

# EMC XtremIO Storage Array

Version 4.0

## Software Installation and Upgrade Guide

P/N 302-002-052  
REV 02

Copyright © 2015 EMC Corporation. All rights reserved. Published in the USA.

Published June, 2015

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

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

XtremIO, EMC<sup>2</sup>, EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (<https://support.emc.com>).

# CONTENTS

<b>Preface</b>	
<b>Chapter 1</b>	<b>Installation Prerequisites</b>
	Hardware and Software Requirements..... 10
	Pre-installation Checklist..... 10
	Mounting the Equipment in the Rack..... 10
	Checking the Hardware Installation ..... 11
	Installation Summary Form..... 11
<b>Chapter 2</b>	<b>Installing the Storage Controllers</b>
	General..... 14
	Connecting the Storage Controller ..... 14
	Configuring the Storage Controller..... 15
	Netmask Representation ..... 15
	Loading the Easy-Install CLI..... 16
	Validating the Installed XtremIO Image on the Storage Controller ..... 16
	Configuring the Storage Controller Management Interfaces ..... 17
	Configuring Storage Controllers in a Multiple Cluster Configuration ..... 39
<b>Chapter 3</b>	<b>Installing the XMS Server</b>
	Introduction..... 42
	Deploying a Virtual XMS ..... 42
	Connecting to the XMS ..... 45
	Configuring the XMS Machine ..... 46
	Configuring the XMS and the Management Interface Parameters ..... 46
	Installing the XtremIO Software ..... 48
	Installing the XMS Software..... 48
	Installing the Storage Controllers Software..... 50
	Installing the XtremIO Software in a Multiple Cluster Configuration ..... 53
<b>Chapter 4</b>	<b>Initializing the Cluster Services</b>
	Forming the Cluster..... 56
	Verifying the Cluster Initialization ..... 59
	Configuring the DNS and NTP Servers..... 60
	XMS HTTPS Access ..... 62
	Accessing the XMS via FQDN ..... 62
	Accessing the XMS via Server Name ..... 62
	Configuring the XMS Login Banner ..... 64
<b>Chapter 5</b>	<b>Registering the Cluster in CSI</b>
	Business Services Portal ..... 68
	Creating a New Case..... 68
	Updating the EMC Install Base After an XtremIO Cluster Upgrade ..... 73

<b>Chapter 6</b>	<b>Generating an XtremIO Log Bundle</b>	
	Generating and Collecting the Bundle .....	76
	Uploading the Log Bundle .....	76
	Generating a Log Bundle following a Cluster Creation Failure .....	77
<b>Chapter 7</b>	<b>Configuring ESRS and Connect-Home</b>	
	ESRS and Connect-Home Requirements .....	80
	Pre-conditions for Deploying ESRS and Connect-Home at a Customer site....	80
	ESRS Integration and Configuration.....	81
	Deploying ESRS GW Configuration on the XMS .....	81
	Deploying ESRS IP Client Configuration on the XMS .....	82
	Setting the IP Client Configuration on the XMS .....	85
	Connect-Home Only Integration and Configuration .....	86
	Deploying Email Configuration on the XMS .....	86
	Deploying FTPS Configuration on the XMS .....	87
	Checking the ESRS and Connect-Home Configuration on the XMS.....	87
	Remotely Accessing an XtremIO Cluster, Using ESRS.....	89
	Locating the Page for your XtremIO Cluster in ServiceLink.....	89
	Launching the ESRS Remote Application on the Managed XtremIO Device.....	90
<b>Chapter 8</b>	<b>Upgrading the Cluster Software (NDU)</b>	
	General.....	92
	Cluster Software Upgrade (NDU and Cold Upgrade) .....	93
<b>Chapter 9</b>	<b>Expanding the Cluster</b>	
	General.....	96
	Expanding the Cluster .....	97
	Expanding a 5TB Starter Kit .....	97
	Expanding a Multiple X-Brick Cluster by Adding X-Bricks.....	100
<b>Chapter 10</b>	<b>Verifying the XtremIO Cluster Installation</b>	
	Cluster Functionality Verification .....	102
	Cluster Configuration Verification .....	103
	Knowledge, Equipment and Documentation .....	107
<b>Appendix A</b>	<b>Software Re-Installation</b>	
	Writing the XtremIO Rescue Image to a USB Drive .....	110
	Re-Installing a Storage Controller .....	112
	Re-Installing a Physical XMS.....	114
<b>Appendix B</b>	<b>Configuring Virtual XMS High-Availability</b>	
	Virtual XMS Failures .....	116
	Configuration Alternatives for Virtual XMS High-Availability .....	116
	Configuring a Highly-Available Virtual XMS, Using vSphere HA .....	117
	Configuring a Highly-Available Virtual XMS, Using vSphere Fault Tolerance .....	120

<b>Appendix C</b>	<b>Miscellaneous ESRS Related Tasks</b>	
	Overriding ServiceLink Default Operation when Launching	
	Remote Applications .....	126
	Miscellaneous ESRS GW Procedures.....	127
	Confirming the XtremIO Cluster as a Managed Device in ServiceLink ...	127
	Locating the Device ID of the ESRS GW .....	128
	Troubleshooting/Restoring ESRS GW Connectivity to ServiceLink .....	130
	Expediting Discovery of the XtremIO Device on ESRS GW .....	132
	Removing a Cluster from ESRS.....	133
<b>Appendix D</b>	<b>IPMI Interface Redirection</b>	
	Enabling IPMI Tunneling .....	136



# PREFACE

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

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

---

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

---

## Purpose

This document provides the required information for installing the EMC XtremIO Storage Array.

## Audience

This document is intended for the EMC field support personnel.

## Related Documentation

The following EMC publications provide additional information:

- ◆ *XtremIO Storage Array Site Preparation Guide*
- ◆ *XtremIO Storage Array Pre-Installation Checklist*
- ◆ *XtremIO Storage Array Hardware Installation and Upgrade Guide*
- ◆ *XtremIO Storage Array Installation Summary Form*
- ◆ *XtremIO Storage Array User Guide*
- ◆ *XtremIO Storage Array FRU Replacements Guide*
- ◆ *XtremIO Storage Array Security Configuration Guide*
- ◆ *XtremIO Storage Array Release Notes*

## Conventions Used in this Document

EMC uses the following conventions for special notices:

---

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

---

### Typographical conventions

EMC uses the following type style conventions in this document:

<b>Bold</b>	Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
<i>Italic</i>	Used for full titles of publications referenced in text
Monospace	Used for: <ul style="list-style-type: none"><li>• System output, such as an error message or script</li><li>• System code</li><li>• Pathnames, filenames, prompts, and syntax</li><li>• Commands and options</li></ul>
<i>Monospace italic</i>	Used for variables
<b>Monospace bold</b>	Used for user input
[ ]	Square brackets enclose optional values
	Vertical bar indicates alternate selections — the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

## Where to Get Help

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

**Product information** — For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at:

<https://support.emc.com>

**Technical support** — Go to EMC Online Support and click **Service Center** to learn about several options for contacting EMC Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement, or with questions about your account.

## Your Comments

Your suggestions help us to continue improving the accuracy, organization and overall quality of the user publications. Send your opinions of this document to:

[techpubcomments@emc.com](mailto:techpubcomments@emc.com)



# CHAPTER 1

## Installation Prerequisites

This chapter includes the following topics:

- ◆ Hardware and Software Requirements..... 10
- ◆ Pre-installation Checklist..... 10
- ◆ Mounting the Equipment in the Rack..... 10
- ◆ Checking the Hardware Installation ..... 11
- ◆ Installation Summary Form..... 11

## Hardware and Software Requirements

For hardware and software and firewall requirements, refer to the *XtremIO Storage Array Site Preparation Guide*.

Make sure that you have a KVM, or keyboard and monitor available on-site in case there is a need to re-install a physical XMS and/or Storage Controllers.

Verify that you have the following tools and packages installed on your laptop or on the computer used for installation:

- ◆ SSH client
- ◆ SFTP client
- ◆ XtremIO latest upgrade package

---

**Note:** When you are downloading a software package, access the EMC Support page and verify that the MD5 checksum of the package you downloaded matches the MD5 checksum that appears in the support page for that package.

---

- ◆ Latest version of the following documents:
  - *XtremIO Storage Array Software Installation and Upgrade Guide* (this document)
  - *XtremIO Storage Array Hardware Installation and Upgrade Guide*
  - *XtremIO Storage Array User Guide*
  - *XtremIO Storage Array Security Configuration Guide*

## Pre-installation Checklist

**During the site preparation:**



1. Access the EMC Support page, at [support.emc.com](http://support.emc.com) for XtremIO.
2. Download and complete the *XtremIO Storage Array Pre-Installation Checklist*.
3. When the site preparation is complete, upload the checklist to FTP.

## Mounting the Equipment in the Rack

For rack mounting and cable handling instructions, refer to the *XtremIO Storage Array Hardware Installation and Upgrade Guide*.

## Checking the Hardware Installation

When the hardware installation is complete, verify the following issues:

- ◆ Confirm that power cabling is correct and that power cables are connected to the correct PDU/Power feed.
- ◆ Confirm that Battery Backup Unit (BBU) protected outlets are connected correctly.
- ◆ Confirm that BBU serial connections are correct.
- ◆ Confirm that Serial Attached SCSI (SAS) cable connections are correct.
- ◆ Confirm that InfiniBand (IB) cabling is correct.
- ◆ Confirm that the dedicated IPMI cables are connected to the  MGMT and the  4 ports.
- ◆ Confirm that Fibre Channel (FC) and iSCSI cables are connected to the correct Storage Controllers and ports with respect to path redundancy.
- ◆ Confirm that the Product Number Serial Tag (PSNT) label is attached.
- ◆ Confirm that all hardware components power up and no fail/warning amber LED is active.
- ◆ For a 5TB Starter Kit, confirm that the SSDs occupy slots 0-12 in the DAE.
- ◆ Verify that the IPMI LED on the rear side of the Storage Controller is not amber.
- ◆ Verify that all the cables have been labeled correctly.

## Installation Summary Form

**During the installation, complete the following actions:**

1. Access the EMC Support page for XtremIO at [support.emc.com](http://support.emc.com).
2. Download the *XtremIO Storage Array Installation Summary Form* and fill it in.
3. After installing the cluster, complete filling the Installation Summary Form and upload the checklist to FTP, when you upload the log bundle. For details, see “[Uploading the Log Bundle](#)” on page 76.

---

**Note:** The Installation Summary form and the log bundle files must be uploaded in the same FTP session.

---



# CHAPTER 2

## Installing the Storage Controllers

This chapter includes the following topics:

- ◆ General..... 14
- ◆ Connecting the Storage Controller ..... 14
- ◆ Configuring the Storage Controller..... 15

## General

This chapter provides the procedures for connecting and then configuring the Storage Controllers.

The following configurations scenarios are described:

- ◆ Single X-Brick cluster
- ◆ Multiple X-Brick cluster with sequential IP address range
- ◆ Multiple X-Brick cluster with manual IP address allocation

## Connecting the Storage Controller

**To connect a Storage Controller:**

1. Power up the cluster's components. For details on powering up the components, refer to the *XtremIO Storage Array User Guide*.
2. Allow the Storage Controller to boot. If a console is used, wait for the OS to load; the login screen appears. Otherwise, wait for the boot sequence to complete (this should take a few minutes) and connect to the Storage Controller via the TECH Ethernet port.

**Note:**

- ◆ The TECH Ethernet port has the following pre-configured IP address:  
169.254.254.1/20 (Subnet mask: 255.255.240.0)
- ◆ The following IP settings may be used in the station connecting to the Storage Controller:  
IP: 169.254.254.2  
Subnet mask: 255.255.240.0

---

**Note:** If the TECH port connection fails or the OS fails to load, re-install the Storage Controller with the appropriate Rescue Image (refer to [“Re-Installing a Storage Controller” on page 112](#)). Before re-installing the Storage Controller, contact EMC support.

---

# Configuring the Storage Controller

## Netmask Representation

Starting from XtremIO version 4.0, instead of using a netmask, the user is required to provide a network prefix that is valid for both ipv4 and ipv6, as described in the following table:

Old Format	New Format
255.255.0.0	/16
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

---

**Note:** When the cluster is upgraded to version 4.0, the netmask representation is changed automatically.

---

## Loading the Easy-Install CLI

To load the Easy-Install CLI:

- ◆ Log in to the Storage Controller installation shell as `xinstall`.

```
login as: xinstall
xinstall@xms's password:
```

```
Install menu
```

```
-----
1. Configuration menu
2. Display local storage controller version
3. Check cluster setup menu
4. Perform factory reset
5. Power menu
6. Perform Built-In Self-Test
7. Modify Storage Controller IP address
99. Exit install menu
```

```
> >
```

## Validating the Installed XtremIO Image on the Storage Controller

---

**Note:** Before proceeding, make sure that all Storage Controllers are running the same XIOS version.

---

To validate the installed XtremIO image on the Storage Controller:

1. In the installation shell, enter the number for the Display local storage controller version menu option; the installed XtremIO image version number is displayed.

```
Install menu
```

```
-----
1. Configuration menu
2. Display local storage controller version
3. Check cluster setup menu
4. Perform factory reset
5. Power menu
6. Perform Built-In Self-Test
7. Modify Storage Controller IP address
99. Exit install menu
```

```
> > 2
4.0.0-xxx
```



2. Confirm that the displayed image version matches the version you are installing. For details on the XtremIO Storage Controller Rescue Image version that should be installed on the Storage Controller, refer to the *Release Notes* of the version you are installing.
3. If the reported installed XtremIO image version is old, re-install the appropriate Storage Controller Rescue image on the Storage Controller.

To re-install the SC Rescue Image on the Storage Controller, refer to [“Re-Installing a Storage Controller” on page 112](#).

## Configuring the Storage Controller Management Interfaces

The Storage Controllers are configured all at once via the InfiniBand infrastructure, following a manual configuration of one Storage Controller.

This section details the procedures for configuring the Cluster’s Storage Controllers in the following scenarios:

- ◆ Single X-Brick cluster
- ◆ Multiple X-Brick cluster with sequential IP address range
- ◆ Multiple X-Brick cluster with manual IP address allocation

**Note:** IPMI interfaces are internal and therefore do not require IP addresses. If you wish to access the IPMI port, refer to [“IPMI Interface Redirection” on page 135](#).

### Configuring the Storage Controllers in a Single X-Brick Cluster

When you are configuring Storage Controllers in a single X-Brick cluster, you need to provide both the local and remote Storage Controller IPs.

**To configure the Storage Controller management interfaces in a single X-Brick cluster:**

1. Log in to one of the Storage Controllers, using the xinstall user credentials.
2. In the Installation Menu, enter the number for the `Configuration` menu option.

```
login as: xinstall
xinstall@XMS's password:

Install menu
-----
1. Configuration menu
2. Display local storage controller version
3. Check cluster setup menu
4. Perform factory reset
5. Power menu
6. Perform Built-In Self-Test
7. Modify Storage Controller IP address
99. Exit install menu

> 1
```

3. In the Storage Controller Configuration Sub-Menu, enter the number for the Configure all Storage Controllers menu option.

```
Storage controller configuration sub-menu
-----
1. Configure all storage controllers
2. Configure local storage controller only
3. Check all storage controller configuration
4. Display all storage controllers configuration
99. Exit sub-menu

> 1
```

4. Wait for the Storage Controller discovery process to complete and confirm the result to proceed with the configuration process (in the example, a single X-Brick cluster should discover two Storage Controllers).

```
Detected 2 storage controllers.
Would you like to continue? (yes/no)
> yes
```

5. Provide the first Storage Controller's (in the example X1-SC1) IP address, network prefix and gateway IP address.

```
Local storage controller:
Please enter the Cluster Name (current value: 'xbrickTMP'):
> XtremIO_Cluster
X-Brick Number: 1
Enter Storage Controller ID ['1' for the bottom storage controller,
'2' for the top storage controller] (current value: ):
> 1
Please enter the storage controller management interface IP address
(current value: ):
> 10.103.224.115
Please enter the storage controller management network prefix
(current value: ):
> 20
Please enter the storage controller default gateway IP address
(current value: ):
> 10.103.224.1
Checking network configurations
Checking management IP setup correctness
PASSED
Checking management IP conflict
PASSED
Checking ib0 IP conflict
PASSED
Checking ib1 IP conflict
PASSED
Network configuration check passed
Storage Controller configuration is valid
Would you like to apply the above configuration changes? (yes/no)
> yes
Configuration saved successfully
```

## 6. Provide the second Storage Controller's IP address

```

Remote storage controller:
Cluster Name: XtremIO_Cluster
X-Brick Number: 1
Storage Controller ID: 2
Please enter the storage controller management interface IP address
(current value: ):
> 10.103.224.117
Management Network Prefix: 20
Management Gateway: 10.103.224.1
Checking network configuration
Checking management IP setup correctness
PASSED
Checking management IP conflict
PASSED
Checking ib0 IP conflict
PASSED
Checking ib1 IP conflict
PASSED
Network configuration check passed
Storage Controller configuration is valid
Would you like to apply the above configuration changes? (yes/no)
>yes
Configuration saved successfully
Summary:
Local storage controller: Configuration saved successfully
Remote storage controller: Configuration saved successfully

```

## 7. Select the menu option for Check cluster setup menu.

```

Install menu
-----
1. Configuration menu
2. Display local storage controller version
3. Check cluster setup menu
4. Perform factory reset
5. Power menu
6. Perform Built-In Self-Test
7. Modify Storage Controller IP address
99. Exit install menu

> 3
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

```

---

**Note:** In a single X-Brick configuration it is not necessary to perform the IB Switch connectivity check.

---

8. Select the menu option for Check DAE controllers connectivity.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 1
Verifying single brick DAE connection
-----
Querying LCC.A serial number from current node ... DONE
Querying LCC.B serial number from current node ... DONE
Querying LCC.A serial number from peer node ... DONE
Querying LCC.B serial number from peer node ... DONE
LCC serial numbers check PASSED
Querying CHASSIS serial number from current node ... DONE
Querying CHASSIS serial number from peer node ... DONE
Chassis serial number check PASSED
```

9. Select the menu option for Check dedicated IPMI connectivity.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 3
Checking dedicated IPMI lan 3 is set
PASSED
Checking eth3 link detected
PASSED
```

10. Select the menu option for Check BBU connectivity.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 4
Checking UPS online status
PASSED
Checking UPS charging status
PASSED
```

11. Select the menu option for Check PSU input.

```

Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 5
Checking PS1 status
PASSED
Checking PS2 status
PASSED

```

12. Select the last menu option (Exit sub-menu) to return to the Install menu.
13. Select the last menu option (Exit) to log out.
14. Connect to the Remote Storage Controller via the TECH Ethernet port.
15. Log in to the Storage Controller, using the xinstall user credentials.
16. Select the menu option for Check cluster setup menu.

```

Install menu
-----
1. Configuration menu
2. Display local storage controller version
3. Check cluster setup menu
4. Perform factory reset
5. Power menu
6. Perform Built-In Self-Test
7. Modify Storage Controller IP address
99. Exit install menu

> 3
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

```

17. Select the menu option for Check dedicated IPMI connectivity.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 3
Checking dedicated IPMI lan 3 is set
PASSED
Checking eth3 link detected
PASSED
```

18. Select the menu option for Check BBU connectivity.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 4
Checking UPS online status
PASSED
Checking UPS charging status
PASSED
```

19. Select the menu option for Check PSU input.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 5
Checking PS1 status
PASSED
Checking PS2 status
PASSED
```

20. Select the last menu option (Exit sub-menu) to return to the Install menu.
21. Select the last menu option (Exit) to log out.

## Configuring the Storage Controllers in a Multiple X-Brick Cluster with Sequential Address Allocation

When you are configuring Storage Controllers in a multiple X-Brick cluster using sequential IP address allocation, you need to provide only the first Storage Controller address and the rest of the Cluster's Storage Controllers are automatically assigned with incrementing IP addresses.

