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

The new snapshot appears under **Snapshots**.

Viewing snapshots

View VMAX3, VNXe, Unity, UnityVSA, and XtremIO snapshots.

The **Snapshots** tab includes all the Snapshots for the storage system.

Procedure

1. In the left pane of the ESI window, select a storage system.
2. Click **Snapshots** in the center pane.
3. Select a snapshot from the list.
4. Click the plus (+) symbol to expand for more details.

Deleting snapshots

Use the **Delete Snapshot** wizard to delete VMAX3, VNXe, XtremIO, Unity, and UnityVSA snapshots.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. Click **Snapshots** in the center pane.
3. Select the snapshot to be deleted.

Hold down the Ctrl key to select more than one snapshot.

Note

If the snapshot is a parent snapshot, you must delete the child snapshots before you can delete the parent snapshot.

4. In the **Actions** pane, click **Delete Snapshot**.
The **Delete Snapshot** wizard appears.
5. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Results

The snapshot is deleted and is no longer listed in the **Snapshots** tab.

Refreshing object types from an XtremIO snapshot

Refresh specified XtremIO object types from a point-in-time snapshot.

ESI enables you to refresh, or restore, a volume, consistency group, snapshot, or snapshot set from as XtremIO snapshot. You can also refresh XtremIO consistency groups or snapshot sets from associated snapshot set tags.

Procedure

1. In the left pane of the ESI window, select the XtremIO storage system.
2. Click **Volumes, Consistency Groups, Snapshots, or SnapshotSets** in the center pane.
3. In the **Actions** pane, click either:
 - The refresh operation for the object type
 - For consistency groups and snapshot sets only, the refresh from the snapshot set tag operation for the object type.
4. From the wizard, do one of the following and click **Next**.
 - If you chose to refresh the object type, select the snapshot from which to refresh
 - If you chose to refresh using the snapshot tag, select the snapshot tag that is associated with the object type
5. Continue through the wizard, clicking **Next** and **Finish**.

If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. To revert to the previously executed step, click **Rollback**.

Restoring a LUN from a VMAX3 snapshot

Use the **Restore Source from Snapshot** wizard to restore a VMAX3 LUN.

Procedure

1. In the left pane of the ESI window, select a VMAX3 storage system.
2. Click **Snapshots** in the center pane.
3. Select a snapshot of the LUN that you want to restore.
4. In the **Actions** pane, click **Restore Source from Snapshot**.

The **Restore Source from Snapshot** wizard appears.

5. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Viewing snapshot LUNs

View snapshot LUN details.

ESI does not support creating snapshot LUNs from the ESI GUI. Therefore, use the ESI PowerShell toolkit to create them. [Getting started with the ESI PowerShell toolkits](#) on page 46 provides more details. You can then view snapshot LUNs in the ESI GUI.

Procedure

1. In the ESI window, select the storage system with the snapshot LUN.
2. Click **LUNs** from the center pane to display a list of snapshot LUNs.
3. Click the plus (+) symbol to view LUN details.

Note

- You cannot view or manage snapshot LUNs for VMAX or VMAX3 systems in the ESI GUI. You can manage VMAX (but not VMAX3) snapshot LUNs using the PowerShell Toolkit.
 - When you create snapshot LUNs for a block storage system, ESI adds a new snapshot LUNs storage pool to the **Storage Pool** tab. This pool groups and presents all the snapshot LUNs created for that storage system in that special storage pool. This pool is only a group and is not an actual storage pool. [Viewing storage pools](#) on page 88 provides details about storage pools.
-

Deleting snapshot LUNs

Use the **Delete LUN** wizard to delete snapshot LUNs.

ESI does not support creating snapshot LUNs from the ESI GUI. Therefore, use the ESI PowerShell toolkit to create them. [Getting started with the ESI PowerShell toolkits](#) on page 46 provides more details. You can then delete snapshot LUNs in the ESI GUI.

Procedure

1. In the ESI window, select the storage system with the snapshot LUN.
2. Click **LUNs** from the center pane and select one or more snapshot LUNs from the list to delete.

Note

Hold down the Ctrl key to select multiple snapshot LUNs.

3. In the **Actions** pane, click **Delete LUN**.
The **Delete LUN** wizard appears.
4. Click **Yes** when prompted for confirmation.
5. Click **Next** to continue through the wizard, and then click **Finish**.

Note

Click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Managing XtremIO tags

Use tags to assign named identifiers to any XtremIO object type within a cluster. The **Tags** column is displayed in all views, which enables enhanced object filtering and isolation capabilities for improved management and monitoring of XtremIO clusters.

You can create, modify, and delete tags using the **Actions** panel or by right-clicking an object to show the context menu.

Procedure

1. Select the **Tags** tab to show the existing tags.
 - To create a tag, in the **Actions** panel, click **Create Tags**, type a name for the tag and select the **Entity Type**.
 - To modify a tag, select the tag, click **Modify Tags**, and type a new name for the tag.
 - To delete a tag, select the tag, click **Delete Tags**.
2. Click **Next** to continue through the wizard, and then click **Finish**.

Managing XtremIO object types with tags

Add tags to XtremIO object types to enable enhanced filtering using the **Tags** column. You can add tags to volumes, consistency groups, snapshots, snapshot sets, initiator groups, initiators, and schedulers.

Before you begin

Create tags as described in [Managing XtremIO tags](#) on page 86.

Procedure

1. Right-click an object type and select **Manage tags**.
2. Do one of the following:
 - To add tags to the selected object type, select the tag or tags to be added.
 - To remove tags from the selected object type, clear the tag or tags to be removed.
3. Click **Next** to continue through the wizard, and then click **Finish**.

Creating consistency groups

Use the **Create New Consistency Group** wizard to create VPLEX and XtremIO consistency groups.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. Click **Consistency Groups** in the center pane.
3. In the **Actions** pane, click **Create Consistency Group**.
The **Create New Consistency Group** wizard appears.
4. Add a name for the consistency group and then click **Next**. If you are creating a consistency group for:
 - An XtremIO system, go to the next step.

- A VPLEX system, go to step 7.
5. On the **View Tags** page, choose an available tag.
 6. In **Add Volumes to Consistency Group** page, choose all available volumes that can be tagged to the consistency group.
 7. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

After you finish

For VPLEX systems, add volumes to the consistency group, as described in [Managing volumes in a VPLEX consistency group](#).

Managing volumes in a VPLEX consistency group

Use the **Add Volume to Consistency Group** wizard or **Remove Volume From Consistency Group** wizard to manage VPLEX volumes in a consistency group.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. Click **Consistency Groups** in the center pane.
3. Select the consistency group to which you want to add a volume or from which you want to delete a volume.
4. In the **Actions** pane, click either:
 - **Add Volume**
 - **Remove Volume**

Depending on your selection, either the **Add Volume to Consistency Group** wizard or **Remove Volume From Consistency Group** wizard appears.

5. Select the volumes that you want to add to or remove from the consistency group.
6. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Viewing consistency groups

View consistency groups for Unity and VPLEX systems.

You can view:

- For each Unity consistency group, the total capacity, total current allocation, thin provisioning setting, member LUNs, snapshots, hosts with LUN access, and hosts with snapshot access
- For each VPLEX consistency group, the consistency group name, number of volumes, visibility, and the storage at which cluster.

Procedure

1. In the left pane of the ESI window, select a Unity or a VPLEX system.
2. Click **Consistency Groups** in the center pane.
3. Select a consistency group from the list.
4. Click the plus (+) symbol to expand and view group details.

Viewing service nodes for block storage systems

Each LUN is assigned an active service node. Service nodes can have multiple ports that can be either Fibre Channel (FC) or iSCSI.

Note

- For VPLEX systems, only FC ports are supported.
- XtremIO systems do not use service nodes.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. Click **Service Nodes** in the center pane.
3. Click the plus (+) symbol to expand the SP A or SP B list.
4. Click **Fibre Channel Target Ports** to view the FC target ports for each SP.
5. Click **iSCSI Target Ports** to view iSCSI target ports for each SP.

Viewing storage pools

You can view the storage pools for a selected storage system, the LUNs (XtremIO volumes) in each storage pool, and the initiators to which each LUN is unmasked.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. Click **Storage Pools** in the center pane.
3. Select a storage pool from the list.
4. Click the plus (+) symbol to expand the storage pool and view the LUNs in that storage pool.
5. Click the plus (+) symbol next to a LUN to view the initiators to which that LUN is unmasked.

Note

When you create snapshot LUNs for block storage systems, ESI adds a new storage pool for snapshot LUNs to the **Storage Pools** tab. This pool lists all snapshot LUNs created for that storage system. This pool is only a list and not an actual storage pool.

Note

Because XtremIO does not use storage pools, the entire XtremIO system is listed as a single storage pool in the **Storage Pools** tab.

Viewing VPLEX storage views

For VPLEX systems, view information about the LUNs, host initiators, and hosts associated with the cluster.

Procedure

1. In the left pane of the ESI window, select a VPLEX storage system.
2. Select a cluster.
3. Click **Storage Views** in the center pane.

Creating VPLEX virtual volumes

Use the **Create Virtual Volume** wizard to create VPLEX virtual volumes.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. Click **Virtual Volumes** in the center pane.
3. In the **Actions** pane, click **Create Virtual Volume**.

The **Create Virtual Volume** wizard appears.

4. On the **Virtual Volume Settings** page, choose the settings for the virtual volume, and then click **Next**.

Option	Description
Virtual Volume Name	Name of the virtual volume to be created.
Create Distributed Volume	Creates a distributed volume. If enabled, the wizard displays additional pages to provide target cluster details.
Source cluster	Select the source cluster from the list box.
Create New Storage Volume	(Optional) Creates a new storage volume in the underlying storage array. If not selected, existing storage volumes are listed in a subsequent step.

5. On the **Storage System** page, select the storage array associated with the selected source cluster and then click **Next**.
6. On the **Storage Pool** page, select the storage pool and then click **Next**.
There is only one global storage pool.
7. Perform one of these steps:
 - If you enabled **Create New Storage** on the **Virtual Volume Settings** page, on the **New LUN** page, set the required parameters and then click **Next**.
 - Otherwise, on the **LUN** page, select a storage volume (LUN) from the list of existing storage volumes and then click **Next**.

8. On the **LUN Masking Settings** page, choose the initiator ports from the list of initiator ports of the VPLEX source cluster, and then click **Next**.
All the initiator ports are selected by default.
9. If you enabled **Create Distributed Volume** on the **Virtual Volume Settings** page, repeat step 5 through step 8 to provide the target cluster details.
10. Click **Next** to continue through the wizard, and then click **Finish**.

Note

Click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

The new virtual volume appears in the list on the **Virtual Volumes** tab.

Viewing VPLEX clusters and virtual volumes

View the details of the virtual volumes for a selected cluster.

Procedure

1. In the left pane of the ESI window, select the VPLEX storage system.
2. Select a cluster.
3. Click **Virtual Volumes** in the center pane.

Deleting VPLEX virtual volumes

Use the **Delete Virtual Volume** wizard to delete a single or multiple VPLEX virtual volumes from a cluster.

Procedure

1. In the left pane of the ESI window, select the VPLEX storage system and then select a cluster.
2. On the **Virtual Volumes** tab, select one or more volumes to delete from the list.
3. In the **Actions** pane, click **Delete Virtual Volume** to access the wizard.
4. Continue through the wizard, clicking **Next** and **Finish**.

If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

The virtual volume is deleted from the list on the **Virtual Volumes** tab.

Viewing VPLEX initiators

Procedure

1. In the left pane of the ESI window, select the VPLEX storage system.
2. Select a cluster.
3. Click **Initiators** in the center pane.

Registering and unregistering VPLEX initiators

Use the **Register Initiator** or **Unregister Initiator** wizards to manage VPLEX initiator registration.

Procedure

1. In the left pane of the ESI window, select the VPLEX storage system and then select a cluster.
2. Click **Initiators** in the center pane.

The list of initiators indicates whether initiators are registered or unregistered with the VPLEX system.

3. Select an initiator from the list.
4. In the **Actions** pane, click either:
 - **Register** to register an unregistered initiator.
 - **Unregister** to unregister a registered initiator.

Depending on your selection, either the **Register Initiator** wizard or the **Unregister Initiator** wizard appears.

5. Continue through the wizards, clicking **Next** and **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Results

The list on the **Initiators** tab is updated accordingly.

Viewing XtremIO initiator groups

View details about initiator groups for XtremIO storage systems in ESI. The **Initiator Groups** tab includes the initiator group names and host bus adapter (HBA) IDs for each group.

Procedure

1. In the left pane of the ESI window, select an XtremIO storage system.
2. Click **Initiator Groups** in the center pane.
3. Select an initiator group from the list.
4. Click the plus (+) symbol to expand for more details, such as the HBA ID.

Viewing XtremIO storage controllers

View details about storage controllers for XtremIO storage systems.

The **Storage Controllers** tab provides details about the FC and iSCSI target ports, such as iSCSI qualified name (IQN) or World Wide Name (WWN), IP address, availability, storage controller ID, and link status.

Procedure

1. In the left pane of the ESI window, select an XtremIO storage system.
2. Click **Storage Controllers** in the center pane.
3. Select a storage controller from the list.
4. Click the plus (+) symbol to expand the controller data and view specifics for FC and iSCSI target ports.

Creating and editing XtremIO schedules

Use the **Create Scheduler** wizard to create schedules for XtremIO volumes and consistency groups.

Schedules determine when snapshots or consistency groups are created and how long they are retained.

Procedure

1. In the left pane of the ESI GUI, select the storage system for which you want to create a schedule.
2. In the center pane, select the **Volumes** tab to display the available volumes or the **Consistency Group** tab to display the available consistency groups.
3. In the **Actions** pane, click **Create Scheduler**.
4. In the wizard, provide the parameters for the new scheduler and click **Next**.

The options are as follows:

Option	Description
Scheduler State	Enable or Disable
Scheduler Type	Explicit (a specific time and date) or Interval (the time between snapshot or consistency group creation). Depending on which type you select, configure the times or intervals.
Keep Last	Number to keep
Keep for	Length of time
Suffix	Type a suffix for the snapshot.
Type	Writable or Read-only

5. Continue through the wizard and click **Finish**.
The new schedule is listed in the **Schedules** tab.
6. To edit existing schedules, right-click the schedule, select **Modify**, and complete the wizard as described in step 4.

Managing file storage

Creating shared folders

Use the **Create Shared Folder** wizard to create one or more shared folders for file storage systems.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. For storage systems that support both block and file protocols, select **File View** from the **Switch View** list box in the center pane.
3. In the **Actions** pane, click **Create Shared Folder**.

