Xsigo Fabric Manager User Guide

Release 4.1.0

Xsigo Systems
70 West Plumeria Drive
San Jose, CA 95134
USA

http://www.xsigo.com
Tel: +1.408.329.5600
Part number: 650-30005-03 Rev A
Published: Jan 2013

Regulatory Compliance Statements

EMI Statement, United States of America (Class A)

“NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.”

EMI Statement, Canada (Class A)

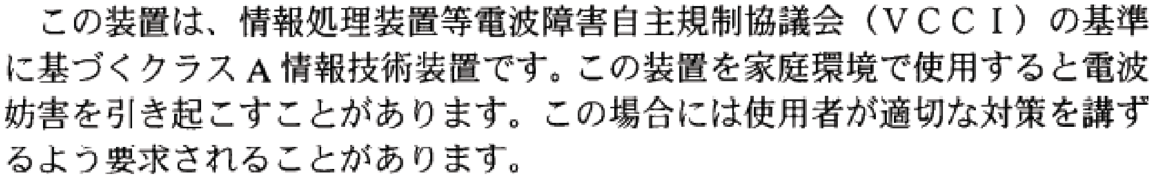
This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

EMI Statement, Europe and Australia (Class A)

“Warning - This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.”

EMI Statement, Japan (Class A)



この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

“This is a Class A product based on the standard of the Voluntary Control Council For Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.”

Lithium Battery - Replacement and Disposal

CAUTION!

Danger of explosion if the lithium battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Laser Caution for I/O Cards (CDRH-US)

USE OF CONTROLS OR ADJUSTMENTS OR PERFORMANCE OF PROCEDURES OTHER THAN THOSE SPECIFIED HEREIN MAY RESULT IN HAZARDOUS RADIATION EXPOSURE.

Complies with 21 CFR Chapter 1, Subchapter J, Part 1040.10.

IEC 60825-1: 1993, A1: 1997, A2: 2001; IEC 60825-2: 2000

Replacement Laser Transceiver Modules

For continued compliance with the above laser safety Standards, only approved Class 1 modules from our approved vendors should be installed in the product. Contact Xsigo Customer Support (see Technical Support Contact Information) for approved-vendor contact information.

Power Cord Set Requirements – General

The requirements listed below are applicable to all countries:

The length of the power cord set must be at least 6.00 feet (1.8 m) and a maximum of 9.75 feet (3.0 m).

All power cord sets must be approved by an acceptable accredited agency responsible for evaluation in the country where the power cord set will be used.

The power cord set must have a minimum current capacity of 13A and a nominal voltage rating of 125 or 250 V ac~, as required by each country's power system.

The appliance coupler on the power cord must meet the mechanical configuration of an EN 60320 / IEC 60320 Standard Sheet C20 connector, which is the connector on the Fabric Director. The C20 connector supports a C19 plug as the mating part on the power cord that connects to the Fabric Director.

Power Cord Set Requirements – Specifics By Country

United States (UL), Canada (CSA)

The flexible power cord set must be UL Listed and CSA Certified, minimum Type SVT or equivalent, minimum No. 18 AWG, with 3-conductors that includes a ground conductor. The wall plug must be a three-pin grounding type, such as a NEMA Type 5-15P (rated 15A, 120V) or Type 6-15P (rated 15A, 250V).

Europe (Austria (OVE), Belgium (CEBEC), Denmark (DEMKO), Finland (SETI), France (UTE), Germany (VDE), Italy (IMQ), Netherlands (KEMA), Norway (NEMKO), Sweden (SEMKO), Switzerland (SEV), U.K. (BSI/ASTA)

The flexible power cord set must be <HAR> Type H03VV-F, 3-conductor, minimum 0.75mm^2 conductor size. Power cord set fittings, particularly the wall plug, must bear the certification mark of the agency responsible for evaluation in the country where it is being used, with examples listed above.

Australia (DFT/SAA)

Cord is as described under “Japan (PSE)” immediately below. Pins in the power plug must be with the sheathed, insulated type, in accordance with AS/NZS 3112:2000.

Japan (PSE)

The appliance coupler, flexible cord, and wall plug must bear a “PSE” Mark in accordance with the Japanese Denan Law. The flexible cord must be Type VCT or VCTF, 3-conductor, 0.75 mm^2 conductor size. The wall plug must be a grounding type with a Japanese Industrial Standard C8303 (15A, 125V) configuration.

Software Compliance – GPL (GPL v2) Licenses and Notices

Xsigo Systems, a wholly owned subsidiary of Oracle, uses certain elements of GNU Public License (GPLv2) code. Under the conditions of the GPL licensing agreement, you are entitled to request a copy of the open source/freeware code. For questions about Xsigo’s use of the GPL code, or to request a copy of the code, you can contact Xsigo by completing the web form at http://pages.xsigo.com/compliance.html. Afterward, Xsigo will contact you to assist you with your request.

Xsigo Systems, eine ganz besessene Tochtergesellschaft von Oracle, gewisse Elemente des GNU Public License (GPLv2) Code. Unter den Bedingungen von der GPL Lizenzvertrag werden Sie berechtigt, eine Kopie der offenen Quelle/ Freewarecodes zu erbitten. Für Fragen um den Gebrauch von Xsigo des GPL Codes oder eine Kopie des Codes zu erbitten, können Sie Xsigo durch Vollenden der Gewebesform an http://pages.xsigo.com/compliance.html kontaktieren. Nachher wird Xsigo Sie kontaktieren, Ihnen mit Ihrer Bitte zu helfen.

Preface

Documentation Purpose and Audience

This guide provides the basic information that you need to install Oracle's Xsigo Fabric Manager GUI and use it to configure and manage multiple Oracle Fabric Directors. This guide presents procedural text for how to use the Fabric Manager GUI for common configuration and management tasks.

This guide is intended for data center administrators, and it assumes that its readers have knowledge and familiarity with common configuration and management tasks related to administering a data center. Although this guide does present some conceptual material about topics and technologies, it is not intended as a complete and exhaustive reference on those topics.

Document Overview

This guide contains the following sections:

- Fabric Manager Overview — Documents conceptual information about Fabric Manager and how it operates in your network.
- Installing Fabric Manager — Documents installing Fabric Manager software and starting the Fabric Manager Server on different server types.
- Working with the Interface — Documents the Fabric Manager interface and its elements; the Summary, Detail frame, wizards, and tables; how to use Fabric Manager controls to navigate the Fabric Manager interface; and how to use controls to sort, filter, and arrange data in the Fabric Manager interface.
- Working with Fabric Manager Jobs — Documents the concept of a Fabric Manager job, and how to view the status of one or more jobs you have submitted, and how to check the recent jobs information for individual features.
- Working with Network Clouds — Documents conceptual information about Network Clouds, what they are used for, and how they are configured.
- Working with Storage Clouds — Documents conceptual information about Storage Clouds, what they are used for, and how they are configured.
- Working with Default Gateways — Documents conceptual information about Xsigo's default gateways, how they are used, and how to configure them.
- Working with the Fabric Director — Documents how to use the Fabric Manager interface to discover Fabric Directors, retrieve hardware, firmware, and software information from them, and manage them; also documents how to use the Fabric Manager interface to retrieve information about SNMP, Active Directory, RADIUS, and other Fabric Director-based features.
- Working with I/O Templates — Documents conceptual information about I/O Templates, what they are used for, how they are configured.
- Working with I/O Profiles — Documents conceptual information about I/O Profiles, what they are used for, how they are configured, and how they are connected to a server.
- Working with Link Aggregation — Documents how to use the Fabric Manager interface to configure and manage link aggregation groups (LAGs) and link-aggregation features on Ethernet links.
- Working with Network QoS — Documents conceptual information about the Fabric Director's network quality of service (QoS) parameters and implementations, and provides procedural text about configuring Network QoS on Network Clouds.

- Working with Physical Servers — Documents how to display information about all the discovered host servers (either physical or virtual machines) connected to all discovered Fabric Directors.
- Working with Server Groups — Documents conceptual information about Xsigo's implementation of server groups, what they are used for, how to configure them, and what functionality is available to server groups.
- Working with Boot Profiles — Documents information about Xsigo's SAN boot and iSCSI Boot solutions, and how to configure SAN Boot Profiles and iSCSI Boot Profiles through Fabric Manager.
- Working with the Topology — Documents information about the Virtual Topology and the different ways of viewing virtual I/O connections and resources, and documents what configuration and management tasks are available through the Virtual Topology.
- Working with Discovery Subnets — Documents the physical topology view of hosts and Fabric Directors in Fabric Manager; also provides information about the IP discovery subnet, and how to configure Fabric Directors and Fabric Manager within a discovery subnet profile.
- Working with VMware Servers — Documents how to integrate Fabric Manager into the VMware vCenter and vSphere frameworks so that Xsigo Fabric Directors and virtual I/O can be managed through vCenter and vSphere.
- Working with Alarms — Documents information about the Fabric Manager Alarms Log and Alarms History, as well as how to filter and clear each.
- Working with High Availability Fabric Manager — Documents information about the High Availability Fabric Manager feature as well as how to configure it to retain a shared configuration between both the active and passive HA Fabric Manager servers.
- Working with Live Monitoring — Documents information about Fabric Manager's Live Monitoring tool, which monitors and displays live, real-time throughput information for host servers and Xsigo vNICs and vHBAs.
- Working with the Task Scheduler — Documents information about the Fabric Manager Task Scheduler, which supports creating a schedule for backup jobs for the Fabric Manager Server or Fabric Director, as well as running an on-demand backup job for the Fabric Manager Server or Fabric Director.
- Working with LUN Masks — Documents information about LUN Mask Profiles and how to configure them.
- Working with SAN QoS — Documents conceptual information about the Fabric Director's SAN quality of service (QoS) parameters and implementations, and provides procedural text about configuring SAN QoS on Storage Clouds.
- Working with Domains — Documents conceptual information about the Fabric Manager Domain Manager and the default domain and subdomains, and how to configure individual domains.
- Working with User Roles — Documents information about the different levels of user accounts that are used in Fabric Manager, documents how to configure user accounts at these levels and assign roles.
- Appendix A: Disabling the IE Security Popup — Documents how to disable a pop-up dialog that can appear in Internet Explorer browsers when Oracle's Xsigo Fabric Manager displays or redisplays pages.

Related Documentation

This document is part of a set of documentation for the Fabric Director. Table 1 shows the other documents in the Fabric Director documentation set.

Table 1 Related Documentation for the Xsigo Systems Fabric Director

Document	Part Number	Revision Level and Date
XgOS Command-Line Interface User Guide	650-30007-03	Rev A 10/2012
Fabric Director Quick Install Guide	650-20022-04	Rev A 10/2012
Fabric Director Hardware and Drivers Installation Guide	650-30008-03	Rev A 10/2012
Fabric Accelerator Quick Start Guide	650-20085-03	Rev A 10/2012
Fabric Performance Manager User Guide	650-20082-02	Rev A 10/2012
XgOS Software Upgrade Guide	650-20028-06	Rev A 10/2012
XgOS Remote Booting Guide	650-20029-08	Rev A 10/2012
XgOS vNIC Switching Configuration Guide	650-20052-02	Rev A 10/2012
Installing Host Drivers on Windows 2008 Servers	650-20081-02	Rev A 10/2012
Hyper-V Setup Guide	650-20040-02	Rev A 10/2012
SAN Install for Windows 2008 Servers	650-20078-03	Rev A 10/2012

Release notes are also available with each major hardware or software release for Oracle's Fabric Director.

Revision Trail

Table 2 shows the revision history for this document.

Table 2 Revision History

Document Title	Document Number	Revision Level and Date
Xsigo Fabric Manager User Guide, V 4.1.0	650-30005-03	Rev A 01/2013
Xsigo Fabric Manager User Guide, V 4.0.0	650-30005-02	Rev A 10/2012

Syntax Usage

Table 3 shows the typographical conventions used in this document.

Table 3 Syntax Usage

Syntax Marker	Means...	Example
bold text, italics	a menu path	***Help>Help***
> (angle bracket)	the next step in a menu path	***Search>Search Equipment...***
bold text	a button name	**New Server Profile...**
italic text	a field or dropdown menu name	the *Description* field the *Properties...* menu
... (ellipsis)	another dialog or menu option will be displayed	**New Server Profile...** (the Server Profile Create page appears)

Technical Support Contact Information

Xsigo customers may contact support via the Xsigo website, telephone or e-mail. In order to expedite troubleshooting, all new support requests must be submitted via the Xsigo self-service portal at: http://support.xsigo.com. In addition to opening cases, the Xsigo Support Portal will allow you to update your support cases, download software, search for and view knowledge-base articles, and access technical documentation.

In order to access the customer support portal, you will need to have a Xsigo Support Portal login. Your account team will provide you with the necessary login information to access the support portal. If you need additional logins for your staff, please contact your account team for assistance.

For all Critical (P1) cases, please call the Xsigo support center at **866-974-4647** (toll free) or **1 408-736-3013** (international). Alternatively, you can email `supportP1@xsigo.com` and you will be responded to within 30 minutes.

Contents

Chapter 1

Chapter 2

Chapter 3

Fabric Manager Overview

Oracle’s Xsigo Fabric Manager is a multi-Director management system created by Xsigo Systems to inventory and manage Oracle Fabric Directors and Xsigo virtual I/O. Oracle’s Fabric Director is a server-client model that supports configuring and managing virtual resources at chassis, module, and server level.

Oracle’s Fabric Manager is a browser-based management system that runs on a remote server. The remote Oracle Fabric Manger server translates configuration and management tasks from Oracle’s Fabric Manager interface, and relays that information to Fabric Directors that are managed by Oracle’s Fabric Manager.

Oracle’s Fabric Manager can run in one of the following ways:

- stand-alone application
- as an extension to the VMware Virtual Center

Oracle’s Xsigo Fabric Manager configuration and management capabilities are the same regardless of whether Oracle’s Fabric Manager is running in stand-alone mode or as an extension to VMware.

Support for the VP780 Fabric Director

Oracle’s Fabric Manager supports management of Xsigo’s flagship VP780, which is a 4 rack-unit virtual I/O platform supporting connectivity to network and storage resources for host servers through 24 InfiniBand ports at up to 40 Gbps per server connection. The VP780 has 15 slots which support a mix of network and storage modules that is appropriate for your network.

Support for the VP560 Fabric Director

Oracle’s Fabric Manager supports management of Xsigo’s VP560, which is a 2 rack-unit virtual I/O platform supporting connectivity to network and storage resources for host servers through 24 InfiniBand ports at up to 40 Gbps per server connection. The VP560 supports has 4 slots which support a mix of network and storage modules that is appropriate for your network.

Oracle’s Fabric Manager as a Stand-Alone Application

In stand-alone mode, Oracle’s Fabric Manager runs on a remote server that controls Fabric Directors. The Fabric Manager system uses additional services to provide manageability:

- Tomcat web server
- Java, JSF
- Xsigo proprietary processes

Figure 1 shows a sample topology in which Fabric Manager is running in stand-alone mode.

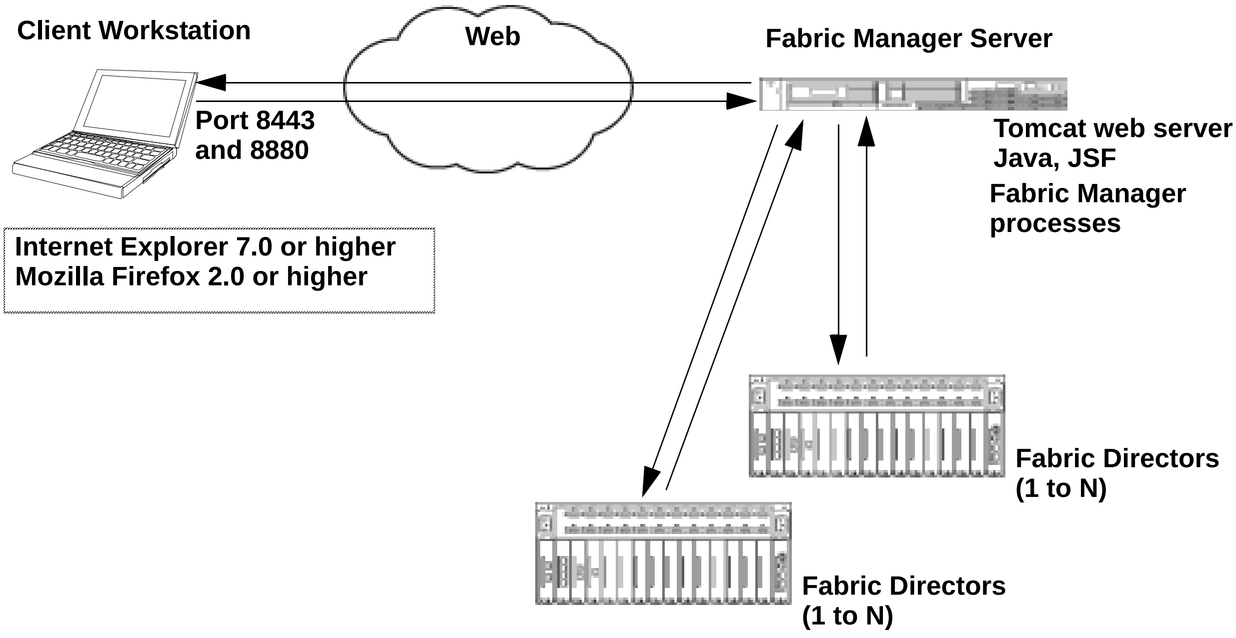


Figure 1 Sample of Fabric Manager Standalone

After Fabric Manager and its components are installed on the physical server that hosts the Fabric Manager software, any client workstation can use Fabric Manager by pointing one of the supported browsers at the Fabric Manager server. Configuration and management requests are sent through the Fabric Manager interface to the Fabric Manager server, which handles the back-end processing and ensures that the client's task is communicated to the Fabric Director and written to the Fabric Director's configuration. When the Fabric Director has acknowledged the client's task, Fabric Manager relays the change back to the Fabric Manager interface where the updated configuration is displayed by the client workstation.

Fabric Manager as an Extension to VMware Virtual Center

Fabric Manager can be installed as an extension to VMware® VirtualCenter Manager or vSphere 4. If you are managing VMware virtual machines through the VMware Virtual Infrastructure Client, you can use the Fabric Manager application after the Fabric Manager VMware Extension is installed to manage the virtual I/O connectivity.

The Fabric Manager system uses additional services to provide manageability:

- Apache web server
- Tomcat web server
- VMware VirtualCenter Management Server 2.5
- VMware Virtual Infrastructure Client 2.5
- VMware vSphere (vCenter) 4 or 5
- Xsigo proprietary processes

In extension mode, Fabric Manager runs on a remote server that interoperates with one more additional servers that support VMware VirtualCenter Manager and Virtual Infrastructure Client or vSphere 4.

Figure 2 shows a sample topology of Fabric Manager installed in extension mode.

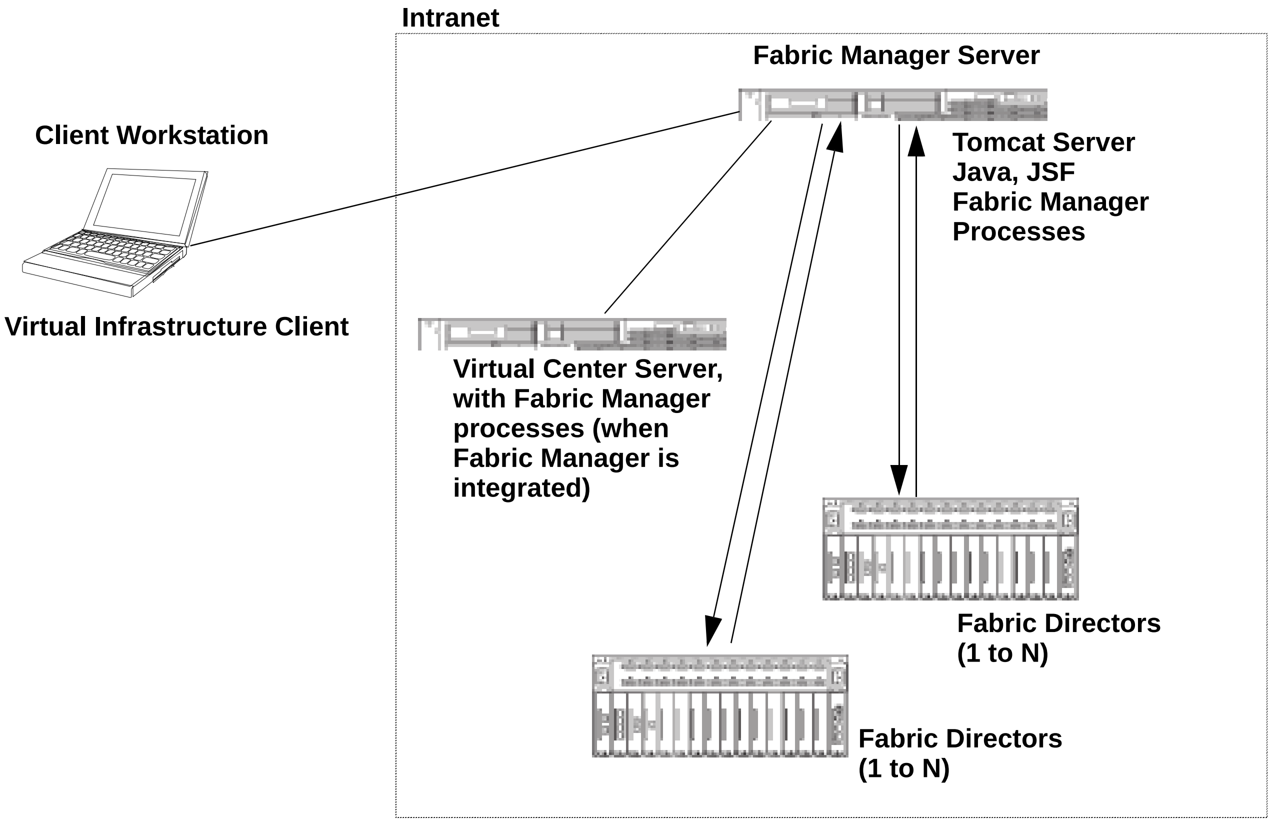


Figure 2 Example of the Fabric Manager VMware Extension

When installed as an extension, Fabric Manager server is connected to other servers that run VMware® VirtualCenter Server and Virtual Infrastructure Client or vSphere 4. It is possible to collocate all servers on one physical or virtual machine. All servers communicate to provide a synchronized view of the network. Fabric Manager provides connectivity and management for Fabric Directors and Xsigo virtual I/O. Because Fabric Manager interface is an extension supported through VMware Virtual Infrastructure Client, management of Xsigo virtual I/O is accessed through tools available in the Virtual Infrastructure Client user interface.

Installing Fabric Manager 5

This chapter documents the following topics:

Meeting Minimum Requirements

Oracle's Fabric Manager runs on a separate Linux or Windows host server, or in a virtual machine. Fabric Manager does not actually run on the Oracle Fabric Director itself. The following platforms support Fabric Manager:

- Windows:
  - Microsoft Windows Server 2003 SP2 and 2008 R2. To install Fabric Manager on this platform, use the install ZIP file named `install-xms-4.1.0`. Double-click the ZIP file to begin extracting the file and running the install wizard. For information about installing Fabric Manager on a Windows Server, see Installing Fabric Manager on a Windows Server after reading Fabric Manager Server Requirements.
- Linux:
  - Red Hat Linux 5 update 2 and higher. To install Fabric Manager on this platform, use the install bundle named `xsigo-xms-4.1.0_rhel5_i686`.

To run Fabric Manager, host servers have been tested to operate when configured to meet the following server and client requirements.

Fabric Manager Server Requirements

For interoperability with Fabric Manager, the physical server that hosts Fabric Manager has been tested to operate when configured with the following:

- Server OS
  - Windows Server 2003 SP2 and Windows Server 2008 R2
  - Red Hat Linux 5 Update 2 or later (32-bit) and equivalents (for example, Centos)
  - VMware ESX Server Classic 4.0 and ESXi 4.0, VMware ESX Server Classic 4.1 and ESXi 4.1. See Consideration for VMware.
- Memory
  - 2 GB minimum, 4 GB or more recommended. (Four GB or more is required if Fabric Manager will be running in VMware Extension mode with VMware VirtualCenter Manager when both applications are hosted on the same physical server.) The same requirements exist if Fabric Manager will be integrated into vSphere 4.
  - vSphere Client—dual core and 4 GB or more of memory (recommended).
- CPU—any server-based, current X86 architecture CPU.
- Java 1.6 (JRE), which is the only version of Java that supports Fabric Manager.

Consideration for VMware

If you will be integrating Fabric Manager into VMware vSphere, and you will be upgrading Fabric Manager after it is integrated into vSphere, Xsigo recommends that you first delete the Fabric Manager integration from vSphere before upgrading Fabric Manager. After Fabric Manager is upgraded, you can then re-integrate the upgraded Fabric Manager into vSphere. The deletion of Fabric Manager from vSphere is not required, but it is best to delete Fabric Manager and perform a fresh integration after any upgrade.

Meeting Client Requirements

For interoperability with Fabric Manager, the clients that will use Fabric Manager have been tested to operate with the following:

- Browsers
  - Mozilla® Firefox 2.0 and higher
  - Microsoft® Internet Explorer 7.0 and later, with all cumulative security updates. Any version of Internet Explorer less than 7.0 is not supported.

Note

For some clients running Internet Explorer 7.0, a browser pop-up sometimes recurrently displays. For information about controlling the pop-up, see Appendix A: Disabling the IE Security Popup.

- Display—1280 x 1024 resolution, 16-bit Medium color mode.
- JavaScript and cookies enabled.

Installing Fabric Manager on a Windows Server

Fabric Manager is supported on Windows Server 2003 SP2 (32-bit only), and Windows 2008 R2 hosts.

Note

If you will be using LDAP/AD for authentication in a Windows domain, install the Fabric Manager software on a Windows server that is a member of that domain.

Fabric Manager is installed through a Windows-based installer called IZpack, which is similar to an InstallShield installer. Fabric Manager is contained in a ZIP file, which then extracts to an EXE file which is the actual installer for Fabric Manager. When you perform this installation procedure, do not install directly from the archive. Instead, unzip the archive to a separate folder (for example, a `temp` folder), then perform the Fabric Manager installation from the unzipped folder.