**To configure the Storage Controllers in a multiple X-Brick cluster, using sequential IP address allocation:**

1. Log in to one of the Storage Controllers, using the xinstall user credentials.
2. In the installation shell, enter the number for the Configuration menu option.

```
login as: xinstall
xinstall@XMS's password:

Install menu
-----
1. Configuration menu
2. Display local storage controller version
3. Check cluster setup menu
4. Perform factory reset
5. Power menu
6. Perform Built-In Self-Test
7. Modify Storage Controller IP address
99. Exit install menu

> 1
```

3. In the Storage Controller Configuration Sub-Menu, enter the number for the Configure all Storage Controllers menu option.

```
Storage controller configuration sub-menu
-----
1. Configure all storage controllers
2. Configure local storage controller only
3. Check all storage controller configuration
4. Display all storage controllers configuration
99. Exit sub-menu

> 1
```

4. Wait for the Storage Controller discovery process to complete and confirm the result to proceed with the configuration process (in the example, a two X-Brick cluster should discover four Storage Controllers).

```
Detected 4 storage controllers.
Would you like to continue? (yes/no)
> yes
```

5. Wait for the connectivity check to complete.

```
Checking connectivity to all storage controllers:
PASSED
Checking connectivity to IB switches:
PASSED
Checking cross connectivity to the IB switches
PASSED
```

6. Perform the IB switch connectivity test by confirming, for each Storage Controller, that the matching LED on the IBSW is blinking.

```
X1-SC1 (connected to port1 in the IB switch) is now blinking. Do you approve? (yes/no)
> yes
X1-SC2 (connected to port2 in the IB switch) is now blinking. Do you approve? (yes/no)
> yes
X2-SC1 (connected to port3 in the IB switch) is now blinking. Do you approve? (yes/no)
> yes
X2-SC2 (connected to port4 in the IB switch) is now blinking. Do you approve? (yes/no)
> yes
```

7. Provide the first Storage Controller's (in the example X1-SC1) IP address, network prefix and gateway IP address.

```
Storage Controller X1-SC1:
Please enter the Cluster name (current value: ):
> XtremIO_Cluster
X-Brick Number: 1
Storage Controller ID: 1
Please enter the storage controller management interface IP
address (current value: ):
> 10.103.224.115
Please enter the storage controller management network
prefix (current value: ):
> 20
Please enter the storage controller default gateway IP
address (current value: ):
> 10.103.224.1
Checking network configurations
Checking management IP setup correctness
PASSED
Checking management IP conflict
PASSED
Checking ib0 IP conflict
PASSED
Checking ib1 IP conflict
PASSED
Network configuration check passed
Storage Controller configuration is valid
Would you like to apply the above configuration changes?
(yes/no)
>yes
Configuration saved successfully
```



8. Reply **yes** to enable sequential IP addresses allocation to the rest of the Storage Controllers.

```
Would you like to use sequential ip addresses to all other
storage Controllers? (yes/no)
> yes
X1-SC2 Management IP: 10.103.224.116
X2-SC1 Management IP: 10.103.224.117
X2-SC2 Management IP: 10.103.224.118
Do you approve? (yes/no)
>yes

X1-SC2:
Checking network configuration
....
Storage Controller configuration checked ok.
Configuration saved successfully
X2-SC1:
Checking network configuration
....
Storage Controller configuration checked ok.
Configuration saved successfully
X2-SC2:
Checking network configuration
....
Storage Controller configuration checked ok.
Configuration saved successfully

Summary:
X1-SC1: Configuration saved successfully
X1-SC2: Configuration saved successfully
X2-SC1: Configuration saved successfully
X2-SC2: Configuration saved successfully
```

9. Select the menu option for Check cluster setup menu.

```
Install menu
-----
1. Configuration menu
2. Display local storage controller version
3. Check cluster setup menu
4. Perform factory reset
5. Power menu
6. Perform Built-In Self-Test
7. Modify Storage Controller IP address
99. Exit install menu

> 3
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu
```

10. Select the menu option for Check DAE controllers connectivity.

```

Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu
> 1
Verifying communication with all 2-brick nodes
-----
Storage Controller X1-SC1: OK
Storage Controller X1-SC2: OK
Storage Controller X2-SC1: OK
Storage Controller X2-SC2: OK

Verifying DAE connection
-----
Checking X-brick 1:
Querying LCC.A serial number from node 1 ... DONE
Querying LCC.B serial number from node 1 ... DONE
Querying LCC.A serial number from node 2 ... DONE
Querying LCC.B serial number from node 2 ... DONE
LCC serial numbers check PASSED
Querying CHASSIS serial number from node 1 ... DONE
Querying CHASSIS serial number from node 2 ... DONE
Chassis serial number check PASSED
Checking X-brick 2:
Querying LCC.A serial number from node 1 ... DONE
Querying LCC.B serial number from node 1 ... DONE
Querying LCC.A serial number from node 2 ... DONE
Querying LCC.B serial number from node 2 ... DONE
LCC serial numbers check PASSED
Querying CHASSIS serial number from node 1 ... DONE
Querying CHASSIS serial number from node 2 ... DONE
Chassis serial number check PASSED

```

11. Select the menu option for Check IB switches connectivity.

```

Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu
> 2
Checking connectivity to IB switches:
PASSED
Checking cross connectivity to the IB switches
PASSED

```

12. Select the menu option for Check dedicated IPMI connectivity.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 3
Checking dedicated IPMI lan 3 is set
PASSED
Checking eth3 link detected
PASSED
```

13. Select the menu option for Check BBU connectivity.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 4
Checking UPS online status
PASSED
Checking UPS charging status
PASSED
```

14. Select the menu option for Check PSU input.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 5
Checking PS1 status
PASSED
Checking PS2 status
PASSED
```

15. Select the last menu option (Exit sub-menu) to return to the Install menu.

16. Select the last menu option (Exit) to log out.

17. Connect to the second Storage Controller via the TECH Ethernet port.

18. Log in to the Storage Controller, using the xinstall user credentials.
19. Select the menu option for Check cluster setup menu.

```
Install menu
-----
1. Configuration menu
2. Display local storage controller version
3. Check cluster setup menu
4. Perform factory reset
5. Power menu
6. Perform Built-In Self-Test
7. Modify Storage Controller IP address
99. Exit install menu

> 3
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu
```

20. Select the menu option for Check dedicated IPMI connectivity.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 3
Checking dedicated IPMI lan 3 is set
PASSED
Checking eth3 link detected
PASSED
```

21. Select the menu option for Check BBU connectivity.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 4
Checking UPS online status
PASSED
Checking UPS charging status
PASSED
```

22. Select the menu option for Check PSU input.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 5
Checking PS1 status
PASSED
Checking PS2 status
PASSED
```

23. Select the last menu option (Exit sub-menu) to return to the Install menu.
24. Select the last menu option (Exit) to log out.
25. Repeat [step 17](#) to [step 24](#) for the rest of the Storage Controllers in all the clusters.

## Configuring the Storage Controllers in a Multiple X-Brick Cluster with Manual Address Allocation

When you are configuring Storage Controllers in a multiple X-Brick cluster using manual IP address allocation, you need to provide the IP addresses for all of the Storage Controllers in the Cluster.

**To configure the Storage Controllers in a multiple X-Brick cluster, using manual IP address allocation:**

1. Log in to one of the Storage Controllers, using the xinstall user credentials.
2. In the installation shell, enter the number for the Configuration menu option.

```
login as: xinstall
xinstall@XMS's password:

Install menu
-----
1. Configuration menu
2. Display local storage controller version
3. Check cluster setup menu
4. Perform factory reset
5. Power menu
6. Perform Built-In Self-Test
7. Modify Storage Controller IP address
99. Exit install menu

> 1
```

3. In the Storage Controller Configuration Sub-Menu, enter the number for the Configure all Storage Controllers menu option.

```
Storage controller configuration sub-menu
-----
1. Configure all storage controllers
2. Configure local storage controller only
3. Check all storage controller configuration
4. Display all storage controllers configuration
99. Exit sub-menu

> 1
```

4. Wait for the Storage Controller discovery process to complete and confirm the result to proceed with the configuration process (in the example, a four X-Brick cluster should discover eight Storage Controllers).

```
Detected 4 storage controllers.
Would you like to continue? (yes/no)
> yes
```

5. Wait for the connectivity check to complete.

```
Checking connectivity to all storage controllers:
PASSED
Checking connectivity to IB switches:
PASSED
Checking cross connectivity to the IB switches
PASSED
```

6. Verify that all the Storage Controllers are not active

```
xtremapp-pm process is running on storage controller X1-SC1. Please verify that the
cluster is not active ('yes' for not active, 'no' for active)? (yes/no)
> yes
xtremapp-pm process is running on storage controller X1-SC2. Please verify that the
cluster is not active ('yes' for not active, 'no' for active)? (yes/no)
> yes
xtremapp-pm process is running on storage controller X2-SC1. Please verify that the
cluster is not active ('yes' for not active, 'no' for active)? (yes/no)
> yes
xtremapp-pm process is running on storage controller X2-SC2. Please verify that the
cluster is not active ('yes' for not active, 'no' for active)? (yes/no)
> yes
```

7. Perform the IB switch connectivity test by confirming, for each Storage Controller, that the matching LED on the IBSW is blinking.

```
X1-SC1 (connected to port1 in the IB switch) is now blinking. Do you approve? (yes/no)
> yes
X1-SC2 (connected to port2 in the IB switch) is now blinking. Do you approve? (yes/no)
> yes
X2-SC1 (connected to port3 in the IB switch) is now blinking. Do you approve? (yes/no)
> yes
X2-SC2 (connected to port4 in the IB switch) is now blinking. Do you approve? (yes/no)
> yes
```



8. Provide the first Storage Controller's (in the example X1-SC1) IP address, network prefix and gateway IP address.

```
Storage Controller X1-SC1:
Enter the Cluster name:
> XtremIO_Cluster
X-Brick Number: 1
Storage Controller ID: 1
Please enter the storage controller management interface IP
address:
> 10.103.224.115
Please enter the storage controller management network prefix:
> 20
Please enter the storage controller default gateway IP address:
> 10.103.224.1
Checking network configurations
Checking management IP setup correctness
PASSED
Checking management IP conflict
PASSED
Checking ib0 IP conflict
PASSED
Checking ib1 IP conflict
PASSED
Network configuration check passed
Storage Controller configuration is valid
Would you like to apply the above configuration changes? (yes/no)
>yes
Configuration saved successfully
```

9. Reply N, to manually allocate the IP addresses to the other Storage Controllers, and supply the IP addresses for the rest of the cluster's Storage Controllers when required.

```
Would you like to use sequential ip addresses to all other storage
controllers? (yes/no)
> no
X1-SC2:
Cluster Name: XtremIO_Cluster
X-Brick Number: 1
Storage Controller ID: 2
Please enter storage controller management interface IP address
(current value: ):
>10.103.224.117
Management Network Prefix: 20
Management Gateway: 10.103.224.1
Checking network configuration
Checking management IP setup correctness
PASSED
Checking management IP conflict
PASSED
Checking ib0 IP conflict
PASSED
Checking ib1 IP conflict
PASSED
Network configuration check passed
Storage Controller configuration is valid.
Would you like to apply the above configuration changes? (yes/no)
>yes
Configuration saved successfully

X2-SC1:
Cluster Name: XtremIO_Cluster
X-Brick Number: 2
Storage Controller ID: 1
Please enter storage controller management interface IP address
(current value: ):
> 10.103.224.120
Management Network Prefix: 20
Management Gateway: 10.103.224.1
Checking network configuration
Checking management IP setup correctness
PASSED
Checking management IP conflict
PASSED
Checking ib0 IP conflict
PASSED
Checking ib1 IP conflict
PASSED
Network configuration check passed
Storage Controller configuration is valid.
Would you like to apply the above configuration changes? (yes/no)
>yes
Configuration saved successfully
```

```

X2-SC2:
Cluster Name: XtremIO_Cluster
X-Brick Number: 2
Storage Controller ID: 2
Please enter storage controller management interface IP address
(current value: ):
>10.103.224.122
Management Network Prefix: 20
Management Gateway: 10.103.224.1
Checking network configuration
Checking management IP setup correctness
PASSED
Checking management IP conflict
PASSED
Checking ib0 IP conflict
PASSED
Checking ib1 IP conflict
PASSED
Network configuration check passed
Storage Controller configuration is valid.
Would you like to apply the above configuration changes? (yes/no)
>yes
Configuration saved successfully

Summary:
X1-SC1: Configuration saved successfully
X1-SC2: Configuration saved successfully
X2-SC1: Configuration saved successfully
X2-SC2: Configuration saved successfully

```

10. Select the menu option for Check cluster setup menu.

```

Install menu
-----
1. Configuration menu
2. Display local storage controller version
3. Check cluster setup menu
4. Perform factory reset
5. Power menu
6. Perform Built-In Self-Test
7. Modify Storage Controller IP address
99. Exit install menu

> 3
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

```

11. Select the menu option for Check DAE controllers connectivity.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu
> 1
Verifying communication with all 2-brick nodes
-----
Storage Controller X1-SC1: OK
Storage Controller X1-SC2: OK
Storage Controller X2-SC1: OK
Storage Controller X2-SC2: OK

Verifying DAE connection
-----
Checking X-brick 1:
Querying LCC.A serial number from node 1 ... DONE
Querying LCC.B serial number from node 1 ... DONE
Querying LCC.A serial number from node 2 ... DONE
Querying LCC.B serial number from node 2 ... DONE
LCC serial numbers check PASSED
Querying CHASSIS serial number from node 1 ... DONE
Querying CHASSIS serial number from node 2 ... DONE
Chassis serial number check PASSED
Checking X-brick 2:
Querying LCC.A serial number from node 1 ... DONE
Querying LCC.B serial number from node 1 ... DONE
Querying LCC.A serial number from node 2 ... DONE
Querying LCC.B serial number from node 2 ... DONE
LCC serial numbers check PASSED
Querying CHASSIS serial number from node 1 ... DONE
Querying CHASSIS serial number from node 2 ... DONE
Chassis serial number check PASSED
```

12. Select the menu option for Check IB switches connectivity.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu
> 2
Checking connectivity to IB switches:
PASSED
Checking cross connectivity to the IB switches
PASSED
```

13. Select the menu option for Check dedicated IPMI connectivity.

```

Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 3
Checking dedicated IPMI lan 3 is set
PASSED
Checking eth3 link detected
PASSED

```

14. Select the menu option for Check BBU connectivity.

```

Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 4
Checking UPS online status
PASSED
Checking UPS charging status
PASSED

```

15. Select the menu option for Check PSU input.

```

Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 5
Checking PS1 status
PASSED
Checking PS2 status
PASSED

```

16. Select the last menu option (Exit sub-menu) to return to the Install menu.

17. Select the last menu option (Exit) to log out.

18. Connect to the second Storage Controller via the TECH Ethernet port.

19. Log in to the Storage Controller, using the xinstall user credentials.
20. Select the menu option for Check cluster setup menu.

```
Install menu
-----
1. Configuration menu
2. Display local storage controller version
3. Check cluster setup menu
4. Perform factory reset
5. Power menu
6. Perform Built-In Self-Test
7. Modify Storage Controller IP address
99. Exit install menu

> 3
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu
```

21. Select the menu option for Check dedicated IPMI connectivity.

```
Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 3
Checking dedicated IPMI lan 3 is set
PASSED
Checking eth3 link detected
PASSED
```

22. Select the menu option for Check BBU connectivity.

```

Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 4
Checking UPS online status
PASSED
Checking UPS charging status
PASSED

```

23. Select the menu option for Check PSU input.

```

Validate system setup sub-menu
-----
1. Check DAE controllers connectivity
2. Check IB switches connectivity
3. Check dedicated IPMI connectivity
4. Check BBU connectivity
5. Check PSU input
99. Exit sub-menu

> 5
Checking PS1 status
PASSED
Checking PS2 status
PASSED

```

24. Select the last menu option (Exit sub-menu) to return to the Install menu.

25. Select the last menu option (Exit) to log out.

26. Repeat [step 18](#) to [step 25](#) for the rest of the Storage Controllers in all the clusters.

## Configuring Storage Controllers in a Multiple Cluster Configuration

Refer to [“Installing the XtremIO Software in a Multiple Cluster Configuration”](#) on page 53.





# CHAPTER 3

## Installing the XMS Server

This chapter includes the following topics:

- ◆ Introduction ..... 42
- ◆ Deploying a Virtual XMS ..... 42
- ◆ Connecting to the XMS ..... 45
- ◆ Configuring the XMS Machine ..... 46
- ◆ Installing the XtremIO Software ..... 48

## Introduction

XMS installation is required only when deploying the first XMS. However, in a multiple cluster environment, when adding clusters, the XMS is already deployed. Therefore, there is no need to install the XMS.

## Deploying a Virtual XMS

---

**Note:** XtremIO is a RAID protected storage or VMware vSphere HCL-approved shared storage if virtual XMS high-availability is required. Shared storage used in this case should not originate from an XtremIO cluster.

---

An OVA image (VMware template machine file type), which includes all the required packages for installing the XMS, is provided.

To install a virtual XMS, deploy the OVA template.

---

**Note:** The OVA template can be deployed by the customer ahead of the installation. If this has been done, skip to “[Connecting to the XMS](#)” on page 45 to connect and configure the deployed virtual XMS.

---

### To deploy an OVA image:

1. Access the EMC Support page for XtremIO.
2. Download the OVA Template. For details on which OVA Template to download from the Support page, refer to the *XtremIO Storage Array Release Notes* of the version you are installing.

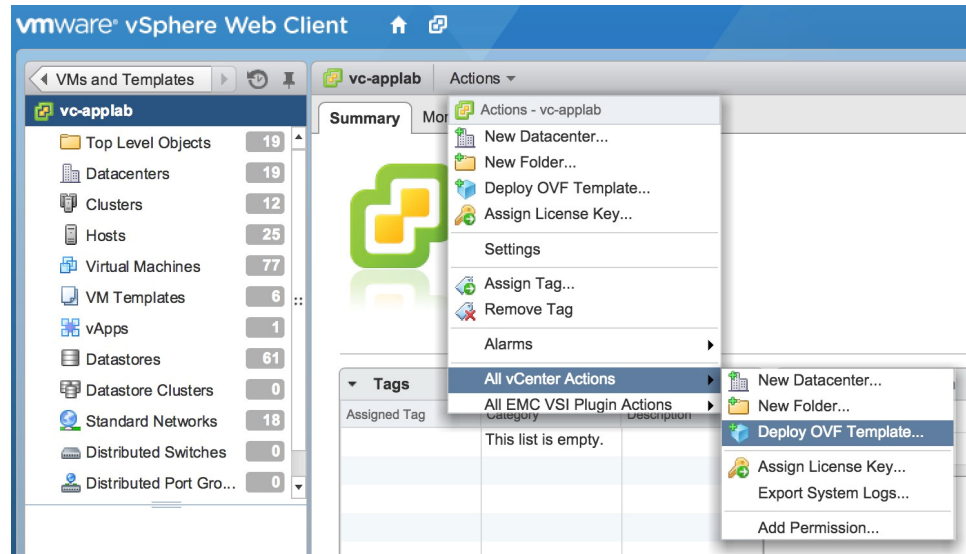
---

**Note:** Before proceeding, access the EMC Support page and verify that the MD5 checksum of the package you downloaded matches the MD5 checksum that appears in the support page for that package.

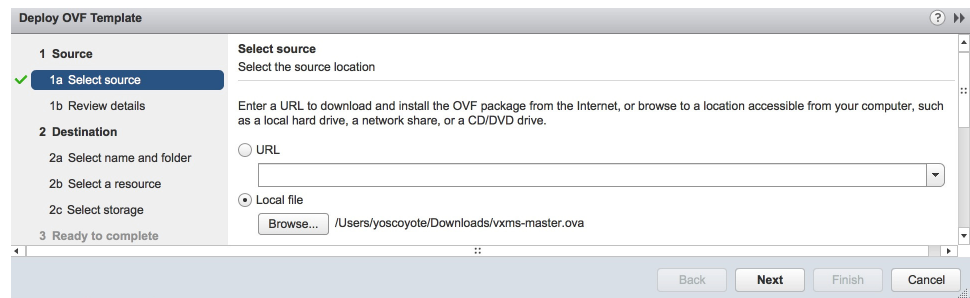
---

3. Log in to the vCenter Server, using the vSphere Web Client.

4. Select an inventory object that is a valid parent object of the virtual XMS machine (e.g. datacenter, folder, cluster, resource pool or host).



5. In the 1a Select Source pane, click **Local file** and then click **Browse**.



6. Select the XMS OVA template and click **Next**.
7. In the 1b Review Details pane, review the details of the OVA Template and click **Next**.
8. In the 2a Select name and folder pane, type a name for the virtual XMS and select a destination folder. Click **Next**.
9. In the 2b Select a resource pane, select a server/cluster to run the virtual XMS and click **Next**.
10. In the 2c Select storage pane, select a datastore to provision the virtual XMS.
11. In the Select virtual disk format drop-down list, select **Thin Provision** disk format for the XMS's virtual disk and click **Next**.

**Note:** It is recommended to deploy a virtual machine with 'Thin Provision' settings to ensure that the XMS does not consume more space than it actually requires. With XtremIO version 4.0, 200GB of disk capacity is pre-allocated for the virtual XMS, following the cluster initialization.

12. In the 2d Select networks pane, configure the network used for the virtual XMS, and click **Next**.

13. In the 3 Ready to complete pane, verify that the virtual XMS VM that is about to be created meets (or exceeds) the following requirements:

Parameter	Value
RAM	8GB capacity
CPU	2 X vCPU
NIC	1 X vNIC
Virtual HD	Single HD with 900GB capacity [recommended (thin-provisioned)]

14. Click **Finish** to deploy the template.
15. Connect to the virtual XMS via a physical console, using a pre-defined IP address or a vSphere Web Client console.
16. Select **Actions > All vCenter Actions > Deploy OVF Template**.

**To configure VM High Availability (recommended):**

- ◆ See [“Configuring Virtual XMS High-Availability” on page 115](#).