The **Create Shared Folder** wizard appears.

4. Select a file storage pool and click **Next**.
5. Continue through the wizard, setting parameters and clicking **Next**.

Note

Click **More Information** for more progress details. If a problem occurs while you are creating a shared folder, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

The fields and descriptions are as follows:

Option	Description
Shared Folder Count	Number of shared folders to create
Sequence Number	The first number to append to the name for the first folder. For example, to create three folders with the appended numbers 15, 16, and 17, type 3 in the Shared Folder Count field and type 15 in the Sequence Number field.
Name	Name of the shared folder or folders
Path	Path to the shared folder or folders
Capacity	Size and unit of measurement for each folder
Service Node	Service node for the folder or folders
Provision Type	Select Thick or Thin
Stop provisioning new shared folders when error occurs	Stops creating new folders if an error occurs during the process

6. Click **Finish**.

Results

The new shared folder or folders appear under **Shared Folders**.

Viewing shared folders

View a list of shared folders.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. For storage systems that support both block and file protocols, select **File View** from the **Switch View** list box in the center pane.
3. Click **Shared Folders** in the center pane.

Mounting shared folders

Mount a shared folder on a selected host.

Procedure

1. Select the shared folder to mount and click **Mount shared folder**.
2. Provide the information required in the wizard, clicking **Next** and **Finish**.
3. Log off and log on to see the results of the operation.

Deleting shared folders

Procedure

1. In the left pane of the ESI window, select the storage system.
2. For storage systems that support both block and file protocols, select **File View** from the **Switch View** list box in the center pane.
3. Click **Shared Folders** in the center pane and select one or more shared folders from the list.
4. In the **Actions** pane, click **Delete Shared Folder**.

The **Delete Shared Folder** wizard appears.

5. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Unmounting shared folders

Procedure

1. Select the **Network Disks** tab and select the mounted folder.
2. Click **Unmount Shared Folder** and continue through the wizard.
3. Log off and log on to see the results of the operation.

Creating shared folder pools

A shared folder pool is a container for shared folders. Grouping shared folders into a shared folder pool enables you to view and access folders from one place.

Before you begin

Create shared folders.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. For storage systems that support both block and file protocols, select **File View** from the **Switch View** list box in the center pane.
3. In the **Actions** pane, click **Create Shared Folder Pool**.

The **Create Shared Folder Pool** wizard appears.

4. Select a file storage pool, and then click **Next**.
5. Continue through the wizard, typing the required parameters and clicking **Next**.

Note

Click **More Information** for more progress details. If a problem occurs while you are creating a shared folder pool, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

6. Click **Finish**.

Results

The new shared folder pool appears under **Shared Folder Pools**.

Viewing shared folder pools

Procedure

1. In the left pane of the ESI window, select the storage system.
2. For storage systems that support both block and file protocols, select **File View** from the **Switch View** list box in the center pane.
3. Click **Shared Folder Pools** in the center pane, and then select the shared folder pool from the list.
4. Click the plus (+) symbol to expand the shared folder pool and view the shared folders.

Extending shared folder pools

After creating a shared folder pool, you can extend or enlarge the size of the pool. The new size must be larger than the current size of the pool.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. For storage systems that support both block and file protocols, select **File View** from the **Switch View** list box in the center pane.

3. In the **Actions** pane, click **Extend Shared Folder Pool**.
4. In the **Extend Shared Folder Pool** wizard, select a file storage pool, and then click **Next**.
5. Under **Shared Folder Pool Setting**, confirm the pool name, type a new larger size, and select the disk size measurement unit (MB, GB, or TB).
6. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Deleting shared folder pools

Procedure

1. In the left pane of the ESI window, select the storage system.
2. For storage systems that support both block and file protocols, select **File View** from the **Switch View** list box in the center pane.
3. Click **Shared Folder Pools** in the center pane, and then select one or more shared folder pools from the list.
4. In the **Actions** pane, click **Delete Shared Folder Pool**.
The **Delete Shared Folder Pool** wizard appears.
5. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Viewing file system service nodes

Procedure

1. In the left pane of the ESI window, select the storage system.
2. For storage systems that support both block and file protocols, select **File View** from the **Switch View** list box in the center pane.
3. In the center pane, click **Service Nodes**.
4. Click the plus (+) symbol to expand for more details.

CHAPTER 8

Managing hosts with the ESI GUI

This chapter contains the following topics:

- [Adding hosts](#)..... 98
- [Viewing registered hosts](#)..... 99
- [Removing hosts](#)..... 99
- [Applying XtremIO host best practices](#)..... 99
- [Viewing SAN initiators](#)..... 100

Adding hosts

ESI requires that you add all supported systems as hosts before you can view or manage these systems in ESI.

Adding Windows system hosts

Procedure

1. In the left pane of the ESI window, click **Hosts**.
2. In the **Actions** pane, click **Add Windows System** or **Add Host**.
3. In the **Add Host** dialog box, specify the following.

Option	Description
IP address/Name	IP address or name of the host
Username and Password	Username and password for the host

Note

Instead of entering a username and password, you can select **Use current Windows credentials**.

4. Click **Test Connection** to test the connection.
5. Click **Add**.

The host appears in the center pane.

Adding Linux system hosts

Procedure

1. In the left pane of the ESI window, click **Hosts**.
2. In the **Actions** pane, click **Add Linux System**.
3. In the **Add Linux Host** dialog box, specify the following.

Option	Description
IP address/Name	IP address or name of the host
Port	<p>Confirm the default value of 22.</p> <hr/> <p>Note</p> <p>If you change this value, the connection fails.</p> <hr/>
Authentication Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Password, to use your Linux password for authentication

Option	Description
	<ul style="list-style-type: none"> • Key-based, to use your Linux encryption key for authentication
Username	If Authentication Type is Password , username for the host
Password	If Authentication Type is Password , username for the host, password for the host
Username	If Authentication Type is Key-based , username for the Linux encryption key
Filepath	If Authentication Type is Key-based , browse for or type the path for the key.
Passphrase	If Authentication Type is Key-based , type the pass phrase for the key.

4. Click **Test Connection** to test the connection.
5. Click **Add**.

The host appears in the center pane.

Viewing registered hosts

View a list of registered hosts, and then view additional information for each of the registered hosts.

Procedure

1. In the left pane of the ESI window, select the storage system.
2. Click **Registered Hosts** in the center pane.
3. Click the plus (+) symbol to expand the registered host information.

Removing hosts

Procedure

1. In the left pane of the ESI window, select **EMC Storage Integrator** or **Hosts**.
2. Select the host from the center pane.
3. In the **Actions** pane, click **Remove System**.
4. Click **Yes** to confirm that you want to remove the host.

Applying XtremIO host best practices

Apply best practices to hosts for XtremIO arrays.

Note

XtremIO systems do not require host registration.

Procedure

1. In the left pane of the ESI GUI, select the host.
2. In the **Actions** pane, click **Apply Host Best Practice**.
3. In the wizard, select **HBA queue depth=256**, if required.
4. Continue through the wizard clicking **Next** and **Finish**.

Viewing SAN initiators

Procedure

1. In the left pane of the ESI window, select **Hosts**.
2. Select the host from the center pane.
3. Click **SAN Initiators**.

The SAN initiator details are listed.

CHAPTER 9

Managing host disks with the ESI GUI

This section contains the following topics.

- [Changing a host disk drive letter or path](#)..... 102
- [Connecting disks to a host](#).....102
- [Creating host disks](#)..... 103
- [Viewing host disks](#)..... 105
- [Expanding host disks](#)..... 105
- [Deleting host disks](#).....106
- [Disconnecting disks from a host](#)..... 106
- [Creating pass-through SCSI disks](#)..... 107
- [Connecting pass-through SCSI disks to a host](#)..... 108
- [Creating raw device mapping disks](#)..... 109
- [Connecting raw device mapping disks to a host](#)..... 111
- [Creating SCSI disks](#)..... 113
- [Connecting SCSI disks to a host](#)..... 114
- [Creating virtual disks](#)..... 115
- [Connecting virtual disks to a host](#)..... 117

Changing a host disk drive letter or path

Procedure

1. In the left pane of the ESI window, select the host.
2. Click **Host Disks** in the center pane.
3. Select a disk from the list.
4. In the **Actions** pane, click **Change Drive Letter and Paths**.
The **Change Drive Letter and Paths** wizard appears.
5. Select the drive letter or mount point.
6. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Results

The drive letter or mount path is changed.

Connecting disks to a host

Procedure

1. In the left pane of the ESI window, select the host.
2. Click **Host Disks** in the center pane.
3. Select a disk from the list.
4. In the **Actions** pane, click **Connect Disk**.
The **Connect Disk** wizard appears.
5. On the **Storage System** page, select the storage system, and then click **Next**.
The page that appears next depends on the type of system.
6. On the **Storage Pool** page, select the storage pool, and then click **Next**.
7. Perform one of these steps, depending on the system:
 - On the **LUN** page, select one or more LUNs, and then click **Next**.
 - For VPLEX systems, on the **Select a Virtual Volume** page, select one or more virtual volumes and then click **Next**.
8. On the **LUN Masking Settings** page, select the initiators and then click **Next**.
9. In the **Review Input Parameters** page, do one of the following:
 - For Unity and XtremIO systems:
 - Click **Script To Clipboard** to copy the partial script for pasting into PowerShell.

- Click **Script To File** to create a PowerShell file that you can save and modify.
 - Review the settings.
- 10. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Creating host disks

Use the **Create Disk** wizard to create host disks.

If the host is a virtual machine that is hosted on a hypervisor, refer to [Creating disks for virtual machines](#) on page 128 before creating virtual disks for virtual machines. The hypervisor must appear in the **Hypervisors** section of the ESI main window. Add a hypervisor host after the hypervisor is connected and listed in the **Hypervisors** section, otherwise, the disk creation will fail.

Note

When creating host disks on XtremIO arrays, follow the recommendations in the **Create Disk** wizard to align with XtremIO best practices.

Procedure

1. In the left pane of the ESI window, select the host.
2. In the **Actions** pane, click **Create Disk**.
The **Create Disk** wizard appears.
3. Select the storage system, and then click **Next**.
 - If you selected a VPLEX system, go to the next step.
 - Otherwise, go to [Step 7](#).
4. On the **Virtual Volume Settings** page, choose the settings for the virtual volume, and then click **Next**.

Option	Description
Virtual Volume Name	Name of the virtual volume to be created.
Create Distributed Volume	Creates a distributed volume. If enabled, the wizard displays additional pages to provide target cluster details.
Source cluster	Select the source cluster from the list box.
Create New Storage Volume	(Optional) Creates a storage volume in the underlying storage array. If not selected, existing storage volumes are listed in a subsequent step.

5. On the **LUN Masking Settings** page, select the initiators and click **Next**.
6. Select the storage system, and then click **Next**.
7. On the **Storage Pool** page, select a storage pool, and then click **Next**.
8. On the **New LUN** page, set the following details for one or more new LUNs, and then click **Next**.

The fields on the page depend on the selected system.

Option	Description
LUN Count	Number of disks to be created
Sequence Number	First number to append to the name for the first LUN <hr/> Note For example, to create three LUNs with the appended numbers 15, 16, and 17, type 3 in the LUN Count field and type 15 in the Sequence Number field.
Name	Name of the disk or disks
Description	Description for the disk or disks
Size	Size and unit of measurement for each disk
Service Node	Storage processor that hosts the disk or disks
Provision Type	Select either Thick or Thin
Stop provisioning new LUNs when error occurs	If an error occurs during the process, stops creating folders.

9. For VPLEX systems, select the initiators and click **Next**.
10. On the **Disk Preparation Settings** page, set details for the disk or disks, and then click **Next**.

Option	Description
Partition Type	Type of partition to be created, either MBR (Master Boot Record) or GPT (GUID Partition Table)
Volume Size	Disk volume size
File System	For MBR partitions: <ul style="list-style-type: none"> • NTFS (New Technology File System) • For Linux only, Ext2, Ext3, or Ext4 For GPT partitions: NTFS is the only available option
Allocation Unit Size	Size of the allocation unit that is measured in bytes
Volume Label	Label for the volume
Drive Letter or Mount Path	Drive letter or a mount path for the disk or disks <hr/> Note For Linux, Mount Path is the only available option

- Continue through the wizard, clicking **Next** and then **Finish**.

For XtremIO systems, on the **Review Input Parameters** page, you have the option to select:

- **Script To Clipboard** to copy the partial script for pasting into PowerShell.
- **Script To File** to create a PowerShell file that you can save and modify.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

The disk or disks appear in the list of **Host Disks** for the specific host and in the LUNs list under **Storage Systems**.

Viewing host disks

Procedure

- In the left pane of the ESI window, select **Hosts**. The list of available hosts appears in the center pane.
- Select a host from the list.
- Click **Host Disks**. The list of host disks is displayed.
- Click the plus (+) symbol to expand the host disk information.

Expanding host disks

Use the **Expand Disk** action to expand host disks that meet the following criteria:

- The disk has only one volume. The volume can be expanded if the host is connected.
- The disk has an associated LUN that can either be expanded or is a file-based disk which is supported by VMware.

Note

With VMware systems, ESI does not support expanding RDM disks that are attached with virtual compatibility mode.

Procedure

- In the left pane of the ESI window, select the host.
- In the center pane, click **Host Disk**, and then select a disk from the list.
- From the menu bar, select **Action > Expand Disk**.
- On the **New Disk Capacity** page, type the new capacity for the disk, select a unit of measurement, and then click **Next**.
- Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

The expanded storage capacity for the disk will display in the **Host Disks** tab.

Deleting host disks

Procedure

1. In the left pane of the ESI window, select the host.
 2. In the center pane, click **Host Disks**, and then select the disk or disks to delete.
-

Note

Hold down the Ctrl key to select multiple disks.

3. In the **Actions** pane, click **Delete Disk**.
The **Delete Host Disk** wizard appears.
 4. Click **Next** to continue through the wizard, and then click **Finish**.
For XtremIO systems, on the **Review Input Parameters** page, you have the option to select:
 - **Script To Clipboard** to copy the partial script for pasting into PowerShell.
 - **Script To File** to create a PowerShell file that you can save and modify.
-

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Disconnecting disks from a host

Procedure

1. In the left pane of the ESI window, select the host.
2. Click **Host Disks** in the center pane, and then select the host disk from the list.
3. In the **Actions** pane, click **Disconnect Disk**.
The **Disconnect Host Disk** wizard appears.
4. Click **Next** to continue through the wizard, and then click **Finish**.
For XtremIO systems, in the **Review Input Parameters** page, you have the option to select:

- **Script To Clipboard** to copy the partial script for pasting into PowerShell.
- **Script To File** to create a PowerShell file that you can save and modify.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Creating pass-through SCSI disks

Use the **Create Disk** wizard to create a pass-through SCSI disk.