When the installer runs for the first time, you will be prompted to create a default installation directory. You must accept the prompt (click ***Yes***) to successfully install Fabric Manager. For subsequent installations, you will not see this prompt as long as the Fabric Manager install directory is present on the Windows Fabric Manager Server.

You also have the option of installing Fabric Manager in a non-default install directory. To install to a non-default directory, you can click ***Browse*** at the appropriate step in the installation procedure, then select the directory where you want Fabric Manager installed.

Note

The installation procedure documented in this section assumes a fresh install (no Fabric Manager software exists on the Fabric Manager server). If you are upgrading from an older version of Fabric Manager (not doing a fresh install), you will need to clear any completed jobs from the Jobs summary in the older version of Fabric Manager before running the upgrade. For information about clearing completed jobs from the Jobs Summary, see Clearing All Jobs in the Jobs Summary.

Caution

It is possible to install Fabric Manager to a non-default device (for example, a USB drive). However, some functions of Fabric Manager expect the default device on the server. For example, the `xms-backups`, `techsupport`, and `director-backups` directories are installed to the local device. Be aware that if you install Fabric Manager to a non-default device (for example, a network drive, a USB drive, and so on) functions that rely on the `xms-backup`, `techsupport`, and `director-backups` directories might not work predictably.

Note

Currently, the Fabric Manager installer does not check the OS version installed on the Windows server.

Fabric Manager requires certain ports. Make sure that ports 80 or 443 (HTTPs) are open for both incoming and outgoing directions for communication between the Fabric Manager Server and the Fabric Director. By default, port 443 is used.

To install Fabric Manager, follow this procedure:

Step 1 Log in to the Windows server that will be running Fabric Manager.

Step 2 Get the Fabric Manager installer for Windows (for example, `install-xms-4.1.0`) onto the Windows server that will be running Fabric Manager.

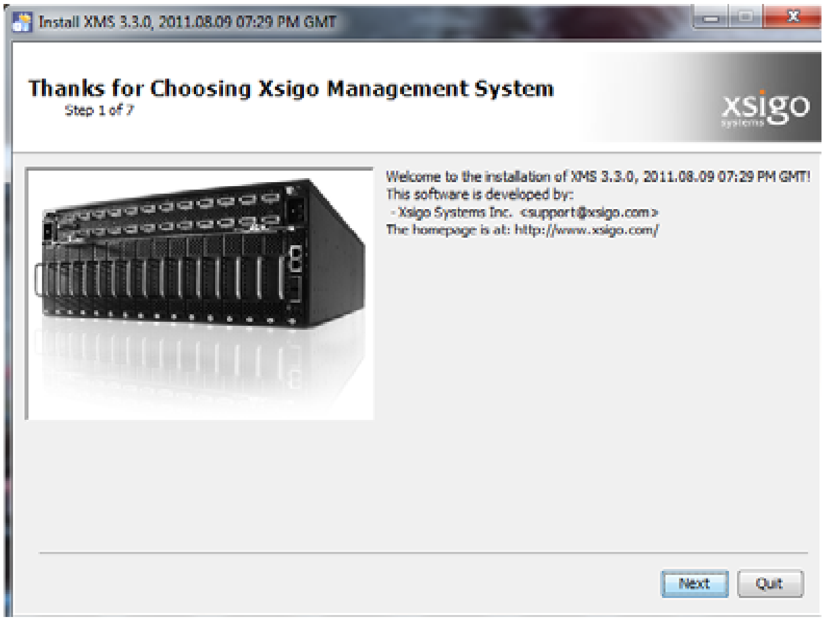
The installer can be downloaded from the Xsigo Customer Support site, or the Xsigo Customer Support secure FTP site. If you need assistance with getting Fabric Manager Installer, contact Xsigo Customer Support as documented in Technical Support Contact Information.

Step 3 Double-click the ZIP file to extract the Fabric Manager executable file and its related content.

Step 4 Double-click the Fabric Manager executable to run the installer. The Xsigo splash screen is displayed momentarily while the Fabric Manager installer begins. See Figure 1.

Figure 1 Fabric Manager Windows Installer — Splash Screen

When the installer runs, the Welcome screen is displayed, as shown in Figure 2.

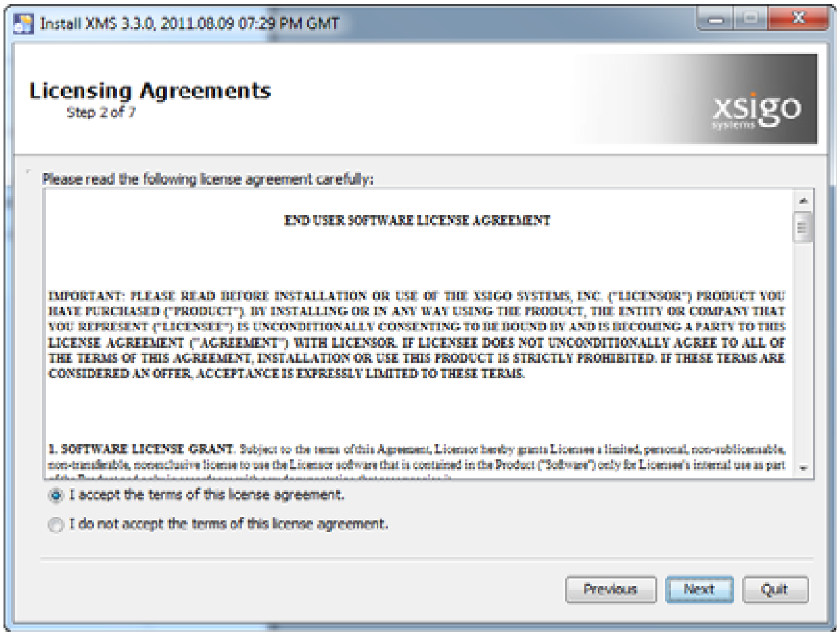

Install XMS 3.3.0, 2011.08.09 07:29 PM GMT

Thanks for Choosing Xsigo Management System
Step 1 of 7

Welcome to the installation of XMS 3.3.0, 2011.08.09 07:29 PM GMT!
This software is developed by:
- Xsigo Systems Inc. <support@xsigo.com>
The homepage is at: http://www.xsigo.com/

Figure 2 Fabric Manager Windows Installer — Welcome Screen

Step 5 Read the Welcome screen and note the support contact information and Xsigo home page, in case you require additional correspondence with Xsigo Systems, then click ***Next*** to display the License Agreement. Figure 3 shows the license agreement.



Install XMS 3.3.0, 2011.08.09 07:29 PM GMT

Licensing Agreements
Step 2 of 7

Please read the following license agreement carefully:

END USER SOFTWARE LICENSE AGREEMENT

IMPORTANT: PLEASE READ BEFORE INSTALLATION OR USE OF THE XSIGO SYSTEMS, INC. ("LICENSOR") PRODUCT YOU HAVE PURCHASED ("PRODUCT"). BY INSTALLING OR IN ANY WAY USING THE PRODUCT, THE ENTITY OR COMPANY THAT YOU REPRESENT ("LICENSEE") IS UNCONDITIONALLY CONSENTING TO BE BOUND BY AND IS BECOMING A PARTY TO THIS LICENSE AGREEMENT ("AGREEMENT") WITH LICENSOR. IF LICENSEE DOES NOT UNCONDITIONALLY AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, INSTALLATION OR USE THIS PRODUCT IS STRICTLY PROHIBITED. IF THESE TERMS ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO THESE TERMS.

1. SOFTWARE LICENSE GRANT. Subject to the terms of this Agreement, Licensor hereby grants Licensee a limited, personal, non-sublicensable, non-transferable, nonexclusive license to use the Licensor software that is contained in the Product ("Software") only for Licensee's internal use as part

● I accept the terms of this license agreement.

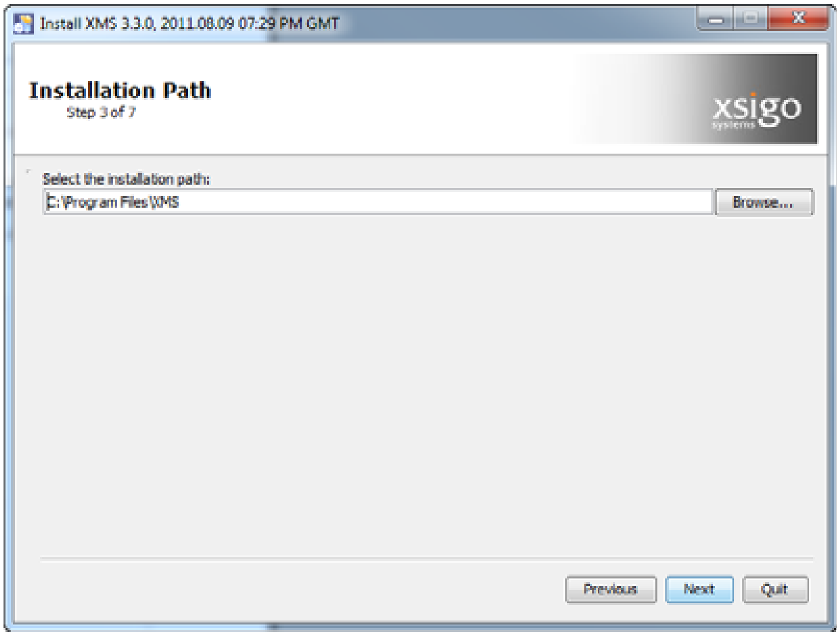
○ I do not accept the terms of this license agreement.

Figure 3 Fabric Manager Windows Installer — Fabric Manager License Agreement

Step 6 Carefully read all of the license agreement, then click either of the choices:

- I accept the terms of this license agreement, to use Fabric Manager in accordance with the stated license agreement. This option activates the ***Next*** button.
- I do not accept the terms of this license agreement, to decide to not install and use Fabric Manager. This option does not allow the installer to continue. You will need to click ***Quit*** to abort the installer.

Step 7 When you accept the license agreement and click ***Next***, the Installation Path dialog is displayed. Figure 4 shows this dialog.



Install XMS 3.3.0, 2011.08.09 07:29 PM GMT

Installation Path

Step 3 of 7

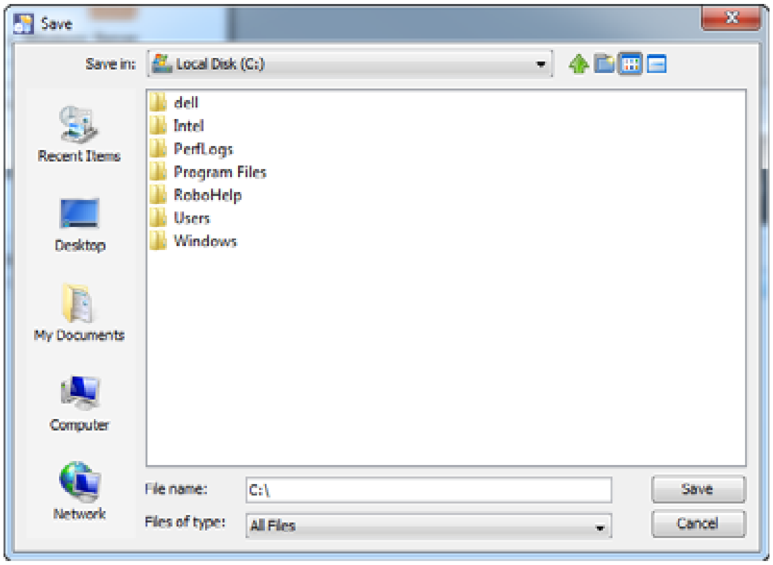
Select the installation path:

C:\Program Files\XMS

Figure 4 Fabric Manager Windows Installer — Installation Path

Step 8 On the Installation Path dialog, you can either accept the default installation directory, or select a non-default installation directory:

- If you accept the installation directory, proceed to Step 10.
- If you select a non-default installation directory, click ***Browse*** to display the Select Path dialog as shown in Figure 5. Proceed to Step 9.



Save

Save in: Local Disk (C:)

dell
Intel
PerfLogs
Program Files
RoboHelp
Users
Windows

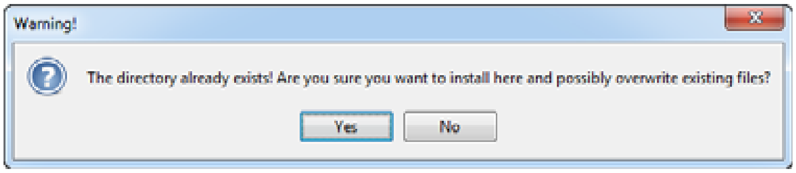
File name: C:\

Files of type: All Files

Figure 5 Fabric Manager Windows Installer — Install Fabric Manager to Non-Default Directory

Step 9 Select the directory in which you want to install Fabric Manager, then click ***Save***. Proceed to Step 11.

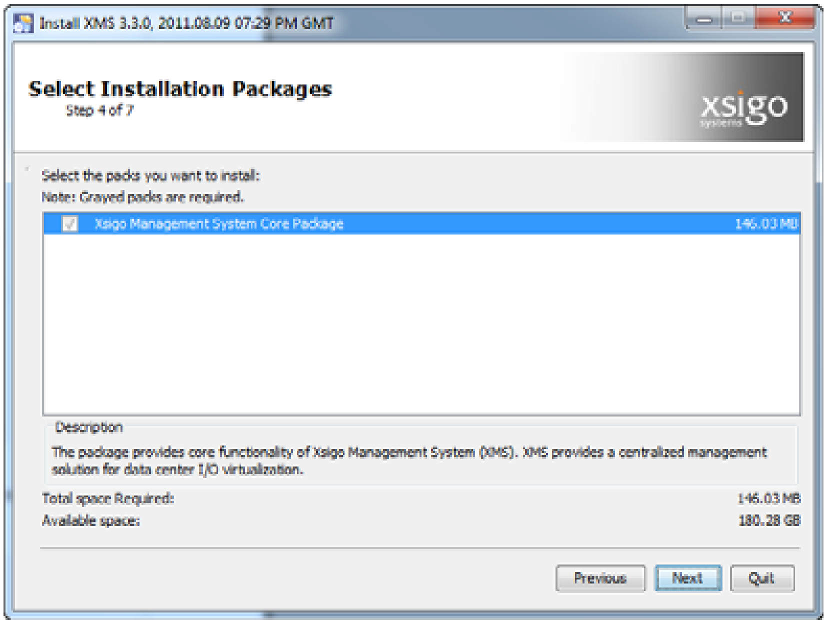
Step 10 Click ***Next*** to display the confirmation dialog that alerts you that the installation directory will be created. This confirmation dialog occurs on a first-time install. If the installation directory already exists on the Windows Fabric Manager server, this dialog is not displayed. Figure 6 shows the confirmation dialog.



The directory already exists! Are you sure you want to install here and possibly overwrite existing files?

Figure 6 Fabric Manager Windows Installer — Create Install Directory Message

Click ***OK*** to create the installation directory, and display the Select Installation Packages dialog. Figure 7 shows this dialog.


Install XMS 3.3.0, 2011.08.09 07:29 PM GMT
Select Installation Packages
Step 4 of 7
xsigo
systems
Description
Previous
Next
Quit

Select the packs you want to install:
Note: Grayed packs are required.

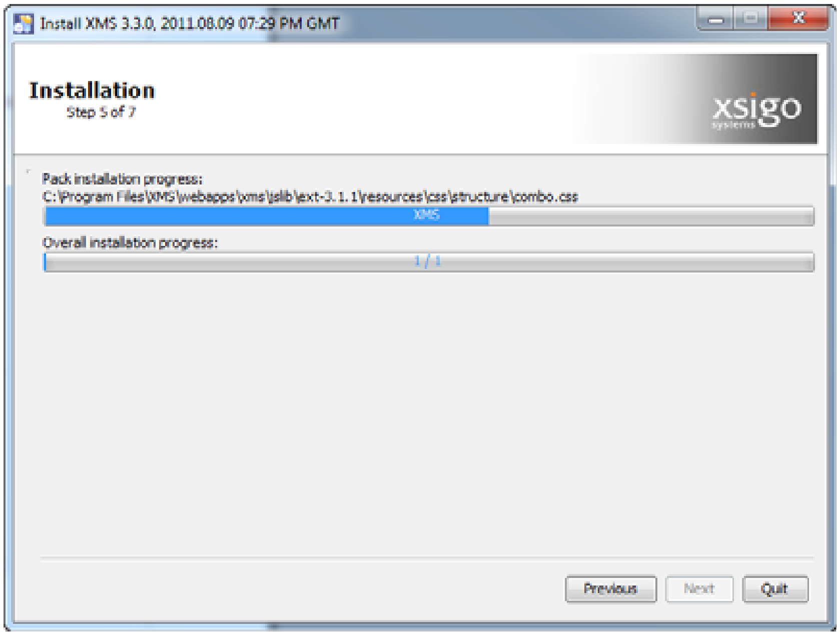
☑ Xsigo Management System Core Package 146.03 MB

The package provides core functionality of Xsigo Management System (XMS). XMS provides a centralized management solution for data center I/O virtualization.

Total space Required: 146.03 MB
Available space: 180.28 GB

Figure 7 Fabric Manager Windows Installer — Select Install Packages

Step 11 Select the “Xsigo Fabric Manager Core Package” option if it is not already selected by default, then click ***Next*** to display the Installation Progress dialog. Figure 8 shows this dialog.



Install XMS 3.3.0, 2011.08.09 07:29 PM GMT

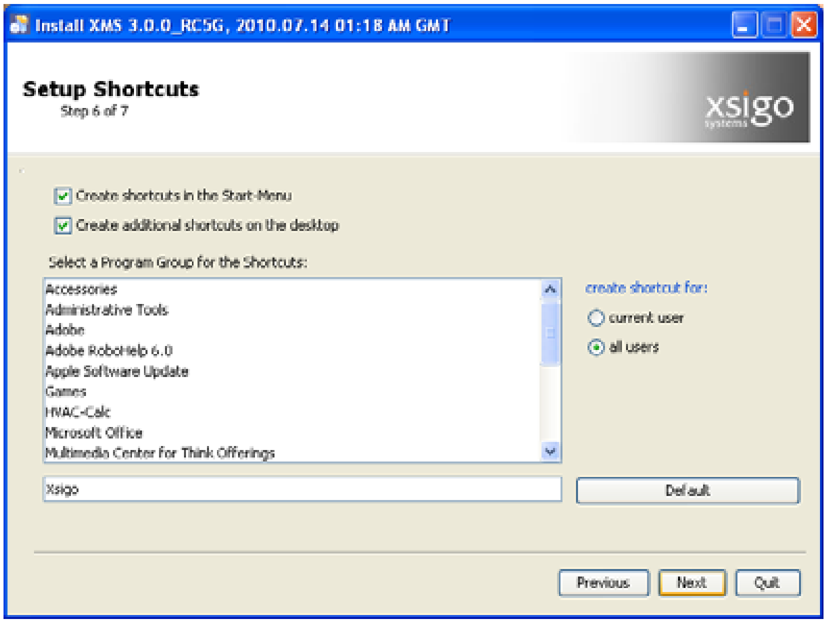
Installation
Step 5 of 7

Pack installation progress:
C:\Program Files\XMS\webapps\xms\jslib\ext-3.1.1\resources\css\structure\combo.css

Overall installation progress:

Figure 8 Fabric Manager Windows Installer — Installation Progress

Step 12 When the Fabric Manager package installation is complete, click ***Next*** to display the Setup Shortcuts dialog. Figure 9 shows this dialog.



Install XMS 3.0.0_RC5G, 2010.07.14 01:18 AM GMT

Setup Shortcuts
Step 6 of 7

☑ Create shortcuts in the Start-Menu

☑ Create additional shortcuts on the desktop

Select a Program Group for the Shortcuts:

Accessories
Administrative Tools
Adobe
Adobe RoboHelp 6.0
Apple Software Update
Games
HVAC-Calc
Microsoft Office
Multimedia Center for Think Offerings

create shortcut for:
○ current user
● all users

Xsigo

Figure 9 Fabric Manager Windows Installer— Setup Shortcuts

Step 13 Use the checkboxes to determine how Fabric Manager shortcuts are installed:

- Use the *Create shortcuts in the Start-Menu* checkbox to allow the installer to put a Fabric Manager shortcut on the Windows *Start* menu. This option is selected by default, so a shortcut to Fabric Manager will be installed on the Windows *Start* menu. This checkbox is a toggle, so clicking alternates between a checkmark (allow the shortcut) and no checkmark (do not allow a shortcut). If you are allowing Fabric Manager shortcuts on the *Start* menu, you also have the option of installing shortcuts at additional locations (for example, on the desktop).
- Use the *Create additional shortcuts on the desktop* checkbox to allow the installer to put a Fabric Manager shortcut on the Windows desktop. This option is selected by default, so a shortcut to Fabric Manager will be installed on the Windows desktop. This checkbox is a toggle, so clicking alternates between a checkmark (allow the shortcut) and no checkmark (do not allow a shortcut).

Step 14 If you are allowing shortcuts on the *Start* menu, click an item in the *Select a Program Groups for the Shortcuts* list to determine where the shortcut will be displayed.

Step 15 If you are allowing shortcuts on the desktop, in the text box below the *Select a Program Groups for the Shortcuts* list, you can enter a name for the Fabric Manager shortcut or select the default location.

Step 16 Use the *create shortcut for:* controls to determine which users on the Windows server will readily see the installed Fabric Manager shortcuts on either the *Start* menu or the desktop:

- Click *Current User* to allow Fabric Manager shortcuts to be created for the user currently logged in to the Windows server.
- Click *All Users* to allow Fabric Manager shortcuts to be created for anyone who can log in to the Windows server.

Step 17 As an option, you can click the ***Default*** button if you want to reset the name and path of the Fabric Manager program to its default value. Clicking ***Default*** resets the program name in the text-entry field next to the ***Default*** button. No other controls on the dialog are reset.

Step 18 When the shortcut installation options have been setup, click ***Next*** to display the Installation Finished dialog. Figure 10 shows this dialog.

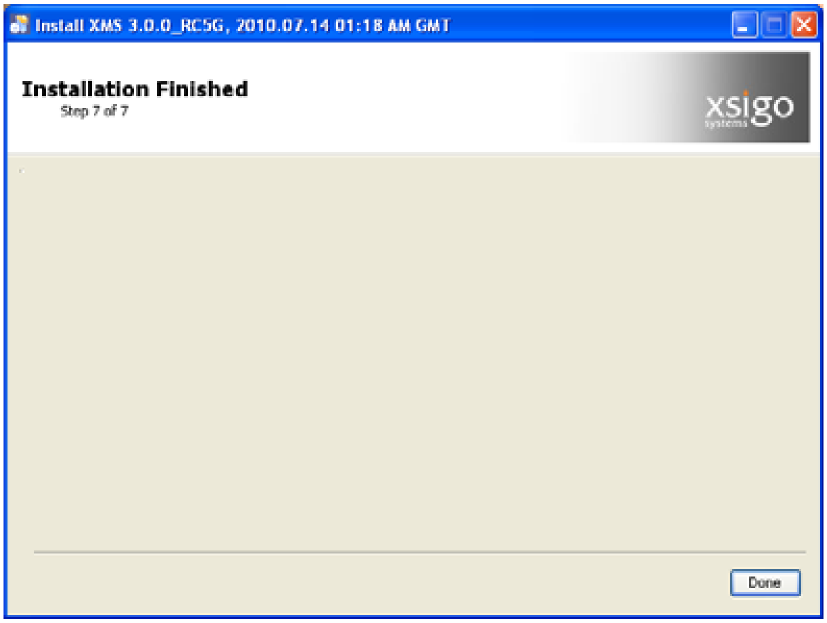


Figure 10 Fabric Manager Windows Installer— Installation Finished

Step 19 Click ***Done*** to close the Fabric Manager installer. At this point, Fabric Manager is installed on the Fabric Manager Windows Server. You can open a supported browser and log in to Fabric Manager as documented in Starting Fabric Manager and Logging In.

Installing Fabric Manager on a Linux Server

Fabric Manager is supported on Linux servers running Red Hat Enterprise Linux 5 Update 2 or later. Installing the Fabric Manager software uses the standard Linux commands, similar to installing or updating the Linux host OS software.

Fabric Manager requires certain ports. Make sure that ports 80 and 443 (HTTPs) are open for both incoming and outgoing directions for Fabric Manager to communicated between the Fabric Manager Server and the Fabric Directors. By default, port 443 is used.

Fabric Manager can be installed from either a TAR ball or from an ISO image.

Note

The installation procedure documented in this section assumes a fresh install (no Fabric Manager software exists on the Fabric Manager server). If you are upgrading from an older version of Fabric Manager (not doing a fresh install), you will need to clear any completed jobs from the Jobs summary in the older version of Fabric Manager before running the upgrade. For information about clearing completed jobs from the Jobs Summary, see Clearing All Jobs in the Jobs Summary.

Installing Fabric Manager from TAR Ball

You can install Fabric Manager directly from the TAR ball. The installation process has the following steps:

1. Unpack the TAR ball on the Fabric Manager Server. This step requires user intervention.
2. Install the Fabric Manager RPM. This step requires user intervention.

To install Fabric Manager directly from the TAR ball, follow this procedure:

Step 1 Log in to the server where Fabric Manager will be installed.

Step 2 Copy the TAR ball from the distribution media (or download it from a repository) to a directory on the server. Make sure that you have at least write and execute privileges on the directory where Fabric Manager will be installed.

Step 3 Run the **`tar xvf`** command and specify the path to the TAR ball as well as the TAR ball's file name. This step unpacks the TAR ball, creates the `/xms_install` directory by default. For example:

```
root@terminus tmp]# tar xvf xsigo-xms-4.1.0_rhel5_i686.tar
./xms_install/
./xms_install/xsigo-xms-4.1.0.noarch.rpm
./xms_install/README.txt
./xms_install/jre-6u17-linux-i586.rpm
[root@terminus tmp]#
```

Note

In this example, the /`tmp` directory is where the TAR ball is unpacked. However, regardless of where it was unpacked, the Fabric Manager RPM always installs to the `/xms_install` subdirectory of the current directory (/`tmp` in this case).