# Connecting to the XMS

## To connect to the XMS:

1. Make sure that the XMS is powered up, as described in the *XtremIO Storage Array User Guide*.
2. Connect to the XMS:
  - Physical XMS:
    1. Power up the XMS (for details, see the *XtremIO Storage Array User Guide*).
    2. Allow the XMS to boot. If a console is used, wait for the OS to load; the login screen appears. Otherwise, wait for the boot sequence to complete (this should take a few minutes) and connect to the XMS via the TECH Ethernet port.

---

### Note:

- The TECH Ethernet port has the following pre-configured IP address:  
169.254.254.1/20.
  - The following IP settings may be used in the station connecting to the XMS:  
IP: 169.254.254.2  
Subnet mask: 255.255.240.0
- 

**Note:** If the TECH port connection fails or the OS fails to load, re-install the physical XMS with the appropriate Rescue Image (refer to [“Re-Installing a Physical XMS” on page 114](#)). Before re-installing the physical XMS, contact EMC support.

---

- Virtual XMS:
  1. Launch the vSphere Client and navigate to **Inventory > Hosts and Clusters**.
  2. In the **Inventory**, locate the Virtual XMS VM.
  3. Right-click the Virtual XMS VM and click **Open Console**.

## Configuring the XMS Machine

The XMS management IP is defined by the Easy-Install process.

---

**Note:** If you are expanding an existing cluster by adding Storage Controllers, the XMS is already deployed and there is no need to re-configure it.

---

## Configuring the XMS and the Management Interface Parameters

To configure the management interface parameters:

1. Log in to the XMS, using the xinstall user credentials.
2. In the Install menu, type the number for the Configuration option.

```
login as: xinstall
xinstall@vxms-xbrick238's password:
Last login: Sun Jan 12 16:29:15 2014 from 10.76.51.31
XtremIO install interface
Checking XMS health
XMS health check passed
Checking network configuration
Checking management IP setup correctness
PASSED
Checking management IP conflict
PASSED
Network configuration check passed

Install menu
1. Configuration
2. Check configuration
3. Display configuration
4. Display installed Xtremapp version
5. Perform XMS installation only
6. Perform "fresh" installation (XMS + storage controllers)
7. Set DC Agent configuration
8. Start DC Agent Installation
9. Set Policy Manager configuration
10. Start Policy Manager Installation
11. Run XMS Recovery
12. Reboot
99. Exit

> 1
```

3. Provide the XMS host name.

```
Please enter the XMS appliance host name (current value: )
> vxms-XtremIO
```

---

**Note:** The request refers to the host name of the XMS.

---

4. Set the DNS configuration (optional).

---

**Note:** If you intend to connect the XMS to ESRS, configuring DNS is mandatory.

---

```

Enter Usage of DNS (Y/N) (previous value: 'Y'):
>Y
Input received: 'Y'
Enter Domain name suffix (previous value: ''):
>MyCompany.com
Input received: 'MyCompany.com'
Enter Primary DNS Server (previous value: )
10.76.208.16
Input accepted 10.76.208.16
Enter Usage of secondary DNS server (Y/N) (previous value: 'N'):
>Y
Input received: 'Y'
Enter Secondary DNS Server (previous value: )
10.76.208.20
Input accepted 10.76.208.20

```

5. Provide the XMS's IP address, network prefix and default gateway IP address.

```

Please enter the XMS management interface IP address (current
value: ):
> 10.103.224.119
Please enter the XMS management network prefix (current value: ):
> 20
Please enter the XMS default gateway IP address (current value: ):
> 10.103.224.1

```

6. Wait for the script to validate the configuration change and approve it.

```

Checking network configuration
Checking management IP setup correctness
PASSED
Checking management IP conflict
PASSED
Network configuration check passed
XMS configuration is valid
Would you like to apply the above configuration changes
(yes/no)? >yes
> yes
Configuration saved successfully

```

## Installing the XtremIO Software

Installing the XtremIO software consists of two steps:

- ◆ Installing the XMS software
- ◆ Installing the Storage Controllers software

When you are installing a new cluster (XMS and Storage Controllers), perform both procedures. However, if you are adding clusters to existing clusters in a multiple cluster configuration, the XMS is already deployed and there is no need to re-install it.

## Installing the XMS Software

---

**Note:** This section is relevant only when deploying a new XMS. In a multiple cluster configuration, if the XMS is running an older xtremapp version than the one that is about to be installed, upgrade the XMS. Refer to [“Cluster Software Upgrade \(NDU and Cold Upgrade\)” on page 93](#) for details.

---

Before installing the XtremIO software on the cluster, you should upload the necessary software package to the XMS, using SFTP.

### To upload the Installation package:

1. Access the EMC Support page for XtremIO to acquire the latest XtremIO software package for the version you are installing. For details on which XtremIO software package to download, refer to the *Release Notes* of the version you are installing.

---

**Note:** Verify that the package version is the latest released version available on the EMC Support page. Refer to EMC KB # 184424 (<https://support.emc.com/kb/184424>) for details.

---

---

**Note:** Before proceeding, access the EMC Support page and verify that the MD5 checksum of the package you downloaded matches the MD5 checksum that appears in the support page for that package.

---

2. Upload the package to the XMS (`/images/`). Use an SFTP client (e.g. Filezilla, WinSCP) to log in as the `xmsupload` user, and transfer the package downloaded on your computer to the XMS.  
When the file transfer is complete, close the SFTP client and re-open the SSH client (putty) to the XMS.



**To install the XMS software:**

1. Log in to the XMS, using the xinstall user credentials.
2. In the Install menu, enter the number for the Perform XMS installation only option.

```

login as: xinstall
xinstall@vxms-xbrick238's password:
Last login: Sun Jan 12 16:29:15 2014 from 10.76.51.31
XtremIO install interface
Checking XMS health
XMS health check passed
Checking network configuration
Checking management IP setup correctness
PASSED
Checking management IP conflict
PASSED
Network configuration check passed

Install menu
1. Configuration
2. Check configuration
3. Display configuration
4. Display installed Xtremapp version
5. Perform XMS installation only
6. Perform "fresh" installation (XMS + storage controllers)
7. Set DC Agent configuration
8. Start DC Agent Installation
9. Set Policy Manager configuration
10. Start Policy Manager Installation
11. Run XMS Recovery
12. Reboot
99. Exit

> 5

```

3. Enter the installation image filename to launch installation.

```

Enter Installation image filename (previous value: ''):
> upgrade-to-4.0.0-xxx.tar
Running: /xtremapp/utils/install.py 0 0
/var/lib/xms/images/upgrade-to-4.0.0-xxx.tar
Installing XMS
Reformatting XMS
Installation ended successfully

```

When installation is completed, the system reboots the XMS and closes the XMS session.

4. Re-log in to the XMS, using the xinstall user credentials to proceed.

## Installing the Storage Controllers Software

Before installing the XtremIO software on the cluster, you should upload the necessary software package to the XMS, using SFTP.

### To upload the Installation package:

---

**Note:** If the package is already deployed, skip this procedure.

---

1. Access the EMC Support page for XtremIO to acquire the latest XtremIO software package for the version you are installing. For details on which XtremIO software package to download, refer to the *Release Notes* of the version you are installing.

---

**Note:** Verify that the package version is the latest released version available on the EMC Support page. Refer to EMC KB # 184424 (<https://support.emc.com/kb/184424>) for details.

---

---

**Note:** Before proceeding, access the EMC Support page and verify that the MD5 checksum of the package you downloaded matches the MD5 checksum that appears in the support page for that package.

---

2. Upload the package to the XMS (/images/). Use an SFTP client (e.g. Filezilla, WinSCP) to log in as the `xmsupload` user, and transfer the package downloaded on your computer to the XMS.  
When the file transfer is complete, close the SFTP client and re-open the SSH client (putty) to the XMS.

**To install the Storage Controllers software**

1. Log in to the XMS, using the xinstall user credentials.
2. In the Install menu, enter the number for the Install Storage Controllers only option.

```
login as: xinstall
xinstall@xms's password:

XtremIO install interface
Checking XMS health
XMS health check passed
Checking network configuration
Checking management IP setup correctness
PASSED
Checking management IP conflict
PASSED
Network configuration check passed

Install menu
-----
1. Configure XMS
2. Check XMS configuration
3. Display XMS configuration
4. Display XMS version
5. Install XMS only
6. Install Storage Controllers only
7. Configure ESRS IP Client
8. Install ESRS IP Client
9. Configure ESRS Policy Manager
10. Install ESRS Policy Manager
11. Recover XMS
12. Power menu
13. Collect log bundle
14. Enable temporary IPMI access
15. Restore XMS data
99. Exit

> 6
```

3. Enter the Management Storage Controller IP (it is recommended to use X1-SC1 as management), the number of X-Bricks and the installation image file name. Wait for the installation to complete successfully.

```
Please enter management Storage Controller
> 10.103.224.115
Please enter expected number of bricks:
> 2
Please enter installation image filename:
> upgrade-to-4.0.0-xxx.tar
Running: /xtremapp/utils/fresh_install.py 10.103.224.115 2
/var/lib/xms/images/upgrade-to-4.0.0-xxx.tar skip-xms

Waiting for storage controllers installation, found 4
storage controllers

Copying upgrade file to all storage controllers:
10.103.224.122, 10.103.224.120, 10.103.224.117,
10.103.224.115

Stopping xtremapp on all storage controllers...
Setting System WWNN/WWPN identifiers
Upgrading Firmwares...
Rebooting storage controllers...
Executing xtremapp-reformat on storage controllers...
Validating all sensors
Waiting for PMs to come up & enable CLST
Installation ended successfully
```

## Installing the XtremIO Software in a Multiple Cluster Configuration

When installing the XtremIO software in a multiple cluster configuration, there are two possible situations:

- ◆ All clusters are new.
- ◆ Some of the clusters and the XMS are already deployed and one or more new clusters are added to them.

**To install the XtremIO software in a multiple cluster configuration when all the clusters are new:**

1. Configure the XMS, using xinstall. Refer to [“Configuring the XMS and the Management Interface Parameters” on page 46.](#)
2. Configure the first cluster, using xinstall. Refer to [“Configuring the Storage Controller Management Interfaces” on page 17.](#)
3. Install the XMS. Refer to [“Installing the XMS Software” on page 48.](#)
4. Install the first cluster’s Storage Controllers. Refer to [“Installing the Storage Controllers Software” on page 50.](#)
5. Create the cluster. Refer to [“Forming the Cluster” on page 56.](#)
6. Configure the next cluster, using xinstall. Refer to [“Configuring the Storage Controller Management Interfaces” on page 17.](#)
7. Install the Storage Controllers of the cluster. Refer to [“Installing the Storage Controllers Software” on page 50.](#)
8. Create the cluster. Refer to [“Forming the Cluster” on page 56.](#)
9. Repeat steps 6 to 8 for all of the remaining clusters.

---

**Note:** The Storage Controller auto discovery process is performed for each cluster separately.

---

**To install the XtremIO software in a multiple cluster configuration when adding new clusters to existing clusters (XMS is deployed):**

1. In the xinstall menu, type the number for the `Display XMS version` menu option. Make sure that the installed XMS has the correct version. If the XMS’s version is older than the one in the added clusters, upgrade the XMS. Refer to [“Cluster Software Upgrade \(NDU and Cold Upgrade\)” on page 93.](#)
2. Configure the first cluster, using xinstall. Refer to [“Configuring the Storage Controller Management Interfaces” on page 17.](#)
3. Install the first cluster’s Storage Controllers. Refer to [“Installing the Storage Controllers Software” on page 50.](#)
4. Create the cluster. Refer to [“Forming the Cluster” on page 56.](#)
5. Repeat steps 2 to 4 for all of the remaining clusters.
6. Re-configure the ESRS GW (if it is deployed). Refer to [“Deploying ESRS GW Configuration on the XMS” on page 81.](#)



# CHAPTER 4

## Initializing the Cluster Services

This chapter includes the following topic:

- ◆ Forming the Cluster ..... 56
- ◆ Verifying the Cluster Initialization ..... 59
- ◆ Configuring the DNS and NTP Servers ..... 60
- ◆ XMS HTTPS Access ..... 62
- ◆ Configuring the XMS Login Banner ..... 64

## Forming the Cluster

To form the cluster:

1. Log in to XMCLI as tech.
2. Verify the XMS version by running the following command:

```
show-xms
```

```
xmcli (tech) > show-xms
Name Index   SW-Version  Xms-IP-Addr  Xms-Mgmt-Ifc REST-API-Protocol-Version IP-Version  ...
xms  1       4.0.0-xxx   10.103.224.119 eth0          2.0          ipv4        ...
```

3. Log in to the XMS shell as xmsadmin.
4. Type tech at the Username prompt.
5. Enter the password to the tech user account.
6. Run the following CLI Command:  

```
create-cluster expected-number-of-bricks=<i>
sc-mgr-host="<j>" cluster-name="<k>"
```

where:

- <i> = the number of X-Bricks in the cluster
- <j> = the management IP address of one of the Storage Controllers (use the same Storage Controller specified in [“Installing the Storage Controllers Software” on page 50](#)).
- <k> = the cluster name

---

**Note:** Clusters that support encryption are created encrypted by default.

---



---

**Note:** Progress indicators enable you to monitor the cluster creation process by displaying the percentage completed and the current phase. It is recommended to keep the CLI window in a maximized mode. Minimizing the window may cause the progress bar to be displayed on new lines instead of the same line.

---

Proceed to the next step when the cluster creation confirmation message `Cluster <cluster-name> [<cluster index in XMS>] created appears.`



The following example shows a successful cluster formation output:

```

Login as: xmsadmin
xmsadmin@10.103.224.115's password:
Last login: Fri Jun 12 02:29:30 2015 from user1.company.com
Username: tech
Password:
Connect XMS on 10.103.224.115:443: 42502: version 4.0 build xxx
xmcli (tech)> create-cluster sc-mgr-host="10.103.224.115" expected-number-of-bricks=2 cluster-name=XtremIO_Cluster
Creating a cluster may cause data loss. Please type the following to continue or hit enter to abort
I confirm that create cluster may cause data loss
Creating cluster "XtremIO_Cluster"...
Cluster-Name      Index Storage-Controller-Name Index Mgr-Addr      Brick-Name Index
XtremIO_Cluster  1      X1-SC1                1      10.103.224.115 X1          1
XtremIO_Cluster  1      X1-SC2                2      10.103.224.116 X1          1
XtremIO_Cluster  1      X2-SC1                3      10.103.224.117 X2          2
XtremIO_Cluster  1      X2-SC2                4      10.103.224.118 X2          2

[-] 0% Discover Cluster Configuration (elapsed time 00:00:28)
[\] 0% Activating Cluster XtremIO_Cluster (elapsed time 00:00:38)
[#####\] 15% Establishing RDMA connections with Storage Controllers (elapsed
time 00:00:51)
[#####] 46% Loading the repository (elapsed time 00:00:56)
[#####|] 61% Activating HAM (elapsed time 00:01:47)
[#####-] 84% SSD firmware upgrade (elapsed time 00:03:53)
[#####] 100% Done! (elapsed time 00:04:07)
Cluster XtremIO_Cluster [1] created

```

**Note:** This step takes approximately 15 minutes for a single X-Brick. In larger environments it may take longer to complete.

- When cluster creation is completed, type `yes` to perform a BBU connectivity check. You can abort the check during a time frame of ten seconds following each BBU check.

**Note:** The BBU connectivity check is mandatory. Failing to perform it may compromise High Availability.

In the following example, the BBU connectivity check has discovered errors.

```

Run BBUs connectivity check (recommended)? (Yes/No): Yes
BBU connectivity check started (may take several minutes)
Validating X1-BBU port 1 connectivity (1/4)
[*****/] 15% (elapsed time 00:00:19)
ERRORS DETECTED:
X1-BBU port 1 connectivity check results: BBU port should be connected to X1-SC1-PSU-R but is currently connected
to X1-SC1-PSU-L
...
Power scheme should be adjusted according to EMC recommendations.
xmcli (tech)>

```

8. If the connectivity check detects errors, take the necessary steps to resolve them and run the `check-bbu-connectivity` command to verify the correction.

---

**Note:** If a BBU is not sufficiently charged, the connectivity check skips it. In this case, wait until this BBU is sufficiently charged and perform the test again.

---



---

**Note:** If the XMS was disconnected during the BBU connectivity check, causing the procedure to abort, it is recommended to run the following command on all BBUs and all outlets:

---

```
modify-bbu-power bbu-id=<BBU ID> outlet=<outlet ID>
```

---

In the following example, the BBU connectivity check has been successful.

```
Run BBUs connectivity check (recommended)? (Yes/No): Yes
BBU connectivity check started (may take several minutes)
Validating X1-BBU port 1 connectivity (1/4)
[#####] 100% Done! (elapsed time 00:01:59)
Connectivity validation passed. Powering on X1-BBU port1
[#####] 100% Done! (elapsed time 00:01:20)
Check will proceed to next step in 10 seconds. Would you like to abort? (Yes/No):
User input timed out - Proceeding

Validating X1-BBU port2 connectivity (2/4)
[#####] 100% Done! (elapsed time 00:01:59)
Connectivity validation passed. Powering on X1-BBU port2
[#####] 100% Done! (elapsed time 00:0:55)
Check will proceed to next step in 10 seconds. Would you like to abort? (Yes/No):
User input timed out - Proceeding

Validating X2-BBU port1 connectivity (3/4)
[#####] 100% Done! (elapsed time 00:01:59)
Connectivity validation passed. Powering on X2-BBU port1
[#####] 100% Done! (elapsed time 00:00:45)
Check will proceed to next step in 10 seconds. Would you like to abort? (Yes/No):
User input timed out - Proceeding

Validating X2-BBU port2 connectivity (4/4)
[#####] 100% Done! (elapsed time 00:01:59)
Connectivity validation passed. Powering on X2-BBU port2
[#####] 100% Done! (elapsed time 00:01:05)
Success: BBU to Storage Controllers power scheme is according to EMC recommendations
xmcli (tech)>
```

9. From the Install menu, select the option for `Disable root ssh accesst` to lock the root access.

## Verifying the Cluster Initialization

To verify the cluster initialization:

1. If you are logged in as `admin`, log out and then log in again as `tech`.
2. Run the following CLI commands (the relevant output fields are highlighted in green):

- `show-clusters-info`

```
xmcli (tech) > show-clusters-info
```

Cluster-Name	Index	State	Conn-State	Activation-Time	... PSNT	... Encryption-Mode	...
xbrick167	1	active	connected	Wed May 20 02:29:30 2015	... XIO00150201000	... Enabled	...

- `show-storage-controllers-info`

```
xmcli (tech) > show-storage-controllers-info
```

Storage-Controller-Name	Index	Mgr-Addr	Brick-Name	Index	Cluster-Name	Index	State	Conn-State	SW-Version	...
X1-SC1	1	10.76.218.197	X1	1	xbrick167	1	healthy	connected	4.0.0-xxx	...
X1-SC2	2	10.76.218.198	X1	1	xbrick167	1	healthy	connected	4.0.0-xxx	...

- `show-xenvs`

```
xmcli (tech) > show-xenvs
```

XEnv-Name	Index	Cluster-Name	Index	CPU(%)	CSID	State	Storage-Controller-Name	Index	Brick-Name	Index
X1-SC1-E1	1	XtremIO_Cluster	1	8	11	active	X1-SC1	1	X1	1
X1-SC1-E2	2	XtremIO_Cluster	1	18	10	active	X1-SC1	1	X1	1
X1-SC2-E1	3	XtremIO_Cluster	1	8	13	active	X1-SC2	2	X1	1
X1-SC2-E2	4	XtremIO_Cluster	1	7	12	active	X1-SC2	2	X1	1

- `show-modules`

```
xmcli (tech) > show-modules
```

Module-Name	Index	Cluster-Name	Index	XEnv-Name	Index	Storage-Controller-Name	Index	Module-Type	State
X1-SC1-C1	2	XtremIO_Cluster	1	X1-SC1-E1	1	X1-SC1	1	CONTROL	active
X1-SC1-C2	3	XtremIO_Cluster	1	X1-SC1-E2	2	X1-SC1	1	CONTROL	active
X1-SC1-D1	1	XtremIO_Cluster	1	X1-SC1-E1	1	X1-SC1	1	DATA	active
X1-SC1-D2	5	XtremIO_Cluster	1	X1-SC1-E2	2	X1-SC1	1	DATA	active
X1-SC1-R1	6	XtremIO_Cluster	1	X1-SC1-E1	1	X1-SC1	1	ROUTER	active
X1-SC1-R2	4	XtremIO_Cluster	1	X1-SC1-E2	2	X1-SC1	1	ROUTER	active
X1-SC2-C1	2	XtremIO_Cluster	1	X1-SC2-E1	3	X1-SC2	2	CONTROL	active
X1-SC2-C2	3	XtremIO_Cluster	1	X1-SC2-E2	4	X1-SC2	2	CONTROL	active
X1-SC2-D1	1	XtremIO_Cluster	1	X1-SC2-E1	3	X1-SC2	2	DATA	active
X1-SC2-D2	5	XtremIO_Cluster	1	X1-SC2-E2	4	X1-SC2	2	DATA	active
X1-SC2-R1	6	XtremIO_Cluster	1	X1-SC2-E1	3	X1-SC2	2	ROUTER	active
X1-SC2-R2	4	XtremIO_Cluster	1	X1-SC2-E2	4	X1-SC2	2	ROUTER	active

3. From the `show-clusters-info` output, confirm that the cluster PSNT matches the PSNT tag that was shipped with the cluster.