If the selected hypervisor supports pass-through SCSI disks, you can select the **Passthrough SCSI Disk** option when you create a disk for a virtual machine. See [Creating raw device mapping disks](#) on page 109 if the hypervisor supports a raw device mapping disk instead.

Procedure

1. In the left pane of the ESI window, select the host.
2. Select the host disk from the center pane.
3. In the **Actions** pane, click **Create Disk**.
The **Create Disk** wizard appears.
4. Select **Passthrough SCSI Disk** as the disk type, and then click **Next**.
5. On the **Storage System** page, select the storage system, and then click **Next**.
6. On the **Storage Pool** page, select the storage pool, and then click **Next**.
7. On the **New LUN** page, set the following details for the disk or disks, and then click **Next**.

Option	Description
LUN Count	Number of disks to be created
Sequence Number	First number to append to the name for the first LUN Note For example, to create three LUNs with the appended numbers 15, 16, and 17, type 3 in the LUN Count field and type 15 in the Sequence Number field.
Name	Name of the disk or disks
Description	Description for the disk or disks
Size	Size and unit of measurement for each disk
Service Node	Storage processor that hosts the disk or disks
Provision Type	Select either Thick or Thin

8. On the **LUN Masking Settings** page, select the initiators and click **Next**.
9. On the **Hypervisor Settings** page, select the SCSI controller and SCSI controller location settings, and then click **Next**.

Note

For hypervisors, ESI does not support creating SCSI controllers. However, ESI uses existing SCSI controllers to create disks for virtual machines.

10. On the **Disk Preparations Settings** page, set the following values for the disk or disks, and then click **Next**.

Option	Description
Partition Type	Type of partition to be created, either MBR (Master Boot Record) or GPT (GUID Partition Table)
File System	Partition Type of MBR or GPT is NTFS as the only available choice
Allocation Unit Size	Size of the allocation unit that is measured in bytes
Volume Label	Label for the volume
Drive letter or mount path	Drive letter or a mount path for the disk or disks

11. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Results

The disk or disks appear in the list of **Host Disks** for the specific host and in the **LUNs** list under **Storage Systems**.

Connecting pass-through SCSI disks to a host

Procedure

1. In the left pane of the ESI window, select the host.
2. Select the host disk from the center pane.
3. In the **Actions** pane, click **Connect Disk**.
The **Connect Disk** wizard appears.
4. On the **Select Disk Type** page, select **Passthrough SCSI Disk**, and then click **Next**.
5. On the **Hypervisor Settings** page, select the controller and location settings, and then click **Next**.

6. On the **Passthrough SCSI Disk** page, select the candidate disk, and then click **Next**.
7. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Creating raw device mapping disks

Use the **Create Disk** wizard to create a raw device mapping disk.

If the hypervisor supports raw device mapping (RDM) disks, you can select the **Raw Device Mapping** option when you create a disk for a virtual machine. See [Creating pass-through SCSI disks](#) on page 107 if the hypervisor uses pass-through SCSI disks instead.

Note

With VMware systems, ESI does not support expanding RDM disks that are attached with virtual compatibility mode.

Procedure

1. In the left pane of the ESI window, select the host.
2. In the **Actions** pane, click **Create Disk**.
The **Create Disk** wizard appears.
3. Select **Raw Device Mapping** as the disk type, and then click **Next**.
4. On the **Storage System** page, select the storage system, and then click **Next**.
5. On the **Storage Pool** page, select the storage pool, and then click **Next**.
6. On the **New LUN** page, set the following details for the new disk or disks, and then click **Next**.

Option	Description
LUN Count	Number of disks to be created
Sequence Number	First number to append to the name for the first LUN Note For example, to create three LUNs with the appended numbers 15, 16, and 17, type 3 in the LUN Count field and type 15 in the Sequence Number field.
Name	Name of the disk or disks
Description	Description for the disk or disks

Option	Description
Size	Size and unit of measurement for each disk
Service Node	Storage processor that hosts the disk or disks
Provision Type	Select either Thick or Thin
Stop provisioning new LUNs when error occurs	Stops creating new LUNs if an error occurs during the process

7. On the **LUN Masking Settings** page, select the initiators and click **Next**.
8. On the **Hypervisor Settings** page, set the following field values, and then click **Next**.

Note

For hypervisors, ESI does not support creating SCSI controllers. However, ESI uses existing SCSI controllers to create disks for virtual machines.

Option	Description
Controller	SCSI controller
Location	SCSI controller location
RDM Compatibility Mode	<p>The type of compatibility (physical or virtual)</p> <hr/> <p>Note</p> <p>If you select Physical in the RDM Compatibility Mode field, the guest operating system can access the hardware directly.</p> <hr/>
Persistence	<p>Types include:</p> <ul style="list-style-type: none"> • Persistent: Changes are immediately and permanently written to the disks. • Independent Persistent: Independent disks are not affected by snapshots. • Independent Non Persistent: Changes to disks are discarded when you shut down your system or revert to the snapshot. <hr/> <p>Note</p> <p>With Physical mode, Persistent is the only available option.</p> <hr/>
Disk Provisioning	<p>Options for creating a virtual disk:</p> <ul style="list-style-type: none"> • Thick Provision Eager Zeroed: All disk space is allocated and any previous content is deleted when the disk is created; this option might take longer than the other two options. • Thick Provision Lazy Zeroed: All disk space is allocated but existing content is not deleted when the disk is created.

Option	Description
	<ul style="list-style-type: none"> • Thin Provision: Allocates only the disk space that is currently needed.

9. On the **Disk Preparations Settings** page, set the following field values for the disk or disks, and then click **Next**.

Option	Description
Partition Type	Type of partition to be created, either MBR (Master Boot Record) or GPT (GUID Partition Table)
Volume Size	Disk volume size
File System	Partition Type of MBR or GPT is NTFS as the only available choice
Allocation Unit Size	Size of the allocation unit measured in bytes
Volume Label	Label for the volume
Drive letter or mount path	Drive letter or a mount path to the disk

10. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

The disk appears in the list of **Host Disks** for the specific host and in the **LUNs** list under **Storage Systems**.

Connecting raw device mapping disks to a host

Use the **Connect Disk** wizard to connect RDM disks to a host.

Procedure

1. In the left pane of the ESI window, select the host.
2. Select the host disk from the center pane.
3. In the **Actions** pane, click **Connect Disk**.
The **Connect Disk** wizard appears.
4. On the **Select Disk Type** page, select the disk type of **Raw Device Mapping**, and then click **Next**.
5. On the **VMware vSphere Settings** page, set the following field values, and then click **Next**.

Note

For hypervisors, ESI does not support creating SCSI controllers. However, ESI uses existing SCSI controllers to create disks for virtual machines.

Option	Description
Controller	SCSI controller
Location	SCSI controller location
RDM Compatibility Mode	Type of compatibility (physical or virtual) Note In physical mode, the guest operating system can access the hardware directly.
Persistence	Types include: <ul style="list-style-type: none"> • Persistent: Changes are immediately and permanently written to the disks. • Independent Persistent: Independent disks are not affected by snapshots. • Independent Non Persistent: Changes to disks are discarded when you shut down your system or revert to the snapshot. Note In Physical mode, Persistent is the only available option.
Disk Provisioning	Select one of the following options if you are creating a virtual disk: <ul style="list-style-type: none"> • Thick Provision Eager Zeroed: All disk space is allocated and any previous content is deleted when the disk is created; this option may take longer than the other two options. • Thick Provision Lazy Zeroed: All disk space is allocated but existing content is not deleted when the disk is created. • Thin Provision: Allocates only the disk space that is currently needed.

6. On the **Passthrough SCSI Disk** page, select the candidate disk, and then click **Next**.
7. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Creating SCSI disks

Use the **Create Disk** wizard to create a SCSI disk.

Note

The SCSI disk option is not available for VMAX storage systems when provisioning storage to virtual machines.

Procedure

1. In the left pane of the ESI window, select the host.
2. In the **Actions** pane, click **Create Disk**.
The **Create Disk** wizard appears.
3. Select **SCSI Disk** as the disk type, and then click **Next**.
4. On the **Storage System** page, verify the information, and then click **Next**.
5. On the **Storage Pool** page, select the storage pool, and then click **Next**.
6. On the **New LUN** page, set the following details for the new disk or disks, and then click **Next**.

Option	Description
Name	Name of the disk or disks
Description	Description for the disk or disks
Size	Size and unit of measurement for each disk
Service Node	Storage processor that hosts the disk or disks
Provision Type	Select either Thick or Thin

7. On the **Disk Preparation Settings** page, set the following details for the disk or disks, and then click **Next**.

Option	Description
Partition Type	Type of partition to be created, either MBR (Master Boot Record) or GPT (GUID Partition Table)
Volume Size	Disk volume size in MB

Option	Description
File System	Partition Type of MBR or GPT is NTFS by default
Allocation Unit Size	Size of the allocation unit measured in bytes
Drive letter or mount path	Drive letter or a mount path for the disk or disks

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

- Click **Next** to continue through the wizard, and then click **Finish**.

The disk or disks appear in the list of **Host Disks** for the specific host and in the LUNs list under **Storage Systems**.

Connecting SCSI disks to a host

Procedure

- In the left pane of the ESI window, select the host.
- Select the host disk from the center pane.
- In the **Actions** pane, click **Connect Disk**.
The **Connect Disk** wizard appears.
- On the **Select Disk Type** page, select **SCSI Disk**, and then click **Next**.
- On the **Storage System** page, review the details, and then click **Next**.
- On the **Storage Pool** page, select a storage pool, and then click **Next**.
- On the **LUN** page, select a LUN, and then click **Next**.
- On the **LUN Masking Settings** page, review the settings, and then click **Next**.
- On the **Review Input Parameters** page, review the settings, and then click **Next** to confirm them.
- On the **Progress** page, click **Next**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

- On the **Summary** page, click **Finish**.

Creating virtual disks

Create additional virtual disks for a virtual machine.

Before you begin

You must add the host before creating virtual disks. Before this option is available, the hypervisor that hosts the virtual machine must appear in the **Hypervisors** section on the main ESI windows and the virtual machine must be listed in the **Hosts** section. When you select the virtual machine in the **Hosts** section, the **Hypervisor** and **Hypervisor type** appear at the top of the center pane (gray information area). If these do not appear, the virtual machine might have been discovered before the hypervisor. If so, remove the virtual machine and add it again as a host.

Procedure

- In the left pane of the ESI window, select the host.
The host has to be a virtual machine that correctly identifies the hypervisor.
- Select the host disk from the center pane.
- In the **Actions** pane, click **Create Disk**.
The **Create Disk** wizard appears.
- Perform one of the following steps:
 - For Unity systems, select **Virtual Disk** as the disk type and then click **Next**.
 - For all other systems, select **Virtual Hard Disk** as the disk type and then click **Next**.
- On the **Create File-based Disk** page, set the following details and then click **Next**.

Option	Description
File Name	Name of the file, including the file extension of VHD, VHDX, or VMDK.
Size	Size of the file in GB.
File-based Disk Type	Select either Fixed or Dynamic (not available for Unity systems).
Location	Location of the virtual hard disk. For Unity systems, the location of the virtual volumes (VVols) datastore.

Note

The page that appears next depends on the type of host that you select:

- The **Hypervisor Settings** page appears if you selected a hypervisor host.
 - The **VMware vSphere Settings** page appears if you selected a VMware vSphere host.
-

- On either the **Hypervisor Settings** or **VMware vSphere Settings** page, set the following details, and then click **Next**.

Option	Description
Controller	Hypervisor or VMware controller
Location	SCSI controller location
Persistence (VMware Settings page only)	Types include: <ul style="list-style-type: none"> • Persistent: Changes are immediately and permanently written to the disks • Independent Persistent: Independent disks are not affected by snapshots • Independent Non Persistent: Changes to disks are discarded when you shut down your system or revert to the snapshot
Disk Provisioning (VMware Settings page only)	Select either Thick or Thin

7. Depending on the hypervisor, the **Disk Preparation Settings** page might appear. If the page appears and the disk does not require these values, skip this step. If the disk requires one or more of the values, set the applicable details, and then click **Next**.

Option	Description
Partition Type	Type of partition to be created, either MBR (Master Boot Record) or GPT (GUID Partition Table)
File System	NTFS is the default.
Allocation Unit Size	Size of the allocation unit measured in bytes
Volume Label	Label for the volume
Drive letter or mount path	Drive letter or a mount path to the disk <div style="border: 1px solid black; padding: 5px;"> <p>Note</p> <p>If you enter a drive letter and folder path that does not exist, ESI will create the specified folder path, and then create the disk.</p> </div>

8. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Connecting virtual disks to a host

Procedure

1. In the left pane of the ESI window, select the host.
2. Select the host disk from the center pane.
3. In the **Actions** pane, click **Connect Disk**.
The **Connect Disk** wizard appears.
4. On the **Select Disk Type** page, select **Virtual Disk**, and then click **Next**.
5. On the **Virtual Hard Disk** page, type the File Path, or browse to select it, and then click **Next**.
6. On the **Hypervisor Settings** page, select the controller and location settings, and then click **Next**.
7. On the **Review Input Parameters** page, review the settings, and then click **Next** to confirm them.
8. On the **Progress** page, click **Next**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

9. On the **Summary** page, click **Finish**.

CHAPTER 10

Managing host clusters with the ESI GUI

This chapter contains the following topics:

- [Adding host clusters](#)..... 120
- [Viewing host clusters and nodes](#)..... 120
- [Removing clusters from a host](#)..... 121
- [Creating cluster disks](#)..... 121
- [Connecting cluster disks to a host cluster](#)..... 123
- [Connecting cluster nodes to a host](#)..... 123
- [Disconnecting cluster disks from a host cluster](#)..... 123
- [Deleting cluster disks from a host cluster](#)..... 124
- [Changing a cluster disk drive letter or path](#)..... 124

Adding host clusters

Procedure

1. In the left pane of the ESI window, select **EMC Storage Integrator** or a host cluster.
 - If you selected **EMC Storage Integrator**, click **Add Host Cluster** in the **Actions** pane.
 - If you selected **Host Clusters**, click **Add Cluster System** in the **Actions** pane.
2. In the **Add Cluster** dialog box, specify the following for the cluster.

Option	Description
IP address/Name	IP address or name of the cluster
Username/Password	Username and password for the cluster
	<p>Note</p> <p>Alternatively, click Use current Windows credentials.</p>

3. Click **Test Connection** to test the connection before adding it.
4. Click **Add**.

The cluster appears in the **Available Systems** list.