Step 4 Change directory to the `/xms_install` directory that was just created. For example:

```
root@terminus tmp]# cd ./xms_install/
```

Step 5 From the `/xms_install` directory, install the `xsigo-xms-XXX` RPM file. For example:

```
root@terminus tmp/xms_install]# rpm -ivh xsigo-xms-4.1.0-1.noarch.rpm
Preparing...             ########################################### [100%]
1:xsigo-xms              ########################################### [100%]
```

When the Fabric Manager RPM is installed, the Fabric Manager services are automatically brought up and should be running. You do not need to restart the Linux server on which you have just installed Fabric Manager.

Step 6 After installation, Fabric Manager is available for use as a stand-alone application. However, if you will be configuring and managing Fabric Manager through VMware Virtual Center, you will need to register Fabric Manager with the Virtual Center Server.

Step 7 As an option, you can check the status of the Fabric Manager services:

```
root@terminus tmp# service xms status
Checking Xsigo XMS tomcat: Running
```

Note

As an option, some service log files exist that you can check for messages in case the installation does not appear to have completed correctly. For information, see Post-Installation Validation and Troubleshooting.

Step 8 Proceed to Starting Fabric Manager and Logging In.

Installing from ISO Image

To install the ISO image, you will perform this procedure on the Linux server that will host Fabric Manager.

The installation script for installing the ISO image is the same as for the TAR ball, because the contents of the ISO file is the same as the `.tar` file. However, the way you extract files from the ISO image is different than the TAR ball. When you have the ISO image, follow this procedure to access the files in the ISO image:

Step 1 Change directory to a directory where you want to install the image, by issuing the **cd** command. For example:

```
[root@terminus ~]# cd /tmp/
```

Step 2 Create a directory where the ISO files will be available by issuing the **`mkdir`** command. For example, to make the files accessible through the `xmsdisk` directory, you would issue:

```
[root@terminus tmp]# mkdir xmsdisk
```

Step 3 Copy the ISO image from the source media by issuing the **`cp`** command. For example:

```
[root@terminus tmp]# cp /xsigo-xms-4.1.0.iso .
```

Step 4 Mount the file system at the directory you created by issuing the **`mount`** command. For example, to mount the file system at the `xmsdisk` directory:

```
[root@terminus tmp]# mount -o loop xsigo-xms-4.1.0.iso xmsdisk
```

Step 5 Change directory to the `xmsdisk` directory. For example:

```
[root@terminus tmp]# cd xmsdisk/
```

Step 6 Unpack the Fabric Manager tar file.

```
[root@terminus tmp/xmsdisk] tar xvf xsigo-xms-4.1.0_rhel5_i686.tar
./xms_install/
./xms_install/xsigo-xms-4.1.0.noarch.rpm
./xms_install/README.txt
./xms_install/jre-6u17-linux-i586.rpm
```

Step 7 Display the contents of the `xmsdisk` directory by issuing the **`ls`** command and compare the files on the source media to the files that were unpacked to ensure that all files were unpacked. For example:

```
[root@terminus tmp/xmsdisk]# ls
./xms_install/
./xms_install/xsigo-xms-4.1.0.noarch.rpm
./xms_install/README.txt
./xms_install/jre-6u17-linux-i586.rpm
```

Step 8 After verifying that all files were unpacked from the ISO image, change directory to the `/xms-install` directory that was just created. For example:

```
[root@terminus tmp]# cd ./xms_install/
```

Step 9 From the `/xms_install` directory, install the `xsigo-xms-XXX` RPM file. For example:

```
root@terminus tmp/xms_install]# rpm -ivh xms_install/xsigo-xms-4.1.0-
1.noarch.rpm
Preparing...              ############################################ [100%]
1:xsigo-xms               ############################################ [100%]
```

When the Fabric Manager RPM is installed, the Fabric Manager services are automatically brought up and should be running. You do not need to restart the Linux server on which you have just installed Fabric Manager.

Step 10 After installation, Fabric Manager is available for use as a stand-alone application. However, if you will be configuring and managing Fabric Manager through VMware Virtual Center, you will need to register Fabric Manager with the Virtual Center Server.

Step 11 As an option, you can check the status of the Fabric Manager services:

```
root@terminus tmp# service xms status
Checking Xsigo XMS tomcat: Running
```

Note

Some service log files exist that you can check for messages in case the installation does not appear to have completed correctly. For information, see Post-Installation Validation and Troubleshooting.

Step 12 Proceed to Starting Fabric Manager and Logging In.

Post-Installation Validation and Troubleshooting

After Fabric Manager is installed, there are a few ways to validate that Fabric Manager is up and running, or discover some error messages if you need to begin troubleshooting. The following sections document how to check Fabric Manager status and gather some troubleshooting information when Fabric Manager is operating in run-time.

Checking Fabric Manager Status

When Fabric Manager is installed and running, you can use the **`service xms`** command to verify that all required services are operating. In particular, the command supports:

- Displaying the Status of Fabric Manager Services (**`service xms status`**)
- Stopping Fabric Manager Services (**`service xms stop`**)
- Starting Fabric Manager Services (**`service xms start`**)

Displaying the Status of Fabric Manager Services

You can use the **`service xms status`** command to display the current status for the services that support Fabric Manager. Issue this command on the Linux server where you installed Fabric Manager. For example:

```
[root@terminus xms_install]# service xms status
Checking Xsigo XMS tomcat: Running
```

In this example, all Fabric Manager services are operating. However, in the following example, Tomcat is not running.

```
[root@terminus xms_install]# service xms status
Checking Xsigo XMS tomcat: Stopped
```

In this situation, you will need to stop all Fabric Manager services and start them again to get Tomcat running.

Stopping Fabric Manager Services

If a service is not running, stop, then start, all services to allow them to gracefully terminate and start up in the correct order. You can use the **`service xms stop`** command to stop all services gracefully and in the proper order. This command stops all services that support Fabric Manager. You cannot use this command to stop individual services.

- All services are stopped when the status for each service shows `OK`
- Stopping services might take a short time
- When you issue **`service xms stop`**, wait for all services to stop before starting them up again

Issue the command on the Linux or Windows server where you installed Fabric Manager. The following example is for a Linux server:

```
[root@terminus xms_install]# service xms stop
Stopping Xsigo XMS:                                        [  OK  ]
```

Starting Fabric Manager Services

When all services are stopped, you can issue the **`service xms start`** command to restart all services in the proper order. This command starts all services. You cannot start individual services because of a dependency that some services come up before others.

Issue the command on the Linux server where you installed Fabric Manager. For example:

```
[root@terminus xms_install]# service xms start
Starting Xsigo XMS:
                                    [  OK  ]
```

All services are started when the status for each service shows `OK`.

Checking the Service Logs

This section provides basic information about logs that receive events if errors occur when Fabric Manager is online, as well as where to look on the Linux or Windows Fabric Manager Server for the logs. The information contained in these logs can be useful for Xsigo Technical Support.

Fabric Manager runs as the sum of multiple different services on the server. Most services have a log file associated with them. Information about runtime Fabric Manager errors are written to different logs on the Fabric Manager Server.

Windows Server

The following logs contain information about Fabric Manager:

- catalina.<date>.log
- catalina.out
- xmsaudit.log.<num>
- director-<director-name>.log

Linux Server

The following logs contain information about Fabric Manager:

- catalina.<date>.log
- catalina.out
- xmsaudit.log.<num>
- director-<director-name>.log

These logs are located in `/opt/xsigo/xms/logs`, and you can display the contents the logs’ contents by using any standard UNIX or LINUX editor—for example, **vi**, **cat**, **emacs**, and so on.

Removing the Fabric Manager Software

The Fabric Manager software can be removed from the Fabric Manager Server like you would remove any Windows or Linux software. When Fabric Manager is removed, you cannot use the Fabric Manager GUI to configure or manage servers or virtual I/O. However, you can still use Oracle's XgOS CLI to manage the fabric in your data center.

Removing the Fabric Manager Software from a Linux Server

To remove the Fabric Manager software from a Linux server, you can use the **`rpm -e`** command. Follow this procedure:

Step 1 Use **`rpm -qa | grep xms`** to query the name of the installed Fabric Manager package.

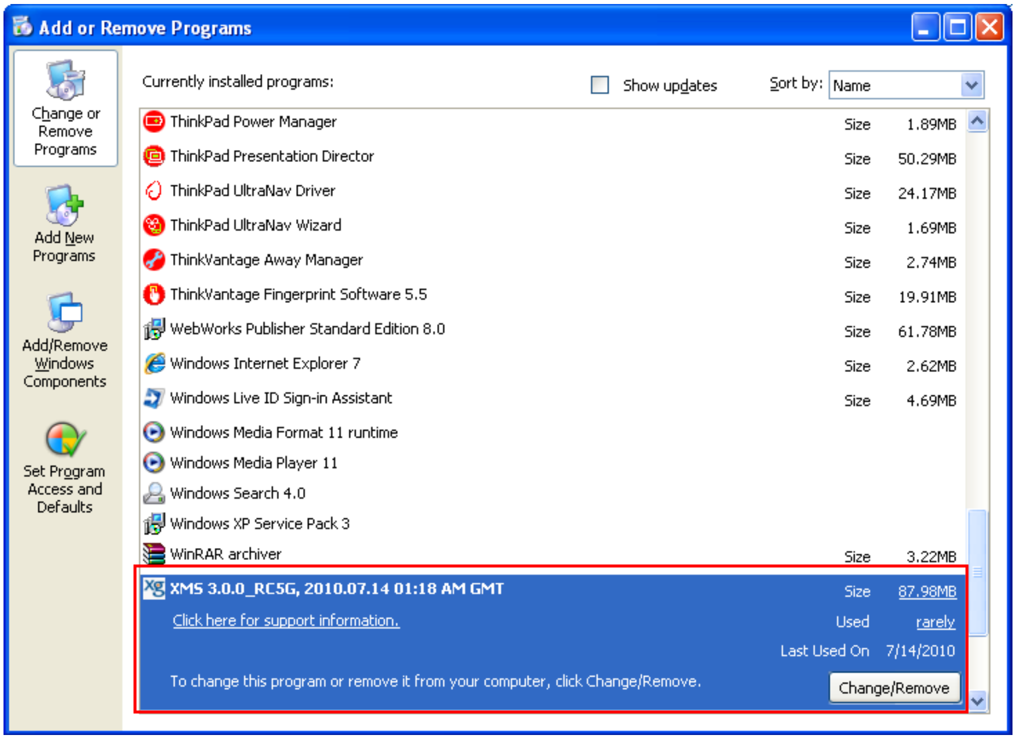
Step 2 From the directory where you installed Fabric Manager:

```
[root@terminus xms_install]# rpm -e xsigo-xms-4.1.0_rhel5_i686.rpm
```

Removing the Fabric Manager Software from a Windows Server

The Fabric Manager Windows installer does not currently have an uninstall option. In the unlikely event that you will want to remove Fabric Manager, you can remove it from a Windows server by using either of the following methods:

- Selecting the Fabric Manager uninstall option of the Fabric Manager install program which is available through the server's Start menu (for example, ***Start->Programs->Fabric Manager->Uninstall***).
- For Windows Server 2003, standard ***Windows Add or Remove Programs*** option (***Start->Settings->Control Panel->Add or Remove Programs***) as shown in Figure 11.



Add or Remove Programs

Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults

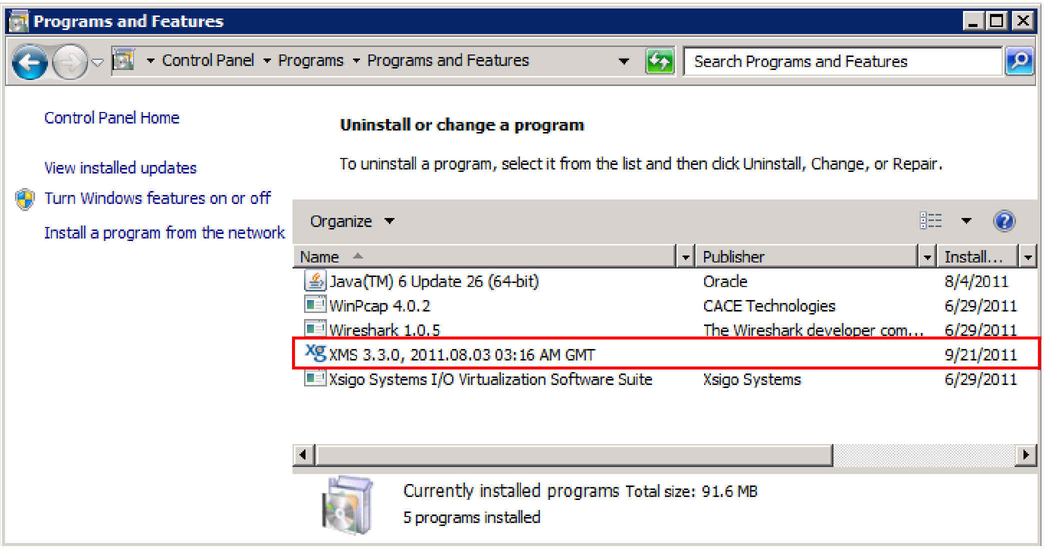
Currently installed programs: ☐ Show updates Sort by: Name

ThinkPad Power Manager	Size	1.89MB
ThinkPad Presentation Director	Size	50.29MB
ThinkPad UltraNav Driver	Size	24.17MB
ThinkPad UltraNav Wizard	Size	1.69MB
ThinkVantage Away Manager	Size	2.74MB
ThinkVantage Fingerprint Software 5.5	Size	19.91MB
WebWorks Publisher Standard Edition 8.0	Size	61.78MB
Windows Internet Explorer 7	Size	2.62MB
Windows Live ID Sign-in Assistant	Size	4.69MB
Windows Media Format 11 runtime		
Windows Media Player 11		
Windows Search 4.0		
Windows XP Service Pack 3		
WinRAR archiver	Size	3.22MB
XMS 3.0.0_RC5G, 2010.07.14 01:18 AM GMT	Size	87.98MB
Click here for support information.	Used	rarely
	Last Used On	7/14/2010

To change this program or remove it from your computer, click Change/Remove. Change/Remove

Figure 11 Removing Fabric Manager from a Windows Server 2003-based Fabric Manager Server

- For Windows Server 2008, standard Uninstall a Program option (***Start->Control Panel->Uninstall a Program***) as shown in Figure 12.



Programs and Features

Control Panel ▸ Programs ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Install...
Java(TM) 6 Update 26 (64-bit)	Oracle	8/4/2011
WinPcap 4.0.2	CACE Technologies	6/29/2011
Wireshark 1.0.5	The Wireshark developer com...	6/29/2011
XMS 3.3.0, 2011.08.03 03:16 AM GMT		9/21/2011
Xsigo Systems I/O Virtualization Software Suite	Xsigo Systems	6/29/2011

Currently installed programs Total size: 91.6 MB
5 programs installed

Figure 12 Removing Fabric Manager from a Windows Server 2003-based Fabric Manager Server

Configuring a Certificate for Fabric Manager

A signed certificate should be installed on the Fabric Manager Server. When installed, Fabric Manager can be validated through the certificate that the Fabric Manager Server presents. The certificate identifies the Fabric Manager user interface as a trusted application. Even though the signed certificate is not a strict requirement, it is recommended. Certificates can be signed through any of the common Certificate Authorities (CAs), such as Verisign®, Digi-Sign®, Thawte®, and so on.

When you configure a security certificate on Fabric Manager, you are allowing the client browser to validate the Fabric Manager Server and create a trust association. Consider the example in Figure 13.

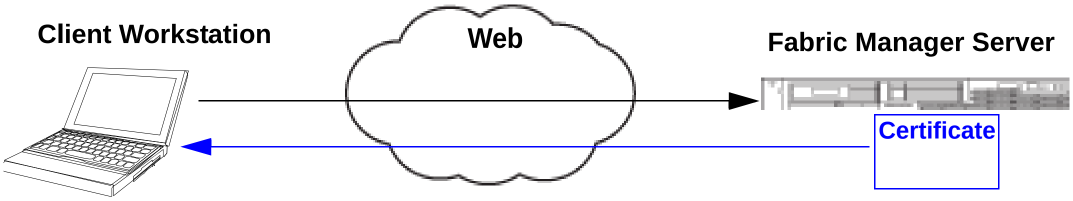


Figure 13 Example of Certificate Use in Fabric Manager Client and Server Environment

In this example, when you attempt to log in to the Fabric Manager Server (the black line) the application (Fabric Manager) starts. At this point, the browser searches for a certificate, and the server presents its certificate to the client browser (the blue line). When the client browser recognizes the certificate as signed by a valid Certificate Authority (CA), the client browser then establishes that the application running in the browser (Fabric Manager) is trusted.

If the certificate is not present, not valid, or cannot be verified, the browser cannot validate the integrity of the Fabric Manager application, and the application running in the browser (Fabric Manager) is not trusted. As a result, the browser displays a warning page whenever you attempt to start Fabric Manager by logging into the Fabric Manager Server.

Configuring a certificate for Fabric Manager requires sending a certificate signing request and installing signed certificates.

Understanding a Certificate Signing Request (CSR)

The Certificate Signing Request (CSR) is a request that is sent to a Certificate Authority (CA). The request consists of an public key and other information that is generated from the Fabric Manager Server. The public key is unique and identifies each Fabric Manager Server.

Besides the public key, you will provide some additional information such as contact emails, country of origin and so on. This information will be included in the CSR so that the CA can assign the signed certificate. Before generating the CSR, you will find it helpful to gather the names of the Fabric Manager Servers on which you will be installing the certificate(s) as well as the host name(s).

Understanding the Signed Certificate

The signed certificate is a series of alphanumeric characters that is installed on the Fabric Manager Server. The signed certificate is generated by the Certificate Authority (CA) and uniquely guarantees the authenticity of Fabric Manager when it attempts to establish HTTPS connectivity to the Fabric Manager Server. When the signed certificate is imported into the Fabric Manager Server, the certificate is used to verify the authenticity of the Fabric Manager Server. Through the HTTPS connection to the Fabric Manager Server, the client attempts to validate Fabric Manager and establish trust. If trust is established, the HTTPS connection is successful, and subsequent HTTPS transactions are secure.

Because a CSR is generated by an individual Fabric Manager Server, you cannot move the resulting signed certificate to a different Fabric Manager Server. Also, when you are importing signed certificates from the CA to the Fabric Manager Server, make sure that you import the correct certificate onto each Fabric Manager Server.

Understanding the keytool Utility

The keytool utility is a powerful tool for generating and managing public and private keys for server certificates. With keytool, you can also manage the keystore on individual servers as well as the required license pairs. Keytool is included in Java Runtime Environment 1.6 package, and the utility runs on any standard server operating system.

Extensive documentation about keytool is available on the web, for example http://docs.oracle.com/javase/1.4.2/docs/tooldocs/solaris/keytool.html. Within the utility itself, help is available by using the `-help` option after Java is installed. For the purpose of creating and installing the license on the Fabric Manager server, you will use the following command options for keytool:

- `-genkeypair`
- `-alias`
- `-keyalg`
- `-keystore`
- `-keysize`
- `-certreq`
- `-file`
- `-import`
- `-trustcacerts`

Verifying That a Certificate Should Be Installed

When you start Fabric Manager, you might see an error page that indicates a certificate error. This error occurs because Fabric Manager cannot be verified as a trusted application because it does not have a certificate that the client browser recognizes as signed by a trusted CA. By default, Fabric Manager has a self-signed certificate which allows the application to be usable without a certificate signed by a CA. As a result, you can log in to Fabric Manager and use the application even if the certificate error occurs.

You can skip past the certificate error by simply clicking *Continue to this website*, and if you do so, you can use Fabric Manager for all supported configuration and management workflows. The functionality of Fabric Manager is not affected by the presence or absence of a CA-signed certificate. If you choose not to install the certificate, you will see an error displayed in the browser's Address bar. Additional information is available through the Certificate Error notification in the browser's Security Status bar.

Configuring the Fabric Manager Security Certificate is not mandatory. However, by not installing a certificate, the certificate error page will be displayed every time you log in to Fabric Manager.

Creating and Installing a CA-Signed Certificate

You can generate a CSR from the Fabric Manager Server. When the Certificate Authority (CA) responds, the certificate is installed and the certificate error is cleared on the next log in to Fabric Manager. Configuring the Fabric Manager security certificate occurs through commands on the management console running on the host Fabric Manager Server. Therefore, make sure that you have a management console available to run the commands. Configuring the Fabric Manager Certificate takes the following steps:

1. Generate a public key for use in the CSR
2. Transmit (export) the CSR to the CA
3. Receive the signed certificate from the CA
4. Install (import) the Certificate on the Fabric Manager Server

Proceed to the appropriate section depending on which type of Fabric Manager server you have in use:

- Creating and Installing a Certificate on a Linux Server
- Creating and Installing a Certificate on a Windows Server

Creating and Installing a Certificate on a Linux Server

The CSR is generated on the Fabric Manager server by creating a public key for the Fabric Manager Server then embedding that key into the CSR. The public key is uniquely associated with the Fabric Manager Server, and cannot be moved or used on a different server. If you provision a new Fabric Manager server and decommission the existing one, you will need to generate a new CSR from the new Fabric Manager server, and install the signed certificate on the new server.

The CSR is generated from the Fabric Manager Server through the keytool utility. By default, Fabric Manager uses a self-signed certificate to allow for installation and use. However, the Fabric Manager signed certificate is not a CA-signed certificate, therefore the browser will not be able to validate Fabric Manager, and an error page will be displayed until you install a CA-signed certificate.

As part of generating a CSR, you will be prompted to enter a password for the keystore, which is a database on the Fabric Manager server that contains all the public keys and signed certificates. The keystore is password protected to keep it secure from anyone who might want to use the keys and certificates for malicious intent. Make sure to remember the password because you will need to enter it when you install the signed certificate.

Note

Certificates have a life span and can expire if not renewed. If you installed a certificate and Fabric Manager was running without the Certificate Error, and suddenly starts displaying the Certificate Error page again, check the expiration date on the certificate.

To create and import a certificate, follow this procedure:

Step 1 Remove any existing certificates:

```
rm opt/xsigo/xms/conf/xms_cacerts
```

Step 2 Use the keytool utility with the `-genkeypair` argument to generate a certificate for the Fabric Manager server:

```
./keytool -genkeypair -alias xms -keyalg RSA -keystore /opt/xsigo/xms/
conf/xms_cacerts -keysize 2048
```

Step 3 Create a certificate signature request:

```
./keytool -certreq -keyalg RSA -alias xms -file /opt/xsigo/xms/conf/
certreq.csr -keystore /opt/xsigo/xms/conf/xms_cacerts
```

Step 4 Edit the CSR to verify that it contains the correct information. If it doesn't, enter the correct information:

```
vi /opt/xsigo/xms/conf/certreq.csr
```

Step 5 Submit the CSR to a certificate authority (CA), such as Verisign as shown in this example:

After you submit the CSR to the CA, you receive an email from CA.

Step 6 Complete the directions in the email to import the intermediate certificates on to the Fabric Manager server.

Step 7 On the Fabric Manager server, use keytool, to create a primary and secondary intermediate certificate files.

For the primary intermediate file:

```
./keytool -import -trustcacerts -alias primaryintermediate -keystore
/opt/xsigo/xms/conf/xms_cacerts -file /opt/xsigo/xms/conf/
primary_inter.cer
```

For the secondary intermediate file:

```
./keytool -import -trustcacerts -alias secondaryintermediate -keystore
/opt/xsigo/xms/conf/xms_cacerts -file /opt/xsigo/xms/conf/
secondary_inter.cer
```

Step 8 Create an SSL certificates file for the intermediate licenses you just created:

```
./keytool -import -trustcacerts -alias xms -keystore /opt/xsigo/xms/conf/
xms_cacerts -file /opt/xsigo/xms/conf/ssl_cert.cer
```

Step 9 Verify that the intermediate key files you created (for example "primaryintermediate" and "secondaryintermediate" are present in `/opt/xsigo/xms/conf/`

Step 10 Send the contents of the `xms_cacerts` directory as a `.txt` file. To do so, you will need to provide the password to access the keystore on the Fabric Manager server.

```
./keytool -list -v -keystore /opt/xsigo/xms/conf/xms_cacerts
>keystorelist.txt

Enter keystore password:  <enter your keystore password>
```

Step 11 Go to the `xms/conf` directory, and find the `server.xml` file.

Step 12 Using vi, emacs, or another standard UNIX editor, add the following lines to server.xml:

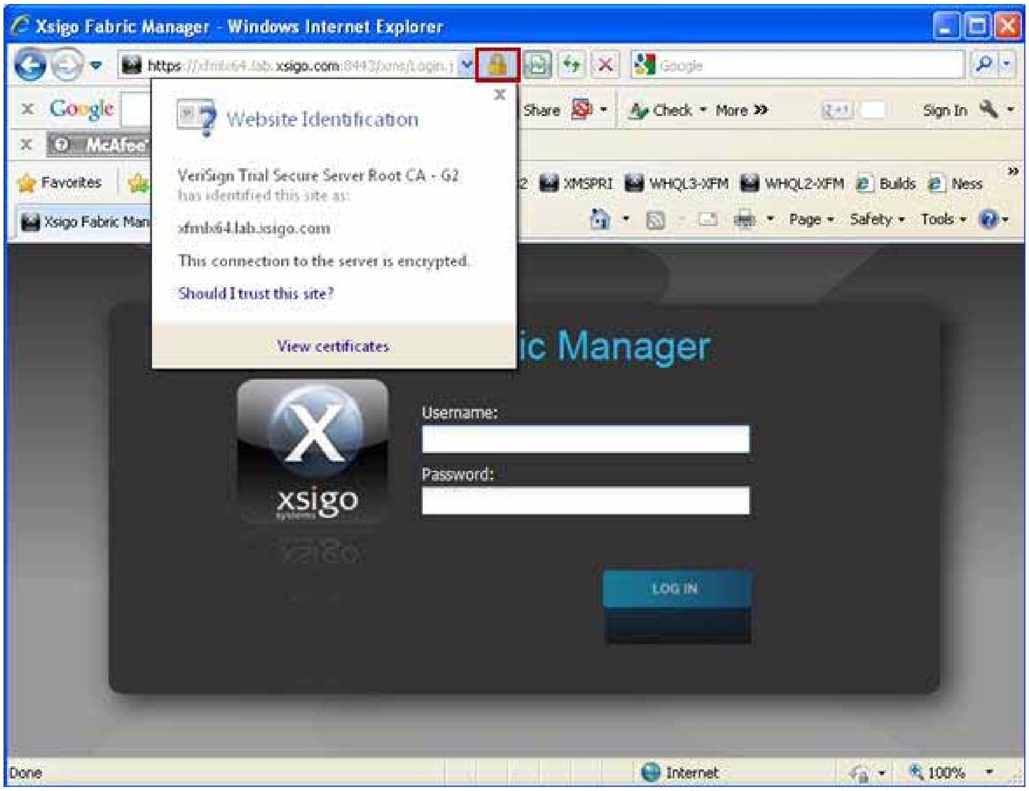
```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
         This connector uses the JSSE configuration, when using APR, the
          connector should be using the OpenSSL style configuration
          described in the APR documentation -->
    <Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true"
               maxThreads="150" scheme="https" secure="true"
       keystoreFile="/opt/xsigo/xms/conf/xms_cacerts"
       keystorePass=<enter the keystore password>
       keyAlias="xms"
               enableLookups="true"
```

Step 13 Restart the Fabric Manager service:

```
service xms stop
service xms start
```

Step 14 Consult the email you received from the CA and follow the instruction for importing the certificate into your browser.