If the cluster PSNT has not been set correctly, contact EMC Support to determine how to resolve this issue, before proceeding with the cluster installation.

## Configuring the DNS and NTP Servers

It is recommended to configure the DNS and NTP servers as part of the system initialization process.

---

**Note:** If you have not configured the DNS servers as part of the Easy-Install (see [“Configuring the XMS and the Management Interface Parameters” on page 46](#)), follow the procedure described in this section.

---

### To configure the DNS servers:

1. Run the following command:

```
modify-dns-servers primary="<server IP address>"  
secondary="<server IP address>"
```

The new configuration is displayed at the prompt with a request to confirm.

2. Check that the data is as configured and confirm.

Following confirmation, the XMS configures the DNS and tries to ping each server. If a ping fails, a warning appears, as shown in the example below:

```
xmcli (admin)> modify-dns-servers primary="10.76.208.16" secondary="8.8.8.8"  
The new primary DNS server will be: "10.76.208.16"  
The new secondary DNS server will be: "8.8.8.8"  
The previous "10.76.208.15, 8.8.8.8" will be replaced.  
Are you sure? (Yes/No): Yes  
xmcli (admin)>
```

3. Verify the DNS configuration by running the following command and checking that the output is as configured:

```
show-dns-servers
```

---

**Note:** It is recommended for the DNS server to support reverse DNS lookup.

---

---

**Note:** DNS configuration is required for ESRS connectivity purposes.

---

**To configure the NTP servers:**

1. Run the following command:

```
modify-datetime ntp-servers=["<server 1 IP address>",  
"<server 2 IP address>"...]
```

2. If the NTP server is in a different time zone than that of the cluster, run the following command:

```
modify-datetime timezone=<time zone>
```

Example:

```
modify-datetime timezone=US/Central
```

---

**Note:** To view the list of available time zones, run the `show-timezones` command.

---

3. Verify the NTP configuration by running the `show-datetime` command and checking that the output is as configured:

```
show-datetime
```

## XMS HTTPS Access

The XtremIO XMS requires HTTPS access, including a self-assigned certificate that matches the XMS server name at the time of the installation or upgrade. Trying to access the XMS with a different server name or FQDN may result in a certificate mismatch and prevents the GUI from loading.

The following procedures provide a solution to these issues and enable HTTP access.

### Accessing the XMS via FQDN

**If your environment supports DNS and you want to access the XMS with FQDN, use the following procedure:**

1. Open an SSH connection to the XMS and log in as `xmsadmin`.
2. Log in to XMCLI as `admin`.
3. Configure the DNS servers, as described in [“Configuring the DNS and NTP Servers” on page 60](#).
4. Change the server name by running the following command:  

```
modify-server-name server-name="<FQDN>"
```
5. Open a browser and enter <https://fqdn/> in the address bar.
6. Download the webstart and launch the XMS GUI.

---

**Note:** If a certificate warning appears indicating a mismatched server name, acknowledge it.

---

7. Verify the server certificate by running the following CLI command:

```
show-server-certificate
```

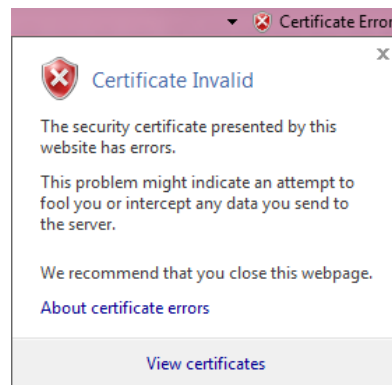
Compare the displayed certificate fingerprints to those of the certificates encountered by the browser.

### Accessing the XMS via Server Name

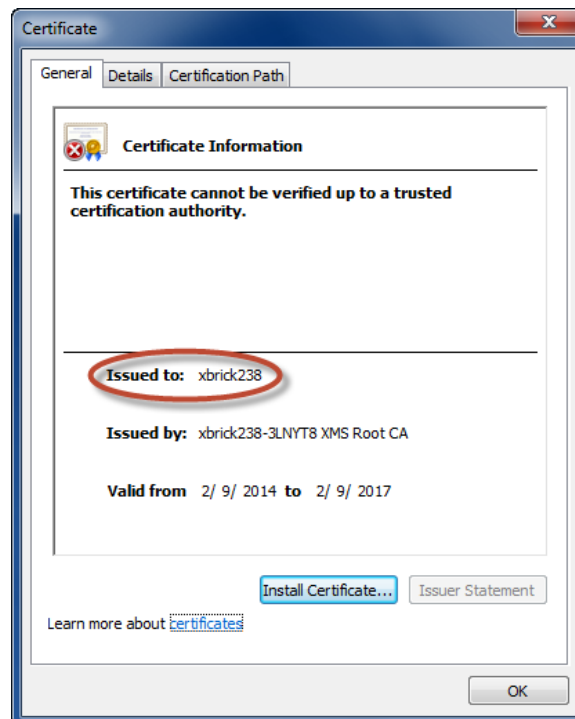
**If your environment does not support DNS and you want to access the XMS, using the server name that was defined during the installation process, or using an IP address, use the following procedure:**

1. Verify that your client can resolve “server name” or edit your hosts file to include an entry for “server IP address” and “server name” (the hosts file location depends on your client operating system).
2. Open a browser and enter <https://server name/> in the URL address bar.

3. Click **Certificate Error** on the address bar to open the certificate error message.



4. In the certificate error message, click **View certificates** to see the server name to which the certificate was issued.



5. Open an SSH connection to the XMS and log in as `xmsadmin`.
6. Log in to XMCLI as `admin`.
7. Change the server name to the name that appears in the certificate, by running the following command:
 

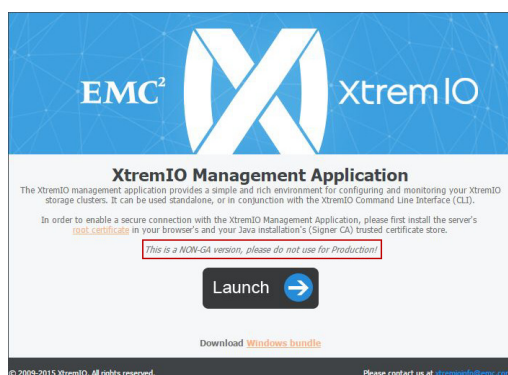
```
modify-server-name server-name="server_name"
```
8. Open a browser and enter <https://server name/> in the URL address bar.
9. Download the webstart and launch the XMS GUI.

## Configuring the XMS Login Banner

XtremIO version 4.0 enables you to customize the XMS login screen by adding text of your selection. This way, in a multi-cluster environment, you can easily distinguish your clusters' XMS from other XMSs.

The text you add is displayed on three screens:

- ◆ XtremIO launch screen



- ◆ XMS login screen



- ◆ Log in to xmcli after providing the user name

```
Username: admin
*****Login Banner*****
Password:
xmcli (admin)>
```



**To configure the XMS login banner:**

- ◆ Run the following CLI command:

```
modify-login-banner banner="<text for new banner>"
```

---

**Note:** When adding a new cluster to an existing multi-cluster configuration with a deployed XMS, there is no need to re-configure the login banner.

---



# CHAPTER 5

## Registering the Cluster in CSI

This chapter includes the following topics:

- ◆ [Business Services Portal .....](#) 68
- ◆ [Creating a New Case.....](#) 68
- ◆ [Updating the EMC Install Base After an XtremIO Cluster Upgrade .....](#) 73

## Business Services Portal

The EMC Business Services Portal provides a centralized location for users to submit requests directly to the Install Base Group. The portal is accessible outside of the EMC Intranet and fully replaces the Microsoft Outlook IB Form process used in the past.

**Note:** You must submit an Install Base Update request after completing the installation.


## Creating a New Case

To create a new case, using the Business Services Portal:

1. Navigate to <http://emc.force.com/BusinessServices> to access the EMC Business Services Portal.



2. In the Business Services Portal home page, scroll to the **Post Sales** section and click the **Install Base Group** hyperlink to open the Install Base Group Case Creation screen.




**Post Sales**

[Global Revenue Operations](#)  
GRO provides the following services: Revenue Recognition, Direct Order Processing & Inquiries, Partner Order Management & Inquiries, Field Inventory Return Creations, and Customer Trade-In's.

[Maintenance Contract Operations](#)  
Maintenance Contract Operations (MCO) is responsible for providing continuous lifecycle management of all maintenance service contracts for EMC.

[Install Base Group](#)  
Install Base Group provides services to update the Install Base. The services provided include: IB Status Change, PDR Update, Move or Party Change, Upgrade/Conversion, Debrief, Model Separation, Model Quantity Update, Microcode Update, Secure Credentials, or Other.



3. In the Case Creation screen, click the **Case Sub Type** drop-down menu and select **IB Status Change**. Click **Select**.

**Case Creation Application**

Populate Case Sub-Type and click Select to view all pertinent fields for Case submission.

Case Sub Type: IB Status Change

Contact Name:

Contact Email:

Theatre: --None--

Priority: Normal

**Select**

Update the status in the Oracle Install Base

4. Complete the first section of the Case Creation Application with the following data:

**Note:** All fields marked in red are mandatory for submission.

Input Field	Input Details
Contact Name	Enter your name.
Contact Email	Enter your Email address.
Theatre	From the drop-down menu, select the theatre associated with the customer's site location.
Priority	From the drop-down menu, select <b>Normal</b> .
Contact Phone	Enter your contact phone number.
Additional Notification Email(s)	Enter supplemental contacts associated to the installation event that hold an interest in monitoring the IB state of the XtremIO cluster. You can add up to three additional contacts.

**Note:** Email recipients added to the 'Additional Notification Email' fields receive updates on the case's state, as well as an automated message from the EMC Install Base Group on each of the following work-request statuses:

- ◆ Open
- ◆ Assigned
- ◆ Resolved

5. Complete the Case Details section with the following data:

**Note:** All fields marked in red are mandatory for submission.

Input Field	Input Details
Federal Case	Select this option if the customer is of U.S. Federal nature. Otherwise, leave the checkbox empty.
Subject	Type “ <b>Please move XtremIO cluster to 'Installed' state</b> ” in this field to provide the EMC IBG team with a request summary.
Description	Type a short description of the installation request. You can use the following sample text: <b>Please update XtremIO S/N 'xPSNTx' to reflect 'Installed' at Site ID 'xSite ID Number'.</b>
Product Family	From the list, select <b>All Other Families</b> .
Serial #/Instance	Enter the XtremIO PSNT of the cluster you are installing, e.g. APM00133128752.
Desired Status	From the drop-down menu, select <b>Install</b> .
Effective Date	Select the current date, e.g. 11/19/2013.
Microcode	Enter the version number of XtremIO software installed on the customer's cluster as part of the installation engagement, e.g. 3.0.2-12.
Party Number	Enter the Site ID associated with the customer's install location, e.g. 11145366.
PDR	Leave this field blank. No preferred dispatch resources are currently available for XtremIO.

The screenshot shows the 'Case Details' form with the following data entered:

- Federal Case:** [ ]
- Subject:** Please move XtremIO cluster to 'Installed' state
- Description:** Please update XtremIO S/N 'APM00133128752' to reflect 'Installed' at Site ID '11145366'
- Product Family:** Data Domain, Isilon, Recoverpoint, VCE. Chosen: All Other Families
- Serial #/Instance:** APM00133128752
- Desired Status:** Install
- Effective Date:** 11/19/2013 (10/29/2013)
- Microcode:** 3.0.2-12
- Party Number:** 11145366
- PDR:** [ ]

Fields marked in red are required for Case submission.

## 6. Complete the Remote Connection section with the following data:

Input Field	Input Details
Connect In	<ul style="list-style-type: none"> <li>Select <b>ESRS</b> if you configured ESRS Gateway (esrsgw) or ESRS IP Client (ipclient) as part of the installation event for inbound connectivity.</li> <li>Select <b>WebEx</b> if the customer only permits troubleshooting the cluster using WebEx connections for remote connectivity. Enter the customer contact name or information for WebEx session use in the 'Connect In Details' field shown below.</li> <li>Select <b>Not Configured</b> if you leave the field empty for any reason, and provide details in the 'Additional Info' field shown below.</li> <li>Select <b>Customer Refused</b> if the customer refused configuration of ESRS (or any remote connect in medium), and provide the refusal details in the 'Additional Info' field shown below.</li> </ul>
Connect In Details	Enter any Connect In configuration details that may prove helpful to others (e.g. special passwords).
Connect Home	<ul style="list-style-type: none"> <li>Select <b>ESRS</b> if you configured ESRS Gateway (esrsgw) or ESRS IP Client (ipclient) as part of this installation event via the XMCLI command 'modify-syr-notifier'.</li> <li>Select <b>Email Home</b> if you configured Email (email) or secure FTP (ftps) as part of the installation event via the XMCLI command 'modify-syr-notifier'.</li> <li>Select <b>Not Configured</b> if you leave the field empty for any reason, and provide details in the 'Additional Info' field shown below.</li> <li>Select <b>Customer Refused</b> if the customer refused configuration of ESRS (or any remote connect in medium), and provide the refusal details in the 'Additional Info' field shown below.</li> </ul>
Connect Home Details	Enter any Connect-Home configuration details that may prove helpful to others (e.g. special passwords).
Additional Info	Enter any special information related to the customer's remote connection status (e.g. customer refusal reason, refusing customer's name, etc).

▼ Remote Connection

Connect In:

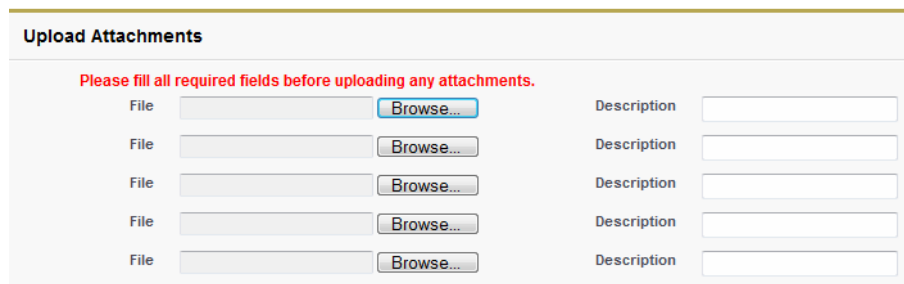
Connect In Details:

Connect Home:

Connect Home Details:

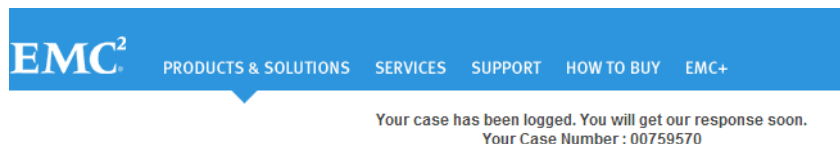
Additional Info:

7. You can include additional documents with your request (e.g. a letter of customer refusal for Connect-In/Connect-Home configuration). To attach a document, scroll to the Upload Attachments section and click **Browse** to select a file. Enter the file details in the **Description** field. You can attach up to five files.



Upload Attachments	
Please fill all required fields before uploading any attachments.	
File <input type="text"/> <input data-bbox="884 436 975 459" type="button" value="Browse..."/>	Description <input type="text"/>
File <input type="text"/> <input data-bbox="884 478 975 501" type="button" value="Browse..."/>	Description <input type="text"/>
File <input type="text"/> <input data-bbox="884 520 975 543" type="button" value="Browse..."/>	Description <input type="text"/>
File <input type="text"/> <input data-bbox="884 562 975 585" type="button" value="Browse..."/>	Description <input type="text"/>
File <input type="text"/> <input data-bbox="884 604 975 627" type="button" value="Browse..."/>	Description <input type="text"/>

8. After providing all the relevant information and including any necessary attachments, click **Submit**. The request is sent to the Install Base Group for review. An automated email notification, updating on the request status, is sent to you and to the additional email addresses submitted with the request.



**Note:** It is recommended to take note of the case number for future reference.



# Updating the EMC Install Base After an XtremIO Cluster Upgrade

In certain cases it is required to update the EMC Install Base records after completing an XtremIO software upgrade, in order to ensure that the site reflects the correct microcode revision at all times. This is especially important in situations where there is no inbound or outbound connectivity from the XtremIO cluster, due to security restrictions.

This procedure describes how to update the Install Base with the active version of XtremIO. It is recommended to perform this procedure upon completion of every software upgrade on the XtremIO cluster.

## To update the EMC Install Base for an XtremIO cluster:

1. Navigate to <http://emc.force.com/BusinessServices>.
2. From the Post Sales menu, select **Install Base Group**.
3. From the Case Sub Type drop-down menu, select **Microcode Update**, and click the **Select** button.
4. Enter your EMC Email address in the **Contact Email** field.
5. From the **Theater** drop-down menu, select the customer's geographical region.
6. If the site you are requesting a microcode update to is either federal or government restricted, check the **Federal Case** checkbox.
7. In the **Subject** field, enter the following string:  
"Requesting XtremIO Microcode Update for PSNT <serial-number PSNT of XtremIO cluster>."
8. In the **Description** field, enter the following string:  
"Please update the XtremIO microcode version to <XtremIO Version> within the EMC Install Base for XtremIO PSNT <serial-number PSNT of XtremIO cluster>."
9. In the Product Family menu:
  - a. From the list of available options, select **All Other Families**.
  - b. Click the Right arrow to add the option to the list of selected products.
10. In the **Serial #/Instance** field, enter the serial-number PSNT of the XtremIO cluster for which you are requesting a microcode update, within the EMC Install Base.
11. In the **Microcode** field, enter XtremIO software version to which you recently upgraded.  
For example: 4.0.0-xxx.
12. Click the **Submit** button in order to send your Install Base update request to the Install Base Group for processing.



# CHAPTER 6

## Generating an XtremIO Log Bundle

This chapter includes the following topics:

- ◆ [Generating and Collecting the Bundle ..... 76](#)
- ◆ [Uploading the Log Bundle ..... 76](#)
- ◆ [Generating a Log Bundle following a Cluster Creation Failure ..... 77](#)

## Generating and Collecting the Bundle

To generate and collect the package:

1. Log in to the XMS CLI as `admin`.
2. Issue a log bundle collection by running the following command:  

```
xmcli (admin)> create-debug-info  
debug-info-name="Initial-Setup"
```

The following message appears:

```
The process may take a while. Please do not interrupt.  
Debug info collected and could be accessed via http://...
```

3. Copy the link to a web browser's address bar and download the package.

## Uploading the Log Bundle

To upload the package:

1. Connect to the XtremIO FTP, using one of the following methods:
  - FTP client - connect to <ftp://ftp.xtremio.com/>, using xinstall user credentials.
  - Browser - go to <http://ftp.emc.com/>. In the list box, select **XtremIO** and type the xinstall user credentials.
2. Create a directory, whose name contains the customer name and cluster PSNT.  
For example:  
`Customer-ABC1234567890`
3. Use the same FTP session to upload two packages to that directory:
  - The log bundle
  - The completed Installation Summary Form (see [“Installation Summary Form” on page 11](#))

## Generating a Log Bundle following a Cluster Creation Failure

XtremIO version 4.0 enables you to generate a log bundle when cluster creation fails. The collected log bundle enables a better understanding of the failure reasons and the ways to resolve them.

### To create a log bundle when cluster creation fails:

1. Log in to the XMS, using the xinstall user credentials.
2. In the Install menu, type the number for the `Collect Log Bundle` option.

```
login as: xinstall
xinstall@xms's password:

Install menu
-----
1. Configuration
2. Check configuration
3. Display configuration
4. Display installed Xtremapp version
5. Perform XMS installation only
6. Perform "fresh" installation (XMS + Storage Controllers)
7. Perform cluster expansion fresh install
8. Set IP Client Configuration
9. Start IP Client Installation
10. Set Policy Manager configuration
11. Start Policy Manager installation
12. Run XMS Recovery
13. Power menu
14. Collect Log Bundle
15. Temporary enable IPMI access
99. Exit

> 14
```

The log bundle is collected from the XMS automatically. However, since the cluster failed to create, there is no access to the Storage Controllers. Provide the IP address of one of the Storage Controllers. The rest of the Storage Controllers are automatically discovered to enable log bundle creation from them as well.



# CHAPTER 7

## Configuring ESRS and Connect-Home

This chapter includes the following topics:

◆ ESRS and Connect-Home Requirements .....	80
◆ Pre-conditions for Deploying ESRS and Connect-Home at a Customer site.....	80
◆ ESRS Integration and Configuration .....	81
◆ Connect-Home Only Integration and Configuration .....	86
◆ Checking the ESRS and Connect-Home Configuration on the XMS.....	87
◆ Remotely Accessing an XtremIO Cluster, Using ESRS.....	89

## ESRS and Connect-Home Requirements

EMC® Secure Remote Support (ESRS) provides a secure, IP-based, distributed remote support solution that enables command, control and visibility of remote support access.