Viewing host clusters and nodes

You can view cluster disks, cluster nodes, and SAN initiators of a host cluster.

Procedure

1. In the left pane of the ESI window, select **Host Clusters**.
2. Select the host cluster.
3. Click **Cluster Disks** from the center pane.

The cluster disks are listed.
4. Click the following tabs in the center pane to view host cluster details:
 - **Cluster Disks**
 - **Cluster Nodes**
 - **SAN Initiators**
5. Click the plus (+) symbols to expand the host cluster information.

Note

Click **Connect to Host** in the **Actions** pane or click the host node to connect to the host. This host must be added to ESI. If not, ESI prompts you to add the host.

Removing clusters from a host

Procedure

1. In the left pane of the ESI window, select **EMC Storage Integrator** or **Host Clusters**.
2. Select one or more clusters from the center pane.

Note

Hold down the Ctrl key to select multiple clusters.

3. In the **Actions** pane, click **Remove System**.
4. Click **Yes** to confirm your selection.

Creating cluster disks

Procedure

1. In the left pane of the ESI window, select the host cluster.
2. In the **Actions** pane, click **Create Cluster Disk**.
The **Create Cluster Disk** wizard appears.
3. In the **Storage System** list box, select a storage system, and then click **Next**.
4. On the **Storage Pool** page, select a storage pool, and then click **Next**.
5. On the **New LUN** page, set the following values for the new disk or disks, and then click **Next**.

Option	Description
LUN Count	Number of disks to be created
Sequence Number	First number to append to the name for the first disk <hr/> Note For example, to create three LUNs with the appended numbers 15, 16, and 17, type 3 in the LUN Count field and type 15 in the Sequence Number field.
Name	Name of the disk or disks
Description	Description of the disk or disks
Size	Size and unit of measurement for each disk
Service Node	Storage processor that hosts the disk or disks

Option	Description
Provision Type	Select either Thick or Thin Note The Thin option is not available if the selected pool does not support thin LUNs.
Application	The type of application, such as Generic Storage . Note This field appears only if a Unity or VNXe storage system is selected.

6. For VMAX3 systems only, on the **LUN Masking Settings** page, select the initiators.
7. On the **Cluster Parameters** page, select one of the following, and then click **Next**:
 - **Cluster Group** and the name of a cluster group
 - **Cluster Shared Volumes** for a shared disk
8. On the **Disk Preparation Settings** page, set the following values, and then click **Next**.

Option	Description
Partition Type	Type of partition to be created, either MBR (Master Boot Record) or GPT (GUID Partition Table)
File System	Partition Type of MBR or GPT is NTFS by default
Allocation Unit Size	Size of the allocation unit in bytes
Volume Label	Label for the volume
Drive letter or mount path	Drive letter or mount path for the disk

9. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

The cluster disk or disks appear in the **Cluster Disks** list for the specified cluster.

Connecting cluster disks to a host cluster

Procedure

1. In the left pane of the ESI window, select the host cluster.
2. In the **Actions** pane, click **Connect Cluster Disk**.
The **Connect Cluster Disk** wizard appears.
3. In the **Storage System** list box, select a storage system, and then click **Next**.
4. On the **Storage Pool** page, select a storage pool, and then click **Next**.
5. On the **LUN** page, select a LUN from the storage pool, and then click **Next**.
6. On the **Cluster Parameters** page, select one of the following, and then click **Next**:
 - **Cluster Group** and the name of a cluster group
 - **Cluster Group** and the name of a cluster group
7. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Connecting cluster nodes to a host

Procedure

1. In the left pane of the ESI window, select the host cluster.
2. Click **Cluster Nodes** from the center pane.
3. Select a cluster node from the list.
4. In the **Actions** pane, click **Connect**.

Disconnecting cluster disks from a host cluster

Procedure

1. In the left pane of the ESI window, select the host cluster.
2. Select the cluster disk from the list.
3. In the **Actions** pane, click **Disconnect Cluster Disk**.
The **Disconnect Cluster Disk** wizard appears.
4. On the **Disconnect Cluster Disk** page, click **Next**.
5. Click **Yes** to confirm your selection.
6. On the **Review Input Parameters** page, review the settings, and then click **Next** to confirm them.

7. On the **Progress** page, click **Next**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

8. On the **Summary** page, click **Finish**.

Deleting cluster disks from a host cluster

Procedure

1. In the left pane of the ESI window, select a host cluster.
2. Select one or more cluster disks to be deleted.

Note

Hold down the Ctrl key to select multiple clusters.

3. In the **Actions** pane, click **Delete Cluster Disk**.
The **Remove Cluster Disk** wizard appears.
4. Verify the cluster disk details, and then click **Next**.
5. Click **Yes** when prompted for confirmation again.
6. On the **Review Input Parameters** page, review the settings, and then click **Next** to confirm them.
7. On the **Progress** page, click **Next**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

8. On the **Summary** page, click **Finish**.

Changing a cluster disk drive letter or path

Procedure

1. In the left pane of the ESI window, select **Host Clusters**.
2. Click **Cluster Disks** in the center pane.
3. Select the cluster disk to change.
4. In the **Actions** pane, click **Change Drive Letter and Paths**.
The **Change Drive Letter and Paths** wizard appears.

5. Change the following values, and then click **Next**.

Option	Description
Drive Letter	Select from the available drive letters.
Mount Path	Click Browse and locate the path.

6. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

The cluster disk appears in the Cluster Disks list with the new disk drive or path.

7. On the **Summary** page, click **Finish**.

The cluster disk appears in the Cluster Disks list with the new disk drive or path.

CHAPTER 11

Managing hypervisors with the ESI GUI

This chapter contains the following topics:

- [Managing virtual machines and disks](#)..... 128
- [Adding, viewing, and deleting hypervisors](#).....134

Managing virtual machines and disks

Creating disks for virtual machines

ESI supports Microsoft Hyper-V and VMware vSphere hypervisors. The disk options in ESI vary depending on what the hypervisor supports.

The following table shows the storage options that are supported by ESI for each hypervisor.

Table 3 Disk options

Disk option	Microsoft Hyper-V	VMware vSphere
Pass-through disk	Yes (Pass-through SCSI)	Yes (RDM)
File-based or virtual disk	Yes (VHD or VHDX file)	Yes (VMDK file)
Datastore		Yes
SCSI disk		Yes
Host disk	Yes	
Cluster shared volumes	Yes	

You can create these disk types for virtual machines:

- SCSI Disks (VMware vSphere) See [Creating SCSI disks](#) on page 113
- Virtual disks (Hyper-V and VMware vSphere) See [Creating virtual disks](#) on page 115
- Pass-through SCSI disks (Hyper-V) See [Creating pass-through SCSI disks](#) on page 107
- RDM disks (VMware vSphere) See [Creating raw device mapping disks](#) on page 109

Note

- For hypervisors, ESI does not support creating new SCSI controllers. However, ESI uses existing SCSI controllers to create disks for a virtual machine.
- For hypervisors, if the virtual disk option is not available, confirm that the applicable hypervisor appears as a connected hypervisor in the **Hypervisors** section in the main ESI window. When you select the virtual machine in the **Hosts** section, the **Hypervisor** and **Hypervisor Type** appear at the top of the center pane (gray information area). If not, the virtual machine might have been discovered before the hypervisor. If so, remove the virtual machine and add it again as a host.
- The order of the pages and steps vary slightly in the **Create Disk** wizard, depending on the disk type that you select.

Creating hypervisor SCSI LUNs

Use the **Create Disk** wizard to create a hypervisor SCSI LUN from a volume.

Procedure

1. In the left pane of the ESI window, select **Hypervisors** and one of the hypervisor servers.
2. Click **SCSI LUNs** in the center pane.
3. In the **Actions** pane, click **Create Disk**.
The **Create Disk** wizard appears.
4. Perform one of these steps:
 - For a VPLEX system, go to the next step.
 - Otherwise, go to [Step 7](#).
5. Select a VPLEX storage system and click **Next**.
6. In the **Virtual Volume Settings** page, choose the settings for the virtual volume, and then click **Next**.

Option	Description
Virtual Volume Name	Name of the virtual volume from which the SCSI LUN will be created.
Create Distributed Volume	Creates a distributed virtual volume. If enabled, the wizard displays additional pages to provide target cluster details.
Select cluster	Select the volume from a particular cluster.
Create New Storage Volume	(Optional) Creates a new virtual volume in the underlying storage array. If not selected, existing virtual volumes are listed in a subsequent step.

7. On the **LUN Masking Settings** page, select a hypervisor initiator and click **Next**.
8. On the **Storage System** page, select the underlying array and click **Next**.
9. On the **Storage Pool** page, select the storage pool and then click **Next**.
There is only one global storage pool.
10. Perform one of these steps:
 - If you enabled **Create New Storage Volume** on the **Virtual Volume Settings** page, on the **New LUN** page, set the required parameters and then click **Next**.
 - Otherwise, on the **LUN** page, select a storage volume (LUN) from the list of existing storage volumes and then click **Next**.
11. On the **LUN Masking Settings** page, choose one or more ports from the list of initiator ports of the VPLEX source cluster, and then click **Next**.

All the initiator ports are selected by default.

12. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Connecting SCSI LUNs

Procedure

1. In the left pane of the ESI window, select **Hypervisors** and one of the hypervisor servers.
2. Click **SCSI LUNs** in the center pane and select a disk from the list.
3. In the **Actions** pane, click **Connect Disk**.
The **Connect Disk** wizard appears.
4. On the **Storage System** page, select the storage system and click **Next**.
5. On the **Select a VirtualVolume** page, select one or more virtual volumes to connect to the hypervisor node and click **Next**.
6. On the **LUN Masking Settings** page, choose from the list of initiator ports and then click **Next**.
7. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Disconnecting or removing SCSI LUNs

The **Disconnect SCSI Disk** wizard and **Delete SCSI Disk** enable you to manage SCSI disks.

Procedure

1. In the left pane of the ESI window, select **Hypervisors** and one of the hypervisor servers.
2. Click **SCSI LUNs** in the center pane and select a disk from the list.
3. In the **Actions** pane, perform one of these steps:
 - To disconnect the SCSI disk, click **Disconnect SCSI Disk**.
 - To delete the SCSI disk, click **Delete SCSI Disk**.

Depending on your choice, either the **Disconnect SCSI Disk** wizard or the **Delete SCSI Disk** wizard appears.

- Continue through the wizard, clicking **Next** and **Finish**.

Managing virtual machines in ESI

Procedure

- In the left pane of the ESI window, select **Hypervisors** and one of the hypervisor servers.
- Click **Virtual Machines** in the center pane and select a virtual machine from the list.
- In the **Actions** pane, click **Connect to Host**.

Note

If the virtual host is already in ESI, click **Connect to Host** to open the pane that displays the host information.

- Click **Yes** to confirm that you want to manage this virtual machine host in ESI. The **Add Host** dialog box appears.
- Review the details for the IP address or host name.

Note

[Adding hosts](#) on page 98 provides more information about adding a host.

- Click **Test Connection** to test the connection before adding it.
- Click **Add**.

The host name appears in the center pane.

Attaching virtual disks

Procedure

- In the left pane of the ESI window, select **Hypervisors** and one of the hypervisor servers.
- Click **Virtual Machines** in the center pane and select a virtual machine from the list.
- In the **Actions** pane, click **Attach Disk**.

The **Attach Disk** wizard appears.

- Identify the disk to attach by selecting one of the following options:
 - Virtual hard disk** - see [Attaching a virtual hard disk](#) on page 132
 - Virtual hard disk and create a virtual disk or LUN** - see [Attaching a virtual hard disk and creating a virtual disk or LUN](#) on page 132
 - Pass-through SCSI disk** - see [Attaching a pass-through SCSI disk](#) on page 133
 - Pass-through SCSI disk and create a virtual disk or LUN** - see [Attaching a pass-through SCSI disk and creating a virtual disk or LUN](#) on page 133

Note

If you create a virtual disk or LUN during this process, select **Create Virtual Disk** or **LUN**. The pages for each disk option are different.

Attaching a virtual hard disk

Procedure

1. On the **Select Disk Type** page, select **Virtual Hard Disk**, and then click **Next**.
2. On the **Virtual Hard Disk** page, type the File Path, or browse to select it, and then click **Next**.

The **Hypervisor Settings** or **VMware Settings** page appears.

3. Select the controller and location settings, and then click **Next**.
 4. Click **Next** to continue through the wizard, and then click **Finish**.
-

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Note

[Creating virtual disks](#) on page 115 provides more details on virtual hard disk and hypervisor settings.

Attaching a virtual hard disk and creating a virtual disk or LUN

Procedure

1. On the **Select Disk Type** page, select **Virtual Hard Disk**.
2. Select **Create Virtual Hard Disk or LUN**, and then click **Next**.
3. On the **Virtual Hard Disk** page, select a file name, location, size, and type *fixed* or *dynamic*, and then click **Next**.

The **Hypervisor Settings** or **VMware Settings** page appears.

4. Select the controller and location settings, and then click **Next**.
 5. Click **Next** to continue through the wizard, and then click **Finish**.
-

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Note

[Creating virtual disks](#) on page 115 provides more details on virtual hard disk and hypervisor settings.

Attaching a pass-through SCSI disk

Procedure

1. On the **Select Disk Type** page, select **Passthrough SCSI Disk** and then click **Next**.
2. On the **Passthrough SCSI Disk** page, select the candidate disk from the list, and then click **Next**.

The **Hypervisor Settings** or **VMware Settings** page appears.

3. Select the controller and location settings, and then click **Next**.
 4. Click **Next** to continue through the wizard, and then click **Finish**.
-

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Note

[Creating pass-through SCSI disks](#) on page 107 provides more details.

Attaching a pass-through SCSI disk and creating a virtual disk or LUN

Procedure

1. On the **Select Disk Type** page, select **Passthrough SCSI Disk**.
2. Select **Create Virtual Hard Disk or LUN**, and then click **Next**.
3. On the **Storage System** page, review the details, and then click **Next**.
4. On the **Storage Pool** page, select the storage pool for the disk, and then click **Next**.
5. On the **New LUN** page, specify the LUN count, sequence number, name, description, and other details for the new LUN, and then click **Next**.

The **Hypervisor Settings** or **VMware Settings** page appears.

6. Select the controller and location settings, and then click **Next**.
7. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Note

[Creating pass-through SCSI disks](#) on page 107 provides more details.