Step 15 When the certificate is correctly imported, start your browser and check the security option to verify that the certificate was installed. Figure 14 shows an example of a successfully installed certificate in Internet Explorer 9.0. The security option is highlighted with a red box.



Xsigo Fabric Manager - Windows Internet Explorer

Website Identification

VeriSign Trial Secure Server Root CA - G2
has identified this site as:

xfmlx64.lab.xsigo.com

This connection to the server is encrypted.

Should I trust this site?

View certificates

Figure 14 Installed Certificate in Internet Explorer 9.0

Step 16 Examine the certificate to make sure that the information you specified is correct, for example:

- in a FireFox browser, you can check the certificate by following this menu path:
  Tools->Options...->Advanced tab->***View Certificates***
- in an Internet Explorer browser, you can check the certificate by following this menu path:
  Tools->Internet Options->Content tab->***Certificates***

Step 17 Log in to Fabric Manager. If the certificate was correctly installed, the certificate error page should no longer be displayed. If you had a previous browser session running Fabric Manager, close the browser completely before logging back in to Fabric Manager after installing the certificate. By doing so, you will flush the browser cache.

Creating and Installing a Certificate on a Windows Server

The CSR is generated on the Fabric Manager server by creating a public key for the Fabric Manager Server then embedding that key into the CSR. The public key is uniquely associated with the Fabric Manager Server, and cannot be moved or used on a different server. If you provision a new Fabric Manager server and decommission the existing one, you will need to generate a new CSR from the new Fabric Manager server, and install the signed certificate on the new server.

The CSR is generated from the Fabric Manager Server through the keytool utility. By default, Fabric Manager uses a self-signed certificate to allow for installation and use. However, the Fabric Manager signed certificate is not a CA-signed certificate, therefore the browser will not be able to validate Fabric Manager, and an error page will be displayed until you install a CA-signed certificate.

As part of generating a CSR, you will be prompted to enter a password for the keystore, which is a database on the Fabric Manager server that contains all the public keys and signed certificates. The keystore is password protected to keep it secure from anyone who might want to use the keys and certificates for malicious intent. Make sure to remember the password because you will need to enter it when you install the signed certificate.

Note

Certificates have a life span and can expire if not renewed. If you installed a certificate and Fabric Manager was running without the Certificate Error, and suddenly starts displaying the Certificate Error page again, check the expiration date on the certificate.

To create and import a certificate on a Windows sever, follow this procedure:

Step 1 Remove any existing certificates by deleting:

```
c:\program files/xms/conf/xms_cacerts file
```

Step 2 Use the keytool utility to generate a certificate for the Fabric Manager server:

```
C:\Program Files\Java\jre7\bin>keytool.exe -genkeypair -alias xms -keyalg
RSA -keystore “c:\program files/xms/conf/xms_cacerts” -keysize 2048
```

Step 3 Create a certificate signature request:

```
C:\Program Files\Java\jre7\bin>keytool.exe -certreq -keyalg RSA -alias
xms -file c:\program files/xms/conf/certreq.csr -keystore xms_cacerts
```

Step 4 Using notepad or another standard Windows file editor, view the CSR to verify that it contains the correct information. If it doesn’t, enter the correct information:

```
c:\program files/xms/conf/certreq.csr
```

Step 5 Submit the CSR to a certificate authority (CA), such as Verisign as shown in this example:

After you submit the CSR to the CA, you receive an email from CA.

Step 6 Complete the directions in the email to import the intermediate certificates on to the Fabric Manager server.

Step 7 On the Fabric Manager server, use keytool to create a primary and secondary intermediate certificate files.

For the primary intermediate file:

```
C:\Program Files\Java\jre7\bin>keytool.exe -import -trustcacerts -alias
primaryintermediate -keystore “c:\program files/xms/conf/xms_cacerts” -
file c:\program files/xms/conf/primary_inter.cer
```

For the secondary intermediate file:

```
C:\Program Files\Java\jre7\bin>keytool.exe -import -trustcacerts -alias
secondaryintermediate -keystore “c:\program files/xms/conf/xms_cacerts” -
file c:\program files/xms/conf/secondary_inter.cer
```

Step 8 Create an SSL certificates file for the intermediate licenses you just created:

```
C:\Program Files\Java\jre7\bin>keytool.exe -import -trustcacerts -alias
xms -keystore “c:\program files/xms/conf/xms_cacerts” -file
c:\ssl\ssl_cert.cer
```

Step 9 Verify that the intermediate key files you created (for example “primaryintermediate” and “secondaryintermediate” are present in `/opt/xsigo/xms/conf/`

Step 10 Send the contents of the `xms_cacerts` directory as a `.txt` file. To do so, you will need to provide the password to access the keystore on the Fabric Manager server.

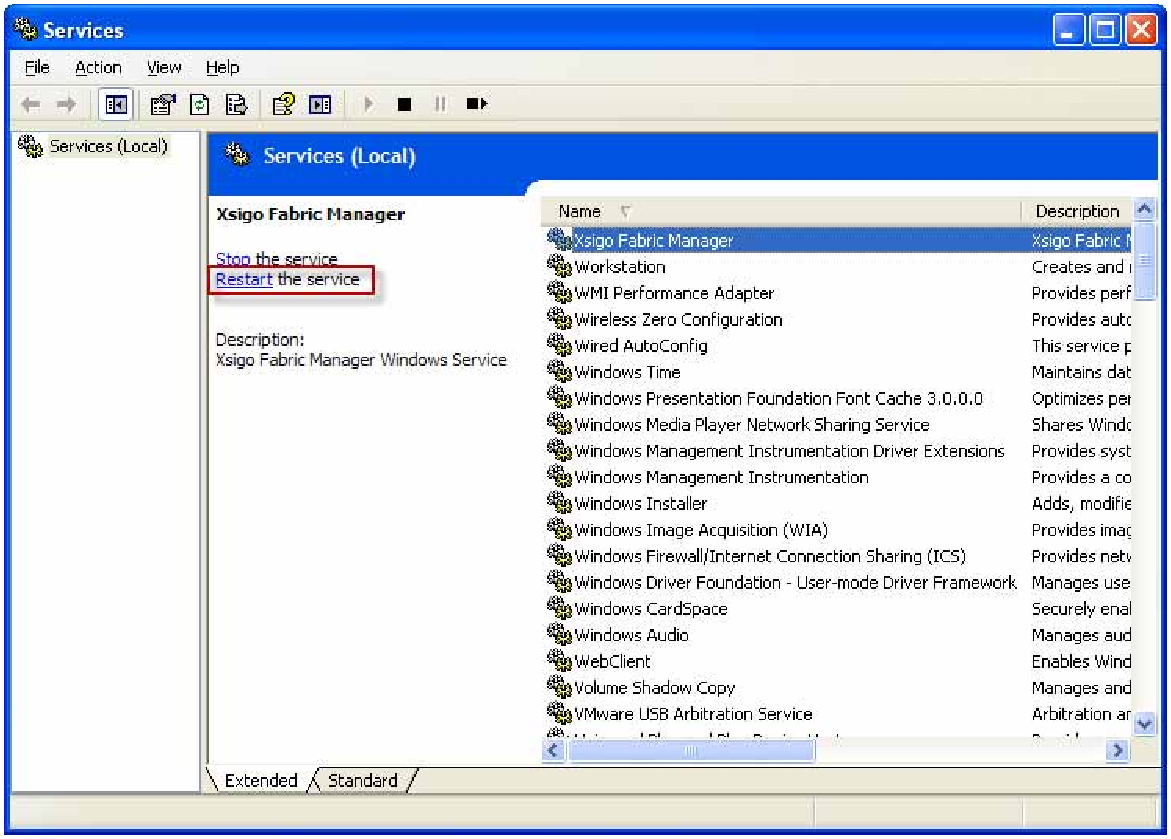
```
C:\Program Files\Java\jre7\bin>keytool.exe -list -v -keystore xms_cacerts
>keystorelist.txt

Enter keystore password:  <enter your keystore password>
```

Step 11 Go to the `xms/conf` directory, and find the `server.xml` file.

Step 12 Using Windows Notepad of another standard Windows file editor, add the following lines to `server.xml`:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
         This connector uses the JSSE configuration, when using APR, the
         connector should be using the OpenSSL style configuration
         described in the APR documentation -->
    <Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true"
               maxThreads="150" scheme="https" secure="true"
       keystoreFile="“c:\program files/xms/conf/xms_cacerts”
       keystorePass=<enter the keystore password>
       keyAlias="xms"
               enableLookups="true"
```

Step 13 Restart the Fabric Manager service through Computer Management on the Windows server. An example is shown in Figure 15.



Xsigo Fabric Manager

Stop the service
Restart the service

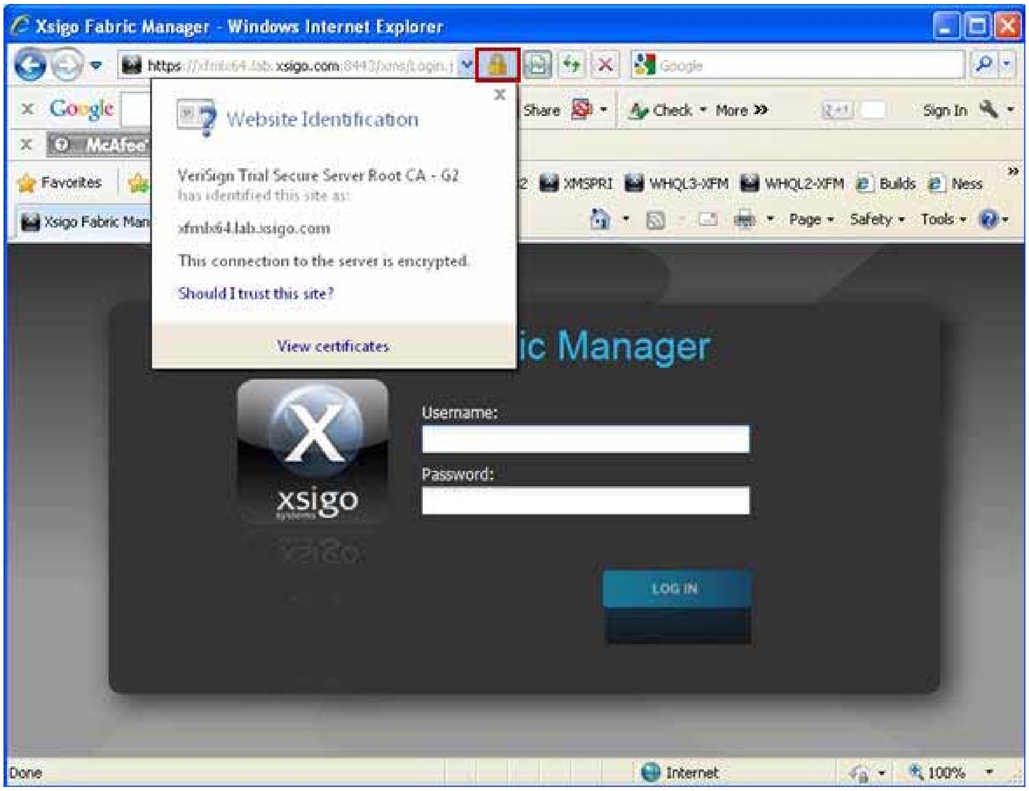
Description:
Xsigo Fabric Manager Windows Service

Name	Description
Xsigo Fabric Manager	Xsigo Fabric N
Workstation	Creates and r
WMI Performance Adapter	Provides perf
Wireless Zero Configuration	Provides autc
Wired AutoConfig	This service p
Windows Time	Maintains dat
Windows Presentation Foundation Font Cache 3.0.0.0	Optimizes per
Windows Media Player Network Sharing Service	Shares Windc
Windows Management Instrumentation Driver Extensions	Provides syst
Windows Management Instrumentation	Provides a co
Windows Installer	Adds, modifie
Windows Image Acquisition (WIA)	Provides imag
Windows Firewall/Internet Connection Sharing (ICS)	Provides netv
Windows Driver Foundation - User-mode Driver Framework	Manages use
Windows CardSpace	Securely enal
Windows Audio	Manages aud
WebClient	Enables Wind
Volume Shadow Copy	Manages and
VMware USB Arbitration Service	Arbitration ar

Figure 15 Windows Fabric Server — Restart the Service

Step 14 Consult the email you received from the CA and follow the instruction for importing the certificate into your browser.

Step 15 When the certificate is correctly imported, start your browser and check the security option to verify that the certificate was installed. Figure 16 shows an example of a successfully installed certificate in Internet Explorer 9.0. The security option is highlighted with a red box.


Xsigo Fabric Manager - Windows Internet Explorer

Website Identification

VeriSign Trial Secure Server Root CA - G2 has identified this site as:

xfmlx64.lab.xsigo.com

This connection to the server is encrypted.

Should I trust this site?

View certificates

Figure 16 Installed Certificate in Internet Explorer 9.0

Step 16 Examine the certificate to make sure that the information you specified is correct, for example:

- in a FireFox browser, you can check the certificate by following this menu path:

  Tools->Options...->Advanced tab->***View Certificates***

- in an Internet Explorer browser, you can check the certificate by following this menu path:

  Tools->Internet Options->Content tab->***Certificates***

Step 17 Log in to Fabric Manager. If the certificate was correctly installed, the certificate error page should no longer be displayed. If you had a previous browser session running Fabric Manager, close the browser completely before logging back in to Fabric Manager after installing the certificate. By doing so, you will flush the browser cache.

Starting Fabric Manager and Logging In

To log in to the Fabric Manager interface, you must provide a valid user name and password.

The default user name and password are different for Fabric Manager on a Windows server or Fabric Manager on a Linux server:

- For Linux, the default user name and password are the same as the default user account on the Linux server (root). Additional user accounts can be configured for Fabric Manager, but they must be configured as non-root user accounts on the Linux server.
- For Windows, the default user name and password are the same as the default administrator account on the Windows server (administrator). Additional, non-admin accounts can be configured for Fabric Manager, but they must be configured as non-administrator accounts on the Windows server.

Note

Because some installations do not allow administrator or root access to servers, Xsigo also provides the `xsigoadmin` account which can be used to log in to the Fabric Manager Server.

You will use this user name and password the first time you access Fabric Manager. One of these accounts (root, administrator, or xsigoadmin) is required to install additionally purchaseable features such as plug ins. Xsigo strongly recommends that after logging into Fabric Manager, you create specific user accounts (instead of continuing to use the root, administrator, or xsigoadmin accounts). When you create these specific user accounts, make sure to assign them with the appropriate roles.

Note

You should have the root default user name and password kept as securely as possible. After initially logging in to Fabric Manager, you should create additional user accounts with specific privileges, as documented in Working with User Roles. When you create the additional non-root user accounts in Fabric Manager, be aware that these user accounts must also exist in the underlying OS (either a Windows user account or a Linux user account). You cannot log in to Fabric Manager if no underlying user account exists at the server's OS level, or if there is any difference between the user names—for example, user name joey at the OS level and joe at Fabric Manager will not pass authentication and allow login to Fabric Manager.

Understanding Fabric Manager and Authentication

Fabric Manager does no authentication of its own. Instead, it presents a log in screen, then passes the user name and password string to the underlying Windows or Linux OS (pass-through), which allows or disallows the authentication. Because Fabric Manager login is a pass through, additional authentication methods are supported, such as LDAP AD. Be aware that the additional user accounts on the Active Directory server(s), the Windows server OS, and the Fabric Manager server must all be congruent. Additional information is available for specific additional authentication methods such as LDAP AD. For more information, see Working with User Roles. When the OS and any other authentication methods complete, the appropriate blob of information is sent to Fabric Manager, which then sets the correct Fabric Manager-level privileges for the authenticated user. When those privileges are applied, they determine which objects in the Fabric Manager GUI are available to the authenticated user. Be aware that the user name can have different rights or privileges at each level, but for Fabric Manager, only the Fabric Manager privileges granted to the user are enforced. For example, user joey at the OS level might be a super user with all rights, but user joey at the Fabric Manager level might be a network administrator user and therefore, only the privileges for a network-admin role are applied, not the super user privileges. In this case, the user joey has different privileges, but only the Fabric Manager privileges are enforced for managing Fabric Directors and virtual I/O through Fabric Manager.

Logging In

When you are logged in, your management session remains active as long as you are actively configuring or managing through Fabric Manager. However, Fabric Manager has a management session inactivity timer of 30 minutes. As a result, if you do not perform a click action (for example, selecting an object or starting a wizard) in Fabric Manager for 30 minutes, you are logged out and must log back in.

You can start Fabric Manager in either of the following ways:

- Through a client browser window. Proceed to Step 1.
- Through the VMware Virtual Infrastructure Client if you installed Fabric Manager as a VMware Extension.

To start Fabric Manager as stand-alone application, follow this procedure:

Step 1 Start one of the supported browsers. For information about supported browsers, see Meeting Client Requirements.

Step 2 Point your browser to `http://<server-name>:8880/xms` where `<server-name>` is the IP address or host name of the Fabric Manager server, plus port 8880. For example