ESRS fulfills the requirements for authentication, authorization and auditing with a secure, highly scalable and fault-tolerant system. This IP-based, firewall-friendly remote access architecture initiates all connections from the customer's site.

ESRS provides rapid remote support by employing two phases:

1. Automated recognition and notification from the customer's site to EMC
2. Interpretation and response from EMC

ESRS configuration options with XtremIO are ESRS GW (both VE and legacy type ESRS gateways) and ESRS IP Client. These three configuration options provide Connect-In and Connect-Home functionalities.

As these configuration options provide the best level of remote support to the cluster, it is highly recommended that you select one of them when completing the XMS installation.

If the customer refuses to use ESRS as a connectivity solution, you must configure the XMS to Connect-Home only. The Connect-Home only options with XtremIO are Email or FTPS. These two options do not provide Connect-In functionality to the XMS, but merely ensure that EMC receives regular configuration report and product alert information from the customer's XtremIO environment.

For further ESRS and Connect-Home pre-requirements, refer to the *XtremIO Storage Array Site Preparation Guide*.

---

**Note:** The use of Connect-Home configuration with XtremIO is considered an exception, as it provides a sub-optimal remote support solution for the XtremIO cluster. Such an exception should be pre-approved.

---

## Pre-conditions for Deploying ESRS and Connect-Home at a Customer site

To learn about the pre-conditions for deploying ESRS and Connect-Home at the customer's site, refer to the *EMC XtremIO Storage Array Site Preparation Guide*.

The cluster used for ESRS Integration must have a configured PSNT. The PSNT is used for identifying the cluster to ESRS.

To establish connectivity, a site-name should be specified. This free text field enables to further identify the cluster's location in addition to the PSNT. If unavailable, enter the customer's name.

To connect to ESRS using a URL, DNS should be configured on the XMS. To learn about setting DNS on the XMS, refer to [“Configuring the DNS and NTP Servers” on page 60](#).



## ESRS Integration and Configuration

This section describes the necessary steps for deploying ESRS configurations on an XtremIO cluster, namely, ESRS GW (both VE and legacy type ESRS gateways) and ESRS IP Client.

### Deploying ESRS GW Configuration on the XMS

This section describes the necessary steps for deploying ESRS GW configuration on the XMS. This configuration provides Connect-In and Connect-Home to and from the XMS. The ESRS GW configuration applies to both VE and legacy type ESRS gateways.

**Note:** XtremIO is not yet ESRS VE RESTful API aware.

#### Setting the ESRS GW Configuration on the XMS

**Note:** This procedure applies to both VE and legacy type ESRS gateways.

##### To set the ESRS GW configuration on the XMS:

1. Connect to the XMS, via the XMCLI, as `admin`.
2. To confirm that the XMS can successfully reach the ESRS GW server, run the following command:

```
check-xms-connectivity
```

3. Configure Connect-Home with the 'esrsgw' connection type, by running the following XMCLI command:

```
xmcli (admin)> modify-syr-notifier enable
site-name="<site-name of customer site>"
connection-type=esrsgw esrs-gw-host="<IP address of primary
ESRS GW>" esrs-gw-host-secondary="<IP address of secondary
ESRS GW>"
```

**Note:** The `modify-syr-notifier` command alerts on any connectivity problem in relation to the ESRS GW. For example:

```
xmcli (admin)> modify-syr-notifier connection-type=esrsgw
esrs-gw-host="1.2.3.4" esrs-gw-host-secondary="1.2.3.5"
site-name="12345678"
Warning: unable to connect to the specified ESRS gateway host
```

**Note:** When using the `modify-syr-notifier` command, provide the IP address of the ESRS GW as the `esrs-gw-host` parameter value. FQDN URL is not supported.

4. Approve the registration of the cluster as an XtremIO managed device on the ESRS GW from the ServiceLink portal. Refer to [“Confirming the XtremIO Cluster as a Managed Device in ServiceLink” on page 127](#) for the procedure.
5. Check ESRS and Connect-Home configuration on the XMS. Refer to [“Checking the ESRS and Connect-Home Configuration on the XMS” on page 87](#) for the procedure.

---

**Note:** [“Miscellaneous ESRS GW Procedures” on page 127](#) also includes other procedures when using an ESRS GW (both legacy and VE type ESRS gateways), such as locating the device ID of the ESRS GW, and troubleshooting connectivity problems between the ESRS GW and ServiceLink.

---

## Deploying ESRS IP Client Configuration on the XMS

This section describes the necessary steps for deploying ESRS IP Client configuration on the XMS. This configuration provides Connect-In and Connect-Home to and from the XMS.

Load the XMS Easy-Install CLI to begin the ESRS IP Client configuration. For details, refer to [“Configuring the XMS and the Management Interface Parameters” on page 46](#).

---

**Note:** ESRS IP Client can be used only in single cluster configuration.

---

### Installing the IP Client DC Agent on the XMS

Before setting the IP Client configuration on the XMS, you should securely install a software module, named the DC agent.

There are four possible scenarios for installing the DC Agent module:

- ◆ **Initial deployment without a proxy-server** – The XtremIO cluster has never been installed with the IP Client previously and the XMS has direct connectivity to ESRS.
- ◆ **Re-deployment without a proxy-server** – The IP Client needs to be re-deployed (e.g. when the XMS was recovered or replaced), and the XMS has direct connectivity to ESRS.
- ◆ **Initial deployment with a proxy-server** – The XtremIO cluster was installed with the IP Client previously, and the XMS has connectivity to ESRS via a proxy-server.
- ◆ **Re-deployment with a proxy-server** – The IP Client needs to be re-deployed (e.g. when the XMS was recovered or replaced), and the XMS has connectivity to ESRS via a proxy-server.

In scenarios that include a proxy-server, you should acquire the following proxy-server related information from the customer:

- ◆ Proxy-server type (http or socks)
- ◆ Proxy server IP address
- ◆ Port number used by the proxy-server
- ◆ User-name and password for using the proxy-server (if required)

Before installing the DC Agent on the XMS, set the IP Client DC Agent installation options.

---

**Note:** To set the IP Client DC Agent installation options, you need to use the CLI menu. To access the CLI menu, refer to [“Connecting to the XMS” on page 45](#).

---

**To confirm that the XMS can successfully reach the ESRS Environment:**

1. Connect to the XMS, via the XMCLI, as `admin`.
2. Run the following XMCLI command:

```
check-xms-connectivity
```

**To set the IP Client DC agent installation options:**

1. From the xinstall menu, select the **Set IP Client configuration** option.
2. Type your EMC Windows NT ID.
3. When the **"Enter selection for re-provisioning of the IP Client DC Agent (Y/N) (previous value: 'N'):"** prompt appears, type **N** for initial deployment of the DC Agent, or **Y** for re-deployment of the DC agent.
4. When the **"Enter selection of Proxy server configuration (Y/N) (previous value: 'N'):"** prompt appears, type **N** if the DC agent should be deployed without a proxy-server, or **Y** if otherwise.
5. If you selected the deployment with a proxy-server option, provide the following proxy-server settings in response to the following questions:
  - proxy type (http or socks)
  - proxy-server IP address
  - proxy-server port number
  - proxy-server username (if used)
6. Proceed to install the IP Client DC Agent with the selected settings.

**To start the IP Client DC Agent installation:**

1. From the CLI menu, select the **Start IP Client Installation** option.
2. Review the ESRS EULA for the ESRS IP Client. Type **YES** to confirm.
3. When prompted, type the RSA SecureID token number that matches the set EMC Windows NT ID.
4. When prompted, if a proxy-user was set for a proxy-server deployment, type the proxy-user account password.

The following actions are performed at this point:

- Secure installation of the DC agent software
- Launching of the required IP Client services on the XMS
- Registration of the XtremIO cluster in ESRS (in initial deployment scenarios)

## Configuring the IP Client DC Agent with an ESRS Policy Manager (Optional)

The IP Client DC Agent can be configured to connect to a customer ESRS Policy Manager. This enables the customer to enforce policies to audit and control ESRS connections to the XMS.

Before you proceed, obtain the following information from the customer:

- ◆ Policy Manager IP address
- ◆ Port number used to connect to the Policy Manager
- ◆ Required connection type to the Policy Manager - secure (https) or non secure (http)
- ◆ In case a proxy-server is required to connect to the Policy Manager, provide the following settings when prompted:
  - Proxy-server type (http or socks)
  - Proxy-server IP address
  - Proxy-server port number
  - Proxy-server username and password (if necessary)

**To confirm that the XMS can successfully reach the customer's existing ESRS policy manager:**

1. Connect to the XMS, via the XMCLI, as `admin`.
2. Run the following XMCLI command:

```
check-xms-connectivity
```

Before Configuring the DC Agent, set the DC Agent connection method to the ESRS Policy Manager.

**To set how the DC Agent connects to an ESRS Policy Manager:**

1. From the xinstall menu, select the **Set Policy Manager configuration** option.
2. When the "**Enter policy manager IP address (previous value: ):**" prompt appears, type the IP address of the Policy Manager.
3. Type the Policy Manager port number.
4. When the "**Enter selection for secure connection to policy manager (Y/N) (previous value: 'N'):**" prompt appears, type **Y** when https connection is required for connecting to the Policy Manager, otherwise type **N**.
5. When the "**Enter selection of Proxy server configuration (Y/N) (previous value: 'N'):**" prompt appears, type **N** when no proxy-server is required to connect to the Policy Manager, otherwise type **Y**.

6. If a proxy-server was selected for the Policy Manager, provide the following settings when prompted:
  - proxy type (http or socks)
  - proxy-server IP address
  - proxy-server port number
  - proxy-server username (if relevant)

Proceed to configure the DC Agent with an ESRS Policy Manager.

**To configure the DC Agent with an ESRS Policy Manager:**

1. From the CLI menu, select the **Start Policy Manager installation** option to start the DC Agent configuration.
2. If a proxy-server was set to connect to the Policy Manager, type the proxy-server IP Address and username.

## Setting the IP Client Configuration on the XMS

Following the DC Agent installation on the XMS, you should set the IP Client configuration on the XMS.

**To set the IP Client configuration on the XMS:**

1. Connect to the XMS as `admin`.
2. Run the following XMCLI command to configure Connect-Home with the 'ipclient' connection type:

```
xmcli (admin)> modify-syr-notifier enable
site-name="<site-name of customer site>"
connection-type=ipclient
```

3. Check ESRS and Connect-Home on the XMS. Refer to [“Checking the ESRS and Connect-Home Configuration on the XMS” on page 87](#) for the procedure.

## Connect-Home Only Integration and Configuration

This section describes the necessary steps for deploying the supported Connect-Home only configurations on an XtremIO cluster, namely, Email and FTPS.

---

**Note:** These configurations **do not** provide Connect-In functionality.

---

### Deploying Email Configuration on the XMS

This section details the required steps for deploying Email configuration on the XMS. This configuration provides only Connect-Home from the XMS.

---

**Note:** When using the Email Connect-Home only, adding a footer (e.g. disclaimer footer) to email messages may impact the processing of SYR notifications from the XMS. To avoid this, make sure that the customer's SMTP server is configured to prevent the XMS from adding a footer to outgoing email messages.

---

---

**Note:** To enable SYR notification from the XMS to be successfully relayed, verify that the appropriate ALLOW rules are added to the customer's SMTP server.

---

#### To deploy Email configuration on the XMS:

1. Log in to XMCLI as admin.
2. Run the following command to confirm that the XMS can successfully reach the customer's SMTP server via port 25:

```
check-xms-connectivity
```

3. Run the following XMCLI command to configure Connect-Home with the 'email' connection type:

```
xmcli (admin)> modify-syr-notifier enable  
site-name="<site-name of customer site>"  
connection-type=email email-server="URL or IP of SMTP  
server" email-sender="Sender E-mail address"  
[email-user="user in SMTP server" email-password="password  
in SMTP server"]
```

---

**Note:** The email-user and email-password parameters are optional. Use the parameters only if connection to the SMTP server requires authentication.

---

4. Check the Connect-Home configuration on the XMS. Refer to [“Checking the ESRS and Connect-Home Configuration on the XMS” on page 87](#) for the procedure.

## Deploying FTPS Configuration on the XMS

This section lists the required steps for deploying FTPS configuration on the XMS. This configuration provides only Connect-Home from the XMS.

### To deploy FTPS configuration on the XMS:

1. Log in to XMCLI as `admin`.
2. Run the following command to confirm that the XMS can successfully reach the production EMC FEP servers:  
  
`check-xms-connectivity`
3. Run the following XMCLI command to configure Connect-Home with the ' `ftps` ' connection type:  
  
`modify-syr-notifier enable site-name="<site-name of customer site>" connection-type=ftps`
4. Check the Connect-Home configuration on the XMS. Refer to [“Checking the ESRS and Connect-Home Configuration on the XMS” on page 87](#) for the procedure.

## Checking the ESRS and Connect-Home Configuration on the XMS

This section lists the required steps for checking and confirming ESRS and Connect-Home configuration on the XMS.

### To check the ESRS and Connect-Home configuration on the XMS:

1. Connect to the XMS as `admin`.
2. Run the `show-syr-notifier` XMCLI command to display the current ESRS or Connect-Home only configuration on the XMS.  
  
`show-syr-notifier` provides the following information:
  - Current configuration of ESRS/Connect-Home on the XMS
  - Current configuration and status of the DC agent running on the XMS (for IP Client configuration)
  - Connectivity status to ESRS

The following examples display possible `show-syr-notifier` command outputs:

- Output for ESRS GW configuration:

---

**Note:** The same output is displayed for both VE and legacy type ESRS gateways.

---

```
xmcli (tech)> show-syr-notifier
Enabled: True
Frequency (hours): 24
ConnectEMC-Config: ----->
Connection Type: ESRS Gateway
URL: https://10.76.223.64:443/incoming
Site Name: 26235204
PSNT: XIOAPPLAB00101
Connection Status: OK
```

- Output for IP Client configuration:

```
xmcli (admin)> show-syr-notifier
Enabled: True
Frequency (hours): 24
ConnectEMC-Config: ----->
Connection Type: IPClient
Site Name: 26235204
PSNT: XIOAPPLAB00101
Connecting to: esrs-core.emc.com on port 443
Connection Status: Connected
Proxy Server: Disabled
Policy Manager: Disabled.
SSL: Enabled, strength 168
Remote Sessions:
XTREMIO-DC XIOAPPLAB00101 CLIViaSSH 127.0.0.1
```

3. Run the following command to check Connect-Home from the XMS:

```
xmcli (admin)> send-syr-notification
```

Verify receiving the following confirmation message:

```
SYR notification sent
```

4. Launch the ESRS CLIViaSSH remote application from ServiceLink to check Connect-In to the XMS (refer to [“Remotely Accessing an XtremIO Cluster, Using ESRS”](#) on page 89 for details).

---

**Note:** This step is only applicable for ESRS GW or ESRS IP Client configurations.

---



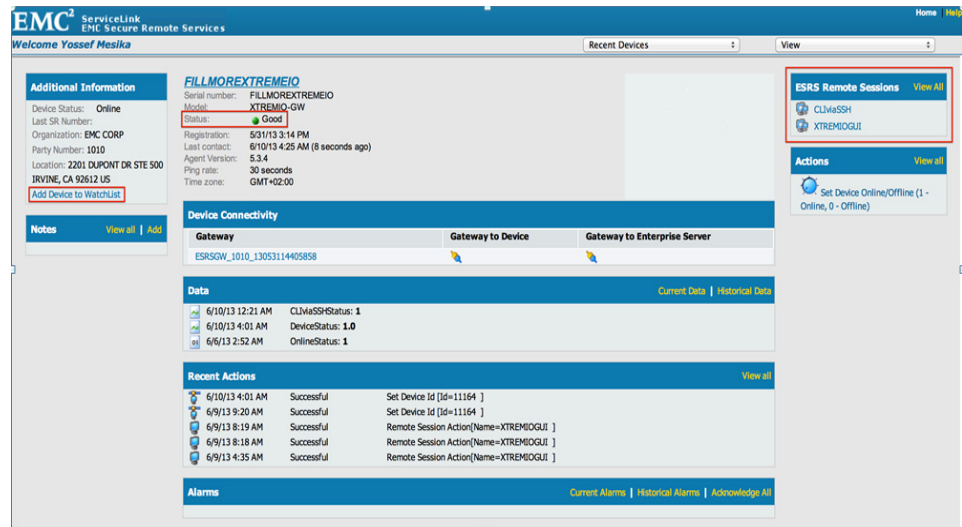
# Remotely Accessing an XtremIO Cluster, Using ESRS

This section describes how to remotely access (Connect-In) an XtremIO cluster, when using the ESRS GW and ESRS IP Client configurations.

## Locating the Page for your XtremIO Cluster in ServiceLink

To locate the ServiceLink page for your XtremIO cluster:

1. Log in to ServiceLink (<https://esrs.emc.com/portal>), using your RSA SecureID credentials.
2. Type the XtremIO cluster's PSNT in the **Browse For Devices** field, preceded by `%` (e.g. %APN12345678901).
3. Click **Search**.
4. From the list of the matching serial numbers, click the cluster PSNT to access the XtremIO cluster status page.



5. Confirm that the XtremIO status indicator is **Good**.
6. Click **Add Device to WatchList** for easier access to the device's status screen from the ServiceLink portal.

## Launching the ESRS Remote Application on the Managed XtremIO Device

Using ESRS, it is possible to launch remote applications on a managed device. With XtremIO, the following remote application is available:

- ◆ CLlviaSSH - open an SSH session to the XMS

---

**Note:** At this point, the XTREMIOGUI does **not** work.

---

### Preparing the Local Desktop for Running ESRS CLlviaSSH Remote Application

**To prepare your desktop for launching the CLlviaSSH remote application:**

1. Install the Putty application on your local machine. Refer to EMC KB # 203674 (<https://support.emc.com/kb/203674>) for details.
2. Extract the putty.exe file to the following directory on your local machine:  
C:\Users\Public\Desktop\  
ServiceLink expects to find putty.exe in this directory when launching CLlviaSSH.
3. After extraction is completed, delete the Putty.zip file from your local machine.

### Launching ESRS CLlviaSSH Remote Application

**To launch the CLlviaSSH remote application on an XtremIO managed device:**

1. Access the ServiceLink page for the XtremIO managed device.
2. Confirm that the status indicator is `Good`.
3. Click **CLlviaSSH** to open a remote SSH session to the device.

# CHAPTER 8

## Upgrading the Cluster Software (NDU)

This chapter includes the following topics:

- ◆ General..... 92
- ◆ Cluster Software Upgrade (NDU and Cold Upgrade) ..... 93

## General

This section provides instructions for performing a cluster software upgrade.

### NOTICE

The XtremIO cluster upgrade process may result in problems including data loss if not performed properly. Therefore, the upgrade process must be performed by EMC personnel only.

---

You can upgrade the cluster by performing one of the following procedures:

- ◆ Non Disruptive Upgrade (NDU) - uses a software package which includes the XtremIO software and the Storage Controllers OS to upgrade the software on a running cluster. The upgrade process is performed while the cluster service is online.
- ◆ Disruptive Upgrade (cold upgrade) - performed when I/O traffic interferes with the upgrade process. In such cases, data is unavailable to the user and I/O traffic is re-continued only after the cluster upgrade is completed.

Performing any of the cluster software upgrade options (NDU or cold upgrade) should be done by submitting a service request to XtremIO Global Tech Support. In general, non-disruptive upgrade will be performed with XtremIO unless recommended otherwise by XtremIO Global Tech Support.

Before performing any upgrade procedure on the cluster, perform the following steps:

- ◆ Contact the XtremIO Global Tech Support to obtain the latest update on the process.
- ◆ Provide the customer with a copy of the target version's *Release Notes* document from the XtremIO Support page.
- ◆ Make sure that the customer is familiar with the XtremIO Support page in [support.emc.com](http://support.emc.com) and can successfully navigate to the appropriate cluster model page and download the corresponding XtremIO documentation and software.

## Cluster Software Upgrade (NDU and Cold Upgrade)

For guidance on how to prepare your environment for an XtremIO Non-Disruptive Software Upgrade (NDU), refer to EMC KB # 203074 (<https://support.emc.com/kb/203074>).

---

**Note:** While XtremIO arrays are engineered and tested for fully non-disruptive upgrades, it is recommended to follow IT management best practices when upgrading your array. To ensure that upgrades are completed in the shortest time and with minimal impact on performance, take advantage of maintenance windows rather than using production hours. This way you can perform upgrades when the load on the array is lightest.

---

To perform a cluster software upgrade, contact the XtremIO Support and submit a service request.



# CHAPTER 9

## Expanding the Cluster

This chapter includes the following topics:

- ◆ General..... 96
- ◆ Expanding the Cluster ..... 97
- ◆ Expanding a Multiple X-Brick Cluster by Adding X-Bricks..... 100

## General

This section provides instructions for performing a cluster expansion.