Removing virtual disks from a hypervisor

Procedure

1. In the left pane of the ESI window, select **Hypervisors** and one of the hypervisor servers.
2. Click **Virtual Machines** in the center pane and select a virtual machine.
3. Click the plus (+) symbol to view the disks in the virtual machine.
4. Select one or more disks to be removed and click **Remove System** in the **Actions** pane.
5. Click **Yes** to confirm that you want to remove the virtual disks.
The **Remove Virtual Disk** wizard appears.
6. Select **Delete the corresponding virtual file or the passthrough SCSI disk** if you also want to delete the file or disk.
7. Confirm the list of disks to be removed.
8. Click **Next** to continue through the wizard, and then click **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Adding, viewing, and deleting hypervisors

Adding hypervisor servers

You can add a Microsoft Hyper-V or VMware vSphere hypervisor server.

Procedure

1. In the left pane of the ESI window, select **EMC Storage Integrator or Hypervisors**.
2. In the **Actions** pane, click **Add Hypervisor**.

3. In the **Add Hypervisor** dialog box, set the following values.

Option	Description
Server	Host name or IP address of the server that you are adding
Type	Select one of the following hypervisor types: <ul style="list-style-type: none"> • Microsoft Hyper-V • VMware vSphere/vCenter Server
Authentication	Select one of the following options: <ul style="list-style-type: none"> • Current Credentials to use existing server credentials • Specify Credentials to specify a username and password for the server

4. Click **Test Connection** to test the connection before adding it.
5. Click **Add**.
The server name appears in the center pane.

Viewing hypervisor hosts

Procedure

1. In the left pane of the ESI window, select **Hypervisors**, and then select one of the hypervisor servers.
2. Click **Hosts** in the center pane.
Hosts details, such as host names, IP addresses, cluster and datacenter names, and the username, appear.

Viewing hypervisor datastores

You can view all datastores for a hypervisor or view datastores for a specific cluster.

Procedure

1. In the left pane of the ESI window, select **Hypervisors**, and then select one of the hypervisor servers.
2. Click **Datastores** in the center pane.
A list of datastores appears. Datastores are identified as VMFS5 and virtual datastores are identified as VVOL types.
3. Select a datastore from the list and then click the plus (+) symbol.
Datastore information, such as LUNs, storage IDs, capacity, and provision types, appears.

Viewing datastores for a specific cluster

Procedure

1. In the left pane of the ESI window, select **Hypervisors**, and then select one of the hypervisor servers.

2. From the left pane, click the plus (+) symbol for the hypervisor, and then click **Datacenter - ESI**.
3. Click the plus (+) symbol for **Datacenter - ESI** and then click the plus (+) symbol for **Cluster**.
4. Select a cluster from the list, and then click **Datastores**.

The datastore information appears for the cluster.

Creating a hypervisor datastore

Create a datastore from a virtual volume.

Procedure

1. In the left pane of the ESI window, select **Hypervisors**, and then select one of the hypervisor servers.
2. Click **Datastores** in the center pane.
3. In the **Actions** pane, click **Create Datastore**.

The **Create Datastore** wizard appears.

4. In the **Select Disk Type** page, choose whether to create the datastore from a new or existing virtual volume and click **Next**.
5. Select the storage system and click **Next**.
6. Select a storage pool and click **Next**.

This page does not appear for VPLEX storage systems.

7. Perform one of the following steps:
 - If you selected to use an existing LUN:
 - For VPLEX systems, in the **Select a Virtual Volume** page, select a virtual volume and click **Next**.
 - For all other systems, in the **Select a LUN** page, select a LUN and click **Next**.
 - If you selected to use a new LUN:
 - For VPLEX systems, in the **Virtual Volumes Settings** page, specify the virtual volume name, select the cluster, enable **Create New Storage Volume**, and then click **Next**.
 - For other systems, in the **New LUN** page, specify the LUN name, description, and size, and then click **Next**.
8. In the **LUN Masking Settings** page, select the hypervisor initiators and click **Next**.
9. Proceed through the wizard to create a new LUN for the virtual volume. until you reach the **Datastore Preparation Settings** page.
10. In the **Datastore Preparation Settings** page, type the name of the datastore.
11. Continue through the wizard, clicking **Next** and **Finish**.

Note

In the **Progress** page of the wizard, click **More Information** for more progress details. If a problem occurs while you are creating a LUN, an error message appears along with options to resume or roll back the process. After the error is resolved, click **Resume** to resume the process. Click **Rollback** to revert to the previously executed step.

Viewing hypervisor virtual volumes

View virtual volumes for Unity and UnityVSA on an EXS hypervisor.

Procedure

1. Select an ESX hypervisor in the left pane of the ESI GUI.
2. Select the **Virtual Volumes** tab.

Details for all virtual volumes are displayed.

Viewing hypervisor virtual machines

View the virtual machines for a hypervisor or view virtual machines for a specific cluster.

Procedure

1. In the left pane of the ESI window, select **Hypervisors**, and then select one of the hypervisor servers.
2. Click **Virtual Machines** in the center pane, and then select a virtual machine from the list.
3. Click the plus (+) symbol.

Disk information for the virtual machine appears.

Viewing virtual machines for a specific cluster

Procedure

1. In the left pane of the ESI window, select **Hypervisors**, and then select one of the hypervisor servers.
2. In the left pane, click the plus (+) symbol for the hypervisor, and then click **Datacenter - ESI**.
3. Click the plus (+) symbol for **Cluster**.
4. Select a cluster from the list, and then click **Virtual Machines**.

Disk information is displayed for the virtual machines in the selected cluster.

Viewing hypervisor SAN initiators and SCSI LUNs

Procedure

1. In the left pane of the ESI window, select **Hypervisors**, and then select one of the hypervisor servers.
2. In the left pane, click the plus (+) symbol for the hypervisor, and then click **Datacenter - ESI**.

3. Click the plus (+) symbol for **Datacenter - ESI** and then click the plus (+) symbol for **Cluster**.
4. Select a cluster from the list, and then click one of the following:
 - **SAN Initiators**
 - **SCSI LUNs**

The SAN initiator or SCSI LUN details appear.

Deleting hypervisor servers

Procedure

1. In the left pane of the ESI window, select **Hypervisors**, and then select one of the hypervisor servers.
2. In the **Actions** pane, click **Remove System**.
3. Click **Yes** to confirm your selection.

Note

When you remove a hypervisor server from ESI, you must remove all the hosts that are managed by that hypervisor server. Then, you must add the hosts in ESI again to perform any provisioning operations on those hosts.

CHAPTER 12

Managing storage with Microsoft SCOM

This chapter contains the following topics:

- [ESI Service and ESI SCOM Management Packs](#)..... 140
- [ESI Service and Management Packs best practices](#).....140
- [ESI Service overview](#)..... 140
- [ESI SCOM Management Pack Files](#)..... 141
- [Using the ESI Monitoring Management Pack](#)..... 141
- [Setting up optional management pack overrides](#)..... 147

ESI Service and ESI SCOM Management Packs

The ESI SCOM Management Packs enable you to manage EMC storage systems with SCOM by providing consolidated and simplified dashboard views of storage entities.

These views enable you to:

- Discover and monitor the health status and health events of EMC storage systems and system components in SCOM.
- Receive alerts in SCOM for possible problems with disk drives, power supplies, storage pools, and other types of physical and logical components.

Note

ESI Service must be installed and set up on the ESI host system. The ESI Service has the same requirements as the ESI host controller.

ESI Service and Management Packs best practices

Follow these recommendations for best performance and scalability:

- For performance and scalability, install ESI on a controller host computer that is dedicated to ESI and separate from the SCOM Management Group machines.
- For load balancing, use multiple SCOM agents to monitor a large number of storage systems. Also, set up multiple SCOM agents to communicate with one or more ESI hosts running the ESI Service.
- To achieve the best scalability, assign storage systems with a large number of components to different SCOM agents running on the most resourceful computers.
- The **Number of Entities** column in SCOM displays information about the number of entities that the ESI Service uses. To view this column, replace *ESI Service IP* and *HTTPS port* with the applicable values and open this link in a web browser: <https://ESI Service IP.HTTPS port/esi/console/RegisteredSystems>.
- For information about the number of entities that SCOM monitors, open the SCOM Operations Console, connect to the SCOM Management Group, and then select **Operations Manager > Agent Performance > Module Count**.

ESI Service overview

The ESI Service is the communications link between ESI and the ESI SCOM Management Packs.

The ESI Service provides the following functionality:

- A common repository for all registered storage systems and related storage system connection information
- Configures and securely stores the settings and access control policies for all of the registered storage systems
- Authorization of storage system access with the Windows Authentication access control settings

- An entity graph, a meta-model, and a query engine for discovering systems and related components
- An HTTP API for remotely accessing the entity graph and remotely viewing policy and configuration information and operations

ESI SCOM Management Pack Files

- `EMC.SI.Library.mp`: Defines properties for supported storage systems and system components and their relationships.
- `EMC.SI.Discovery.mp`: Contains all of the discoveries for all of the ESI storage systems and system components. At a set interval, the ESI Service creates and updates the collection of classes and relationships that are defined in the library. It discovers all registered storage systems and all of their physical and logical components. Collected data is stored in the System Center Operations Manager database.
- `EMC.SI.Monitoring.mp`: Contains the monitors, rules, and diagnostics for the storage systems and the physical and logical system components. These include disk drives, power supplies, and logical components, such as storage pools and storage volumes. It also monitors the available capacity of some components. Alerts generate when abnormal conditions are detected or the available capacity limit has been reached for a component. Data is stored in the System Center Operations Manager database and data warehouse.
- `EMC.SI.Presentation.mp`: Presents all registered storage systems, systems components, and view definitions that appear in the SCOM console.
- `EMC.SI.Reporting.mp`: Reports on the health and capacity of the storage systems and system components. For example, you can view a report for available storage capacity, storage pool capacity, and snapshot pool capacity in a storage environment. You can also view a report on the most common alerts that were generated during the previous week.
- `EMC.SI.Customization.xml`: Contains all of the overrides and customizations for your storage environment. Import this management pack only during an initial installation. If you import it again, you lose all of the overrides and customizations. The version number of this management pack is 1.0.0.0, which is different from the other management packs. You can increment the version number when you make changes.

Using the ESI Monitoring Management Pack

The ESI Monitoring Management Pack can discover and monitor many different system components using SCOM agents. The monitoring agent retrieves data from the ESI Service by using a RESTful HTTPS connection, which in turn retrieves the data from the supported (registered) systems. The monitoring data is added to the SCOM database.

The ESI Monitoring Management Pack views the components of EMC systems as a topology map. The health of each level depends on the health of the components that roll up to the component.

At the lowest level, the SCOM Management Group monitors the physical and logical components, such as disk drives, power supplies, storage volumes, and virtual volumes. The ESI management packs monitor the operational state of the components. For example, when one or more storage or virtual volumes are in an

unhealthy state, then the unhealthy state is rolled up to the storage groups containing the volumes.

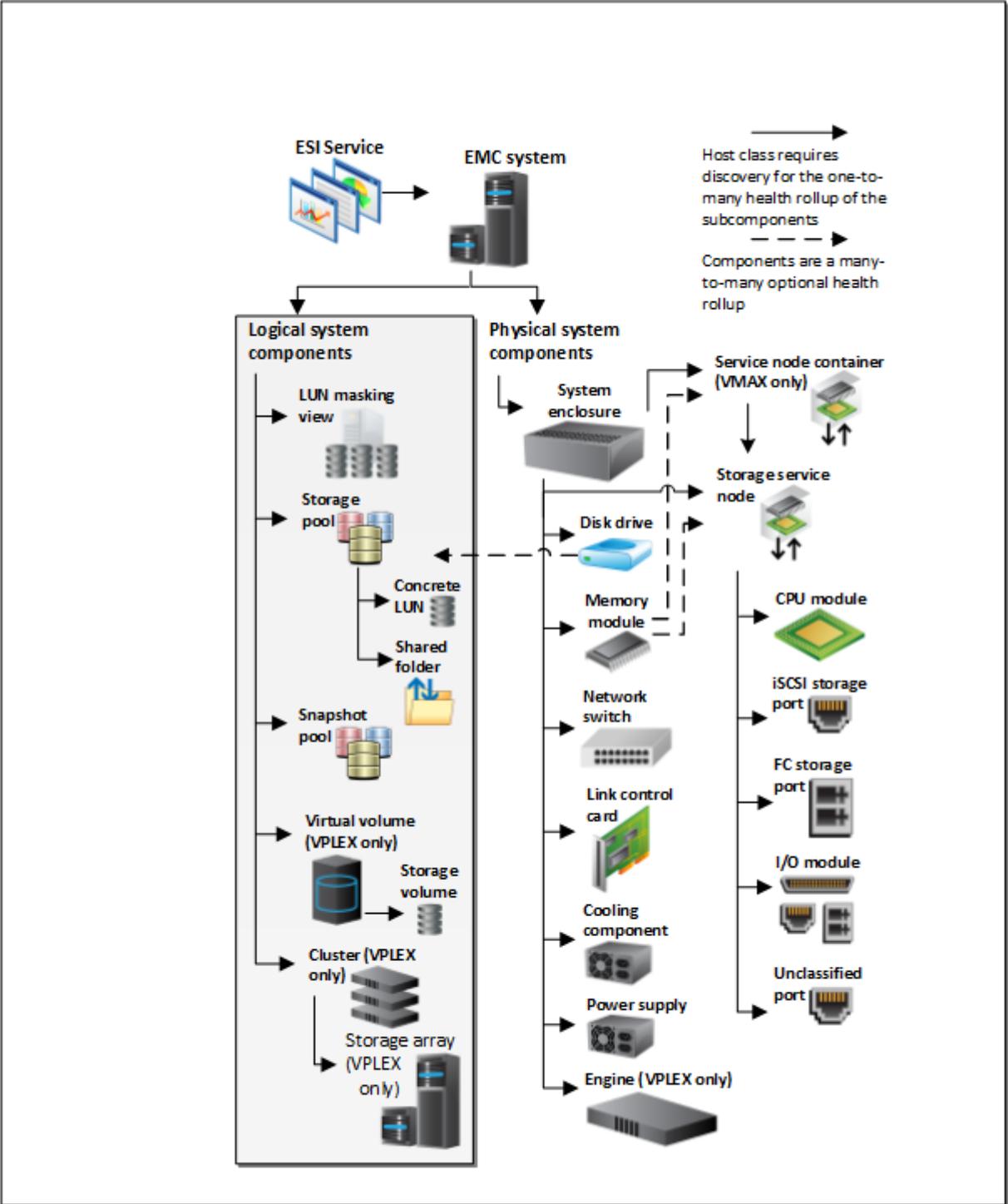
The ESI Monitoring Management Pack provides the following monitors:

Monitor	Action at the set interval
Component health monitors check the health of the system physical components, such as the disk drives and power supplies, and the logical components, such as the storage pools, storage volumes, and virtual volumes. Refer to Monitoring component health on page 144 for more information.	Check the operational status of all of the physical and logical components of a specific class and raise alerts when abnormal conditions are detected.
Capacity monitors check the available capacity of a number of physical and logical system components. Refer to Monitoring capacity on page 146 for more information.	Check the available and subscribed capacity of the components and issue alerts if limits are met or exceeded. These monitors also collect data for SCOM displays and reports.
Viewing monitors on page 147 Viewing and rule monitors provide view of supported systems and the ESI service.	Check the execution of the management pack components and generate alerts when errors occur.