```
http://gorilla:8880/xms
```

would start a Fabric Manager session on the Fabric Manager server named “gorilla”.

Note

Fabric Manager supports both HTTP and HTTPS, so you can also use port 8443 when pointing your browser to the Fabric Manager Server—for example, `http://gorilla:8443/xms`

Figure 17 shows the Fabric Manager Login page.

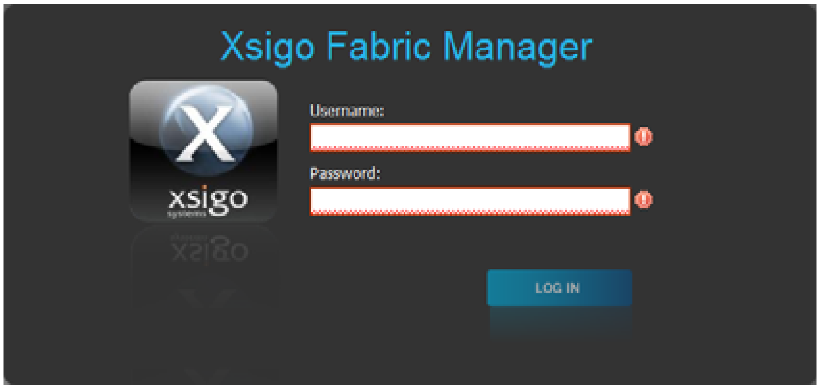


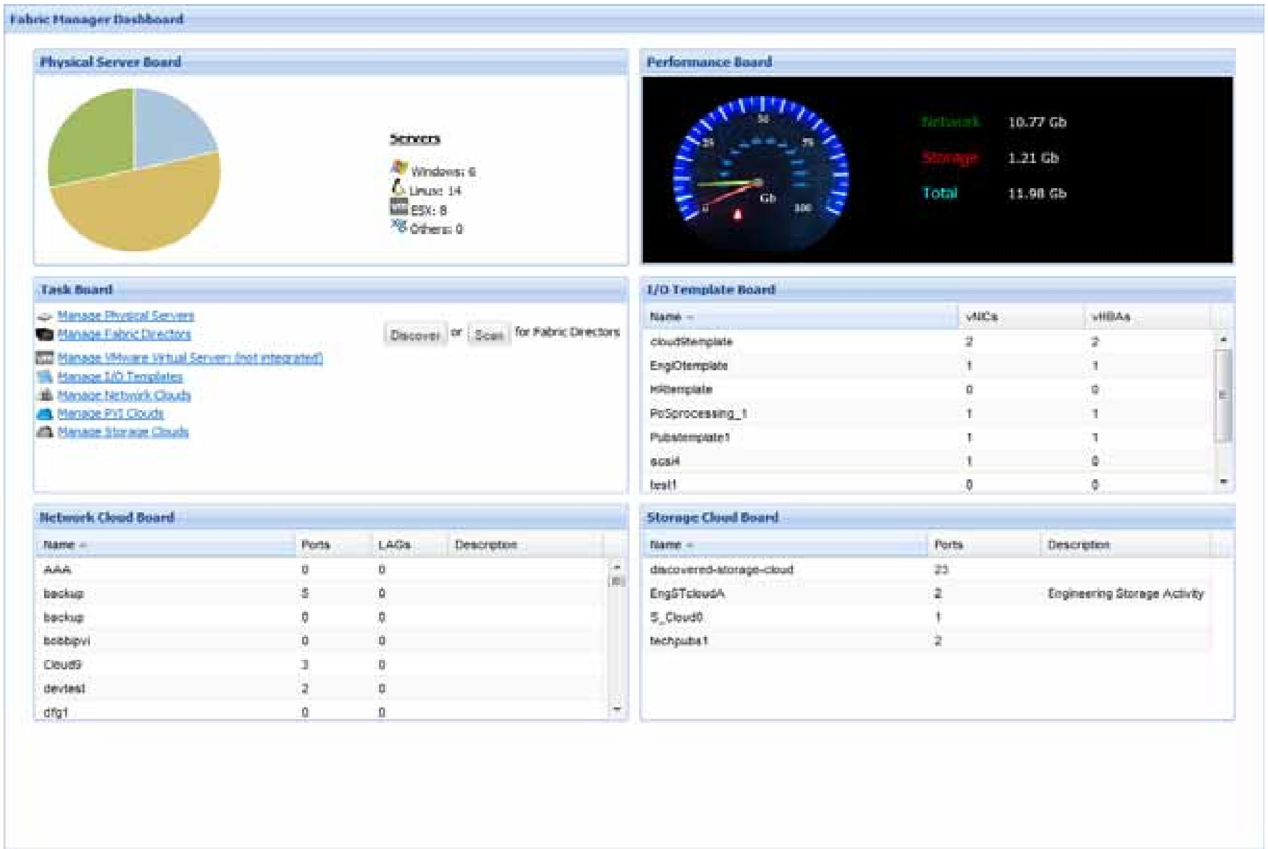
Figure 17 Fabric Manager Login Page

Note: You might see a pop-up dialog notifying you of the suggested screen resolution.

Step 3 In the *User Name* field, enter a valid user name.

Step 4 In the *Password* field, enter the password for the user name you are specifying.

Step 5 Click ***Login*** to display the Welcome page. Figure 18 shows this page.



Fabric Manager Dashboard

Physical Server Board

Servers
Windows: 6
Linux: 14
ESX: 8
Others: 0

Performance Board

Network	10.77 Gb
Storage	1.21 Gb
Total	11.98 Gb

Task Board

I/O Template Board

Name	vNICs	vHBAs
cloud9template	2	2
EngIOtemplate	1	1
HRtemplate	0	0
PoSprocessing_1	1	1
Pubstemplate1	1	1
scsi4	1	0
test1	0	0

Network Cloud Board

Name	Ports	LAGs	Description
AAA	0	0	
backup	5	0	
backup	0	0	
bobbipvi	0	0	
Cloud9	3	0	
devtest	2	0	
dfg1	0	0	

Storage Cloud Board

Name	Ports	Description
discovered-storage-cloud	23	
EngSTcloudA	2	Engineering Storage Activity
S_Cloud0	1	
techpubs1	2	

Figure 18 Fabric Manager Dashboard

Step 6 If you will be managing Fabric Manager through VMware Virtual Infrastructure, you will need to register Fabric Manager with the Virtual Center Server (*Service Manager->VMware Integration*). Otherwise, you can manage Fabric Manager through one of the supported browsers. Proceed to the next step.

Step 7 On the Task Board, click ***Discover...*** to discover one or more Fabric Directors. For information, see Working with the Fabric Director.

Note

In Internet Explorer browsers, you might see a pop up dialog that repeatedly prompts you about secure and non-secure content, and requires you to confirm that you want the content displayed. This is due to an IE browser security setting that is triggered when Fabric Manager pages are displayed or redisplayed. For information about disabling this pop up, see Appendix A: Disabling the IE Security Popup.

Migrating Pre-3.0.0 Fabric Manager Configurations to Fabric Manager 3.0.0 and Later

When Fabric Manager manages an Oracle Fabric Director that already has one or more Server Profiles bound to servers, you can use that Server Profile as an I/O Template for other servers by converting it to an I/O Template. Converting a server profile is especially useful if your data center is using Fabric Manager 2.8.2 or later and you want to retain the same virtual I/O after upgrading to Fabric Manager 3.0.0 or later. By saving a server configuration as an I/O Template, the template can be imported back onto a server(s) after Fabric Manager 3.0.0 or later is installed.

Note

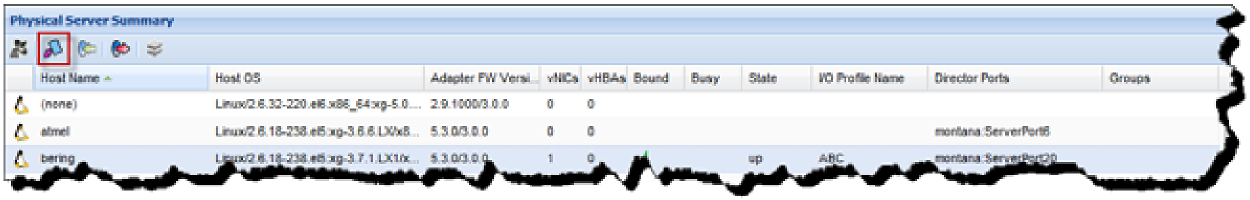
This procedure is required only if you have been using a version of Fabric Manager earlier than 3.0.0 and want to preserve configured elements of the older Oracle Fabric Manager deployment in the current version of Oracle's Fabric Manager.

To convert server profiles to I/O Templates:

Step 1 Display the Physical Server Summary.

Step 2 On the Physical Server Summary, select the discovered server that you want to save as an I/O Template. This step activates the ***Save Server Configuration as an I/O Template*** button.

Step 3 Click the ***Save Server Configuration as an I/O Template*** button, as shown in Figure 19.



Physical Server Summary

Host Name	Host OS	Adapter FW Versi...	vNICs	vHBAs	Bound	Busy	State	I/O Profile Name	Director Ports	Groups
(none)	Linux/2.6.32-220.el6.x86_64:xg-5.0....	2.9.1000/3.0.0	0	0						
atmel	Linux/2.6.18-238.el5:xg-3.6.6.LX/x8...	5.3.0/3.0.0	0	0					montana:ServerPort6	
bering	Linux/2.6.18-238.el5:xg-3.7.1.LX1/x...	5.3.0/3.0.0	1	0			up	ABC	montana:ServerPort20	

Figure 19 Saving a Server Configuration as a Template

Working with the Interface

This chapter documents:

Learning the Fabric Manager Interface

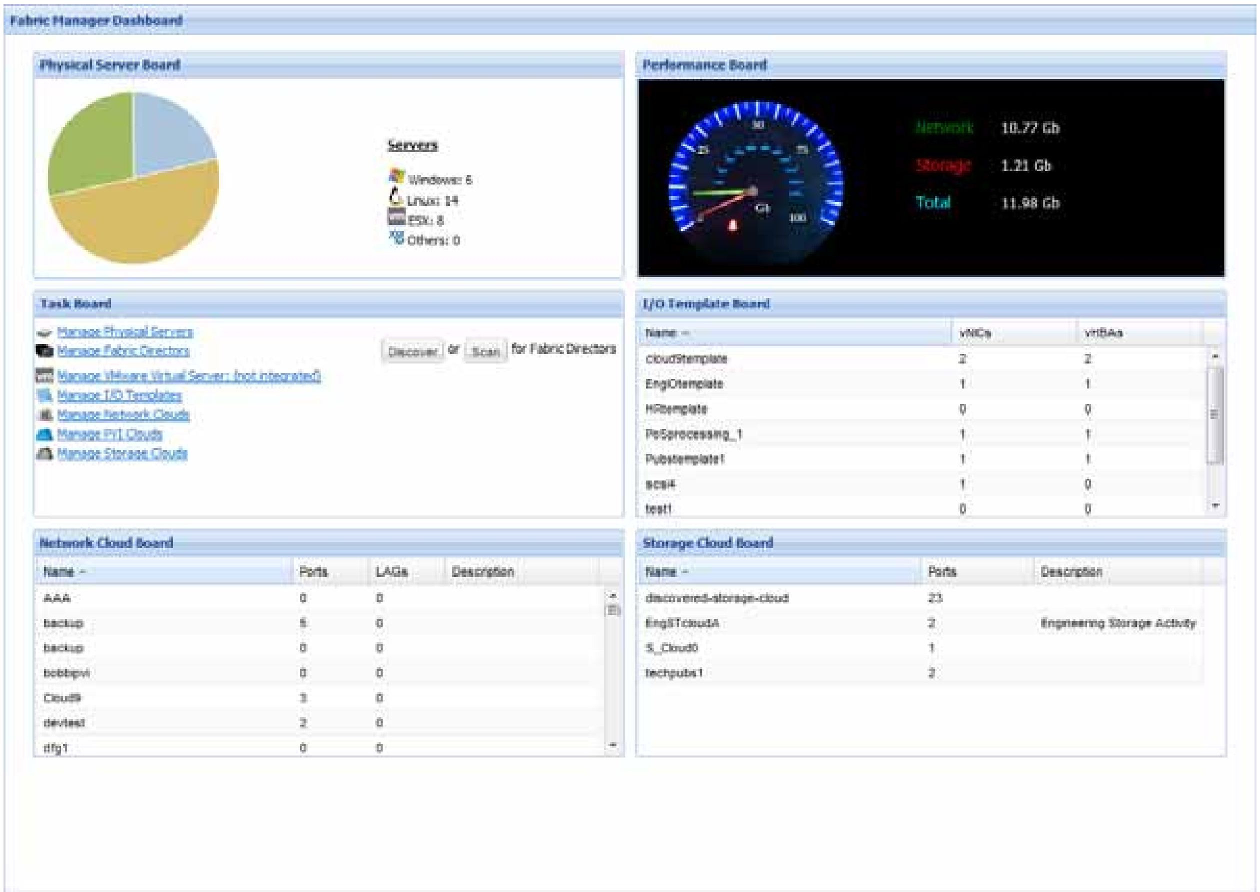
Oracle's Fabric Manager interface is a graphical user interface that enables you to configure and manage Oracle Fabric Directors and the virtual network and storage resources associated with the Fabric Directors. Additional management and configuration is supported for additional functionality, such as host servers, storage targets, access control, and so on.

Fabric Manager runs on a stand-alone server called the Fabric Manager Server, which can be either Linux or Windows based, or as an add-on service that can be integrated into a VMware vSphere or Virtual Infrastructure Server. When Fabric Manager is installed, the Fabric Manager interface provides an intuitive and robust management suite for virtualized I/O that is extended seamlessly to various types of Windows, Linux, and ESX host servers.

The Fabric Manager interface contains the following components:

- the banner
- the navigation panel
- the work panel, which can contain either multiple sub-boards, or different frames for summary information, detailed information, and information about recent jobs that are sent from the Fabric Manager client to the Fabric Manager Server, and in turn to the Fabric Director.

Figure 1 shows an example of the Fabric Manager interface.



Fabric Manager Dashboard

Physical Server Board

Servers

Windows: 6
Linux: 14
ESX: 8
Others: 0

Performance Board

Network 10.77 Gb
Storage 1.21 Gb
Total 11.98 Gb

Task Board

Manage Physical Servers
Manage Fabric Directors
Manage VMware Virtual Server: (not integrated)
Manage I/O Templates
Manage Network Clouds
Manage PVI Clouds
Manage Storage Clouds

I/O Template Board

Name -	vNICs	vHBAs
cloud5template	2	2
EngIOtemplate	1	1
HRtemplate	0	0
PeSprocessing_1	1	1
Pubstemplate1	1	1
scsi4	1	0
test1	0	0

Network Cloud Board

Name -	Ports	LAGs	Description
AAA	0	0	
backup	5	0	
backup	0	0	
bobbipvi	0	0	
Cloud9	3	0	
devtest	2	0	
dfg1	0	0	

Storage Cloud Board

Name -	Ports	Description
discovered-storage-cloud	23	
EngSTcloudA	2	Engineering Storage Activity
S_Cloud0	1	
techpubs1	2	

Figure 1 Xsigo Fabric Manager User Interface

Understanding the Banner

The banner contains buttons and icons that enable you to get general information about Fabric Manager, and the Fabric Directors that Fabric Manager has discovered. Through the Banner, you can:

- logout of the Fabric Manager Server. In addition to explicitly logging out, Fabric Manager has an inactivity timer of 30 minutes. As long as you are actively using Fabric Manager, the inactivity timer is not triggered. However, if no click or keyboard action is detected for 30 minutes, the Fabric Manager automatically closes any currently active session. You can log back in as usual, and the inactivity timer is reset.
- see which user account is logged in to the Fabric Manager Server as well as what role is assigned to that user account
- determine which domain the Fabric Manager Server and its managed Fabric Director(s) are part of
- set the UI to projector mode, which is a conditional setting that is available on pages that contain dark backgrounds. This option supports setting the dark backgrounds to a light background that is easier to see when Fabric Manager is displayed over a video projector.
- get version information for the Fabric Manager software installed on the Fabric Manager Server
- get help text for configuration and management tasks available through Fabric Manager

- see a quick, at-a-glance tally of the current alarms through icons that summarize the number of critical, major, warning, and minor alarms reported by the Fabric Manager Server or Fabric Director. Additional alarm information is provided in more detail through the Alarm Log and Alarm History options on the Navigation panel.
- perform Fabric Manager maintenance tasks, such as backing up and restoring the Fabric Manager configuration.

Figure 2 shows the banner.

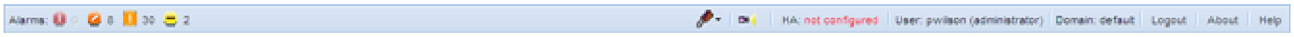


Figure 2 Banner

Understanding the Navigation Panel

The navigation panel appears as a list on the left side of the Fabric Manager. The navigation panel is divided into logical groupings of related functionality. These groupings are known as “managers” with the exception of the first grouping, which is the General option.

Each manager in the list expands and collapses one level to display links that you can use for configuration and management of one or more entities within it. For example, the Server Resource Manager contains functionality related to physical servers. The one exception is the General option, which contains system-wide information, such as Topology and Alarm information. The navigation panel is a common point for starting most work flows, so you can use it as a first step in most configuration and management tasks.

Note

The navigation panel is a starting point, but you can also use the “Task Board” and other of the sub-boards on the Dashboard. Through the Dashboard and its contents you can access some of the most common tasks in configuring your virtual I/O. The Dashboard is useful for accessing common tasks, but the Navigation panel provides a more complete starting point for configuration and management tasks.

Figure 3 shows the Navigation panel with all options closed.

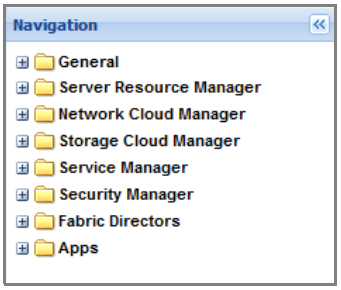
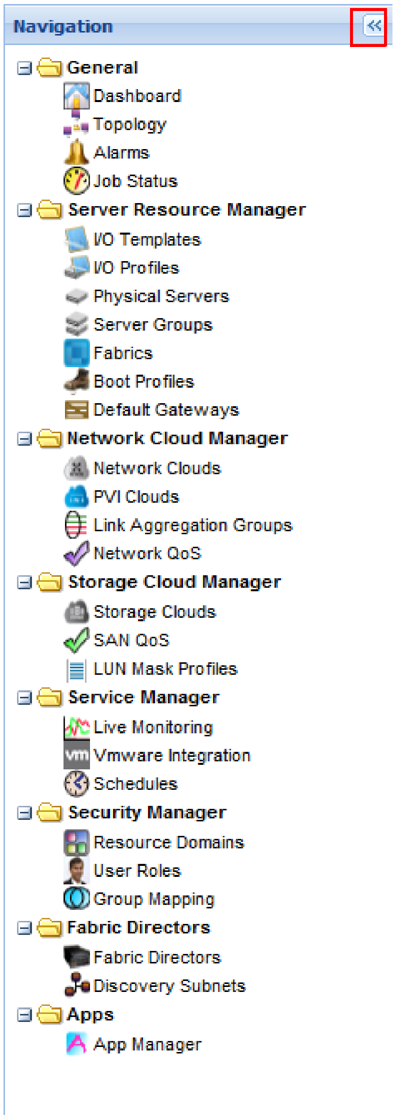


Figure 3 Navigation Panel

You can use the navigation panel to display appropriate icons that allow configuration and management in the main work area of the work panel. For example, if you wanted to create QoS on a vNIC, you would open the *Network Cloud*

Manager on the navigation panel, then click *Network QoS* to display the Network QoS Summary in the work panel of the Fabric Manager interface.

You can toggle the navigation panel between hide and display by clicking the button in the upper right corner of the navigation panel. Hiding the navigation panel gives you more room in the Fabric Manager work area for configuration and management, and in wide tables, allows more columns to be displayed. Figure 4 shows the hide and display toggle switch for the navigation panel.



Hide and Display Navigation Panel

Figure 4 Navigation Panel Toggle Switch

The navigation panel contains the following items:

- General Option
- Server Resource Manager

- Network Cloud Manager
- Storage Cloud Manager
- Service Manager
- Security Manager
- Fabric Directors
- Apps

General Option

The *General* option in the navigation panel contains the Dashboard, Topology, Alarms, and Job Status options. Figure 5 shows the *General* option.

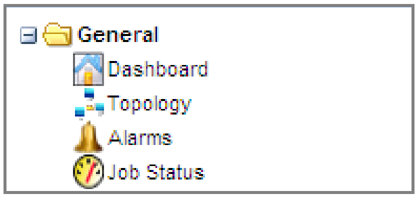


Figure 5 Navigation Panel - General Option

Through the *Dashboard* link you can display the Dashboard. (See Figure 1.) The Dashboard contains multiple sub-boards that give you quick, at-a-glance information about various elements of the Fabric Director(s) and servers under management by the Fabric Manager. The Dashboard contains the following sections:

- The Physical Server Board, which shows a pie graph of the distribution of different server types discovered in the network, based on host OS type
- The Performance Board, which shows a speedometer with the following information:
  - aggregate network throughput of all vNICs managed by Fabric Manager
  - aggregate storage throughput of all vHBAs managed by Fabric Manager
  - total traffic throughput, which is the sum of network and storage traffic on all vNICs and vHBAs that are managed by Fabric Manager
- The Task Board, which contains the following links and controls:
  - Manage Physical Servers
  - Manage Fabric Directors, including discovering specific Fabric Directors by either IP address or system name, or scanning the network for all connected Fabric Directors that are online and running.
  - VMware Virtual Center Server, which displays whether the Fabric Manager is currently integrated into a VMware Virtual Infrastructure. By default, Fabric Manager does not automatically register with the Virtual Infrastructure.So, when Fabric Manager is installed, no integration information is displayed until you explicitly integrate Fabric Manager into the VMware Virtual Infrastructure.
  - Manage I/O Templates
  - Manage Network Clouds
  - Manage Storage Clouds

- The I/O Template Board, which shows a table of all the configured I/O Templates in Fabric Manager. I/O Templates are displayed regardless of whether they are deployed on a server or not
- The Network Cloud Board, which shows a table of all the configured Network Clouds in Fabric Manager. Network Clouds are displayed regardless of whether they are deployed on a server or not
- The Storage Cloud Board, which shows a table of all the configured Storage Clouds in Fabric Manager. Storage Clouds are displayed regardless of whether they are deployed on a server or not

Through the *Topology* link you can display the Topology Overview. In the Topology Overview, you can see how individual servers and server groups (if any) are connected to their respective Network and Storage Clouds through the Fabric Director(s) in the network. Additional views are available through the Topology page. These additional views allow for different ways to see the virtual interconnectivity of servers, Fabric Directors, Network and Storage clouds, targets, ports, vNICs, and vHBAs. For more information about the Topology, see Working with Discovery Subnets.

Through the *Alarms* link you can display the Alarms page which displays the current active alarms on the *Alarms Summary* tab and the historical information for alarms on the *Alarm History Summary* tab. For more information about the Alarms Summary, see Working with Alarms.

Through the *Job Status* link you can display information about jobs that are occurring on the Fabric Manager Server. Some jobs are self contained (called primary jobs), but others contain sub-jobs. Any primary job is listed as an entry on the Jobs Status page, but jobs that contain sub-jobs are listed as an expandable or collapsible job on the Job Status page. For such jobs, you can expand the sub-jobs to see more granular information about the status of each sub-job. For more information about the Job Status, see Working with Fabric Manager Jobs.

Server Resource Manager

The *Server Resource Manager* in the navigation panel displays information about the physical servers connected to the Fabric Directors that Fabric Manager has discovered. Figure 6 shows the Server Resource Manager on the navigation panel.

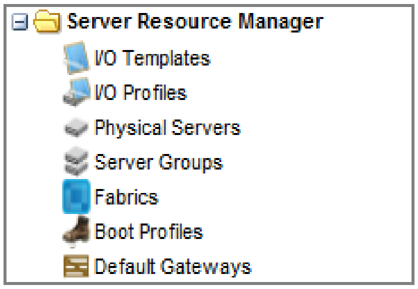


Figure 6 Navigation Panel — Server Resource Manager

The *Server Resource Manager* contains a list of the following links:

- I/O Templates, which links to information about all the I/O Templates configured in Fabric Manager. If you click the I/O Templates link, a table is displayed that contains all configured I/O Templates and information about them. For more information about creating and managing I/O Templates, see Working with I/O Templates.
- I/O Profiles, which links to information about all the I/O Profiles configured in Fabric Manager. If you click the link, a table is displayed that contains all of the created I/O Profiles as well as information about them, and other functions that are related to configuring and managing I/O Profiles. For more information about I/O Profiles, see Working with I/O Profiles.

- Physical Servers, which links to information about the physical servers discovered by Fabric Manager. If you click the link, a table is displayed that contains all of the physical servers as well as information about each of them. For more information about physical servers, see Working with Physical Servers.
- Server Groups, which links to information about all the server groups configured in Fabric Manager. If you click the Server Groups link, a table is displayed that contains all configured server groups and information about them. For more information about server groups, see Working with Server Groups.
- Fabrics, which links to information about all the individual InfiniBand fabrics under management in Fabric Manager. Fabrics are used by Xsigo Fabric Accelerator, which is a separately purchaseable feature. If purchased, when you click this link, a table of all the individual Xsigo Fabrics under management is displayed. Xsigo Fabrics allow the configuration of Private Virtual Interconnects (PVIs), which support "east-west" traffic—for example, vMotion traffic. If you do not have Xsigo Fabric Accelerator installed, this option is still available, but it is inactive (greyed out) on the navigation panel. For more information, see the *Xsigo Fabric Accelerator Quick Start Guide*.
- Boot Profiles, which links to information about optional configurations for supporting SAN Boot and iSCSI Boot of physical servers. If you click the Boot Profiles link, a table is displayed that contains all the Boot Profiles configured in Fabric Manager for physical host servers. For more information about Boot Profiles, see Working with Boot Profiles.
- Default Gateways, which links to information about default gateways configured in Fabric Manager and information about the gateways and how they are associated with host servers. If you click the Default Gateways link, a table is displayed that contains all configured default gateways and information about them. For information about default gateways, see Working with Default Gateways.

Network Cloud Manager

The *Network Cloud Manager* in the navigation panel displays information about features configurable in Fabric Manager's IP network clouds and their child elements. Figure 7 shows the Network Cloud Manager on the navigation panel.

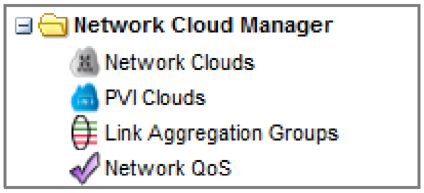


Figure 7 Navigation Panel — Network Cloud Manager

The *Network Cloud Manager* contains the following options:

- Network Clouds, which links to information about Network Clouds that have been configured in Fabric Manager. If you click the Network Clouds link, a table is displayed that contains all Network Clouds, ports, and network properties associated with the Network Clouds. For more information about Network Clouds, see Working with Network Clouds.
- PVI Clouds, which links to information about Private Virtual Interconnect Clouds which are part of the Xsigo Fabric Accelerator feature. Xsigo Fabric Accelerator is a separately purchaseable feature. If purchased, when you click this link, a table of all the configured PVI Clouds is displayed as well as information about each of them. For more information, see the *Xsigo Fabric Accelerator Quick Start Guide*.