---

**Note:** If you wish to upgrade the cluster software (NDU), refer to the [“Upgrading the Cluster Software \(NDU\)” on page 91](#).

---

You can expand the cluster by performing one of the following procedures:

- ◆ Cluster expansion - performed when a 10TB Starter X-Brick (5TB) is expanded to a full 10TB X-Brick. The expansion process includes installing 12 additional SSDs and then adding them to the cluster.
- ◆ Multiple X-Brick cluster expansion - expanding a multiple X-Brick Cluster by adding X-Bricks.

Before performing any expansion procedure, make sure that the customer is familiar with the XtremIO Support page in [support.emc.com](http://support.emc.com) and can successfully navigate to the appropriate cluster model page and download the corresponding XtremIO documentation and software.



## Expanding the Cluster

You can expand the cluster in three ways:

- ◆ Expand a 5TB Starter Kit cluster by adding SSDs
- ◆ Expand a multiple X-Brick cluster by adding X-Bricks

### Expanding a 5TB Starter Kit

This section describes the procedure for adding the newly-installed SSDs to a 5TB Starter Kit cluster as part of the cluster expansion. The procedure should be repeated for each new SSD.

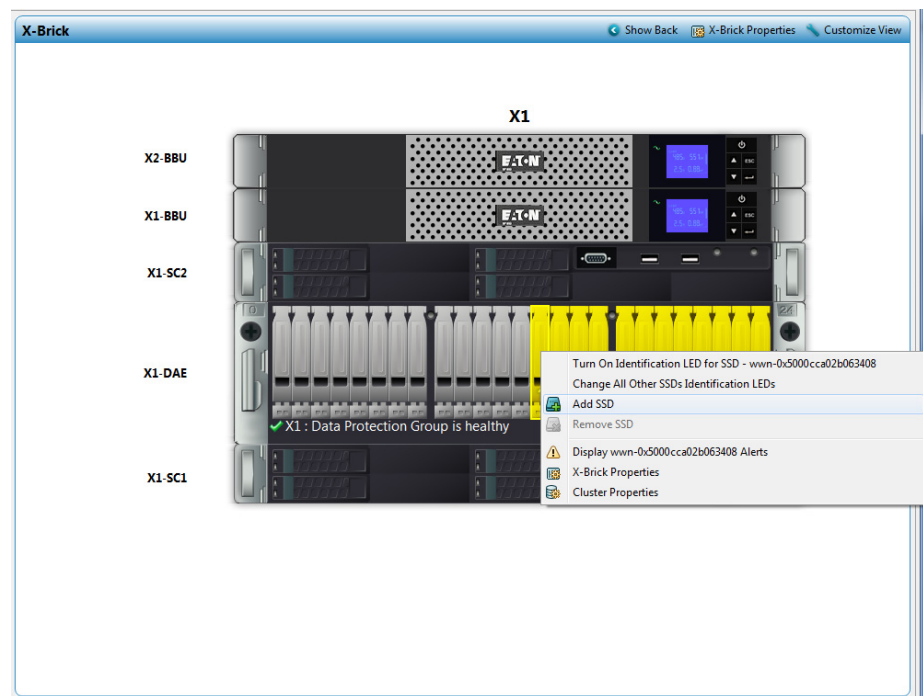
**Note:** This procedure should be performed following an SSD installation to a 5TB Starter Kit. See *XtremIO Hardware Installation Guide* for details.

You can perform the cluster expansion procedure via GUI or CLI.

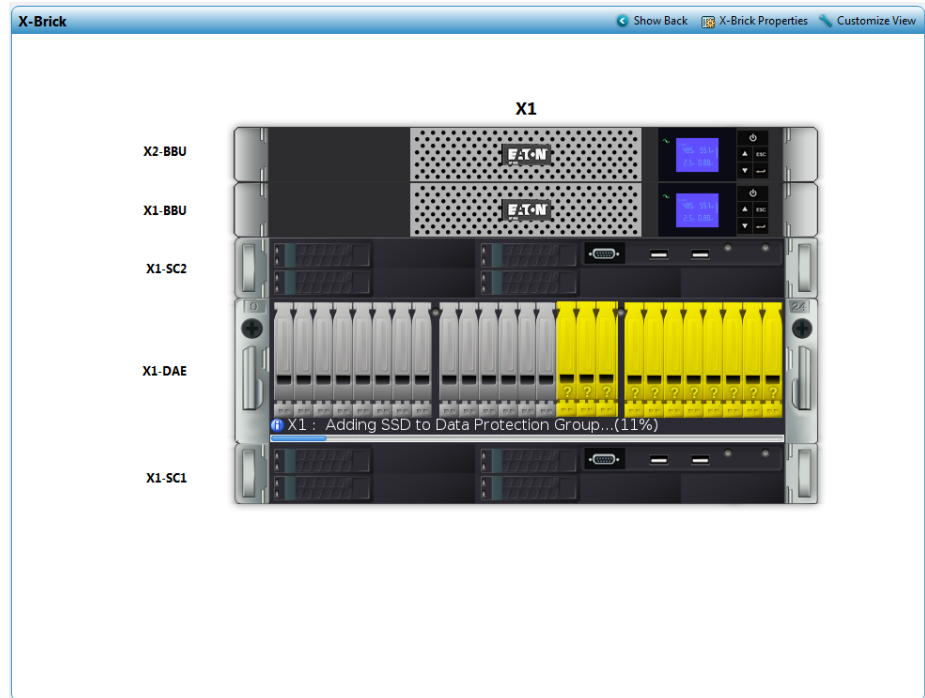
### Expanding the Cluster Using the GUI

To expand the cluster, using the GUI:

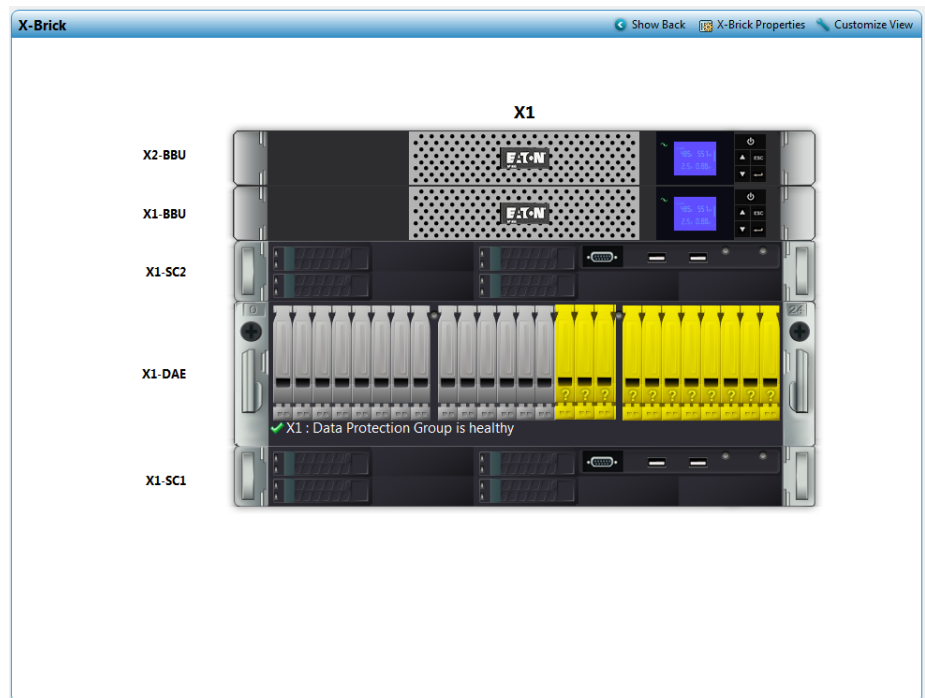
1. Log in to XtremIO as `tech`.
2. Click the **Hardware** icon on the menu bar to open the Hardware workspace; the new SSDs appear in yellow in the X-Brick pane.



3. Right-click a new SSD and select **Add SSD**; The SSD's color changes from yellow to gray. You can monitor the SSD integration process using the progress bar, located under the DAE.



4. Wait for the SSD integration to complete.



- Repeat steps 3-4 for all the new SSDs.

---

**Note:** The new SSDs should be added sequentially to the cluster.

---

- When all the new SSDs are added to the cluster, Click the **Dashboard** icon to open the Dashboard view.
- Verify that the cluster's physical capacity (displayed on the Storage pane) is 6.99TB

---

**Note:** The cluster's physical capacity indicator may take a minute to display the updated capacity.

---

## Expanding the Cluster Using the CLI

To expand the cluster, using the CLI:

- Log in to xmcli as tech.
- Run the following command:

```
show-ssds
```

```
xmcli (tech)> show-ssds
SSD-Name          Index Brick-Name Index Slot # ... State      Position-State
WWN-0x5000cca013136cf4 14    X1          1      13    not-in-rg    good
WWN-0x5000cca0131365f0 15    X1          1      14    not-in-rg    good
WWN-0x5000cca01312ca6c 16    X1          1      15    not-in-rg    good
.
.
WWN-0x5000cca013124b24 1      X1          1      0      in-rg        good
WWN-0x5000cca013124b3c 2      X1          1      1      in-rg        good
.
.
```

Note the index numbers of the SSDs with "not-in-rg" state.

- Run the following command to add the leftmost new SSD:

```
add-ssd brick-id=<brick index> ssd-uid="<SSD name>"
```

```
xmcli (tech)> add-ssd ssd-uid="wnn-0x5000cca013136cf4" brick-id=1
SSD wnn-0x5000cca013136cf4[14] added to Brick X1 [1]
xmcli (tech)>
```

- Run the following command to assign the leftmost SSD:

```
assign-ssd dpd-id=1 ssd-id="<SSD name>"
```

- Wait for the SSD integration to complete.

```
xmcli (tech)> assign-ssd dpd-id="X1-DPG" ssd-id="wnn-0x5000cca013136cf4"
SSD wnn-0x5000cca013136cf4[14] assigned to DPGX1-DPG[1]
xmcli (tech)>
```

- Repeat steps 3-5 for all the other new SSDs (15 to 25).

## **Expanding a Multiple X-Brick Cluster by Adding X-Bricks**

To expand a multiple X-Brick cluster by adding X-Bricks, refer to the *EMC XtremIO Hardware Installation and Upgrade Guide*.

# CHAPTER 10

## Verifying the XtremIO Cluster Installation

The purpose of this procedure is to verify that the XtremIO Storage Array is correctly installed after being racked and initialized by a field support specialist.

---

**Note:** Although this procedure may be time consuming, it is recommended to perform it to expose possible installation problems and to ensure that the cluster is ready for use by the customer.

---

This chapter includes the following topics:

- ◆ Cluster Functionality Verification ..... 102
- ◆ Cluster Configuration Verification ..... 103
- ◆ Knowledge, Equipment and Documentation ..... 107

## Cluster Functionality Verification

### To verify cluster functionality:

1. Confirm that the GUI (XMS) is operational, as follows:
  - a. Log in to the GUI.
  - b. Verify that no unexpected alerts appear on the Alerts list.
  - c. Check the cluster's health by running the following CLI command:

```
show-clusters
```

Verify that the cluster's state is `active` and its connection state is `connected`.
  - d. If not verified before, verify that ESRS is properly configured, using the following command:

```
send-sysr-notification
```
  - e. Configure Email, SNMP and SMTP Notifications, if applicable.
2. Create a new volume and assign it to a host, as follows:
  - a. Verify that the host is able to discover the new LUN.
  - b. Verify that the host is configured and connected according to EMC XtremIO best practices, as detailed in the *XtremIO Storage Array User Guide*.
  - c. Verify that the host is able to execute I/O with the new LUN.
  - d. Verify that Email, SNMP and SMTP notifications were sent following a volume creation.

## Cluster Configuration Verification

To verify cluster configuration:

1. In a multiple cluster environment, find the relevant cluster by running the following command:

```
xmcli <tech> show-clusters-info
Cluster-Name  Index  State  Conn-State  Activation-Time  ...  PSNT  ...
Cluster01    1      active connected  Sun Apr 19 14:27:45 2015 XIO00150201423 ...
Cluster02    2      active connected  Tue Mar 24 20:15:06 2015 XIO00150201415 ...
```

Verify that the PSNT label, which is attached to the cluster, matches the PSNT in the SO document and the PSNT on the cluster, as presented by the XMCLI command.

**Note:** In a multiple cluster environment, all of the following commands should specify the cluster index by using the cluster-id=<n> parameter, where n is the cluster number.

2. Confirm that all Storage Controllers are healthy, by running the following command:

```
show-storage-controllers
```

Expected output:

```
xmcli <tech> show-storage-controllers cluster-id=1
Storage-Controller-Name ... State      Health-State  Enabled-State ... Conn-State
X1-SC1                  healthy      healthy      enabled      connected
X1-SC2                  healthy      healthy      enabled      connected
X2-SC1                  healthy      healthy      enabled      connected
X2-SC2                  healthy      healthy      enabled      connected
```

Verify that the Storage Controllers Conn-State is connected and that all of the Storage Controllers are healthy and enabled.

3. Confirm that all DAEs have redundant power, by running the following command:

```
show-daes-psus
```

Expected output:

```
xmcli <tech> show-daes-psus cluster-id=1
Name          Index ... Power-Feed State      Input Location ... DAE-Name DAE-Index ...
X1-DAE-PSU1   1      ... PWR-A      healthy on      right  X1-DAE  1
X1-DAE-PSU2   2      ... PWR-B      healthy on      left   X1-DAE  1
X1-DAE-PSU1   3      ... PWR-A      healthy on      right  X1-DAE  1
X1-DAE-PSU2   3      ... PWR-B      healthy on      left   X1-DAE  1
```

Verify that the state of all PSUs is healthy and that Input is on.

4. Confirm that the Storage Controllers have redundant power, by running the following command:

```
show-storage-controllers-psus
```

Expected output:

```
xmcli <tech> show-storage-controllers-psus cluster-id=1
Name          Index ... Power-Feed State      Enabled-State Input Location ...
X1-SC1-PSU-L  1      ... PWR-A    healthy   enabled    on    right
X1-SC1-PSU-R  1      ... PWR-B    healthy   enabled    on    left
X1-SC2-PSU-L  1      ... PWR-A    healthy   enabled    on    right
X1-SC2-PSU-R  1      ... PWR-B    healthy   enabled    on    left
...
```

Verify that the state of all PSUs is *healthy* and that Input is *on*.

5. Confirm that the InfiniBand Switches have redundant power, by running the following command:

```
show-infiniband-switches-psus
```

Expected output:

```
xmcli <tech> show-infiniband-switches-psus cluster-id=1
Name          Index ... Index-in-Cluster Location Input-Power State
IB-SW1-PSU1   1      ... 1                left    on    healthy
IB-SW1-PSU2   2      ... 2                right   on    healthy
IB-SW2-PSU1   3      ... 1                left    on    healthy
IB-SW2-PSU2   4      ... 2                right   on    healthy
```

Verify that the state of all PSUs is *healthy* and that Input is *on*.



## 6. Confirm that InfiniBand ports have no errors, by running the following commands:

- `show-storage-controllers-infiniband-counters`

Expected output:

```
xmcli <tech> show-storage-controllers-infiniband-counters cluster-id=1
Cluster-Name      ... Symb-Errs Symb-Errs-pm ... Intg-Errs-pl Rmt-Phys-Errs-pl
XtremIO_Cluster   ... 0       0             ... 0           0
XtremIO_Cluster   ... 0       0             ... 0           0
XtremIO_Cluster   ... 0       0             ... 0           0
XtremIO_Cluster   ... 0       0             ... 0           0
```

Verify that all the error counters (Symb-Errs, Symb-Errs-pm, Recovers, Recovers-pm, Lnk-Downed, Lnk-Downed-pm, Rcv-Errs, Rcv-Errs-pm, Rmt-Phys-Errs, Rmt-Phys-Errs-pm, Integ-Errs, Integ-Errs-pm, Rcv-Errs-pl, Recovers-pl, Lnk-Downed-pl, Symb-Errs-pl, Intg-Errs-pl, Rmt-Phys-Errs-pl), are "0".

- `show-storage-controllers-infiniband-ports`

Expected output:

```
xmcli <tech> show-storage-controllers-infiniband-ports cluster-id=1
Name      Index Port-Index Peer-Type      Link-Rate-In-Gbps Port-State ... Health-Level
X1-SC1-IB1 1      1      StorageController 40             up      ... level_1_clear
X1-SC1-IB2 2      2      StorageController 40             up      ... level_1_clear
X1-SC2-IB1 3      1      StorageController 40             up      ... level_1_clear
X1-SC2-IB2 4      2      StorageController 40             up      ... level_1_clear
```

Verify that for all ports Link-Rate-In-Gbps is "40" and Port-State is "up".

## 7. Confirm that there are no SAS errors on the active SAS connections, by running the following command:

```
query class="Node" prop-list=["sas1_port_rate",
"sas1_port_state", "sas1_hba_port_health_level",
"sas2_port_rate", "sas2_port_state",
"sas2_hba_port_health_level"]
```

**Note:** This test should be executed using tech role.

Execution example:

```
xmcli <tech> query class="Node" prop-list=["sas1_port_rate",  
"sas1_port_state", "sas1_hba_port_health_level",  
"sas2_port_rate", "sas2_port_state",  
"sas2_hba_port_health_level"]  
  
Storage-Controller-Name: X1-SC1  
Index: 1  
SAS1-Port-Rate: 6gbps  
SAS1-Port-State: up  
SAS1-Port-Health-Level: level_1_clear  
SAS2-Port-Rate: 6gbps  
SAS2-Port-State: up  
SAS2-Port-Health-Level: level_1_clear  
Storage-Controller-Name: X1-SC2  
Index: 2  
SAS1-Port-Rate: 6gbps  
SAS1-Port-State: up  
SAS1-Port-Health-State: level_1_clear  
SAS2-Port-Rate: 6gbps  
SAS2-Port-State: up  
SAS2-Port-Health-Level: level_1_clear  
Storage-Controller-Name: X2-SC1  
Index: 3  
SAS1-Port-Rate: 6gbps  
SAS1-Port-State: up  
SAS1-Port-Health-State: level_1_clear  
SAS2-Port-Rate: 6gbps  
SAS2-Port-State: up  
SAS2-Port-Health-Level: level_1_clear  
Storage-Controller-Name: X2-SC2  
Index: 4  
SAS1-Port-Rate: 6gbps  
SAS1-Port-State: up  
SAS1-Port-Health-State: level_1_clear  
SAS2-Port-Rate: 6gbps  
SAS2-Port-State: up  
SAS2-Port-Health-Level: level_1_clear
```

Verify that all SAS ports are up and have 6gbps rate.

## Knowledge, Equipment and Documentation

- ◆ Verify that the customer is introduced to the XtremIO Support page on the EMC Support portal.
- ◆ Verify that the customer is notified about the support flow and knows how to open an SR.
- ◆ Introduce the customer to the *XtremIO Storage Array User Guide* for information on using the XtremIO Storage.
- ◆ Introduce the customer to the *XtremIO Storage Array Host Configuration Guide* for information on configuring hosts.



# APPENDIX A

## Software Re-Installation

This section provides instructions for downloading and re-installing a software image on the Storage Controller and XMS.

This section includes the following topics:

- ◆ [Writing the XtremIO Rescue Image to a USB Drive .....](#) 110
- ◆ [Re-Installing a Storage Controller .....](#) 112
- ◆ [Re-Installing a Physical XMS.....](#) 114

## Writing the XtremIO Rescue Image to a USB Drive

Before writing the XtremIO rescue image to a USB drive, perform the following steps:

**Note:** Verify that you have a USB drive that is of at least 2GB in capacity.

1. Locate the XtremIO Rescue Image in the XtremIO Support page (in [support.emc.com](http://support.emc.com)).

For details on the XtremIO Storage Controller Rescue Image or XtremIO virtual XMS Rescue Image to download from the Support page, refer to the *Release Notes* of the version you are installing.

2. Download the image locally to the machine where the USB drive will be created.

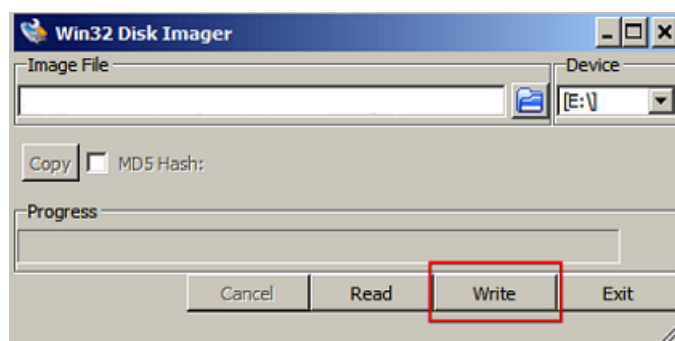
**Note:** When you are downloading a software package, access the EMC Support page and verify that the MD5 checksum of the package you downloaded matches the MD5 checksum that appears in the support page for that package.