The EMC Storage Integrator Monitoring Management Pack monitors all systems that are registered to the ESI Service and all of the physical and logical system components. The following figure shows which system components are monitored and the health rollup component relationships.

If you are supporting mission-critical applications on VMAX and VNX storage systems, you can also set up fault monitoring, fault reporting, call home, and remote diagnostics features to ensure redundancy for VNX and VMAX arrays.

Figure 2 EMC System Components Monitored by the ESI Monitoring Management Pack



Monitoring component health

When a warning or critical error occurs in a physical or logical component, the health status of the affected component changes and generates an alert. Use the alert description and product knowledge to troubleshoot the issue.

If a component fails and disappears from the data that is collected by ESI Service, an alert is generated to investigate the failure. Use this alert to determine the root cause of a failure. You can also use the component count values that are stored in the database to detect long term trends.

The following rules apply to each component:

- Two collection rules save the count values to the database (DB) and data warehouse (DW) for the specified components of a specified class per parent instance.
- If a component count changes, one warning alert is generated and updated in the active alerts folder in SCOM. If the alert rule for the specified component is enabled, the rule collects data every 90 minutes and calculates the total component count. Multiple alert generations are suppressed to reduce the number of alerts that are generated for the same failure.
The first table below lists the collection and alert rules that are enabled by default and the second table lists the rules that are disabled by default. The total counts for enclosures and LUN storage service nodes includes all of the components in the class hierarchy. The disabled rules are optional for investigating problem alerts. You can enable one or more of the disabled rules when a component or hardware problem requires investigation.

Table 4 Enabled component collection and alert rules

Component	Enabled collection and alert rules
Enclosure	<ul style="list-style-type: none"> • EMC SI Enclosure Physical Components Total Count Collection Rule (DB) • EMC SI Enclosure Physical Components Total Count Collection Rule (DW) • EMC SI Enclosure Physical Components Total Count Alert Rule
LUN storage service node	<ul style="list-style-type: none"> • EMC SI LUN Storage Service Node Physical Components Total Count Collection Rule (DB) • EMC SI LUN Storage Service Node Physical Components Total Count Collection Rule (DW) • EMC SI LUN Storage Service Node Physical Components Total Count Alert Rule
Cluster (VPLEX)	<ul style="list-style-type: none"> • EMC SI VPLEXCluster Count Collection (DB) • EMC SI VPLEXCluster Collection (DW) • EMC SI VPLEXCluster Alert Rule
Cooling component	<ul style="list-style-type: none"> • EMC SI Cooling Component Count Collection (DB) • EMC SI Cooling Component Count Collection (DW) • EMC SI Cooling Component Count Alert Rule

Table 4 Enabled component collection and alert rules (continued)

Component	Enabled collection and alert rules
Disk drive	<ul style="list-style-type: none"> • EMC SI Disk Drive Count Collection(DB) • EMC SI Disk Drive Count Collection(DW) • EMC SI Disk Drive Count Alert Rule
Engine (VPLEX)	<ul style="list-style-type: none"> • EMC SI Engine Count Collection (DB) • EMC SI Engine Count Collection (DW) • EMC SI Engine Count Alert Rule
FC storage port	<ul style="list-style-type: none"> • EMC SI Fc Storage Port Count Collection (DB) • EMC SI Fc Storage Port Count Collection (DW) • EMC SI Fc Storage Port Count Alert Rule
iSCSI storage port	<ul style="list-style-type: none"> • EMC SI iSCSI Storage Port Count Collection (DB) • EMC SI iSCSI Storage Port Count Collection (DW) • EMC SI iSCSI Storage Port Count Alert Rule
Link control card	<ul style="list-style-type: none"> • EMC SI Link Control Card Collection (DB) • EMC SI Link Control Card Collection (DW) • EMC SI Link Control Card Count Alert Rule
Memory module	<ul style="list-style-type: none"> • EMC SI Memory Module Count Collection (DB) • EMC SI Memory Module Count Collection (DW) • EMC SI Memory Module Count Alert Rule
Power supply	<ul style="list-style-type: none"> • EMC SI Power Supply Count Collection (DB) • EMC SI Power Supply Count Collection (DW) • EMC SI Power Supply Count Alert Rule

Table 5 Disabled component collection and alert rules

Component	Disabled collection and alert rules
CPU module	<ul style="list-style-type: none"> • EMC SI CPU Module Count Collection (DB) • EMC SI CPU Module Count Collection (DW) • EMC SI CPU Module Count Alert Rule
Device	<ul style="list-style-type: none"> • EMC SI Storage Device Count Collection (DB) • EMC SI Storage Device Count Collection (DW) • EMC SI Storage Device Count Alert Rule
Extent (VPLEX)	<ul style="list-style-type: none"> • EMC SI Extent Count Collection (DB) • EMC SI Extent Count Collection (DW)

Table 5 Disabled component collection and alert rules (continued)

Component	Disabled collection and alert rules
	<ul style="list-style-type: none"> • EMC SI Extent Count Alert Rule
I/O module	<ul style="list-style-type: none"> • EMC SI IO Module Count Collection (DB) • EMC SI IO Module Count Collection (DW) • EMC SI IO Module Count Alert Rule
Storage array (VPLEX back-end storage system)	<ul style="list-style-type: none"> • EMC SI Storage Array Collection (DB) • EMC SI Storage Array Collection (DW) • EMC SI Storage Array Alert Rule
Storage service node	<ul style="list-style-type: none"> • EMC SI Storage Service Node Count Collection (DB) • EMC SI Storage Service Node Count Collection (DW) • EMC SI Storage Service Node Count Alert Rule
Storage volume	<ul style="list-style-type: none"> • EMC SI Storage Volume Count Collection (DB) • EMC SI Storage Volume Count Collection (DW) • EMC SI Storage Volume Count Alert Rule
Network switch	<ul style="list-style-type: none"> • EMC SI Network Switch Count Collection(DB) • EMC SI Network Switch Count Collection(DW) • EMC SI Network Switch Count Alert Rule
Unclassified port	<ul style="list-style-type: none"> • EMC SI Unclassified Port Count Collection (DB) • EMC SI Unclassified Port Count Collection (DW) • EMC SI Unclassified Port Count Alert Rule
Virtual volume (VPLEX)	<ul style="list-style-type: none"> • EMC SI Virtual Volume Count Collection (DB) • EMC SI Virtual Volume Count Collection (DW) • EMC SI Virtual Volume Count Alert Rule

Monitoring capacity

The available capacity of storage and snapshot pools and groups are monitored. Alerts are generated when certain thresholds are exceeded. These monitors allow a storage administrator to ensure that adequate capacity is available on a system.

The following table shows the default thresholds for the capacity monitors. If the thresholds are not appropriate for your environment, you can override them, either for all instances of the monitors or for specific snapshot, storage pools, or virtual volume.

Table 6 Capacity monitoring threshold values:

Capacity monitors	Warning Thresholds	Error Thresholds
Snapshot Pool available capacity	20%	10%
Storage Pool available capacity	20%	10%
Storage Pool subscribed capacity	70%	90%

Viewing monitors

In the **Monitoring** tab of the **Operations Console**, the EMC Storage Integrator folder contains views for monitoring the supported systems and the ESI Service:

- The top **Active Alerts** view lists the open alerts for all of the systems.
- The **Overall Topology** view displays a hierarchical diagram of all the monitored systems.
- The **ESI Service Overall Health** and the **ESI Windows Service Overall Health** views list the health state and active alerts for the ESI Service and ESI Windows Service.
- Each physical and logical component has an **Overall Health** view showing health state and active alerts.
- The **Diagnostics** folder contains views that are related to the health of the management pack monitoring facilities. The **Monitoring Delays, Errors and Timeouts** view displays events and alerts for monitoring failures, which include: ESI Service authorization problems, communication timeouts, and problems with resource availability on the monitoring agents. The other views display performance data for the ESI Service. Some of the rules collecting this data are disabled by default, so some data might be unavailable. If you have monitoring problems, EMC Support might ask that you enable one or more of these rules for diagnostic tests.

Setting up monitoring maintenance mode

When a monitored object, such as a disk drive or power supply, goes offline for maintenance, the ESI Service detects the condition and might generate numerous alerts and notifications.

To prevent ESI Service and the ESI SCOM Management Packs from creating alerts and notifications, you can set the monitored object to maintenance mode.

When an object is in maintenance mode, alerts, notifications, rules, monitors, automatic responses, state changes, and new alerts are suppressed by SCOM.

For more information on setting a monitored object to maintenance mode in SCOM, refer to *How to Put a Monitored Object into Maintenance Mode in Operations Manager 2007* or *Operations Manager Maintenance Mode (for 2012)* on [Microsoft TechNet](#).

Setting up optional management pack overrides

Change intervals during a customization or when you make significant storage environment changes.

You can also reduce network traffic and increase network performance for your specific storage environment by performing these procedures:

- [Disabling performance data collection](#) on page 148
- [Changing discovery interval overrides](#) on page 148
- [Changing monitoring interval overrides](#) on page 149

After you change intervals and make changes to your overrides and customizations, export and save a copy of the `EMC.SI.Customization.xml` file as a backup of your customization values. If you lose a needed customization, you can import this backup copy to recover your specific customization.

How to Monitor Using Overrides on Microsoft TechNet provides more information on creating overrides.

Disabling performance data collection

To reduce network traffic or to improve performance on servers with slow WAN links, disable the rules that collect performance data.

Each performance counter has a rule for the:

- Operational database
- Data warehouse

Procedure

1. Open the SCOM Operations Console and connect to the SCOM Management Group.
2. Select **Go > Authoring**.
3. In the left pane, select **Rules**.
4. Change the scope to **EMC SI Snapshot Pool** and **EMC SI Storage Pool**.
5. Select and double-click the rule that you want to disable.

Note

The collection rules for the operational database include (DB) in the name. Collection rules for the data warehouse include (DW) in the name.

6. Open the **Override properties** and select to edit the overrides for **all objects of class**.
7. Select the **EMC Storage Integrator Customizations** management pack.
8. Change the **Enabled** property to **False**.
9. Click **Apply** and verify the changed values.
10. Click **OK**, and then click **Close**.
11. Repeat this procedure for each rule that you want to disable.

After you finish

When you disable either rule, you cannot view performance data in the Operations console or in reports. Enable the rules again before you use the views or run any performance data reports.

Changing discovery interval overrides

When you install a new system or change an existing system, the ESI Service takes a set amount of time to send these changes to the ESI management packs on the

SCOM agents. To trigger the discovery of changes, change the override setting for the EMC SI Service Discovery.

Procedure

1. Open the **Override Properties** window for the EMC SI Service Discovery.
2. Clear the **Enabled** override checkbox and then click **Apply**.
3. Before closing the window, select the **Enabled** override checkbox to reset the override. This triggers the discovery of all changes to components regardless of the interval values.

The default intervals for discovery of new components vary depending on the component. If you want SCOM to discover newly added components quicker than the set interval, temporarily change the interval setting. After the changes are discovered, change the interval setting back to the preferred setting for the storage environment.

To change the discovery interval:

4. Open the SCOM Operations Console and connect to the SCOM Management Group.
5. Select **Go > Authoring**.
6. In the left pane, select **Object Discoveries**.
7. Locate and double-click the EMC Discovery for the desired object class.
8. Open the Override properties and select to edit the overrides **for all objects of class**.
9. Change the **Interval (sec)** property to the preferred value. The default values vary depending on the specific object or component.

Note

- You can temporarily reduce the interval to 600 or more seconds (10 minutes) to enable quick discovery of new components.
 - Do not change the **Discovery Timeout (sec)** value. If you reduce it, discoveries can fail before all of the data is retrieved. If you increase it, performance problems can occur.
-

10. Select the **EMC Storage Integrator Customizations** management pack.
11. Click **Apply** and verify the changed values.
12. Click **OK**, and then click **Close**.

Changing monitoring interval overrides

By default, the monitors communicate with the ESI Service approximately every six minutes to check the status of the systems. In a large storage environment, the ESI controller host, the SCOM agent, or the SCOM Management Group machines might experience a resource (CPU or memory capacity) shortage. Increasing the monitoring interval alleviates this type of shortage.

The ESI Service interval setting that is combined with the ESI Service system refresh interval number is the maximum frequency for receiving monitor updates in SCOM. For example, with this interval set to 600 seconds (about 10 minutes) and the ESI Service system refresh interval set to 30 minutes, an updated health state can take up

to 40 minutes. The time intervals can affect the data performance. [Changing the system refresh interval](#) on page 34 provides details on the ESI Service interval.

Refer to *How to Monitor Using Overrides* on Microsoft TechNet for more details.

Procedure

1. Open the SCOM Operations Console and connect to the SCOM Management Group.
2. From the menu bar, select **Go > Authoring** or select **Authoring** from the lower-left pane.
3. From the left pane, select **Monitors**.
4. Locate and double-click the EMC component and monitor that you want to change.
5. Open the Overrides properties and select one of the following choices:
 - For all objects of class: To override the rule for all objects
 - For a specific object of class: To override for a specific object.
6. Select the **EMC Storage Integrator Customizations** management pack.
7. Change the **Interval (sec)** property to the preferred time. The default value is 600 seconds (about 10 minutes).
8. Click **Apply** and verify the changed values.

Note

Do not change the **Timeout Value (sec)**. If you reduce it, monitors can fail before all of the data is retrieved. If you increase it, performance problems can occur.

CHAPTER 13

Troubleshooting

This chapter contains the following topics:

- [Troubleshooting EMC systems and hypervisors](#).....152
- [Troubleshooting the ESI VMAX Adapter](#)..... 155
- [Troubleshooting the ESI RecoverPoint Adapter](#).....156
- [Troubleshooting the SQL Server Adapter](#)..... 157
- [Troubleshooting the ESI Service and ESI SCOM Management Packs](#)..... 157
- [Troubleshooting Active Directory Services](#)..... 163
- [ESI logs](#).....164
- [EMC Sales and Customer Service contacts](#)..... 164

Troubleshooting EMC systems and hypervisors

This section describes known problems and limitations for storage systems and hypervisors.