- Link Aggregation Groups, which links to information about link aggregation groups (LAGs) configured in Fabric Manager and the ports assigned to them. If you click the Link Aggregation Groups link, a table is displayed that contains the LAG configured in Fabric Manager as well as the ports that constitute each LAG. For more information about LAGs, see Working with Link Aggregation.
- Network QoS, which links to information about network Quality of Service (QoS) Profiles that have been configured in Fabric Manager. If you click the Network QoS link, a table is displayed that contains all Network QoS Profiles and information about them. For more information about creating and managing Network QoS, see Working with Network QoS.

Storage Cloud Manager

The *Storage Cloud Manager* in the navigation panel displays information about all the Fibre Channel-connected storage targets discovered by Fabric Manager, as well as controls for managing them. Through this option, you can create Storage Clouds, LUN Masks, set SAN QoS parameters for vHBAs, and so on.

Figure 8 shows the *Storage Cloud Manager* on the navigation panel.

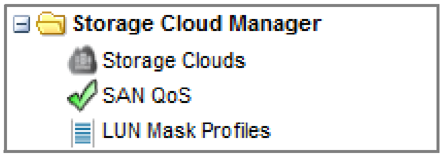


Figure 8 Navigation Panel —Storage Cloud Manager

- Storage Clouds, which links to information about Storage Clouds that have been configured in Fabric Manager. If you click the Storage Clouds link, a table is displayed that contains all Storage Clouds, ports, and storage properties associated with the Storage Clouds. For more information about creating and managing Storage Clouds, see Working with Storage Clouds.
- SAN QoS, which links to information about storage Quality of Service (QoS) profiles that have been configured on vHBAs on discovered Fabric Directors. If you click the SAN QoS link, a table is displayed that contains all SAN QoS Profiles and information about them. For more information about creating and managing SAN QoS, see Working with SAN QoS.
- LUN Mask Profiles, which links to information about LUN Masks to filter the storage targets that are available to host servers. If you click this link, a table is displayed that contains all the LUN Masks, as well as properties associated with each LUN Mask. For more information about creating and managing LUN Masks, see Working with LUN Masks.

Service Manager

The Service Manager supports features that allow for live, real-time performance monitoring, integrating Fabric Manager into VMware, and fault recovery. Figure 9 shows the options available in the Service Manager.

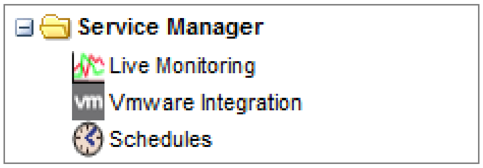


Figure 9 Navigation Panel — Service Manager

The Service Manager contains the following topics:

- Live Monitoring, which links to a statistics and performance grapher that shows live, real-time throughput on a per-server, per-vNIC, or per-vHBA basis. For more information about Live Monitoring, see Working with Live Monitoring.
- VMware Integration, which links to a configuration page that supports the integration of Fabric Manager into a VMware Virtual Infrastructure environment. For more information about integrating Fabric Manager into a VMware management framework, see Working with VMware Servers.
- Schedules, which links to a table of configurable schedules. The schedules enable you to configure a specific date and time at which scheduled tasks (such as Fabric Manager Server or Fabric Director backup) will occur. If you click this link, a table of all the configured scheduled tasks will occur on a daily, weekly, or monthly basis. Through the table, you can also perform an on-demand backup of Fabric Manager Servers or Fabric Directors as needed. For more information, see Working with the Task Scheduler.

Security Manager

The Security Manager contains options that allow the configuration of Fabric Directors in specific network domains as well as the configuration of Fabric Manager and Fabric Director users and roles:

- Resource Domains, which links to a wizard and summary tables that allow for flexibility in where the Fabric Director(s) and Fabric Manager Server are configured in the overall network, or specific sub-domains within the overall network. For information about resource domains, see Working with Domains.
- User Roles, which links to dialogs that enable configuring specific user accounts for network administrators and assigning Fabric Manager roles to each account. The Fabric Manager role for a user account supersedes any roles or privileges assigned through the Windows or Linux OS. For information about User Roles, see Working with User Roles.
- Group Mapping, which links to dialogs that enable specifying a mapping between a user's group configured in an external identity management system (IMS), such as Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) and a Fabric Manager role or domain. For more information, see Working with User Roles.

Figure 10 shows the Security Manager.

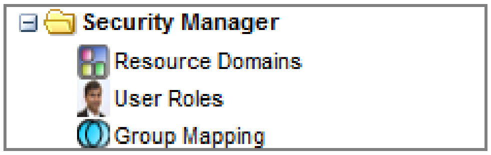


Figure 10 Navigation Panel — Security Manager

Fabric Directors

The *Fabric Directors* option on the navigation panel contains links related to the Fabric Director chassis and the IP subnet in which it is installed and where the Fabric Director can be discovered. Through this option you can view detailed information about each managed Fabric Director, all hardware inventoried in Fabric Manager, and Fabric Director-based software and hardware features that available on the Fabric Director.

Figure 11 shows the Xsigo Fabric Directors option.

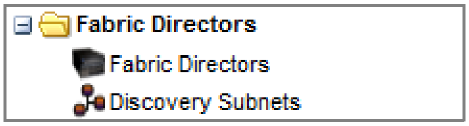

Fabric Directors
Fabric Directors
Discovery Subnets

Figure 11 Navigation Panel — Fabric Directors Option

The Fabric Directors option contains the following links:

- Fabric Directors, which links to information about the Fabric Directors that Fabric Manager has discovered. If you click the link, a table is displayed that contains all of the Fabric Directors as well as information about each of them. For information about managing Xsigo Fabric Directors, see Working with the Fabric Director.
- Discovery Subnets, which allows Fabric Manager to discover Fabric Directors that are located in a different IP subnet by establishing a connection between the Fabric Manager server and a Fabric Director which acts as a proxy within that remote subnet. Discovery subnets must be manually configured to allow contact between the Fabric Manager Server and the proxy off of its local subnet. For more information about Discovery Subnets, see Working with Discovery Subnets.

Apps

The *Apps* option on the navigation panel contains links related to various Fabric Manager applications that can be added to the Fabric Manager GUI to provide additional, licensable functionality. Through this option you can install, configure, and manage additional applications.

Apps
App Manager

Figure 12 Navigation Panel — Apps Option

The contents of the Apps option will vary based on which additional applications you have purchased and installed. For example, one of Fabric Manager's application called Fabric Performance Monitor (which is separately purchaseable) might be installed. If so, that application would be listed by name in the Apps option. The name would function as a link to a separate set of pages where the application is managed.

The Apps option contains Fabric Manager App Manager, option, which links to a information about the individual applications that have been installed into Fabric Manager. This option is always present because it is the utility in Fabric Manager that supports additional applications to seamlessly plug in to the core Fabric Manager product.

As additional Xsigo applications are made available, the Apps Manager will be used to install them into Fabric Manager for use.

Understanding The Work Panel

The work panel is the main work area for Fabric Manager. Most configuration and management tasks occur through the work panel. The work panel has consistent layout for most features, but there are some exceptions. The work panel is typically divided into the following parts:

- the Summary, which is the top frame in the work panel. The Summary is a high-level listing of all instances of specific object—for example, the Physical Server Summary contains a list of all physical servers that Fabric Manager is managing. The Summary contains some basic information about general properties for the objects.
- the Details frame, which is the middle frame in the work panel. The Details frame is a single instance of an object selected in a Summary. For example, the Physical Server Details frame contains information about a single physical server that you selected in the Physical Server Summary. The Details frame contains additional information that is specific to the selected object.

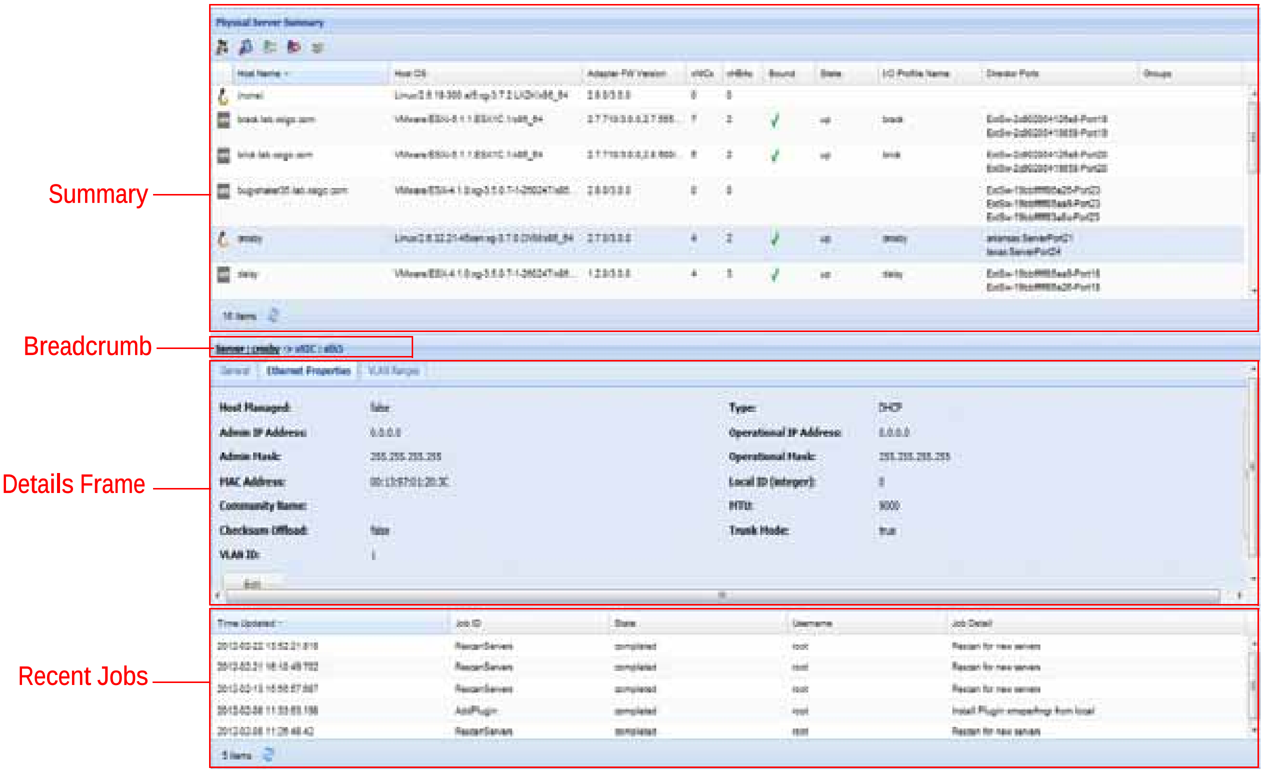
  The Details frame typically contains tabs that organize chunks of similar information in an intuitive and easy-to-use way. Some details frames are nested. For example, the Physical Server Details frame contains a *vNICs* tab, which lists all vNICs in the selected physical server. Each vNIC name on the *vNICs* tab is a link to another level of details frame—in this case, the vNIC Details. By using a combination of tabs and links in the Details frame, it is possible to drill-down to low-level details about a selected object.

  Due to the amount of nesting in the Details frame, a breadcrumb trail (“breadcrumbs” in this documentation) are available on the detail frame’s banner. Breadcrumbs are a user interface navigation tool of incremental hyperlinks that allow you to see the current level of depth for the current dialog or frame. You can also use the breadcrumbs to retrace your clicks.
- Recent Jobs, which is the bottom frame in the work panel. The Recent Jobs frame is a list of the status of recently attempted configuration or management tasks. For example, if you attempt to discover a Fabric Director, the Recent Jobs frame will show an interpretable result based on the interaction between the Fabric Manager client, Fabric Manager Server, and Fabric Director. By default, the Recent Jobs frame shows results for the three most recently attempted tasks, but scroll bars on the frame allow you to view older results.

Note

Some exceptions to this layout are:
* the Overview page, which has a number of sub-boards
* the I/O Template Editor, which has one top frame for general properties and one large workspace for assembling the I/O Template’s building blocks
* the Topology page, which has one large work area and click-and-drag options for moving and connecting servers, as well as right-clickable objects that display pop-up menus

Figure 13 shows an example of a typical Fabric Manager work panel.



Physical Server Summary

	Host Name	Host OS	Adapter FW Version	vNICs	vHBAs	Bound	State	I/O Profile Name	Director Ports	Groups
	inonel	Linux/2.6.18-308.el5.xg-3.7.2.LXDH/x86_64	2.8.0/3.0.0	0	0					
	brack.lab.xsigo.com	VMware/ESXi-5.1.1.ESXiC.1/x86_64	2.7.710/3.0.0,2.7.555...	7	2	✓	up	brack	EvsSw-2d60200412fa6-Port18 EvsSw-2d602004185f8-Port18	
	brick.lab.xsigo.com	VMware/ESXi-5.1.1.ESXiC.1/x86_64	2.7.710/3.0.0,2.8.800/...	8	2	✓	up	brick	EvsSw-2d60200412fa6-Port20 EvsSw-2d602004185f8-Port20	
	bugshaker35.lab.xsigo.com	VMware/ESX-4.1.0.xg-3.5.0.7-1-260247/x86...	2.8.0/3.0.0	0	0				EvsSw-19bbffff80a28-Port23 EvsSw-19bbffff85aa8-Port23 EvsSw-19bbffff83a8c-Port23	
	crosby	Linux/2.6.32-21-Xserver.xg-3.7.0.DVB/x86_64	2.7.0/3.0.0	4	2	✓	up	crosby	arkansas.ServerPort21 texas.ServerPort24	
	daisy	VMware/ESX-4.1.0.xg-3.5.0.7-1-260247/x86...	1.2.0/3.0.0	4	5	✓	up	daisy	EvsSw-19bbffff85aa8-Port18 EvsSw-19bbffff80a28-Port18	

16 items

Server : crosby -> vNIC : eth3

General | Ethernet Properties | VLAN Ranges

Host Managed:	false	**Type:**	DHCP
Admin IP Address:	0.0.0.0	**Operational IP Address:**	0.0.0.0
Admin Mask:	255.255.255.255	**Operational Mask:**	255.255.255.255
MAC Address:	00:13:97:01:20:3C	**Local ID (integer):**	0
Community Name:		**MTU:**	9000
Checksum Offload:	false	**Trunk Mode:**	true
VLAN ID:	1		

Edit

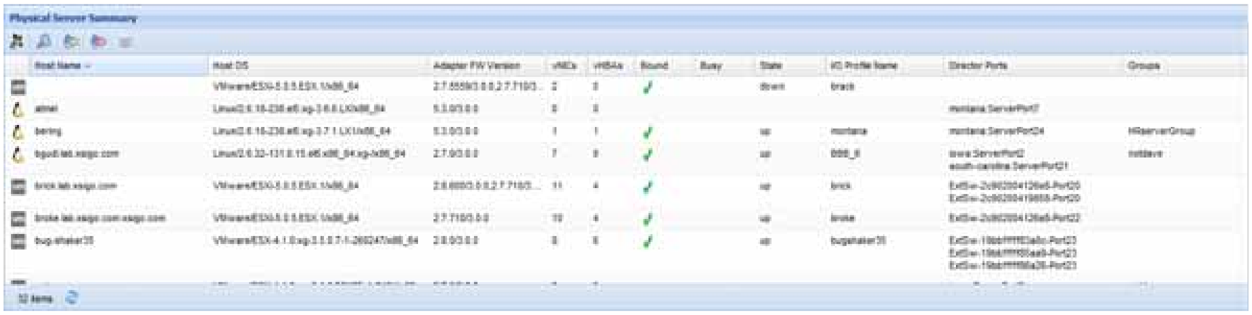
Time Updated	Job ID	State	Username	Job Detail
2012-02-22 13:52:21.818	RescanServers	completed	root	Rescan for new servers
2012-02-21 16:10:49.702	RescanServers	completed	root	Rescan for new servers
2012-02-13 16:56:57.887	RescanServers	completed	root	Rescan for new servers
2012-02-08 11:33:55.198	AddPlugin	completed	root	Install Plugin vmwarePlugin from local
2012-02-08 11:28:48.42	RescanServers	completed	root	Rescan for new servers

5 items

Figure 13 Example of Work Panel Components

Filtering and Sorting Table Displays

The Fabric Manager Summary pages, and also some of the details pages, display their data in tables. For example, Figure 14 shows an example of the Physical Server Summary.



Physical Server Summary

	Host Name	Host OS	Adapter FW Version	vNICs	vHBAs	Bound	Busy	State	I/O Profile Name	Director Ports	Groups
		VMware/ESXi-5.0.5.ESX.1/x86_64	2.7.555/3.0.0,2.7.710/3...	2	0	✓		down	brack		
	almei	Linux/2.6.18-238.el5.xg-3.6.0.LX/x86_64	5.3.0/3.0.0	0	0					montana.ServerPort7	
	bering	Linux/2.6.18-238.el5.xg-3.7.1.LX/x86_64	5.3.0/3.0.0	1	1	✓		up	montana	montana.ServerPort24	HRserverGroup
	bgudi.lab.xsigo.com	Linux/2.6.32-131.0.15.el6.x86_64.xg-/x86_64	2.7.0/3.0.0	7	8	✓		up	BBB_8	iowa.ServerPort2 south-carolina.ServerPort21	notdave
	brick.lab.xsigo.com	VMware/ESXi-5.0.5.ESX.1/x86_64	2.8.800/3.0.0,2.7.710/3...	11	4	✓		up	brick	EvsSw-2c60200412fa6-Port20 EvsSw-2c602004185f8-Port20	
	broke.lab.xsigo.com.xsigo.com	VMware/ESXi-5.0.5.ESX.1/x86_64	2.7.710/3.0.0	10	4	✓		up	broke	EvsSw-2c60200412fa6-Port22	
	bug-shaker35	VMware/ESX-4.1.0.xg-3.5.0.7-1-260247/x86_64	2.8.0/3.0.0	8	6	✓		up	bugshaker35	EvsSw-19bbffff83a8c-Port23 EvsSw-19bbffff85aa8-Port23 EvsSw-19bbffff80a28-Port23	

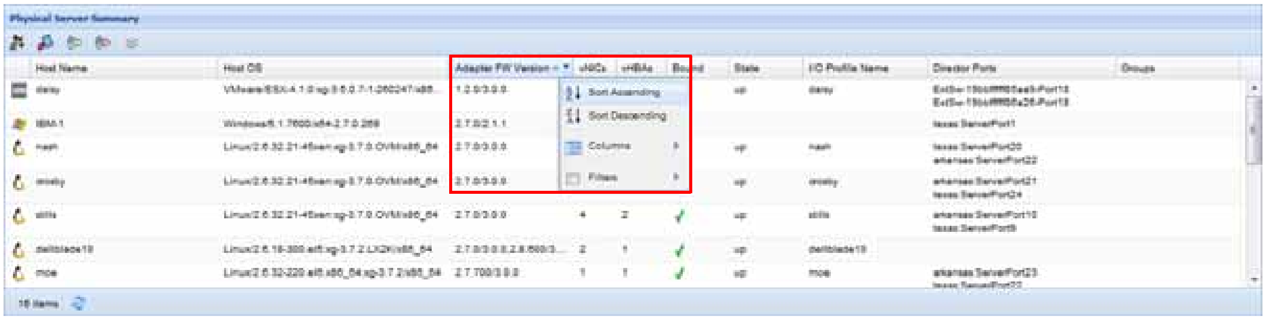
32 items

Figure 14 Sample Table Display

On a table, you can sort and filter information to make displaying pertinent information much easier. Sorting and filtering occur on a per-column basis through a dropdown menu at the right edge of each column heading. To activate the sort and filter controls, click the heading of the column that you want to sort, and a downward arrow appears. The downward arrow is the dropdown menu where the sort and filter options are available.

Sorting

Sorting involves selecting a column and rearranging each entry on the table in either ascending or descending order. All table entries are arranged based on the column(s) that you select. For example, you can arrange the adapter firmware versions installed on servers in ascending order to bring the earliest firmware driver version to the top of the table, as shown in Figure 15.



Physical Server Summary

Host Name	Host OS	Adapter FW Version	vNICs	vHBAs	Bound	State	I/O Profile Name	Director Ports	Groups
daisy	VMware/ESX-4.1.0:xg-3.5.0.7-1-260247/x86...	1.2.0/3.0.0				up	daisy	ExtSw-1S0cfffff05ae5-Port13 ExtSw-1S0cfffff05a26-Port13	
IBM-1	Windows/6.1.7600:x64-2.7.0.269	2.7.0/2.1.1						texas:ServerPort1	
nash	Linux/2.6.32.21-45xen:xg-3.7.0.OVM/x86_64	2.7.0/3.0.0				up	nash	texas:ServerPort20 arkansas:ServerPort22	
mosby	Linux/2.6.32.21-45xen:xg-3.7.0.OVM/x86_64	2.7.0/3.0.0				up	mosby	arkansas:ServerPort21 texas:ServerPort24	
stills	Linux/2.6.32.21-45xen:xg-3.7.0.OVM/x86_64	2.7.0/3.0.0	4	2	✓	up	stills	arkansas:ServerPort10 texas:ServerPort9	
dellblade10	Linux/2.6.18-300.el5:xg-3.7.2.LX2K/x86_64	2.7.0/3.0.0,2.8.600/3...	2	1	✓	up	dellblade10		
moe	Linux/2.6.32-220.el6.x86_64:xg-3.7.2/x86_64	2.7.700/3.0.0	1	1	✓	up	moe	arkansas:ServerPort23 texas:ServerPort22	

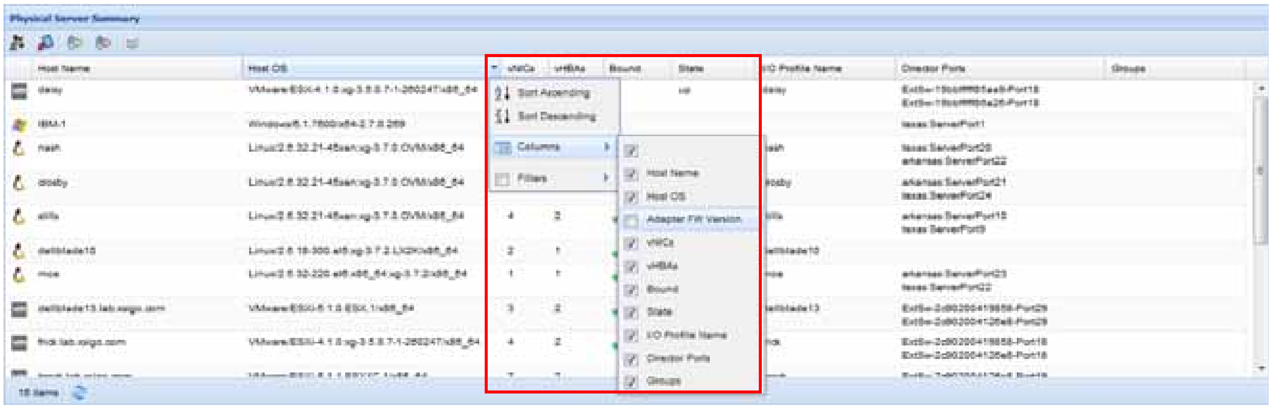
16 items

Figure 15 Sorting a Column

Filtering

Filtering involves either masking out columns in the table display, or entering criteria into a text-entry box and filtering out any table entries that do not use the criteria.

- To completely filter out a column in the table, click the column heading and select *Columns*. Then, click the resulting checkbox as shown in Figure 16. The presence of a checkmark indicates that the field is displayed. The checkbox is a toggle, so clicking the checkbox to remove the checkmark causes the selected field to be filtered. You can filter or display the column as needed by adding or removing the checkbox. In Figure 16, the Adapter Firmware Version version field is filtered out of the table display.



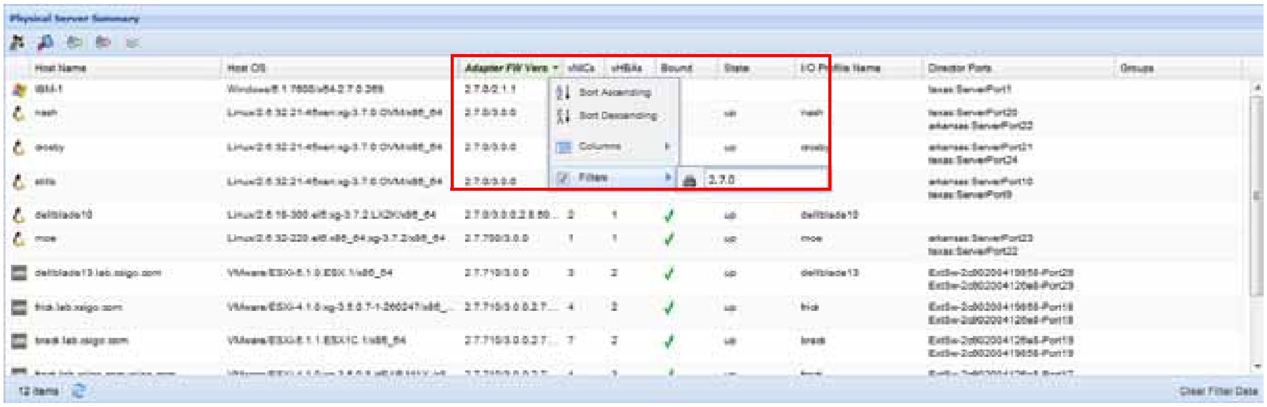
Physical Server Summary

Host Name	Host OS	vNICs	vHBAs	Bound	State	I/O Profile Name	Director Ports	Groups
daisy	VMware/ESX-4.1.0:xg-3.5.0.7-1-260247/x86_64				up	daisy	ExtSw-1S0cfffff05ae5-Port13 ExtSw-1S0cfffff05a26-Port13	
IBM-1	Windows/6.1.7600:x64-2.7.0.269						texas:ServerPort1	
nash	Linux/2.6.32.21-45xen:xg-3.7.0.OVM/x86_64					nash	texas:ServerPort20 arkansas:ServerPort22	
mosby	Linux/2.6.32.21-45xen:xg-3.7.0.OVM/x86_64					mosby	arkansas:ServerPort21 texas:ServerPort24	
stills	Linux/2.6.32.21-45xen:xg-3.7.0.OVM/x86_64	4	2	✓		stills	arkansas:ServerPort10 texas:ServerPort9	
dellblade10	Linux/2.6.18-300.el5:xg-3.7.2.LX2K/x86_64	2	1	✓		dellblade10		
moe	Linux/2.6.32-220.el6.x86_64:xg-3.7.2/x86_64	1	1	✓		moe	arkansas:ServerPort23 texas:ServerPort22	
dellblade13.lab.xsigo.com	VMware/ESXi-5.1.0:ESX.1/x86_64	3	2	✓		dellblade13	ExtSw-2c9020041985B-Port29 ExtSw-2c90200412Ba8-Port29	
frick.lab.xsigo.com	VMware/ESXi-4.1.0:xg-3.5.0.7-1-260247/x86_64	4	2	✓		frick	ExtSw-2c9020041985B-Port18 ExtSw-2c90200412Ba8-Port18	

16 items

Figure 16 Filtering a Column

- To filter table contents by specific criteria, click the column heading and select *Filters* to display a text-entry box where you specify the filter criteria. Then, enter the filter criteria in the text-entry box as shown in Figure 17. Either press ***Enter*** or click the binoculars icon to start filtering. Figure 17 shows an example of filtering the “Driver Version” field based on version 2.7.0 as the criteria.



Host Name	Host OS	Adapter FW Vers	vNICs	vHBAs	Bound	State	I/O Profile Name	Director Ports	Groups
IBM-1	Windows/6.1.7600/x64 2.7.0.369	2.7.0/2.1.1						texas:ServerPort1	
nash	Linux/2.6.32-21-45xen.xg-3.7.0.OVM/x86_64	2.7.0/3.0.0				up	nash	texas:ServerPort20 arkansas:ServerPort22	
dusty	Linux/2.6.32-21-45xen.xg-3.7.0.OVM/x86_64	2.7.0/3.0.0				up	dusty	arkansas:ServerPort21 texas:ServerPort24	
ellis	Linux/2.6.32-21-45xen.xg-3.7.0.OVM/x86_64	2.7.0/3.0.0						arkansas:ServerPort10 texas:ServerPort9	
dellblade10	Linux/2.6.18-308.el5.xg-3.7.2.LX2K/x86_64	2.7.0/3.0.0.2.8.80...	2	1	✓	up	dellblade10		
moe	Linux/2.6.32-220.el6.x86_64.xg-3.7.2/x86_64	2.7.790/3.0.0	1	1	✓	up	moe	arkansas:ServerPort23 texas:ServerPort22	
dellblade13.lab.xsigo.com	VMware/ESXi-5.1.0.ESX.1/x86_64	2.7.710/3.0.0	3	2	✓	up	dellblade13	ExtSw-2c00200419958-Port23 ExtSw-2c002004120a8-Port23	