To write the XtremIO image to a USB drive (on Windows 7):

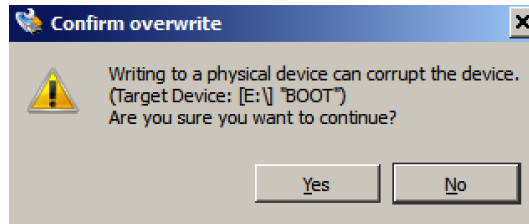
**Note:** Before you proceed, verify that the USB drive is available.

1. Download and unpack the *Win32 Disk Imager* utility (<http://sourceforge.net/projects/win32diskimager/>).
2. Launch the *Win32 Disk Imager* utility on the local machine.
3. Insert the USB drive into the USB port on the Windows machine.
4. Under **Image File** in the Win32 Disk Imager dialog box, click the folder icon and select the XtremIO Rescue Image file you downloaded earlier.
5. Under **Device**, click the drop-down menu and select the device drive letter for the USB drive.

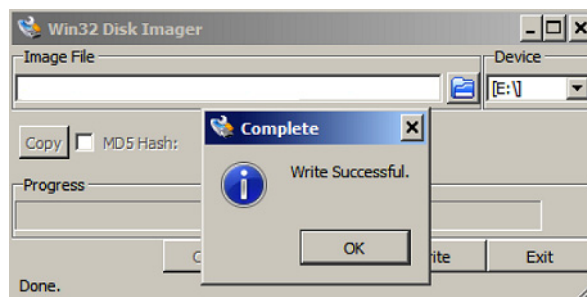
**Note:** Use Window Explorer to ensure that the correct drive letter is selected.



6. Click **Write** to write the image file to the USB Drive; a warning appears to indicate that existing data on the selected drive will be overwritten.



7. Verify that the correct drive letter is selected and click **Yes** to confirm.
8. Follow the write operation progress. When the operation is completed, a message appears indicating that the write was successful.



9. Click **OK**.
10. From the Windows Notification Area, click the **Safely Remove Hardware and Eject Media** icon.



11. From the menu, select **Eject USB drive**.

**Note:** The menu option includes the USB drive's brand name (e.g. "Cruzer Blade" appears when SanDisk Cruzer Blade USB drive is used).

Wait for the "Safe to Remove Hardware" message to appear in the Notification Area and remove the USB drive.

## Re-Installing a Storage Controller

---

**Note:** Unless instructed otherwise in this document, always consult with XtremIO Support before re-installing a Storage Controller.

---

An X-Brick Storage Controller image is available for USB flash drives to restore a Storage Controller to its original state.

Extract the image to a USB flash drive (refer to [“Writing the XtremIO Rescue Image to a USB Drive” on page 110](#)) and connect the USB flash drive to the Storage Controller USB port.

---

**Note:** Before starting the procedure, verify that you have a KVM or keyboard and monitor connected.

---

### To re-install a Storage Controller:

1. Power-cycle the Storage Controller by unplugging and reconnecting its two power cables.
2. As the Storage Controller powers up, press **F6** to enter the boot device menu.
3. When prompted, type the BIOS password to display the boot device menu.

---

**Note:** If the boot device menu is not displayed, F6 was pressed too late. Go back to Step 1 and repeat the procedure.

---

4. In the boot device menu, select **USB device**.

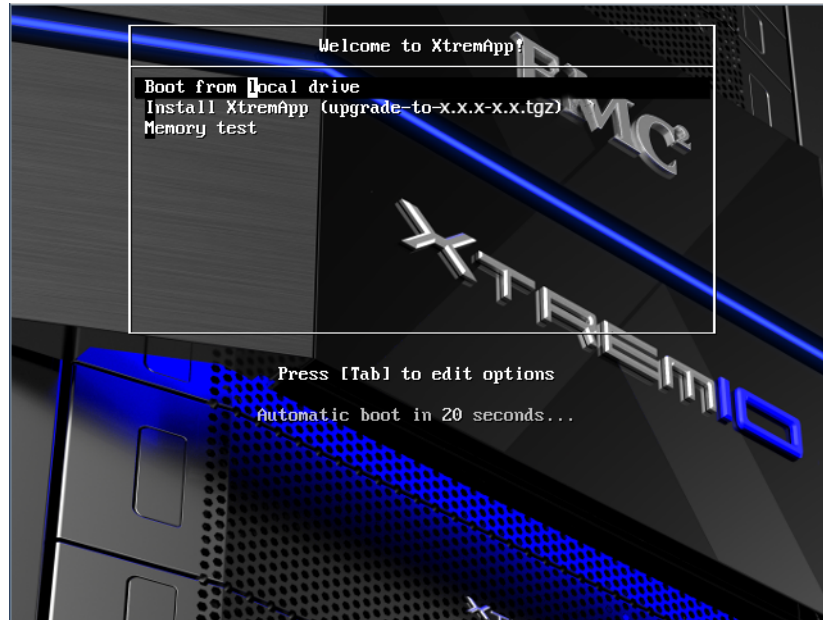
---

**Note:** The menu option includes the USB drive’s brand name (e.g. "Cruzer Blade" appears when SanDisk Cruzer Blade USB drive is used).

---



5. When the Storage Controller is booted-up, select **Install XtremApp** from the GRUB menu.



6. Wait for the installation to complete and for the Storage Controller to reboot.
7. Remove the USB drive.

## Re-Installing a Physical XMS

---

**Note:** Always consult with XtremIO Support before re-installing the physical XMS.

---

An XMS image is available for USB flash drives to install on the physical XMS node.

Extract the image to a USB flash drive (refer to [“Writing the XtremIO Rescue Image to a USB Drive” on page 110](#)) and connect the USB flash drive to the XMS USB port.

---

**Note:** Before starting the procedure, verify that you have a KVM or keyboard and monitor connected.

---

### To re-install an XMS:

1. Power-cycle the XMS by unplugging and reconnecting its two power cables.
2. As the XMS powers up, press **F6** to enter the boot device menu.
3. When prompted, type the BIOS password to display the boot device menu.

---

**Note:** If the boot device menu is not displayed, **F6** was pressed too late. Go back to Step 1 and repeat the procedure.

---

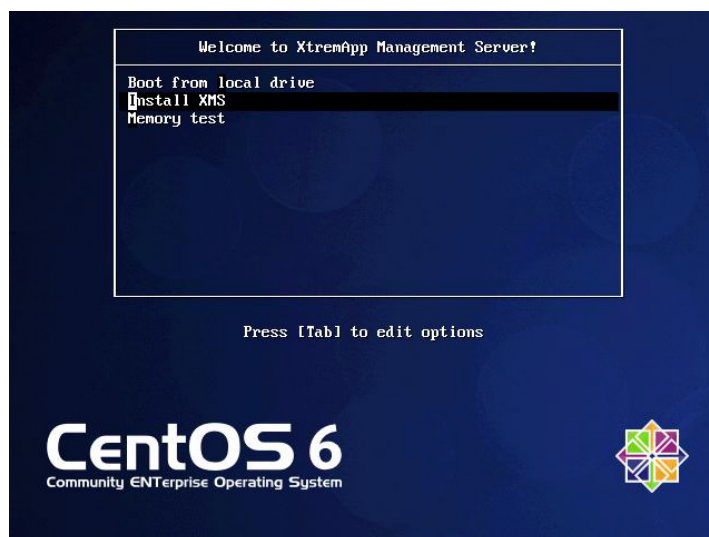
4. In the boot device menu, select **USB device**.

---

**Note:** The menu option includes the USB drive’s brand name (e.g. "Cruzer Blade" appears when SanDisk Cruzer Blade USB drive is used).

---

5. When the server is booted-up, select **Install XMS** from the GRUB menu.



6. Wait for the installation to complete and for the XMS to reboot.
7. Remove the USB drive.

# APPENDIX B

## Configuring Virtual XMS High-Availability

This section provides instructions for using vSphere HA features, which assist in avoiding the need to perform an XMS restore.

This section includes the following topics:

- ◆ Virtual XMS Failures ..... 116
- ◆ Configuration Alternatives for Virtual XMS High-Availability ..... 116

## Virtual XMS Failures

The XMS, as a single component in the XtremIO cluster, is vulnerable to host and network failures. When such failures occur, I/O to the XtremIO Storage Array is not affected. However, no monitoring and/or configuration changes (creating or deleting volumes, etc.) are possible in such a case.

When using a virtual XMS topology, it is possible to take advantage of vSphere HA features to easily overcome such failures.

The virtual XMS should be configured to withstand the following failures:

- ◆ Failure due to a power loss or hardware malfunction to the physical host running the virtual XMS
- ◆ Failure due to a network connectivity loss to the physical host running the virtual XMS (loss of connection between the XMS and the X-Brick)

## Configuration Alternatives for Virtual XMS High-Availability

**Two configuration alternatives are available for virtual XMS High-Availability:**

- ◆ **VSphere HA** - Ensures Virtual XMS availability and protects it from VM failure in the following manners:
  - Restarting the virtual XMS on another host within the ESX cluster.
  - Continuously monitoring the virtual XMS and resetting it in case of failure detection.

Using these protection strategies enables the virtual XMS to be accessible up to two minutes after a failure is identified.

See [“Configuring a Highly-Available Virtual XMS, Using vSphere HA” on page 117](#).

- ◆ **VSphere Fault Tolerance** - Provides a higher level of availability than vSphere HA. This will allow the Virtual XMS to remain accessible when any of the failures mentioned above occur.

See [“Configuring a Highly-Available Virtual XMS, Using vSphere Fault Tolerance” on page 120](#).

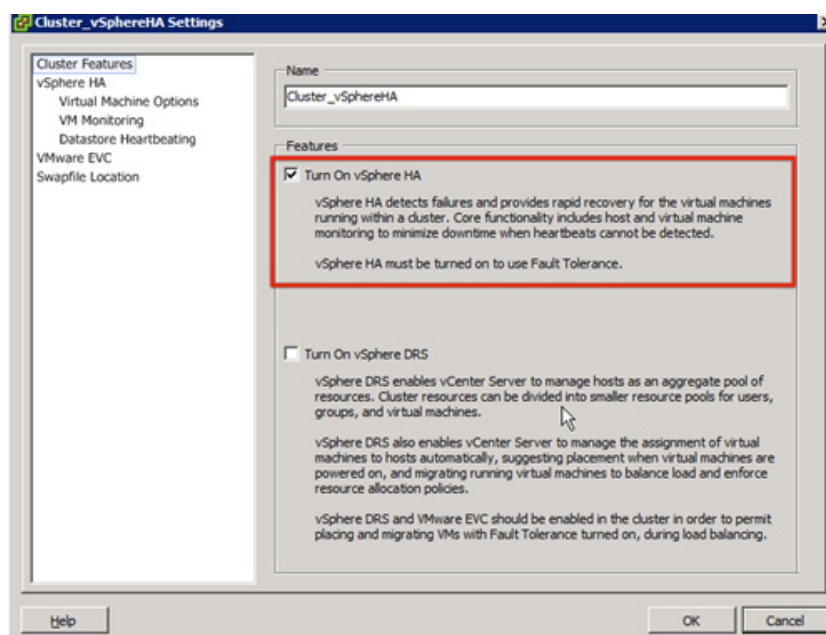
## Configuring a Highly-Available Virtual XMS, Using vSphere HA

The requirements for this configuration are as follows:

- ◆ **Licensing:** vSphere license for vCenter Server and ESX should include the vSphere HA feature with VMware vSphere 4.1 or VMware vSphere 5.x.
- ◆ **Resources:** ESX cluster hosts should have sufficient resources to allow a fail-over of the VM, holding the Virtual XMS.
- ◆ **IP Addresses:** All hosts are required to have static IP addresses. If DHCP is used to distribute IP addresses, IP reservations should be set to allow each host to keep a consistent IP address across reboots.
- ◆ **Network Planning:** At least one common management network is required among all ESX hosts. The best practice vSphere HA documentation recommends having at least two (ESXi 5.x - VMkernel network with the Management traffic checkbox enabled, ESX 4.1 - service console network).
- ◆ **Datastores:** To ensure that the VM can run on any ESX host (member of the cluster), all hosts should have access to the same datastore (where the VM is located). To minimize any dependency between the VM and the XtremIO storage, this shared storage should not be originating from the same XtremIO Storage Array.
- ◆ **VM Monitoring:** VM requires VMware Tools to be installed. The VMware Tools are part of the Virtual XMS OVF template.

**To configure a Highly-Available Virtual XMS, using vSphere HA:**

1. Create a vSphere HA Cluster, using the vSphere Client, as follows:
  - a. Select the **Hosts & Clusters** view.
  - b. Right-click **Datacenter** in the Inventory tree and select **New Cluster**.
  - c. Complete the New Cluster wizard (do not enable vSphere HA [or DRS] at this time).
  - d. Based on your plan for the resources and networking architecture of the cluster, use the vSphere Client to add hosts to the cluster. Add at least two hosts to the cluster.
  - e. Right-click the cluster and click **Edit Settings**; the cluster's Settings dialog box opens, enabling you to modify the vSphere HA (and other) settings for the cluster.
  - f. On the **Cluster Settings** page, select **Turn On vSphere HA**.

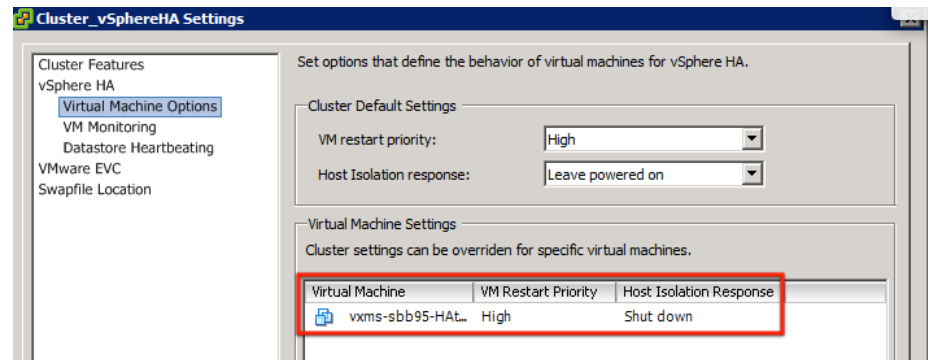


2. Configure the vSphere HA settings according to the customer's needs, as follows:

- a. Host Monitoring Status
- b. Admission Control
- c. Virtual Machine Options:

For the virtual XMS:

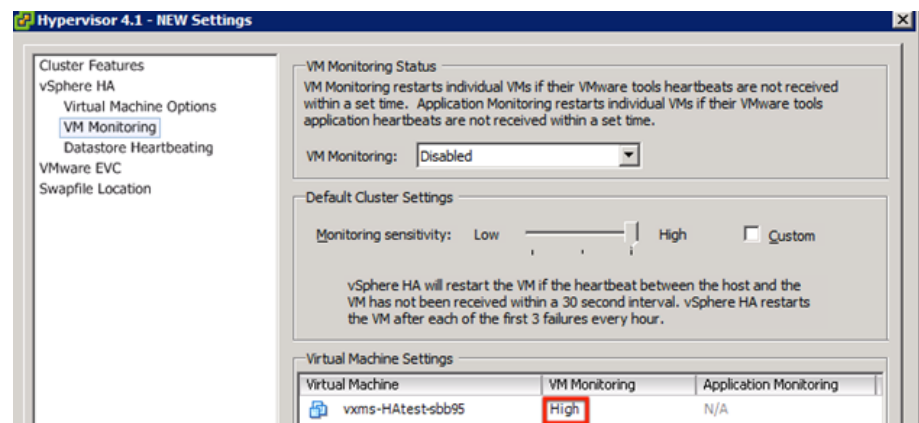
- Set the **VM restart priority** to **High**.
- Set the **Host Isolation response** to **Shut Down**.



d. VM Monitoring:

For the XMS VM:

- Set the **VM Monitoring** to **High**.



e. Datastore Heartbeating:

- Provide at least two datastores, located in shared storage, to be used to monitor hosts and VMs.

3. Migrate the virtual XMS VM to the vSphere HA cluster:

Migrate the online virtual XMS into the cluster, using vMotion.

The XtremIO Storage Array remains operational throughout the migration.

---

**Note:** From this point, any failure that is identified causes the vCenter Server to shut the virtual XMS off and restart the virtual XMS on another host in the vSphere HA cluster. The failover should take approximately 1 to 2 minutes to complete, during which time the virtual XMS is inaccessible.

---

## Configuring a Highly-Available Virtual XMS, Using vSphere Fault Tolerance

The requirements for this configuration are as follows:

- ◆ **Licensing:** vSphere license for vCenter Server and ESXi should include the vSphere FT feature.
- ◆ **Fault Tolerance Software:** At least two FT-certified hosts, running the same Fault Tolerance version or host build number. The Fault Tolerance version number appears on a host's Summary tab in the vSphere Web Client or vSphere Client.
- ◆ **VSphere HA:** vSphere HA must be enabled before Fault-Tolerant VM can be enabled.
- ◆ **Hardware:** Hosts must have processors from the FT-compatible processor group. It is also highly recommended that the hosts' processors be compatible with one another. For more information regarding the supported processors, see the VMware knowledge base article at <http://kb.vmware.com/kb/1008027/>.
- ◆ **Fault-Tolerance Certified H/W:** Hosts must be certified for Fault Tolerance. Go to <http://www.vmware.com/resources/compatibility/search.php> and select **Search by Fault Tolerant Compatible Sets** to determine if your hosts are certified.
- ◆ **BIOS:** Each ESX host must have **Hardware Virtualization (HV)** enabled in the BIOS.

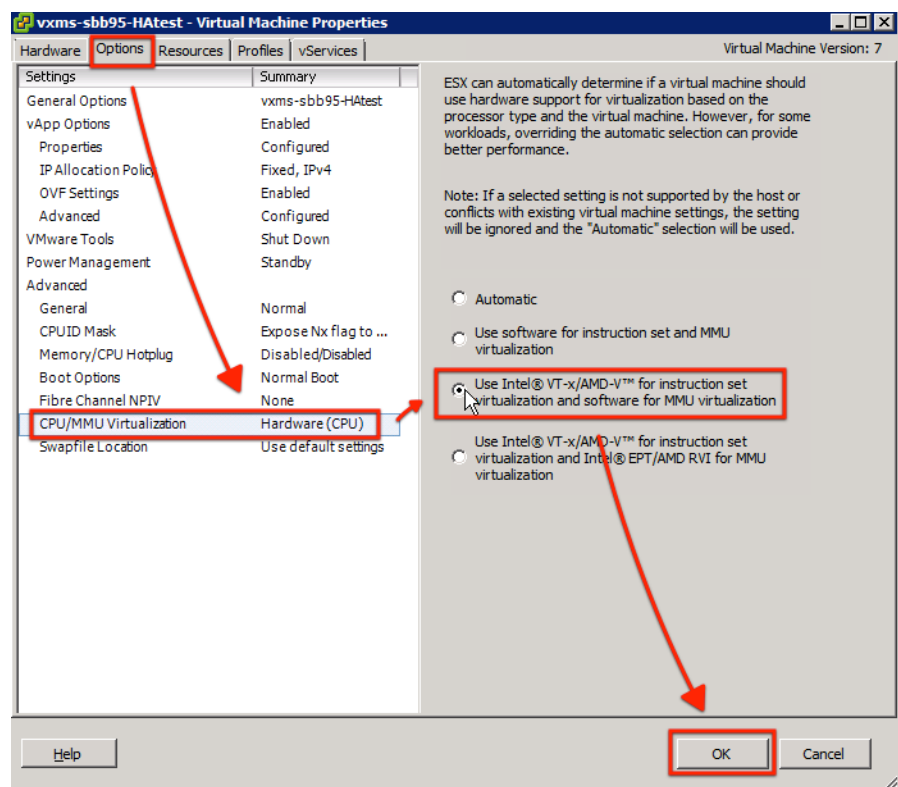
In addition, the following requirement should be made on the Virtual XMS VM:

- ◆ **Disk:** The Virtual XMS virtual machine must be stored in a virtual machine disk (VMDK) file that is thick provisioned.



### To configure a Highly-Available Virtual XMS, using vSphere FT:

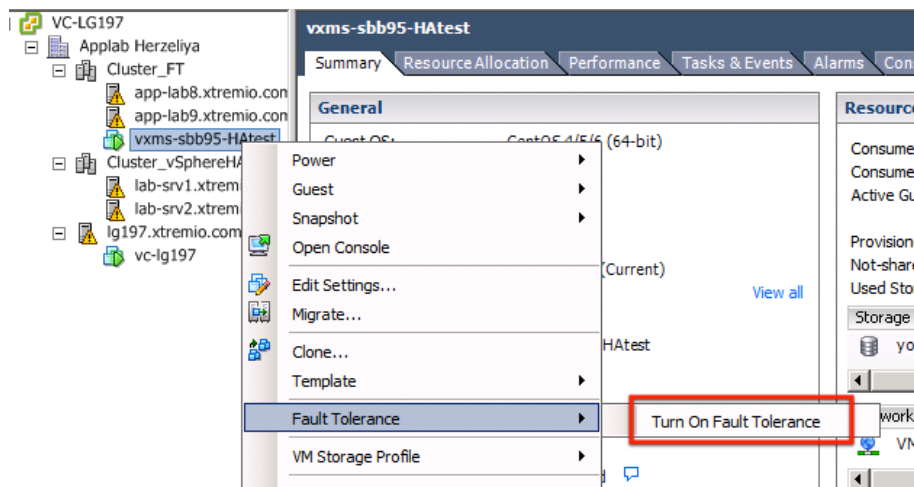
1. Use the vSphere HA Cluster created in earlier steps.
2. Prepare the Virtual XMS VM for vSphere Fault Tolerance, using the vSphere Client, as follows:
  - a. Select the **Hosts & Clusters** view.
  - b. In the **Inventory**, right-click the Virtual XMS VM.
  - c. Select **Edit Settings** to display the virtual machine properties screen.
  - d. Click the **Options** tab and then **CPU/MMU Virtualization**.
  - e. In the right pane, select **Use Intel VT-x/AMD-V for instruction set virtualization and software for MMU virtualization**.