Symptom	Prevention, resolution, or workaround
ESI does not provision LUNs in oversubscribed storage pools.	The ESI GUI does not support oversubscribed storage pools. Use ESI PowerShell Toolkit to provision LUNs in oversubscribed storage pools.
When a valid description is typed in the Storage Pool Description field, the description might not appear in the column on the Storage Pool tab.	This is a known problem. The description display is for more information and is not critical for system operations.
<ul style="list-style-type: none"> ESI fails to connect to Windows clusters or failover clusters. ESI cannot create, delete, or disconnect a cluster disk. 	<ul style="list-style-type: none"> Confirm that the clusters are healthy, which is an ESI requirement. Before deleting or disconnecting a cluster disk, remove disk resource dependencies.
Ping system timeout fails.	Set the timeout value according to your network status in ESI.
You are unable to connect to a Windows server.	<ul style="list-style-type: none"> Check that firewall rules are enabled on both controller and controllee hosts. Check that remote PowerShell is enabled on both controller and controllee hosts. Check that DNS is configured correctly.
Rescan fails to find a LUN.	<ul style="list-style-type: none"> Check that the FC Zoning is configured correctly. Check that the iSCSI initiator is logged in to the target port. Check that the multipath software is configured correctly.
<ul style="list-style-type: none"> Storage-related data does not display in the host view or cluster view. The Storage pools in the create disk wizard do not load and the wizard is blank. 	<ul style="list-style-type: none"> ESI shows storage related information for a disk or shared folder only when the corresponding storage systems are registered. Verify that the corresponding storage systems are registered with ESI (under Storage Systems). If not, register these storage systems. The storage system might be taking longer than the default time-out value of 60 seconds. Set a higher time-out value (in seconds) in the following Registry key: Key: HKLM\SOFTWARE\EMC\WSI\Config DWORD Value Name: DefaultOperationTimeout

Symptom	Prevention, resolution, or workaround
<p>One of the following error messages occurs:</p> <ul style="list-style-type: none"> • Unable to get host system with given parameters. • EmcVdsProxyService is not available. The operation 'RemoveHostSystem' is unsuccessful. 	<p>This might occur when trying to connect ESI to a Windows host by using ESI PowerShell cmdlets that are running within a remote PowerShell session. ESI does not support running the cmdlets within a remote PowerShell session on the ESI controller host.</p>
<ul style="list-style-type: none"> • When a storage system is added to ESI, it is not listed in PowerShell. • When a storage system is added in PowerShell, it is not listed in ESI. 	<p>Log out of the other application and then reopen it to refresh the list.</p>
<p>PowerShell scripts from earlier versions of ESI that use the <code>Connect-EmcSystem</code> PowerShell cmdlet fail with the "Parameter ConnectionName is needed to create the Host System Object" error.</p>	<p>For <code>ConnectEmcSystem</code>, use <code>ConnectionName</code> instead of <code>HostSystemName</code> for the <code>Creation</code> parameter.</p>
<ul style="list-style-type: none"> • The <code>Set-EmcLunAccess</code> PowerShell cmdlet fails. • An unmasking operation fails. 	<p>Before unmasking a LUN or using the cmdlet, ESI requires that you register all iSCSI and FC HBAs or host initiators used to unmask LUNs on the storage system.</p>
<p>Retrieval of host disks failed: Operation <code>RefreshDisks</code> failed on VDS proxy... error occurs.</p>	<p>When the VDS load operation uses the target host FQDN, this name resolution error occurs. To resolve this error, you must configure the Windows host file on the ESI controller host system with both the short (NETBIOS) and long (FQDN) host names.</p>
<p>For XtremIO systems, errors occur when using the following cmdlets:</p> <ul style="list-style-type: none"> • <code>Get-EmcStorageRegisteredHost</code> • <code>Get-EmcStorageRegisteredInitiator</code> • <code>New-EmcStorageRegisteredHost</code> • <code>New-EmcStorageRegisteredInitiator</code> • <code>Remove-EmcStorageRegisteredHost</code> • <code>Remove-EmcStorageRegisteredInitiator</code> 	<p>ESI does not support using the ESI PowerShell cmdlets related to registering hosts for XtremIO.</p>
<p>In ESI, right-clicking a tree node does not display all the menu options.</p>	<p>This is the default behavior of the MMC framework. Select an item, and then right-click to display the menu options.</p>

Symptom	Prevention, resolution, or workaround
When creating a disk, ESI fails or creates the incorrect volume size.	If you create a host disk and ESI fails or creates the incorrect volume size, you might need to increase the disk size.
If the file system type is FAT32, provisioning a storage volume fails.	FAT32 file system type for volumes is no longer supported in this release.
When you specify both the <code>-ID</code> and <code>-ConcreteLun</code> parameters together with the <code>Get-EmcLun</code> ESI PowerShell cmdlet, an <code>AmbiguousParameterSet</code> exception error occurs.	The <code>-ConcreteLun</code> switch parameter specifies the Concrete LUN type as an optional parameter, through which only Concrete LUNs can be filtered out. Do not use this parameter with the <code>-ID</code> parameter. This parameter supports only block storage systems.
When you create a virtual hard disk or pass-through SCSI disk for a virtual machine, no IDE controllers are listed.	ESI does not support IDE-based disks. Use hypervisors to create IDE-based disks.
For hypervisors, you cannot create new SCSI controllers for virtual machines.	ESI does not support creating new SCSI controllers for creating disks for virtual machines. Use the hypervisor to create new SCSI controllers. Then use ESI to create and attach the disks for virtual machines with these SCSI controllers.
For hypervisors, the Connect to Host action leads to the following error message: <code>Can't retrieve IP from MAC address:...or host name is empty.</code>	Confirm the following: <ul style="list-style-type: none"> • The virtual machine is a part of a reachable domain. • The supported Windows operating system is installed on that virtual machine. • The IP of that virtual machine is configured correctly. • The ESI-mandatory firewall settings are configured correctly if you want to manage the virtual machine in ESI.
For VMware, you cannot expand RDM disks that are attached with virtual compatibility mode.	For VMware systems, ESI does not support RDM disks that are created with virtual compatibility mode. Use ESI to provision disks without the virtual compatibility mode setting.
For a VMware ESX host that is connected with ESI to a virtual machine, when expanding a file-based disk on the virtual machine, the operation fails with an <code>Access to resource settings on the host is restricted to the server that is managing it</code> error message.	This is a VMware restriction for expanding file-based disks, which requires the operation to only succeed when only the vCenter host is connected and the ESX host is disconnected from ESI. Try removing the ESX host and adding the vCenter hypervisor again in ESI. Then try the expand operation again.
For VNX systems, the local administrator account status appears as Offline .	This occurs when a VNX storage array is added with a global account without administrator rights or a local administrator account, and the status is shown as Offline . VNX systems require administrator accounts with a global scope.

Symptom	Prevention, resolution, or workaround
For VNX systems, unable to connect a host disk.	If the VNX storage array does not have Access Logix enabled, the host disk connection fails. VNX block storage systems must have Access Logix enabled on a storage array before you connect a host disk on a Windows host.
For VNX systems, advanced snapshot LUNs can be viewed on the LUNs tab in the ESI GUI, but are not listed in ESI PowerShell.	You can view advanced snapshot LUNs in the ESI GUI. Even though the snapshots exist, you cannot currently view the list with the <code>Get-EmcSnapshotLuns</code> cmdlet.
For VNXe and Hyper-V, when you use the <code>New-EmcLun</code> cmdlet to create a LUN for Hyper-V, a "LUN does not exist" error occurs.	Update your VNXe system to version 2.3.1.20364.
For Unity and VNXe, a snapshot cannot be promoted.	If the resource has no access to the snapshot, a snapshot cannot be promoted for a host. Set up host access to the snapshot, and then the snapshot can be promoted for that host.
When adding a Unity or VNXe system, the <code>System cannot find the file specified</code> error appears when you click Test Connection .	The Unity or VNXe Unisphere CLI is not available on the controller host where ESI is running. Download and install Unisphere CLI from the EMC Online Support website. After installing Unisphere CLI on the controller host, try adding the system again.
When creating volumes for XtremIO, the Login Status is Unknown on the LUN Masking Settings page in the Create Disk wizard.	ESI cannot display the port addresses for all zoned storage system ports for XtremIO systems in the ESI GUI.

Troubleshooting the ESI VMAX Adapter

This section describes known problems and limitations for the ESI VMAX Adapter.

Symptom	Prevention, resolution, or workaround
When creating disks with the Create Disk wizard for VMAX, <code>no appropriate storage system found</code> appears as the only option on the Storage System page.	ESI does not support provisioning disks for host systems (VMware, Windows, and so on) with only iSCSI initiators (HBAs) on VMAX storage systems.
A Symmetrix system with serial not found: 123400688 error occurs when you are adding VMAX systems.	<ul style="list-style-type: none"> When adding VMAX systems to ESI, if you did not include the initial zeroes at the beginning of the serial number, an error will occur. Ensure that you include all of the required twelve digits, which might include a prefix of zeroes. For example: 000123400688.

Symptom	Prevention, resolution, or workaround
Unable to apply a FAST VP policy to an existing storage group.	Try binding the existing LUN or storage pool in the policy storage tier with the Unisphere SYMCLI commands or SMC.
Fails to add a LUN to an existing meta, meta volume, or composite LUN.	<ul style="list-style-type: none"> • Confirm that the LUN is bound. • Confirm that the specified meta volume is striped and the correct size is specified for the LUN.
The <code>Expand-EmcLun</code> cmdlet fails.	<ul style="list-style-type: none"> • Check that the specified capacity is the exact number of bytes for LUN sizes. • For striped meta volumes, check that the specified capacity is the exact multiple for the stripe size.
<p>The following tasks are not available:</p> <ul style="list-style-type: none"> • Cannot create, view, or remove snapshot LUNs in ESI. • When using the following ESI PowerShell cmdlets, results are incomplete or incorrect: <ul style="list-style-type: none"> ▪ <code>Get-EmcSnapshotLun</code> ▪ <code>New-EmcCandidateSnapshotLun</code> ▪ <code>New-EmcSnapshotLun</code> ▪ <code>Remove-EmcSnapshotLun</code> ▪ <code>Restore-EmcSnapshotLun</code> 	These tasks and cmdlets are not available, because snapshot LUNs for VMAX systems are not supported in this release. Support for snapshot LUNs for VMAX is planned for a future release of ESI.

Troubleshooting the ESI RecoverPoint Adapter

This section describes known problems and limitations for troubleshooting the ESI RecoverPoint Adapter.

Symptom	Prevention, resolution, or workaround
When enabling image access to a replica copy, the following error appears: <code>The specified replica copy has no valid snapshot, which is required to enable access to the copy.</code>	Check that the replica copy is enabled, and that the link state is active.
After failing over to a remote replica copy, when enabling the replica copy that used to be the local copy, the following error appears: <code>at least one of the enabled replica copies doesn't have a defined link to the production copy</code>	Use the <code>New-EmcReplicaLink</code> PowerShell cmdlet to create a link from the new production copy to the former local copy.

Symptom	Prevention, resolution, or workaround
<p>When using VMAX with the Exchange Integration, after adding a mailbox database copy on the remote site and adding subsequent copies, the following errors might appear:</p> <ul style="list-style-type: none"> • device is involved in a RecoverPoint Rcopy session and cannot be modified • a specified device is involved in a Remote Copy session and cannot be modified 	<p>The copies are in an EMC RecoverPoint session, so the SMI-S provider prevents all write operations. Do one of the following:</p> <ul style="list-style-type: none"> • Use the ESI GUI or PowerShell Toolkit to disable the replica copy manually, add the copies on the remote site, and then enable the replica copy. For other subsequent copies, repeat these steps. • Alternatively, only add subsequent copies on the local site and maintain only one remote copy on the remote site.

Troubleshooting the SQL Server Adapter

This section describes known problems and limitations for troubleshooting the ESI SQL Server Adapter.

Symptom	Prevention, resolution, or workaround
<p>ESI sets the virtual machine state as Unknown and displays the following connection message: <code>Failed to connect to one or more SQL Servers.</code></p>	<p>This connection message occurs if ESI scans a server and the firewall is blocking the ESI connection or you are not authenticated to access the SQL Server instance. If you select to add the unknown instances, the servers with no detected SQL Server instances are listed as Unknown in ESI.</p>
<p>When you add a SQL Server database to an availability group, the following error occurs: <code>Cannot drop the database database ID, because it does not exist or you do not have permission."</code></p>	<ul style="list-style-type: none"> • Confirm that the ESI host is connected with the correct permissions. • You might have specified a local path for the Shared Network Location field. Shared Network Location must be a Universal Naming Convention (UNC) path.

Troubleshooting the ESI Service and ESI SCOM Management Packs

This section describes known problems and limitations for troubleshooting the ESI Service and ESI SCOM Management Packs.