frick.lab.xsigo.com	VMware/ESX-4.1.0.xg-3.5.0.7-1-260247/x86_...	2.7.710/3.0.0.2.7...	4	2	✓	up	frick	ExtSw-2c00200419958-Port18 ExtSw-2c002004120a8-Port18	
brad.lab.xsigo.com	VMware/ESXi-5.1.1.ESX1C.1/x86_64	2.7.710/3.0.0.2.7...	7	2	✓	up	brad	ExtSw-2c002004120a8-Port19 ExtSw-2c00200419958-Port19	

Figure 17 Filtering by User-Defined Criteria

When the filter operation completes, the filtered table contents are displayed. Also, the checkbox to the left of the *Filter* menu option contains a checkmark. The checkmark indicates that the table contents displayed are the filtered contents.

Using the Maintenance Menu

The Maintenance Menu contains common tasks for managing the Fabric Manager Server and Fabric Manager GUI. These features tend to be outside the realm of actually configuring and managing host servers and their vNIC and vHBA connections. The Maintenance menu is a dropdown menu available on the Fabric Manager banner, and appears as a screwdriver icon as shown in Figure 18

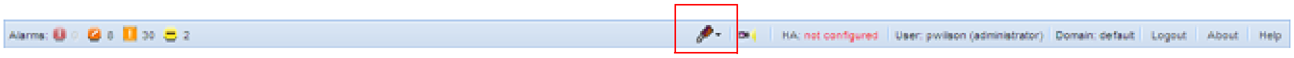


Figure 18 Banner — Maintenance Menu

The Maintenance Menu has the following options:

- Backing Up The Fabric Manager Configuration
- Restoring the Fabric Manager Server Configuration
- Migrating Pre-3.0.0 Fabric Manager Configurations to Fabric Manager 3.0.0 and Later
- Allowing or Preventing Unlisted Users Access to Fabric Manager
- Downloading Fabric Manager Log Files
- Cleaning Up the Fabric Manager Database

Backing Up The Fabric Manager Configuration

The current Fabric Manager configuration can be backed up on the Fabric Manager Server. When the configuration is backed up, the existing settings, virtual resources, and all other configured functionality in the Fabric Manager GUI are saved to a config file that you can name.

Be aware that there is a running a config and one or more backed up configs (if a Fabric Manager config has been saved). These two configurations can be different.

When the configuration is backed up, it is saved into `/opt/xsigo/xms/xms-backups`. It is not required that you provide a unique name for the configuration when you back it up. When a configuration is backed up, a time stamp is appended to the name that you give to the backed up configuration. For example, when you save the configuration as `XMS-Config-Indy` for the Fabric Manager Server named “Indy”, the backup processes add a time stamp so that the file name might then become `Indy__2010-11-30_13_59_22_865`.

Backing up the Fabric Manager configuration occurs locally on the Fabric Manager Server, and no option exists to save the configuration to a central repository (for example, a LUN in the SAN). However, if you want to place the Fabric Manager configuration off of the Fabric Manager Server, you can simply back up the config on the Fabric Manager Server, then copy it off of the server to whichever location you desire.

Note

Xsigo strongly recommends that you backup the Fabric Manager Server configuration and the Fabric Director configuration at the same time. Backup the Fabric Manager Server, and when that operation is done, then back up the Fabric Director. Also, when restoring the backed up configuration, restore the Fabric Director configuration first, and when that operation is complete, then restore the Fabric Manager Server configuration.

To back up the Fabric Manager configuration, follow this procedure:

Step 1 Click the *Maintenance* icon, which looks like a screwdriver on the banner.

Step 2 From the *Maintenance Tasks* dropdown menu, select the Configure Backup Locations options, as shown Figure 19.

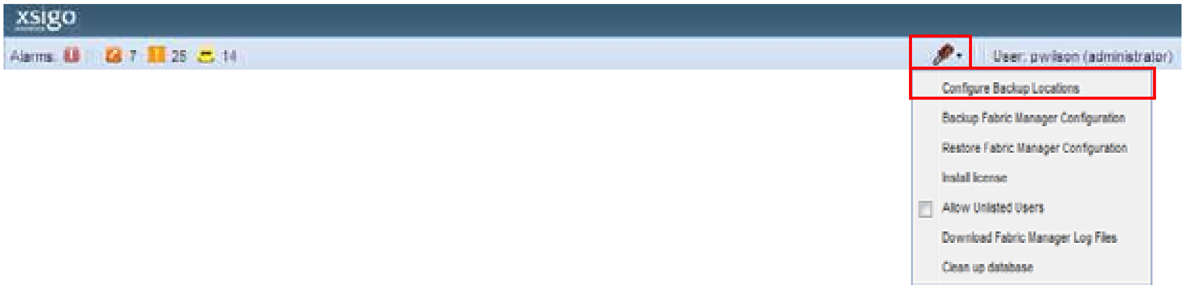
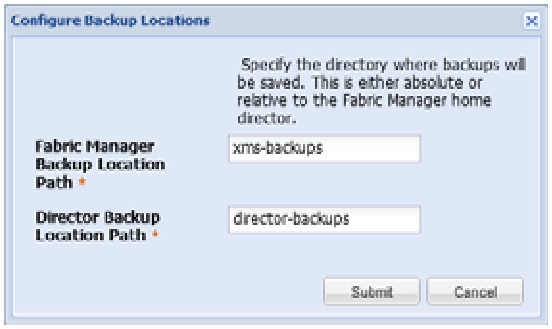

xsigo
Alarms: 7 25 14
User: pwilson (administrator)
Configure Backup Locations
Backup Fabric Manager Configuration
Restore Fabric Manager Configuration
Install license
Allow Unlisted Users
Download Fabric Manager Log Files
Clean up database

Figure 19 Fabric Manager Maintenance Menu — Backing Up the Fabric Manager Configuration

When you select this option, the Configure Backup Locations dialog is displayed. See Figure 20.



Configure Backup Locations

Specify the directory where backups will be saved. This is either absolute or relative to the Fabric Manager home director.

Fabric Manager Backup Location Path *: xms-backups

Director Backup Location Path *: director-backups

Figure 20 Configure Backup Locations

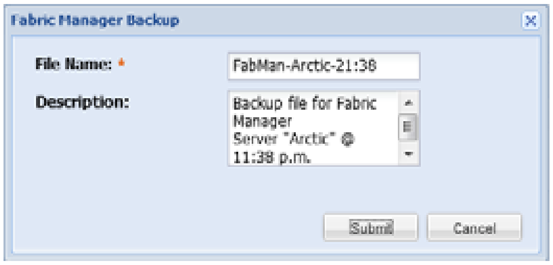
Step 3 In the *Fabric Manager Backup Location Path* field, enter the directory location as either an absolute or relative file path from the Tomcat home directory.

Step 4 In the *Director Backup Location Path* field, enter the directory location as either an absolute or relative path from the Tomcat home directory.

Step 5 Click ***Submit***.

Step 6 From *Maintenance Tasks* dropdown menu, select the *Backup Fabric Manager Configuration* option.

When you select this option as shown in Figure 19 to display the Fabric Manager Backup dialog. Figure 21 shows the Fabric Manager Backup dialog.



File Name: * FabMan-Arctic-21:38

Description: Backup file for Fabric Manager Server "Arctic" @ 11:38 p.m.

Figure 21 Fabric Manager Backup Dialog

Step 7 In the *File Name* field, enter an alphanumeric character string for the name that you want to give to the Fabric Manager configuration. Because multiple configs can be saved, Fabric Manager appends a timestamp to the file name that you enter.

Step 8 As an option, in the *Description* field, you can enter an alphanumeric character string that describes the config file that you are backing up.

Step 9 When the Fabric Manager config file has been named, and any description provided, click ***Submit***. At this point, the configuration is saved. You do not need to reset the server, or start a new Fabric Manager session.

Backing Up and Restoring Fabric Manager Config when Doing a Fresh Install of Fabric Manager

Some cases might require the Fabric Manager software to be completely removed. Some examples are:

- a disk crashes and users want to keep the configuration
- a VM is rebuilt and users want to keep the configuration
- you completely uninstall a version of Fabric Manager and install a newer version, instead of upgrading

To successfully back up and restore the Fabric Manager configuration when you will be removing Fabric Manager, you will need to use a specific procedure. This restriction does not exist if you upgrade the Fabric Manager server. When the Fabric Manager Server is upgraded, the configuration database is kept, and so is the relevant record of a saved configuration. Therefore, the config database has knowledge of the saved config file, and can restore the config.

To perform a backup of an existing config prior to doing a fresh install of the Fabric Manager software, follow this procedure:

Step 1 Perform a Fabric Manager backup.

This step places the Fabric Manager config as an XML file into the `xms-backups` directory.

Step 2 Copy the XML file from the `xms-backups` directory to somewhere else—for example, to a network drive.

Step 3 Remove Fabric Manager, by either **`rpm -e xsigo-xms`** (Linux) or ***Start-Programs->Fabric Manager->Uninstall*** (Windows).

At this point, Fabric Manager is completely removed, including the `xms-backups` directory. However, since the saved config is in a safe location, it can be restored when Fabric Manager is re-installed.

Step 4 Re-install Fabric Manager by either **`rpm -Uvh xsigo-xms`** (Linux) or running the Windows Fabric Manager Installer (**`install-xms-4.1.0.exe`**).

At this point, Fabric Manager is installed, including the `xms-backups` director which is where the Fabric Manager restore feature looks for the backed up config file.

Note

For Windows servers, Xsigo recommends not running the installer from the distribution CD. Instead, copy the distribution CD contents to the server's hard drive, then run the installer.

Step 5 Copy the saved file from its current location (for example, from the network drive) to the new `xms-backups` directory.

Step 6 Restore the Fabric Manager config from the backup by selecting the appropriate backup config file.

Restoring the Fabric Manager Server Configuration

Through Fabric Manager you can restore any saved configuration. By restoring the configuration, you are reloading the saved configuration into Fabric Manager. Be aware that the restored configuration can be different than the current running configuration, and Fabric Manager does not automatically take a snapshot or save the current configuration before restoring the save configuration. As a result, any pending configuration (for example, I/O Template changes in progress on the I/O Template Editor) or any differences between the current Fabric Manager configuration and the config that will be restored are not saved.

When you restore the Fabric Manager configuration, Fabric Manager reads the contents of `/opt/xsigo/xms/xms-backups`, and displays a list of available configurations to load. When selected, that configuration is loaded instantly, without needing to reboot the Fabric Manager server. If multiple Fabric Manager configurations exist with unique names, you can select whichever Fabric Manager configuration you want to load.

Restoring the Fabric Manager configuration occurs locally from the `/opt/xsigo/xms/xms-backups` directory. No option exists to restore a Fabric Manager configuration that is stored in a central repository (for example, a LUN in the SAN). However, if the Fabric Manager configuration you want to restore is off of the Fabric Manager server itself, you can simply copy the Fabric Manager configuration you want into `/opt/xsigo/xms-backups`, then restore the configuration from that directory.

To restore a Fabric Manager config, follow this procedure:

Step 1 Click the *Maintenance* icon, which looks like a screwdriver on the banner.

From *Maintenance Tasks* dropdown menu, select the *Restore Fabric Manager Configuration* option as shown in Figure 22 to display the Fabric Manager Backup dialog.

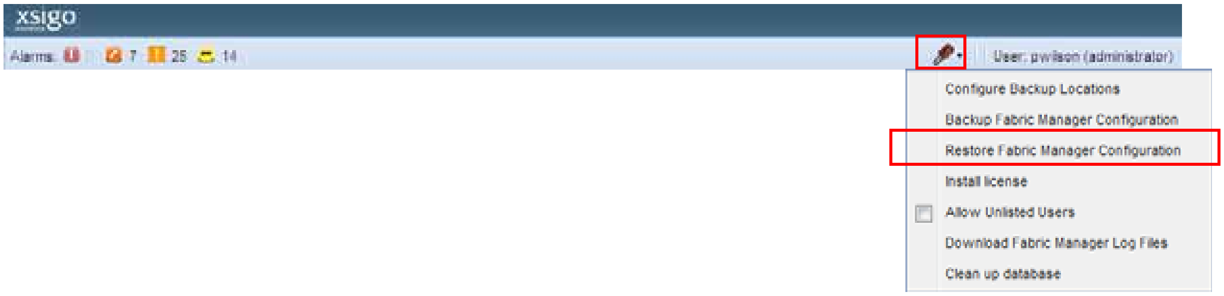
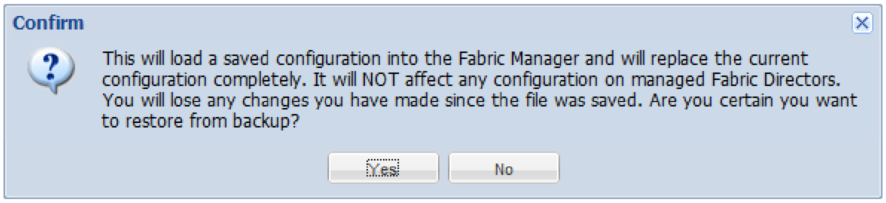

xsigo
Alarms: 0 7 25 14
User: pwilson (administrator)
Configure Backup Locations
Backup Fabric Manager Configuration
Restore Fabric Manager Configuration
Install license
□ Allow Unlisted Users
Download Fabric Manager Log Files
Clean up database

Figure 22 Fabric Manager Maintenance Menu — Restoring the Fabric Manager Configuration

When you select the restore option, a confirmation dialog is displayed that prompts you for verification that you actually intend to restore the Fabric Manager configuration. Figure 23 shows the confirmation dialog.

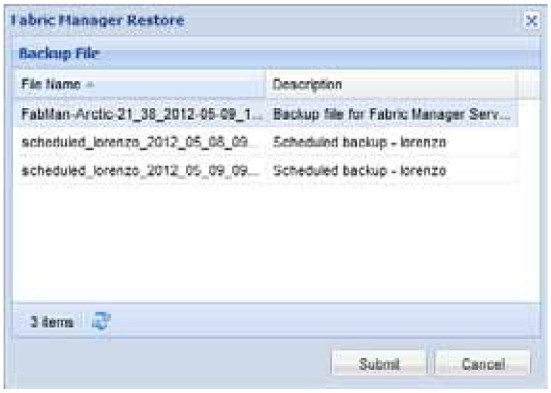


Confirm

This will load a saved configuration into the Fabric Manager and will replace the current configuration completely. It will NOT affect any configuration on managed Fabric Directors. You will lose any changes you have made since the file was saved. Are you certain you want to restore from backup?

Figure 23 Fabric Manager Restore Confirmation Dialog

Step 2 Read the confirmation dialog carefully, then select ***Yes*** to restore the Fabric Manager configuration. When you select ***Yes***, the Fabric Manager Restore Configuration dialog is displayed. Figure 24 shows this dialog.



Fabric Manager Restore

Backup File

File Name	Description
FabMan-Arctic-21_38_2012-05-09_1...	Backup file for Fabric Manager Serv...
scheduled_lorenzo_2012_05_08_09...	Scheduled backup - lorenzo
scheduled_lorenzo_2012_05_09_09...	Scheduled backup - lorenzo

3 items

Figure 24 Fabric Manager Restore—Select Fabric Manager Config

Step 3 On the Fabric Manager Restore dialog, select the backup file that you want to restore. This step activates the ***Submit*** button.

Step 4 Click ***Submit*** to load that Fabric Manager configuration.

Allowing or Preventing Unlisted Users Access to Fabric Manager

Fabric Manager user accounts are created in the Linux or Windows OS of the Fabric Manager Server. When the user passes authentication, that user then receives a role that is granted and enforced by Fabric Manager. If no specific Fabric Manager role is assigned, the user account defaults to the operator role (read-only mode).

However, for tighter data center security, Xsigo provides the ability to completely block an unassigned user account instead of allowing it to default to the operator role. When a user account is blocked, the Fabric Manager Login dialog is displayed, but login will fail when the user name and password are specified.

The Unlisted Users feature is accessible through the *Allow Unlisted Users* checkbox on the Fabric Manager Maintenance Tasks menu. By default, unlisted users are allowed to access Fabric Manager in read-only mode, but you can change this behavior by toggling the checkbox.

To prevent unlisted users from accessing Fabric Manager, follow this procedure:

Step 1 Click the *Fabric Manager Maintenance* icon, which looks like a screwdriver on the banner. Figure 21 shows this option.

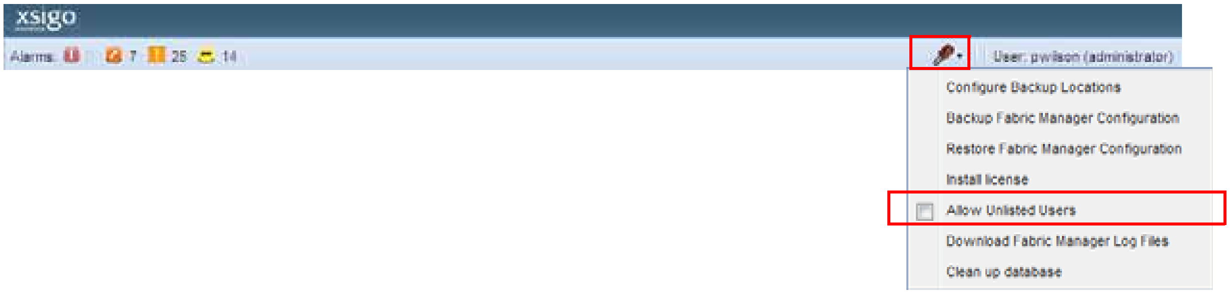

xsigo
Alarms: 7 25 14
User: pwilson (administrator)
Configure Backup Locations
Backup Fabric Manager Configuration
Restore Fabric Manager Configuration
Install license
□ Allow Unlisted Users
Download Fabric Manager Log Files
Clean up database

Figure 25 Fabric Manager Maintenance Menu — Preventing Unlisted Users Access to Fabric Manager

Step 2 Click the check box to allow or prevent unlisted users access to Fabric Manager as needed:

- Place a check mark in the checkbox to allow unlisted users to access Fabric Manager with read-only rights. This setting is the default.
- Remove the check mark from the checkbox to prevent unlisted users from accessing Fabric Manager at all. When this setting is applied, unlisted users are presented with the log in dialog, but will not be able to successfully log in to Fabric Manager.

Downloading Fabric Manager Log Files

Fabric Manager Log files are kept in the `/opt/xsigo/xms/logs` directory. Different log files are kept for different purposes including tomcat, catalina, installation, and error logs. Logs are either current or historical, which is indicated by the file name:

- a current file, which is the most recent log file for the Fabric Manager server. A current file is named with the format <name>`.log`—for example, `xms.log` is the current Fabric Manager Server log file, `xms-schedule.log` is the current Fabric Manager schedule log file, and `director-infiltrator.log` is the current log file for a Fabric Director named “infiltrator”
- a historical file, which is a log file that has rotated from a current file to an older file that contains data that is no longer current, but has been kept. A historical file is named with the format <name>`.log.`<number>—for example, `xms.log.44` is the 44th historical file for the Fabric Manager Server, and `director-infiltrator.log.17` is the 17th historical log file for the Fabric Director named “infiltrator”.

Through Fabric Manager, you can download the logs from the Fabric Manager Server to a local client (for example, a laptop or desktop workstation) so that the logs can be examined if needed. Logs are packaged as a ZIP archive before downloading to minimize the size of the download and the amount of disk space required on the client when the files complete their download. Because the files are zipped, you should ensure that you have enough disk space to fully unzip them, or depending on your compression program, you can selectively extract and unzip only certain files that you need. The choice is completely up to you.

Note

Depending on the number of files in the logs directory, and the number of Oracle Fabric Directors under management, gathering log files, zipping, them and downloading them to a client will take some time. Please be patient and allow the process to complete.

You have some choice in the log files that you want to download:

- All, which downloads the entire contents of `/opt/xsigo/xms/logs` as one large ZIP file. This option downloads current files and historical files.
- Recent Logs only, which downloads only the current files in `/opt/xsigo/xms/logs` as one large ZIP file.

Downloading the Fabric Manager Log files is supported through a menu item on the Fabric Manager Maintenance dropdown menu. To download the Fabric Manager logs, follow this procedure:

Step 1 On the Fabric Manager Maintenance menu, click *Download Fabric Manager Log Files*. Figure 26 shows this menu option.

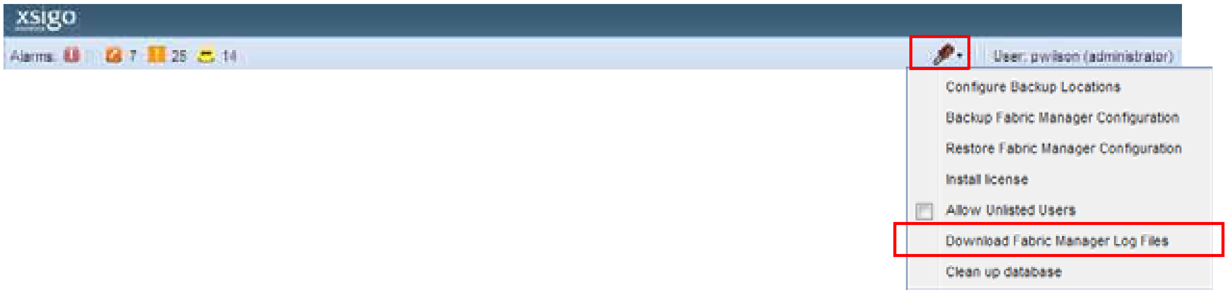
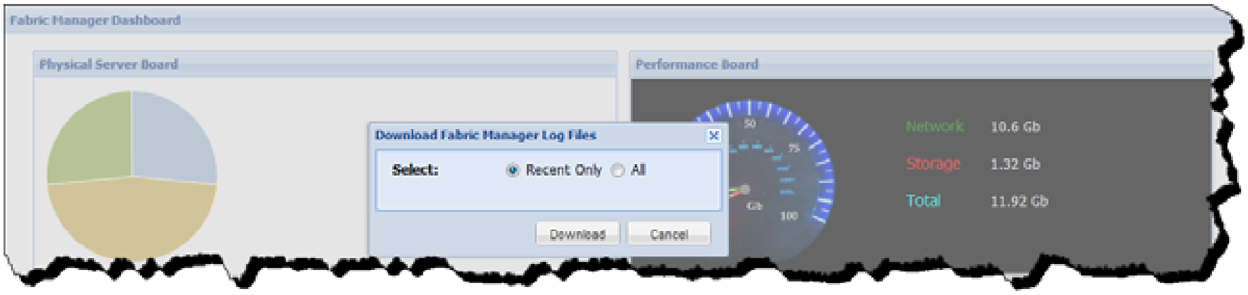

xsigo
Alarms: 7 25 14
User: pwilson (administrator)
Configure Backup Locations
Backup Fabric Manager Configuration
Restore Fabric Manager Configuration
Install license
Allow Unlisted Users
Download Fabric Manager Log Files
Clean up database

Figure 26 Maintenance Menu — Download Fabric Manager Log Files

When you select Download Fabric Manager Files, a popup dialog that will enable you to choose the type of download you want, either Recent Files or All files.

Step 2 On the Download Fabric Manager Log Files dialog, select either ***Recent Only*** or ***All*** as shown in Figure 27.



Fabric Manager Dashboard

Physical Server Board

Performance Board

Network	10.6 Gb
Storage	1.32 Gb
Total	11.92 Gb

Download Fabric Manager Log Files

Select: ● Recent Only ○ All

Download Cancel

Figure 27 Download Fabric Manager Log Files

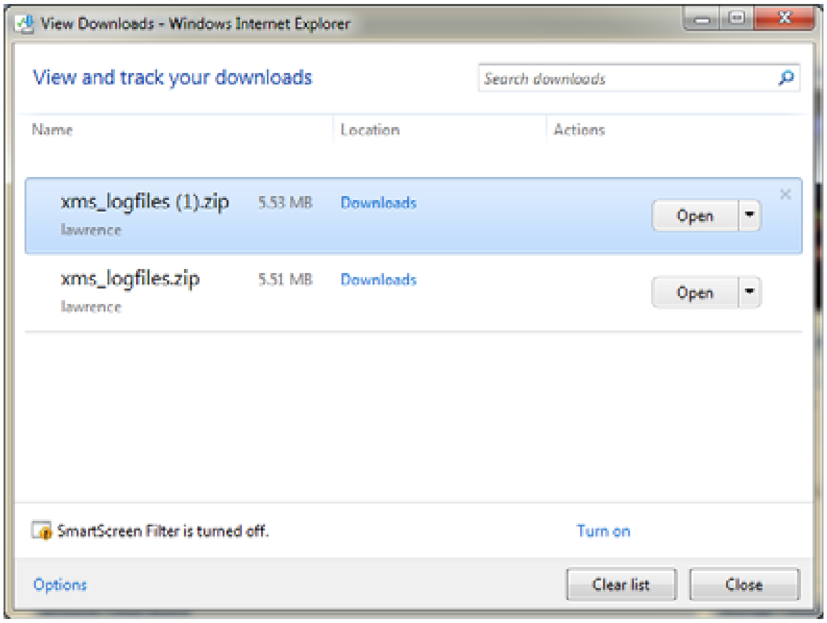
Step 3 On the Download Fabric Manager Log Files dialog, select the appropriate button:

- Recent Only
- All

Step 4 Click ***Download***. A confirmation dialog is displayed by your browser to either save the files to a specific location or open them. Choose one of the following:

- Select ***Save*** to download the files to a location that you select
- Select ***Open*** to save the files to a default download location

Step 5 When the files complete their download, you can unzip them and open the file(s) you want to see. The files are named `xms_logs.zip`. An example is shown in Figure 28.



View Downloads - Windows Internet Explorer

View and track your downloads

Search downloads

Name		Location	Actions
xms_logfiles (1).zip lawrence	5.53 MB	Downloads	Open
xms_logfiles.zip lawrence	5.51 MB	Downloads	Open

SmartScreen Filter is turned off. Turn on

Options Clear list Close

Figure 28 Viewing Downloaded Fabric Manager Log Files Archive

Step 6 When the files are on your Fabric Manager client, you can unzip them and use them as needed.

Cleaning Up the Fabric Manager Database

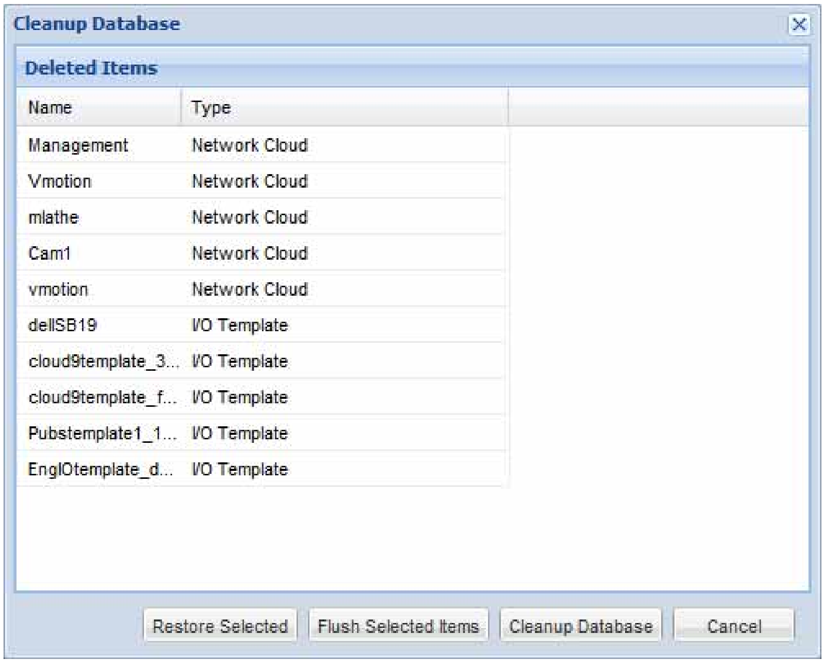