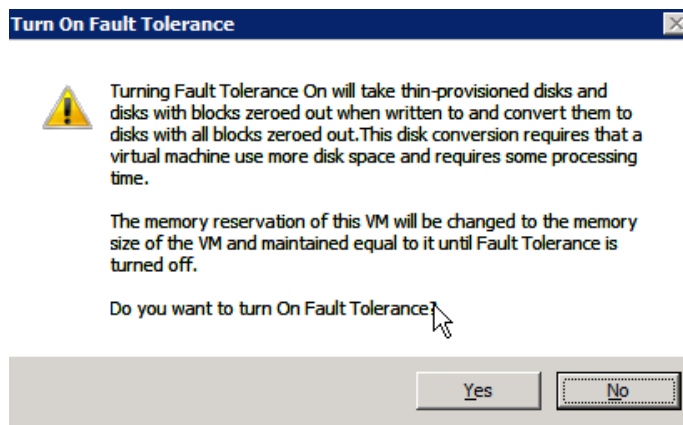
- f. Click **OK** to apply.

The VM must be power cycled or vMotioned to another host for the settings to apply. Once done, you can enable Fault-Tolerance.

3. Enable vSphere Fault Tolerance on the Virtual XMS VM:
  - a. Select the **Hosts & Clusters** view.
  - b. In **Inventory**, right-click the Virtual XMS VM and click **Turn On Fault Tolerance**.



- c. A warning window may appear, stating that the virtual disk of the Virtual XMS VM will be converted to all blocks zeroed out. Click **Yes** to accept.



**Note:** From this point on, the primary Virtual XMS VM is running on one ESX host and a secondary Virtual XMS VM is running on a different second host. The secondary VM executes the same series of instructions as the Primary Virtual XMS does, while only a single virtual machine image (the Primary Virtual XMS) executes workload on the XtremIO storage.

#### Fault Tolerance

Fault Tolerance Status: **Protected**

Secondary Location: [app-lab9.xtremio.com](#)

Total Secondary CPU: 168 MHz

Total Secondary Memory: 122.00 MB

vLockstep Interval: 0.011 seconds

Log Bandwidth: 140 KBps

The screenshot shows the vCenter Server interface. On the left, a tree view displays the hierarchy: VC-LG197 > Applab Herzeliya > Cluster\_FT > vxms-sbb95-HAtest. The 'vxms-sbb95-HAtest' VM is highlighted with a red box. A red arrow points from this VM to the 'Cluster\_FT' summary page on the right. The summary page shows a table of virtual machines:

Name	State	Status	Host
vxms-sbb95-HAtest	Powered On	Normal	<a href="#">app-lab8.xtremio.com</a>
vxms-sbb95-HAtest (secondary)	Powered On	Normal	<a href="#">app-lab9.xtremio.com</a>

**Note:** The vCenter Server fails-over to the secondary Virtual XMS VM when it identifies a failure. However, unlike the vSphere HA based configuration, the Virtual XMS remains accessible throughout the failover.



# APPENDIX C

## Miscellaneous ESRS Related Tasks

This section describes various ESRS-related tasks. This information is applicable only when using an ESRS GW (both VE and legacy type ESRS gateways) or ESRS IP client.

This section includes the following topics:

- ◆ [Overriding ServiceLink Default Operation when Launching Remote Applications ...](#) 126
- ◆ [Miscellaneous ESRS GW Procedures.....](#) 127

## Overriding ServiceLink Default Operation when Launching Remote Applications

---

**Note:** The following information is relevant only if the ServiceLink GUI Launch Application buttons fail.

---

The AutoLaunch.ini file contains the application call locations of all remote utilities for EMC's product portfolio. These calls can be launched within ServiceLink after a remote support session is established to the XtremIO Storage Array.

This file is updated to support automatic launching of SSH whenever the end-user invokes the CLlviaSSH ESRS remote application.

If remote application buttons in ServiceLink fail, it is possible to download a local copy and adjust the AutoLaunch.ini file to resolve the failures.

Refer to EMC KB # 203670 (<https://support.emc.com/kb/203670>) for the steps to download and configure an Autolaunch.ini file on your local machine.

Launching an XtremIO CLlviaSSH session through ServiceLink, automatically initiates a PuTTY session. At this point you can authenticate against the cluster, using your preferred credential (xinstall, xmsadmin, etc.).

## Miscellaneous ESRS GW Procedures

**Note:** These procedures can be used for both VE and legacy type ESRS gateways.

### Confirming the XtremIO Cluster as a Managed Device in ServiceLink

To confirm the XtremIO cluster as a managed device from the ServiceLink portal after running the `modify-syr-notifier` XMCLI command on the XMS:

1. Log in to ServiceLink (<https://esrs.emc.com/portal>), using your RSA SecureID credentials.
2. Type the Device ID in the Browse For Devices field, preceded by `%` (e.g. %ESRSGW\_1010\_13061111471591), to access your ESRS GW page.
3. Click **Search**.

**Note:** If the Device ID of the ESRS GW is unknown, refer to [“Locating the Device ID of the ESRS GW” on page 128](#) for the steps to retrieve it.

4. From the matching device IDs list, click the ESRSGW device name to open its status screen.
5. Confirm that the status of the ESRS GW is 'Good' (otherwise, refer to [“Troubleshooting/Restoring ESRS GW Connectivity to ServiceLink” on page 130](#)).
6. In the Additional Information pane, click **Managed Devices** to display the list of devices currently managed by the ESRS GW.
7. Locate the entry associated with your XtremIO device. The device's state should be Pending Add, and its status should display a red icon.

Managed Devices							Add		Approve All		Sync Now
Serial Number	Product	Site Id	Organization	IP	GW1	GW2	Status	State	Action		
 XTREMIO SVT001	XTREMIO	11145366	SERVICE PLANNING - SVT SERVICE	10.241.185.111				Pending Add	edit   remove   approve		

8. In the Action column, click **approve** to change the device's state to Managed.

Managed Devices							Add		Approve All		Sync Now
Serial Number	Product	Site Id	Organization	IP	GW1	GW2	Status	State	Action		
 XTREMIO SVT001	XTREMIO	11145366	SERVICE PLANNING - SVT	10.241.185.111				Managed	edit   remove		

Page 1 of 1    Items 1 - 1 of 1

9. Click **Sync Now** to synchronize ServiceLink and the customer's ESRS GW; a popup window appears stating 'This action will immediately push out the device list to all relevant Gateways'.
10. Click **'OK'** to proceed.

---

**Note:** Due to a sync delay, the device's status may take up to 30 minutes to change from red to green.

---

---

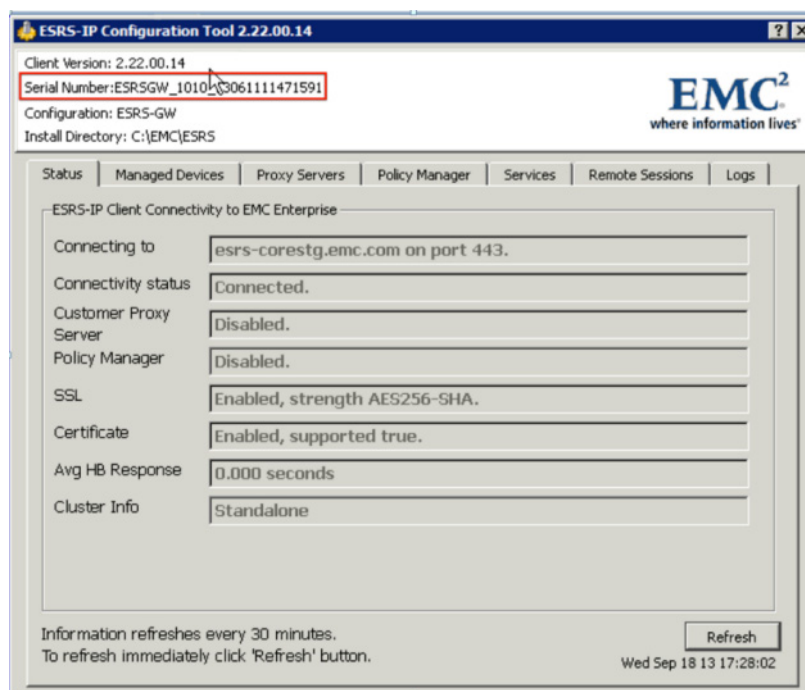
**Note:** If required, refer to ["Expediting Discovery of the XtremIO Device on ESRS GW" on page 132](#) for expediting the XtremIO device discovery in ServiceLink.

---

## Locating the Device ID of the ESRS GW

### To find the Device ID of a legacy type ESRS GW:

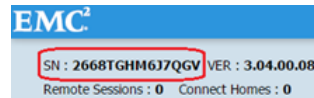
1. With the customer's assistance, access the Windows system running the ESRS GW (e.g. using remote desktop or WebEx).
2. Open the ESRS IP Configuration Tool at **Start > ESRS > Configuration Tool**; the Device ID of the ESRS GW is displayed at the top of the ESRS IP Configuration window, adjacent to the Serial Number field.





**To find the device ID of the VE type ESRS gateway:**

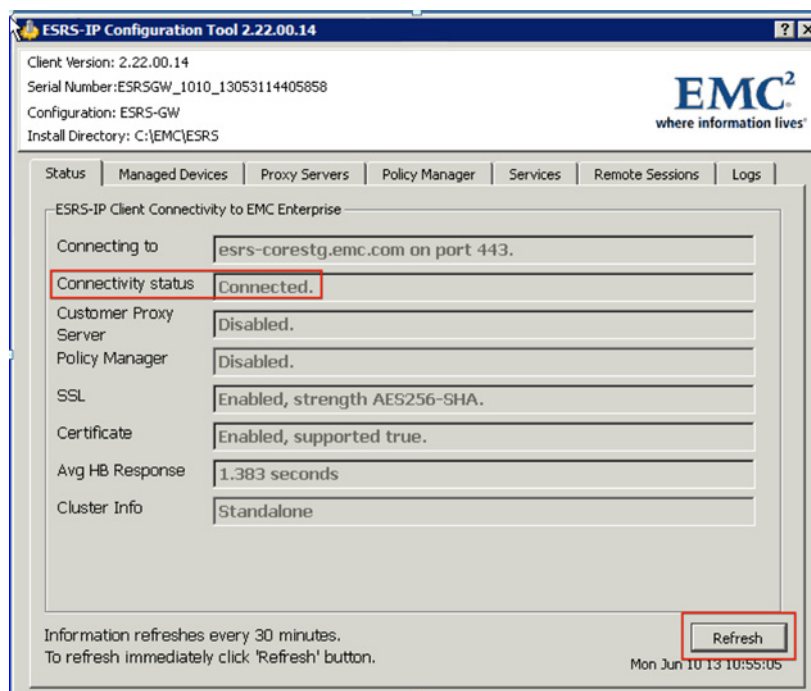
1. With the customer's assistance, access a machine on the customer's network, capable of contacting the ESRS VE via a standard web browser (e.g. using remote desktop or WebEx).
2. Using a standard web browser, establish an HTTPS Web UI session to the ESRS VE and log into the console, using the administrative (admin) credentials.
3. Within the ESRS VE Web UI, locate the **SN** field in the top right hand corner of the opening pane. The value in this field represents the Device ID of the ESRS VE.



## Troubleshooting/Restoring ESRS GW Connectivity to ServiceLink

To restore the connectivity status of the legacy type ESRS GW when its ServiceLink status is not Good:

1. Access the customer's Windows system running the ESRS GW (e.g. using remote desktop).
2. Open the ESRS IP Configuration Tool at **Start > ESRS > Configuration Tool**.



3. The ESRS GW Connectivity Status should be **Connected**. Otherwise, work with the customer to troubleshoot the connectivity problem.
4. When the connectivity issue is resolved, return to the ESRS IP Configuration Tool and click **Refresh**.

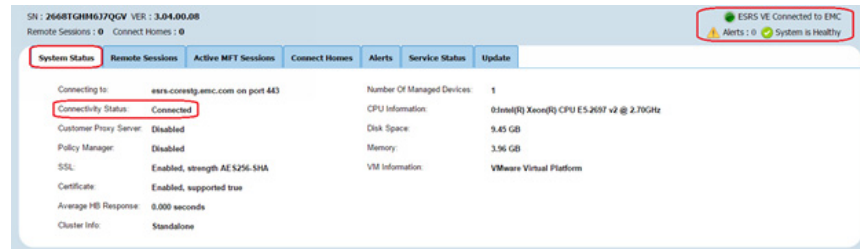
**Note:** The connectivity status should revert back to Connected within one to two minutes.

5. Return to the ServiceLink Portal and confirm that the ESRS GW device status is Good.

To restore the connectivity status of the VE type ESRS GW when its ServiceLink status is not Good:

1. With the customer's assistance, access a machine on the customer's network capable of contacting the ESRS VE via a standard web browser (e.g. using remote desktop or WebEx).
2. Using a standard web browser, establish an HTTPS Web UI session to the ESRS VE and log into the console using the administrative (admin) credentials.
3. Click the **System Status** tab on the ESRS VE Web UI.

4. The ESRS VE Connectivity Status should be **Connected**. Otherwise, work with the customer to troubleshoot the connectivity problem. Additionally, confirm that the **ESRS VE is Connect to EMC** via a green status icon and the **System is Healthy** with a green check mark in the upper right hand corner of the page.



5. When the connectivity issue is resolved, return to the ESRS VE Web UI session and refresh the browser session by striking the **F5** key on your keyboard.

**Note:** The connectivity status should revert back to Connected withing one to two minutes.

6. Return to the ServiceLink Portal and confirm that the ESRS VE device status is **Good**.

## Expediting Discovery of the XtremIO Device on ESRS GW

**To expedite the discovery of the XtremIO device, recently added to the legacy type ESRS GW via the ServiceLink portal:**

1. Connect to the ESRS GW cluster (e.g. using Remote Desktop).
2. Launch the ESRS IP Configuration Tool at **Start > ESRS > Configuration Tool**.
3. Click the **Managed Devices** tab.
4. Click **Refresh** (located at the bottom of the pane) to initiate a poll between ServiceLink and your ESRS Gateway.
5. From the managed devices list within the ESRS Configuration Tool, locate the device you recently approved via ServiceLink.  
If the device is not visible immediately, wait for 5 minutes and click **Refresh** again.

**To expedite the discovery of the XtremIO device, recently added to an VE type ESRS GW via the ServiceLink portal:**

1. With the customer's assistance, access a machine on the customer's network capable of contacting the ESRS VE via a standard web browser (e.g. using remote desktop or WebEx).
2. Using a standard web browser, establish an HTTPS Web UI session to the ESRS VE and log into the console, using the administrative (admin) credentials.
3. Click the **Devices** drop-down menu and select **Manage Device** within the ESRS VE Web UI.
4. Click **Refresh** (located at the bottom of the ESRS VE Web UI) to initiate a poll between ServiceLink and your VE type ESRS gateway).
5. From the managed devices list within the ESRS VE Web UI, locate the device you recently approved via ServiceLink.
6. If the device is not visible immediately, wait for five minutes and click **Refresh** again.

## Removing a Cluster from ESRS

**Note:** This procedure applies only to clusters connected to ESRS, using the ESRS GW configuration (legacy an VE type gateways).

This procedure should be used when the cluster is moved to another XMS, or when the cluster is physically moved from the customer's site.

### To remove a cluster from ESRS:

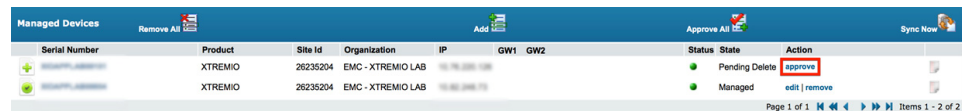
1. Access ServiceLink (<https://esrs.emc.com>) and locate the status page of the cluster using its S/N PSNT.
2. On the cluster's status page, confirm that the cluster's connectivity status is **connected**. If the status is disconnected, troubleshoot the connectivity status of the cluster to ESRS. Refer to [“Checking the ESRS and Connect-Home Configuration on the XMS” on page 87](#) for details.
3. On the cluster's status page, click the ESRS GW connecting the cluster to ESRS to access the status page of the GW machine. If the cluster is connected to an ESRS cluster (i.e. it uses more than a single GW machine), click one of the GW machines from the cluster status page in ServiceLink.
4. From the status page of the GW machine, click **managed devices** and locate the affected cluster on the list, using its S/N PSNT.
5. Click **Remove** to remove the cluster from the ESRS GW.



Serial Number	Product	Site Id	Organization	IP	GW1	GW2	Status	State	Action
26235204	XTREMIO	26235204	EMC - XTREMIO LAB	10.162.248.73			Managed		edit   remove
26235204	XTREMIO	26235204	EMC - XTREMIO LAB	10.162.248.73			Managed		edit   <b>remove</b>

The state of the cluster changes from Managed to Pending Delete.

6. Click **Approve** to delete the cluster from ESRS.



Serial Number	Product	Site Id	Organization	IP	GW1	GW2	Status	State	Action
26235204	XTREMIO	26235204	EMC - XTREMIO LAB	10.162.248.73			Pending Delete		<b>approve</b>   remove
26235204	XTREMIO	26235204	EMC - XTREMIO LAB	10.162.248.73			Managed		edit   remove

The cluster is removed from the GW managed device list.

7. Click **Sync Now** to synchronize the device removal between ESRS and the GW machine.



# APPENDIX D

## IPMI Interface Redirection

This section describes the IPMI Interface redirection procedure.

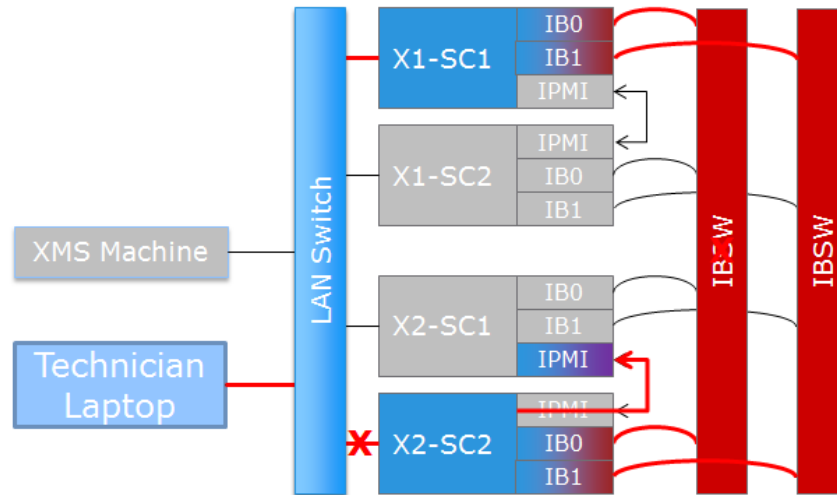
This section includes the following topics:

- ◆ [Enabling IPMI Tunneling.....](#) 136

## Enabling IPMI Tunneling

The XtremIO cluster uses a separate port, dedicated to IPMI, using internal addresses. As a result, the user cannot access the IPMI IP address directly. However, the technician can access a Storage Controller, via the peer Storage Controller, using IPMI tunneling.

The following figure describes the IP tunneling scheme:



In the example, the technician wants to access Storage Controller X2-SC1. Access via the peer Storage Controller (X2-SC2) fails because X2-SC2 is not responding. The technician then uses X1-SC1 as a proxy and accesses the peer Storage Controller via the IB Switch. If the used IB port is down (in the example, IB0), the technician can specify the other IB port (IB1).

### To enable IPMI tunneling:

1. Log in to the XMS, using the xinstall user credentials.
2. From the Install menu, type the number for `Enable temporary IPMI access.`
3. Provide the IP address of the Storage Controller that would be used to transfer IPMI traffic (the proxy Storage Controller). Usually, this is one of the Storage Controllers from X1.
4. Provide the name of the Storage Controller you wish to access (e.g. X2-SC2).
5. Provide the relevant IB port. If the specified IB port is down, you can confirm switching to the other IB port.

---

**Note:** The IPMI tunneling is performed using HTTPS to access port 80 of the proxy Storage Controller.

---