Symptom	Prevention, resolution, or workaround
<p>When upgrading to the latest version of the ESI SCOM Management Packs, reimporting the management packs in SCOM fails.</p>	<p>When upgrading, SCOM requires that you delete the existing ESI version 2.1 SCOM Management Packs from SCOM before you can install and import the latest version of the SCOM Management Packs.</p>

Symptom	Prevention, resolution, or workaround
	<p>Installing ESI SCOM management packs on page 38 provides instructions.</p>
<p>After upgrading ESI and importing the latest version of the ESI SCOM Management Packs, your override settings for the ESI SCOM management packs no longer exist in SCOM.</p>	<p>The <code>EMC.SI.Customization.xml</code> management pack file contains your SCOM overrides and customizations. When importing the management packs into SCOM, you might have overridden this file and lost your settings. You can reimport the latest backup copy of this file to retrieve your customizations.</p> <hr/> <p>Note</p> <p>This file is installed with version number 1.0.0.0. You can increment the version number when you make changes.</p> <hr/> <p>How to Import a Management Pack in Operations Manager 2007 and How to Import an Operations Manager Management Pack on Microsoft TechNet provides instructions for importing the management packs.</p>
<p>After upgrading ESI, <code>EMC.WinApps.Service.DirectoryServicesSystemDb.*</code> errors occur in your ESI Service event log.</p>	<p>If you are using AD or AD LDS, you might not have unpublished all systems from the ESI Service before upgrading. Clean up the AD container used for the ESI Service, restart the service, and then republish the systems to the ESI Service.</p>
<p>SCOM degrades the health state of the snapshot pool for reserved LUN pools of VNX block systems, regardless of the true health state of the reserved LUN pool in Unisphere, which causes a warning error and generates an alert.</p>	<p>Unisphere does not provide an operational status for reserved LUN pools, so SCOM defaults to "unknown" for the health state of the snapshot pool. This unknown state in SCOM degrades the health of the system, which generates an incorrect warning error and alert in SCOM. Disable the health monitor for the snapshot pools in SCOM to avoid this incorrect warning error and alert. How to Enable or Disable a Rule or Monitor on Microsoft TechNet provides instructions.</p>
<ul style="list-style-type: none"> • SCOM does not discover or monitor some or all system components. • Event 104 appears in the SCOM agent event log, which includes basic connection information and an HTTPS link to EMC SI Service that cannot be completed. • EMC SI Service Discovery in SCOM cannot connect to the ESI Service, or the connection time is unacceptable. • Workflow processes are timing out. 	<ul style="list-style-type: none"> • Confirm that the firewall settings are correct for both the SCOM agent and ESI Service. • Enable and use EMC SI Windows Service Monitoring to confirm that the ESI Service is running on the ESI host. • Open this link on the SCOM Agent machine: <code>https://ESI Service IP:https port/esi/console/graph/Entities?class=StorageSystem</code>, replacing <i>ESI Service IP</i> and <i>https port</i> with the applicable values. Then confirm that the load time displayed at the bottom of the page is less than one second. Repeat this step a few times for consistent results. • Confirm that the SCOM agent connects successfully with the ESI Service. The

Symptom	Prevention, resolution, or workaround
	<p>connection information and link are provided in Event 104. Use the credentials specified in Setting up the Run As profile for the EMC SI Monitoring account on page 39.</p> <p>Open the HTTP link provided in the Event 104 description and confirm that the event completes in less than two minutes. If the connection fails, investigate the cause and update EMC SI discovery overrides accordingly. Changing discovery interval overrides on page 148 provides more details for changing the overrides.</p>
<ul style="list-style-type: none"> • The list of physical or logical components displayed in the views is not current. • SCOM does not discover new system changes. 	<p>If the components do not appear after the set interval refresh time has passed, clear and reset the Enabled override properties setting for the EMC SI Service Discovery in SCOM:</p> <ol style="list-style-type: none"> 1. Open the EMC SI Service Discovery Overrides Properties window. 2. Clear the check box for the Enabled override setting and click Apply. 3. Select the Enabled check box again. <p>This override change triggers the discovery process. Check the Operations Manager event log on the SCOM agent for two sequences: Event 1201 followed by Event 1210. If these occurred, then the discoveries should be current.</p>
<p>The Subscribed Capacity Presentation view in SCOM does not display the system serial numbers.</p>	<p>Create a group for each system and a favorite view for the group:</p> <ol style="list-style-type: none"> 1. In Operations Manager, go to Authoring > Groups > Create a new Group, enter a name, and select EMC Storage Integrator Customizations management pack to save changes. 2. Select Dynamic Members > Create/Edit rules and select EMC SI Storage System > Add. 3. Select Serial Number Equals <i>serial number</i> and click Create. 4. To create a view for the group, select My Workspace > Favorite Views > New > Performance View. Type a name for the view and select collected by specify rules > Storage Pool Available Capacity Performance Collection and click Create. <p>Only the pools of the specified systems are displayed.</p>

Symptom	Prevention, resolution, or workaround
<ul style="list-style-type: none"> • Updates for the component health status take more than 40 minutes to update in the SCOM views. • Long delays exist between changes in health of components and the changes being updated in SCOM views. 	<ul style="list-style-type: none"> • Confirm that the related SCOM agent is running without performance problems. If errors occur, troubleshoot them as described in the previous resolution. • Reduce the ESI Service System Refresh Interval, which is set to 30 minutes by default. Changing discovery interval overrides on page 148 has more details. • Reduce the Interval override for monitors that experience latency, which by default is set to six minutes. • Changing discovery interval overrides on page 148 has more details.
<p>One or more systems do not appear in the SCOM view and are not discovered by SCOM.</p>	<ul style="list-style-type: none"> • Confirm that the related SCOM Agent successfully connects to the ESI Service. • Confirm that the system is registered with the ESI Service. • Confirm that the System Filter file exists on the related SCOM agent and has the correct list of ESI Service Registered System Friendly Names.
<ul style="list-style-type: none"> • SCOM agent is experiencing performance problems due to a large number of monitored component instances. • List of discovered components is not complete. Health state of components is not current and other suggestions do not work. • Event 6022 from the Health Service Script does not appear in the Operations Manager event log on the SCOM agent machine for more than 15 minutes. • Performance counters related to the CPU or memory usage are typically hitting the maximum limits. • Event 21411 from the Health Service modules appears and includes the process will be dropped because it has been waiting in the queue for more than 10 minutes message. • Event 1101 from the Health Service appears multiple times in the Operations Manager Event log on the SCOM agent computer. 	<p>Increase the local data queue on the SCOM agent machine by updating the Registry key:</p> <ol style="list-style-type: none"> 1. Replace <MG> with the SCOM management group name and size, which can be between the default 15360 (15 MB) and 102400 (100 MB): HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Services\HealthService\Parameters \ Management Groups\<MG> \MaximumQueueSizeKb 2. Restart the HealthService. <p>Try the Flush Health Service and Cache task. To do this:</p> <ol style="list-style-type: none"> 1. In Operations Manager, go to Monitoring > Operations Manager > Agent-Details > Agent Health State. In Agent State view, click the SCOM agent machine. 2. In the Health Service Tasks section of the Actions pane, run the Flush Health Service and Cache task. <p>Adding resources to share the monitoring can improve data and I/O performance for large storage environments. Add more SCOM agents or more ESI Services to share the monitoring of multiple systems with heavy traffic. With more than one SCOM agent to monitor one or more ESI Services, you can assign fewer systems to each SCOM agent or each ESI</p>

Symptom	Prevention, resolution, or workaround
	<p>Service. Use the System Filter file to assign systems to different SCOM agents.</p> <p>Sample event logs on page 162 can also provide assistance with diagnosing issues.</p>
<ul style="list-style-type: none"> • SCOM agent changes to a gray state or the discovery is not complete within an acceptable time. • Too many LUN masking views are being discovered. • SCOM does not discover all of the storage groups. • The system has more storage groups than SCOM discovers. 	<p>The discovery override for the EMC SI Storage Group limits the number of discovered instances in SCOM. Confirm that the override has the correct limit.</p> <p>The maximum limit for this override is 5000. To improve performance, change the discovery override to a smaller number.</p>
<ul style="list-style-type: none"> • The ESI Service or the SCOM agents have connection problems. • Time-out error message Event 104 or Event 21402 occurs. 	<p>Check the Operations Manager event log for any events and connect to ESI Service from a web browser on the SCOM agent computer. Refer to Changing HTTP connection defaults on page 28 for more details.</p> <p>Sample event logs on page 162 include an Event 21402 log example.</p>
<p>Proxy Monitoring is not available (grayed out) in Operations Console and Event 623 occurs in Operations Manager.</p>	<p>If the Proxy Monitoring agent is monitoring systems with a large number of components, distribute system monitoring to more proxy agents .</p> <p>Alternatively, make the registry change as described in One or more management servers and their managed devices are dimmed in the Operations Manager Console of Operations Manager.</p>
<p>SCOM does not discover a VPLEX system.</p>	<p>Check event logs for ESI Service errors and also confirm the following:</p> <ul style="list-style-type: none"> • SCOM Management Pack is set up with the correct ESI Service host and SSL port 54501. • ESI Service is running. • The user is in an administrator group (if UAC is enabled, the web browser must be launched with Run As Administrator). • The remote connection to ESI Service uses one of the following: <ul style="list-style-type: none"> ▪ http://<host>:54500/esi/console ▪ https://<host>:54501/esi/console • The firewall settings are correct for both the SCOM agent and ESI Service. • The SSL Certificate on the ESI Service host is set up correctly: <code>Get-ChildItem cert:\LocalMachine\My</code>

Symptom	Prevention, resolution, or workaround
	<ul style="list-style-type: none"> The latest service packs and cumulative updates are deployed on the SCOM agents and clients. SCOM server and agent systems meet the minimum system requirements.
Event 21114 occurs in the Operations Manager event log.	Confirm that HKLM\System\CurrentControlSet\Services\HealthService\Parameters\PersistenceVersion Store Maximum has been changed to 5120 (decimal) .
A VPLEX system does not appear in SCOM for the SCOM monitoring agent.	Check the event log for Event 104 and confirm that the ESI Service connection information is set up correctly in SCOM.
VPLEX discovery times out.	<ul style="list-style-type: none"> The SCOM agent might be monitoring too many systems. Check the event log for events: 6024, 2114, 21402. Use the System Filter file to assign systems to specific SCOM agents.

Sample event logs

The key information is highlighted as bold text in the following event log examples. The events generated from the monitoring agent **Operation Manager** event log and alerts are also added to the **Monitoring Delays, Errors and Timeouts** view in the **Diagnostics** folder.

The following is an example of an event log with connection problems. In this example, Event 21402 occurred because of a disk drive component problem. By locating the problem component class, you can then decide which component monitor to troubleshoot and maybe change that specific time-out interval override while resolving the problem:

```

Log Name: Operations Manager
Source: Health Service Modules
Date: 9/19/2012 1:24:59 PM
Event ID: 21402
Task Category: None
Level: Warning
Keywords: Classic
User: N/A
Computer: PATHENDGSCOM.PATHENDG.emc.com
Description:
Forced to terminate the following process started at 1:24:43 PM
because it ran past the configured time-out 600 seconds.
Command executed: "C:\Windows\system32\cscript.exe" /nologo
"GetEntityStatus.js" 10.5.222.40 7001
c85793d1108ee9f4c30a970941593d7c966a2748 DiskDrive none none True
True false 0
Working Directory: C:\Program Files\System Center Operations
Manager 2007\Health Service State\Monitoring Host Temporary Files
1\126109\
One or more workflows were affected by this.
Workflow name: many
Instance name: many
Instance ID: many
Management group: JerryAir
    
```

The following is an example of an event log that has overloaded resources:

```

Event 21411
Level Warning
Source Health Service Modules
The process will be dropped because it has been waiting in the queue
for more than 10 minutes.
Command executed:      "%windir%\system32\cscript.exe" /nologo
"DiscoverLunStorageServiceNode.js" {934DBB77-5CDA-4EF8-
E2D5-37DE605B11A9} {A86B6475-C74D-7AF0-1B69-AEA88050B9EF}
ZBSCOM2007.ZBEMC.dev 10.5.222.40 7001
3f08b7000dc65c9f29417af195d75cac12f5ea3e
6bec6ca7f35635f45d6d5f54c6e4d7996f3e37b8 none none True False 0
Working Directory:
One or more workflows were affected by this.
Workflow name: EMC.ESI.LunStorageServiceNodeDiscoveryRule
Instance name: Bus 1 Enclosure 1
Instance ID: {A86B6475-C74D-7AF0-1B69-AEA88050B9EF}
Management group: ZBDEV
    
```

Troubleshooting Active Directory Services

This section describes known problems, limitations, or suggestions for troubleshooting the use of Microsoft Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS) with applications supported by ESI.

Symptom	Prevention, resolution, or workaround
<p>The following error occurs when you add systems to ESI Applications that use AD LDS:</p> <pre> EMC.WinApps.Fx.Common.Directory.EsiDirectoryException: Protocol = 'Ldap', Result = 'NotExist'. NoSuchAttribute 00000057: LdapErr: DSID-0C090D11, comment: Error in attribute conversion operation, data 0, v23f0 - System.DirectoryServices.Protocols.DirectoryOperationException: The requested attribute does not exist. </pre>	<p>Confirm that you configured the AD LDS instance schema with msDS-App-Configuration and msDS-Settings. If not, extend the AD LDA instance, and try the operation again. For more information, refer to Setting up AD LDS on page 24.</p>
<p>The following error occurs when you add systems to ESI Applications that use AD DS:</p> <pre> EMC.WinApps.Fx.Common.Directory.EsiDirectoryException: Protocol = 'Ldap', Result = 'NotExist'. NoSuchObject 0000208D: NameErr: DSID-03100213, problem 2001 (NO_OBJECT), data 0, best match of: 'DC=EMC,DC=Storage,DC=Integrator,DC=COM' ---> System.DirectoryServices.Protocols.DirectoryOperationException: The object does not exist. </pre>	<ul style="list-style-type: none"> • For ESI, MMC, and the ESI PowerShell Toolkit, confirm that the container for the user exists. • For the ESI Service, confirm that a container exists for each ESI Service machine name. • Confirm that ESI has read and write permissions for the container and it is accessible to ESI. For more information, refer to Setting up Directory Services integration for ESI applications on page 24.

ESI logs

ESI log details include the following:

- **ESI Controller Default log location:** C:\Users\administrator.ESIAD\AppData\Local\EMC\ESI\Logs
- **Default log level:** Verbose (Valid log levels: Verbose, Information, Warning, Error, Critical)
- **Log level settings:** C:\Program Files\EMC\EMC Storage Integrator\EMC.WinApps.GUI.Mmc.dll.config

To change the log level, edit the initializeData parameter as shown in the Log level setting.

Figure 3 Log level setting

```

6 .....<source name="WSICentralSource">
7 .....<listeners>
8 .....<clear />
9 .....<add type="EMC.WinApps.Fx.Diagnostics.FxTraceListener, EMC.WinApps.Fx.Common" name="tex
10 .....    traceFilePath="%LOCALAPPDATA%\EMC\ESI\Logs"
11 .....    prefix="ESITrace"
12 .....    traceOutputOptions="DateTime, ProcessId, ThreadId"
13 .....    singleFileLengthLimit="1024000"
14 .....    totalFileLengthLimit="40960000">
15 .....<filter type="System.Diagnostics.EventTypeFilter" initializeData="Information" />
16 .....<!-- Other valid settings for traceOutputOptions: ProcessId, ThreadId, Multiple value
17 .....<!--<filter type="EMC.WinApps.Fx.Diagnostics.AdapterTraceFilter, EMC.WinApps.Fx.Common
18 .....</add>
19 .....<!--<add type="System.Diagnostics.ConsoleTraceListener" name="consoleListener" />-->
20 .....</listeners>
21 .....</source>

```

EMC Sales and Customer Service contacts

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

- **Product information:** For documentation, release notes, and software updates, or for information about EMC products, licensing, and service, go to [EMC Online Support](#) (registration required).
- **Technical support:** Go to EMC Customer Service on the EMC Online Support website. To open a service request through EMC Online Support, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.