On each Fabric Manager Server, there is a database of objects that are under management. When upgrading between versions of Fabric Manager, new objects might be added, and older objects might not be used anymore. Because of upgrades, you are not completely removing the existing database and installing a fresh database (like you do when you perform a fresh install of Fabric Manager). As an option, Fabric Manager offers a way to clean up the database. When you clean up the Fabric Manager database, you have options to:

- restore selected objects in the Fabric Manager database
- remove selected objects from the Fabric Manager database
- clean up the entire database

The first two options allow you to selectively administer specific items in the database, and the third option does a widespread cleanup of old items.

To clean up the Fabric Manager database, follow this procedure:

Step 1 On the Fabric Manager Maintenance menu (the screwdriver icon on the Fabric Manager toolbar), click the Clean Up Database option to display the Cleanup Database dialog, as shown in Figure 29.



Cleanup Database

Deleted Items

Name	Type
Management	Network Cloud
Vmotion	Network Cloud
mlathe	Network Cloud
Cam1	Network Cloud
vmotion	Network Cloud
dellSB19	I/O Template
cloud9template_3...	I/O Template
cloud9template_f...	I/O Template
Pubstemplate1_1...	I/O Template
EnglOtemplate_d...	I/O Template

Figure 29 Cleanup Database

Step 2 From the dialog, select one or more objects that you want to clean up in the database.

Step 3 Click either of the following options:

- Restore Selected, to restore an earlier version of the selected item in the current Fabric Manager database.
- Flush Selected Items, to clear the selected items out of the database. This option is useful for uncluttering the database of old objects that are left over.

Step 4 As an option, you can click Cleanup Database to have Oracle Fabric Manager programmatically cleanup everything that it can.

Working with Fabric Manager Jobs 63

This chapter contains the following topics:

- Understanding Jobs
- Displaying the Jobs Summary

Understanding Jobs

Oracle Fabric Manager is a client-server software bundle that enables you to configure server and virtual I/O needs based on an application's or network's needs.

- The Fabric Manager Server accepts configuration and management inputs from the Fabric Manager Client, then relays that information to Oracle Fabric Directors.
- Fabric Manager also retrieves information from Oracle Fabric Director(s), host servers, and other devices in the network and relays that information to the Fabric Manager Client.

Each time you click to submit a configuration or management task that has multiple steps, you create a job, which is the requested configuration action. Jobs are always asynchronous, but jobs can be either quick or long-running. All jobs in Fabric Manager are displayed in one of two locations:

- the Jobs Summary
- the Recent Jobs Summary

Jobs Summary

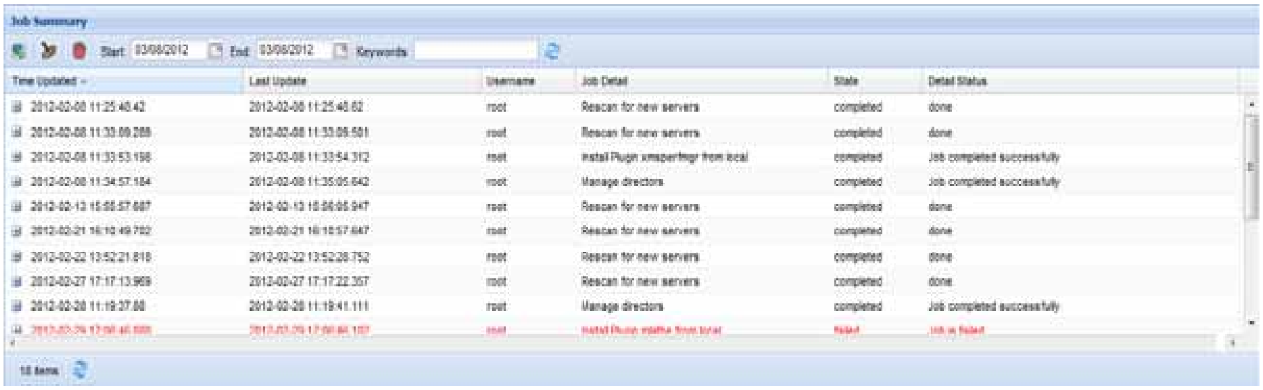
The Jobs summary shows a list of all jobs that have occurred recently. The Jobs Summary contains all the most recent jobs, to a maximum of the last 30 jobs. Jobs are displayed in the Jobs Summary regardless of whether they completed successfully or not.

Note

You can use the Jobs Summary to retrieve information about whether a feature is in the process of being configured, or if the job has stalled. Depending on the message displayed in the Jobs Summary, you might find it helpful to use this information if you have to contact Xsigo Technical Support.

The Jobs Summary also contains sub-jobs which are an expandable option for each completed job in the Jobs Summary. By clicking the plus sign (+) to expand the primary job, you display the sub-jobs for that primary job. Through the sub-jobs you can see more granular information about step-by-step tasks that comprise the primary job.

Figure 1 shows the Jobs Summary. Notice that a few of the primary jobs have been expanded to display their sub-jobs.



Job Summary

Start: 03/08/2012 End: 03/08/2012 Keywords:

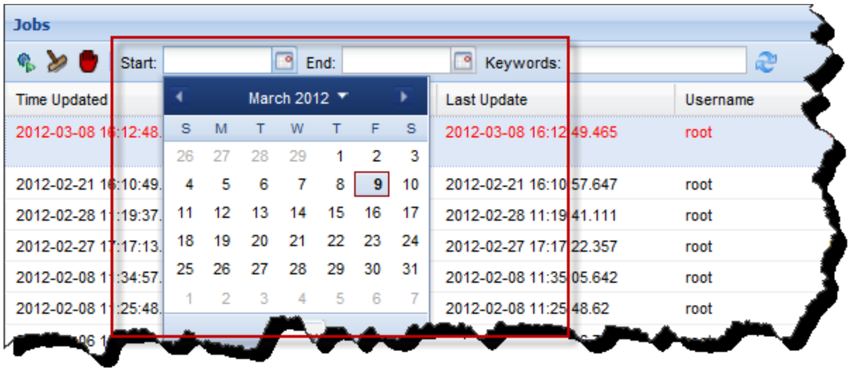
Time Updated	Last Update	Username	Job Detail	State	Detail Status
2012-02-08 11:25:40.42	2012-02-08 11:25:40.62	root	Rescan for new servers	completed	done
2012-02-08 11:33:09.288	2012-02-08 11:33:09.581	root	Rescan for new servers	completed	done
2012-02-08 11:33:53.158	2012-02-08 11:33:54.312	root	Install Plugin xmsperfmgr from local	completed	Job completed successfully
2012-02-08 11:34:57.184	2012-02-08 11:35:05.642	root	Manage directors	completed	Job completed successfully
2012-02-13 15:55:57.687	2012-02-13 15:56:05.947	root	Rescan for new servers	completed	done
2012-02-21 16:10:49.702	2012-02-21 16:10:57.647	root	Rescan for new servers	completed	done
2012-02-22 13:52:21.818	2012-02-22 13:52:28.752	root	Rescan for new servers	completed	done
2012-02-27 17:17:13.969	2012-02-27 17:17:22.357	root	Rescan for new servers	completed	done
2012-02-28 11:19:27.88	2012-02-28 11:19:41.111	root	Manage directors	completed	Job completed successfully
2012-02-29 17:00:46.[illegible]	2012-02-29 17:00:48.[illegible]	root	Install Plugin [illegible] from local	failed	Job is failed

18 items

Figure 1 Jobs Summary

The Jobs Summary lists jobs by the timestamp at which the job was started. Jobs are listed in sequential order with the most recent jobs at the top of the Job Summary. The Jobs Summary contains a maximum of 30 jobs.

The Jobs Summary contains a calendar tool which allows you to select a date or date range as a filter for the Jobs Summary's contents. By selecting a date or date range, you can display any jobs that occurred at that time. All alarms that do not match the date criteria are not displayed. When using the calendar tool, the filtered content should be displayed after you select the date or date range. However, you can always click the ***Refresh*** button to display the filtered content in the Jobs Summary. Figure 2 shows an example of the date range and calendar tool.



Time Updated	Last Update	Username
2012-03-08 16:12:48.	2012-03-08 16:12:49.465	root
2012-02-21 16:10:49.	2012-02-21 16:10:57.647	root
2012-02-28 11:19:37.	2012-02-28 11:19:41.111	root
2012-02-27 17:17:13.	2012-02-27 17:17:22.357	root
2012-02-08 11:34:57.	2012-02-08 11:35:05.642	root
2012-02-08 11:25:48.	2012-02-08 11:25:48.62	root

Figure 2 Jobs Summary — Date Range and Calendar Tool

Also, the Jobs Summary contains a keyword search function. The *Keywords* field enables additional filtering of the Jobs Summary by allowing you to enter specific words or phrases to filter the contents of the Jobs Summary. For example, you could enter "cre" to filter the Jobs Summary to display all "create" jobs. The keywords you enter are matched against the characters in the Job Description field.

Table 1 shows the fields in the Job Summary and explains what each field means.

Table 1 Contents of the Job Summary

Field	Indicates
Time Updated	The timestamp at which the job was completed. For primary jobs with sub-jobs, this field also indicates when each of the sub-jobs was attempted.
Last Update	The last timestamp that any activity occurred for the primary job.
Username	The name (if available) of the logged in user or administrator that initiated the job.

Table 1 (continued) Contents of the Job Summary

Field	Indicates
Job Detail	A string that provides additional details (if any) for the requested job and the object associated with that job. For example, the string "ApplyIOProfile 'pubstest' indicates that Fabric Manager is attempting to apply (bind) the I/O Profile named "pubstest" to one or more physical servers. The server name is also displayed if known.
State	The current state of the job, either complete, pending, or failed.
Detail Status	A string that summarizes the requested job and the object associated with that job. For example, the string "Successfully Applied IOProfile" indicates that Fabric Manager has successfully applied (bound) an I/O Profile to one or more physical servers.

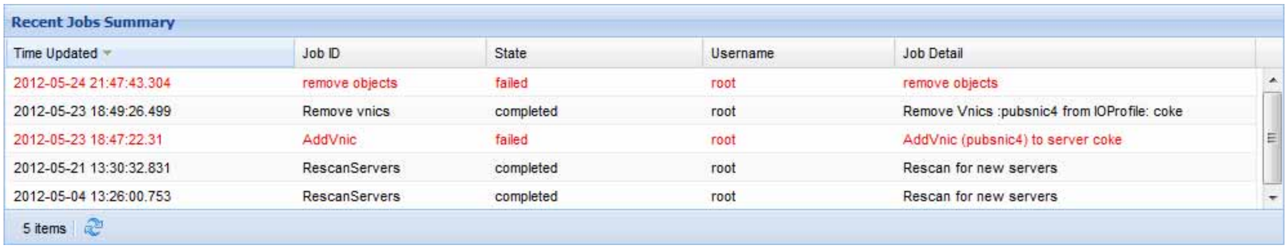
Recent Jobs Summary

On the page for each feature, you can see information about the 5 most recent jobs that occurred from any page in Fabric Manager. The Recent Jobs Summary is at the bottom of a feature or device's page.

Note

You can use the Recent Jobs Summary to retrieve information about whether a feature is in the process of being configured, or if the job has stalled. Depending on the message displayed in the Recent Jobs Summary, you might find it helpful to use this information if you have to contact Xsigo Technical Support.

The Recent Jobs Summary is related to the Jobs Summary in that clearing the Jobs Summary also clears the Recent Jobs frame. Figure 3 shows an example of the Recent Jobs frame.



Recent Jobs Summary

Time Updated	Job ID	State	Username	Job Detail
2012-05-24 21:47:43.304	remove objects	failed	root	remove objects
2012-05-23 18:49:26.499	Remove vnics	completed	root	Remove Vnics :pubsnic4 from IOProfile: coke
2012-05-23 18:47:22.31	AddVnic	failed	root	AddVnic (pubsnic4) to server coke
2012-05-21 13:30:32.831	RescanServers	completed	root	Rescan for new servers
2012-05-04 13:26:00.753	RescanServers	completed	root	Rescan for new servers

5 items

Figure 3 Sample Recent Jobs Summary

Table 2 shows the contents of the Recent Jobs Summary and explains what each field means.

Table 2 Contents of the Recent Jobs Summary

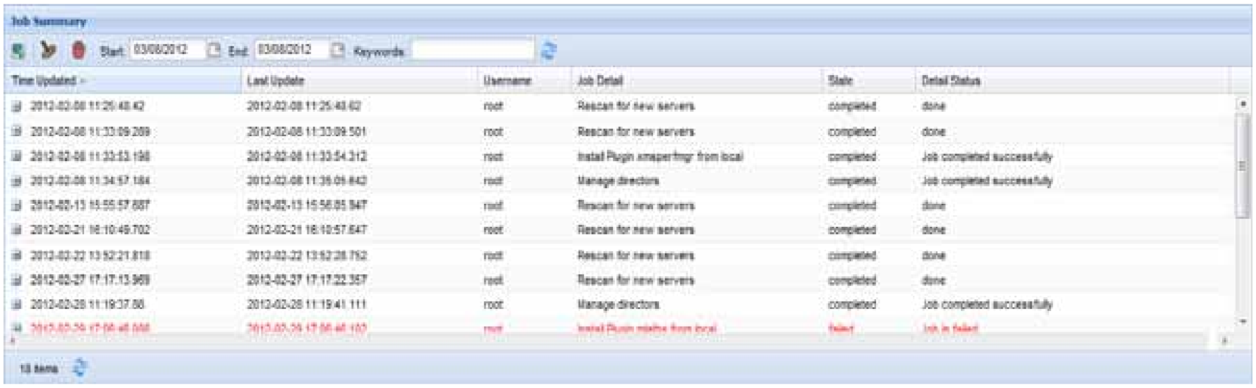
Field	Indicates
Time Updated	The timestamp at which the job was either started, restarted, completed, or failed.
Job ID	A string that summarizes the requested job and the object associated with that job. For example, the string “ApplyIOProfile” indicates that Fabric Manager is attempting to apply (bind) an I/O Profile to one or more physical servers.
State	The current state of the job, either complete, pending, or failed.
User Name	The name (if available) of the logged in user or administrator that initiated the job.
Job Detail	A string that provides additional details (if any) for the requested job and the object associated with that job. For example, the string “ApplyIOProfie ‘pubstest’ indicates that Fabric Manager is attempting to apply (bind) the I/O Profile named “pubstest” to one or more physical servers. The server name(s) is also displayed if known.

Displaying the Jobs Summary

The Jobs Summary contains a table of all the jobs that Fabric Manager has attempted regardless of their state, success, or failure. The Jobs Summary contains all jobs and lists summary information. Fabric Manager does not have a separate Details frame for each of the jobs in the Jobs Summary.

To display the Jobs Summary, follow this procedure:

Step 1 On the Navigation Frame, select *General->Jobs Status* to display the Jobs Summary. Figure 4 shows the Jobs Summary.



Time Updated	Last Update	Username	Job Detail	State	Detail Status
2012-02-08 11:25:48.42	2012-02-08 11:25:48.62	root	Rescan for new servers	completed	done
2012-02-08 11:33:09.289	2012-02-08 11:33:09.501	root	Rescan for new servers	completed	done
2012-02-08 11:33:53.198	2012-02-08 11:33:54.312	root	Install Plugin xmeperfmgr from local	completed	Job completed successfully
2012-02-08 11:34:57.184	2012-02-08 11:35:09.842	root	Manage directors	completed	Job completed successfully
2012-02-13 15:55:57.887	2012-02-13 15:56:05.947	root	Rescan for new servers	completed	done
2012-02-21 16:10:49.702	2012-02-21 16:10:57.647	root	Rescan for new servers	completed	done
2012-02-22 13:52:21.818	2012-02-22 13:52:28.752	root	Rescan for new servers	completed	done
2012-02-27 17:17:13.969	2012-02-27 17:17:22.357	root	Rescan for new servers	completed	done
2012-02-28 11:19:37.88	2012-02-28 11:19:41.111	root	Manage directors	completed	Job completed successfully
2012-02-29 17:06:46.[illegible]	2012-02-29 17:06:46.[illegible]	root	Install Plugin [illegible] from local	failed	Job is failed

Figure 4 Jobs Summary

The Jobs Summary supports the following options:

- Showing All Jobs
- Showing All Active Jobs

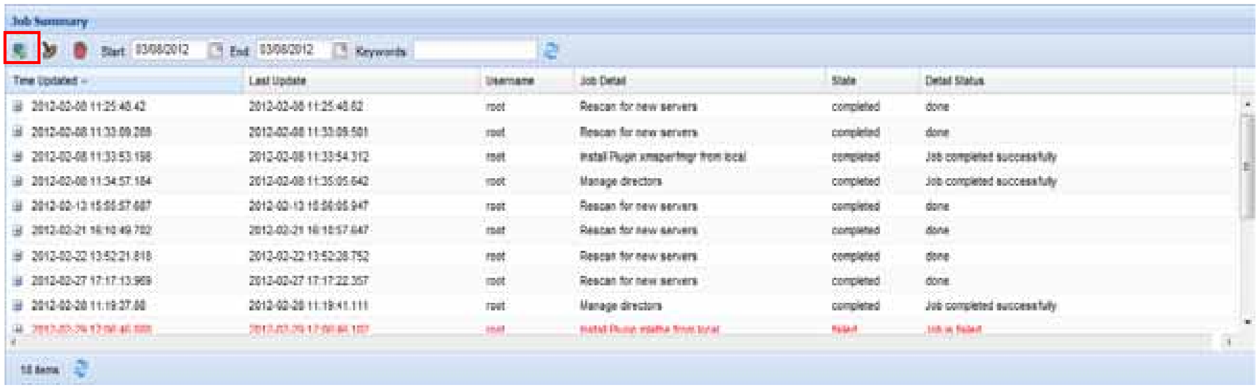
- Clearing All Jobs in the Jobs Summary
- Cancelling Selected Jobs in the Jobs Summary

Showing All Jobs

Jobs in the Jobs Summary are all jobs that have been attempted regardless of state. As a result, jobs that are in any state are displayed.

To filter the active jobs in the Jobs Summary, follow this procedure:

Step 1 On the Navigation Frame, select *General->Jobs Status* to display the Jobs Summary. Figure 5 shows the Jobs summary.



Time Updated	Last Update	Username	Job Detail	State	Detail Status
2012-02-08 11:25:48.42	2012-02-08 11:25:48.62	root	Rescan for new servers	completed	done
2012-02-08 11:33:09.288	2012-02-08 11:33:09.501	root	Rescan for new servers	completed	done
2012-02-08 11:33:53.198	2012-02-08 11:33:54.312	root	install Plugin xmsperfmgr from local	completed	Job completed successfully
2012-02-08 11:34:57.184	2012-02-08 11:35:05.642	root	Manage directors	completed	Job completed successfully
2012-02-13 15:55:57.687	2012-02-13 15:56:05.947	root	Rescan for new servers	completed	done
2012-02-21 16:10:49.702	2012-02-21 16:10:57.647	root	Rescan for new servers	completed	done
2012-02-22 13:52:21.818	2012-02-22 13:52:28.752	root	Rescan for new servers	completed	done
2012-02-27 17:17:13.969	2012-02-27 17:17:22.357	root	Rescan for new servers	completed	done
2012-02-28 11:19:27.88	2012-02-28 11:19:41.111	root	Manage directors	completed	Job completed successfully
[illegible]	[illegible]	root	install Plugin [illegible] from local	failed	Job is failed

Figure 5 Jobs Summary

Step 2 On the Jobs Status summary, click the ***Show All Active Jobs*** button, as shown in Jobs Summary.

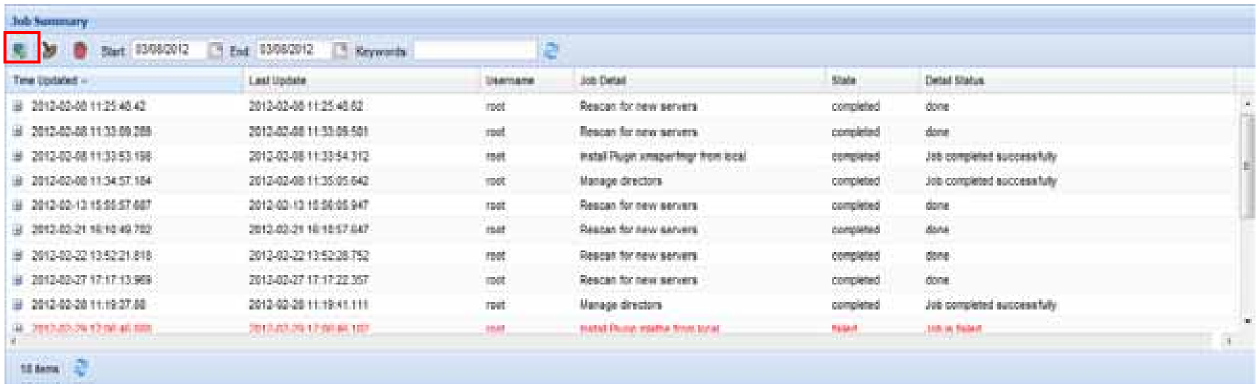
When you click the ***Show All Jobs*** button, the Jobs Status Summary is filtered to display only the jobs with “active” state. This button is a toggle, so clicking repeatedly switches between displaying all active jobs and all jobs (including non-active ones). You will notice that the button changes when it toggles between ***Show All Jobs*** and ***Show All Active Jobs***.

Showing All Active Jobs

The Jobs Summary shows all jobs that have been attempted regardless of state. As a result, jobs that are in any state are displayed. You can filter the Jobs Summary to display all active jobs, which are jobs that are currently in progress. Be aware that jobs can take a while to complete based on the number of subjobs that are contained in the parent job. For example, if you attempt to unbind a Server Profile from a server, that job might contain individual subjobs for removing the vNICs and vHBAs that are connected to the host. While those subjobs are completing, the overall unbind job will still be active.

To filter the active jobs in the Jobs Summary, follow this procedure:

Step 1 On the Navigation Frame, select *General->Jobs Status* to display the Jobs Summary. Figure 6 shows the Jobs summary.



Job Summary

Start 03/08/2012 End 03/08/2012 Keywords

Time Updated	Last Update	Username	Job Detail	State	Detail Status
2012-02-08 11:25:40.42	2012-02-08 11:25:40.62	root	Rescan for new servers	completed	done
2012-02-08 11:33:09.288	2012-02-08 11:33:09.581	root	Rescan for new servers	completed	done
2012-02-08 11:33:53.198	2012-02-08 11:33:54.312	root	install Plugin xmspertmgr from local	completed	Job completed successfully
2012-02-08 11:34:57.184	2012-02-08 11:35:05.642	root	Manage directors	completed	Job completed successfully
2012-02-13 15:55:57.687	2012-02-13 15:56:05.947	root	Rescan for new servers	completed	done
2012-02-21 16:10:49.702	2012-02-21 16:18:57.647	root	Rescan for new servers	completed	done
2012-02-22 13:52:21.818	2012-02-22 13:52:28.752	root	Rescan for new servers	completed	done
2012-02-27 17:17:13.969	2012-02-27 17:17:22.357	root	Rescan for new servers	completed	done
2012-02-28 11:19:27.88	2012-02-28 11:19:41.111	root	Manage directors	completed	Job completed successfully
[illegible]	[illegible]	root	install Plugin [illegible] from local	failed	Job is failed

18 items

Figure 6 Jobs Summary

Step 2 On the Jobs Status summary, click the ***Show All Active Jobs*** button, as shown in Jobs Summary.

When you click the ***Show All Active Jobs*** button, the Jobs Status Summary is filtered to display only the jobs with “active” state. This button is a toggle, so clicking repeatedly switches between displaying all active jobs and all jobs (including non-active ones). You will notice that the button changes when it toggles between ***Show All Jobs*** and ***Show All Active Jobs***.

Clearing All Jobs in the Jobs Summary

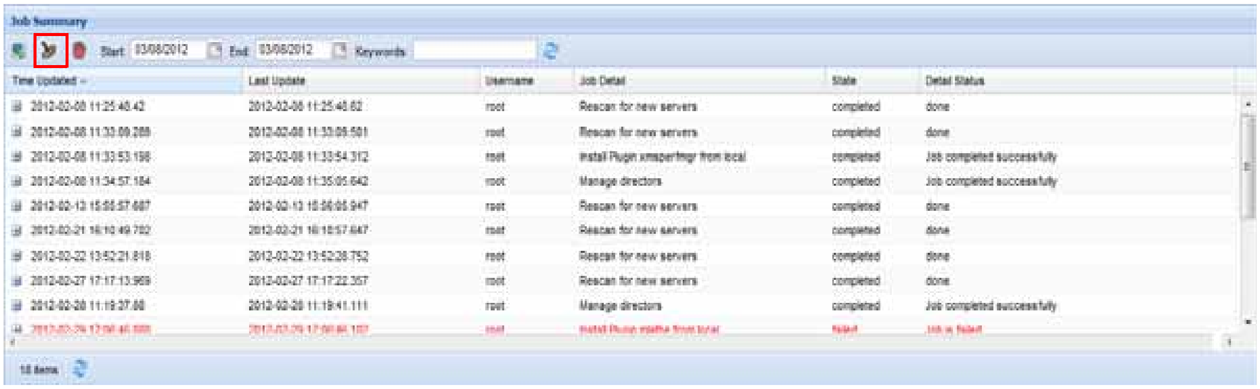
Jobs are persistent across reboot, and Fabric Manager service restarts:

- Jobs are kept in the Jobs Summary until they are explicitly batch removed.
- Jobs are not aged out, or removed when a pending job completes.
- Jobs can be cleared only by removing them as a batch by an administrator-level account.
- Individual jobs cannot be removed. Jobs must be explicitly removed as a batch by an administrator.

When you clear the jobs in the Jobs Summary, you are removing all completed or failed jobs only. Jobs that are in any other state are not cleared.

To clear all Jobs from the Jobs Summary, follow this procedure:

Step 1 On the Navigation Frame, select *General->Jobs Status* to display the Jobs Summary. Figure 7 shows the Jobs Summary.



Job Summary

Time Updated	Last Update	Username	Job Detail	State	Detail Status
2012-02-08 11:25:40.42	2012-02-08 11:25:40.62	root	Rescan for new servers	completed	done
2012-02-08 11:33:09.288	2012-02-08 11:33:09.501	root	Rescan for new servers	completed	done
2012-02-08 11:33:53.198	2012-02-08 11:33:54.312	root	Install Plugin xmsperfmgr from local	completed	Job completed successfully
2012-02-08 11:34:57.184	2012-02-08 11:35:05.642	root	Manage directors	completed	Job completed successfully
2012-02-13 15:05:57.687	2012-02-13 15:06:05.947	root	Rescan for new servers	completed	done
2012-02-21 16:10:49.702	2012-02-21 16:10:57.647	root	Rescan for new servers	completed	done
2012-02-22 13:52:21.818	2012-02-22 13:52:28.752	root	Rescan for new servers	completed	done
2012-02-27 17:17:13.969	2012-02-27 17:17:22.357	root	Rescan for new servers	completed	done
2012-02-28 11:19:27.88	2012-02-28 11:19:41.111	root	Manage directors	completed	Job completed successfully
2012-02-29 17:00:40.[illegible]	2012-02-29 17:00:40.107	root	Install Plugin [illegible] from local	failed	Job is failed

10 items

Figure 7 Jobs Summary

Step 2 Click the eraser icon to remove all jobs from the Job Summary. The Job Summary will be repopulated when the next administration or configuration tasks are submitted.

Cancelling Selected Jobs in the Jobs Summary

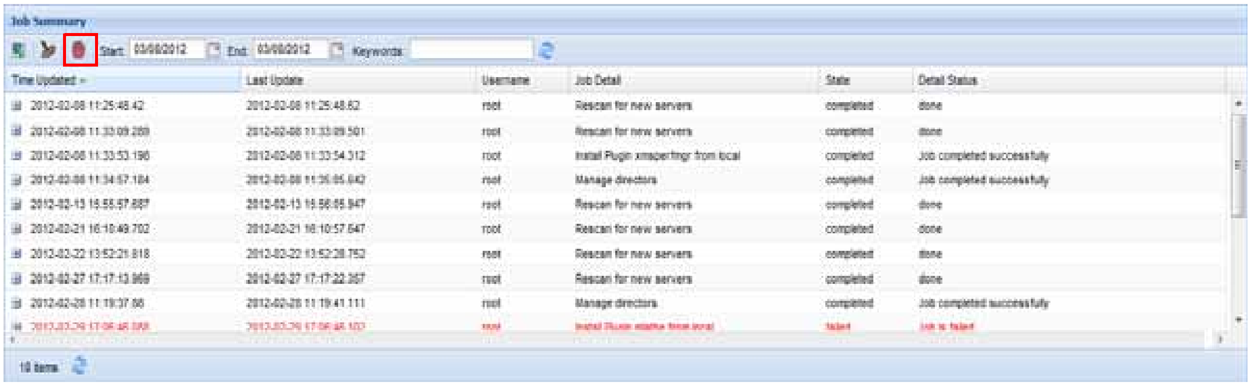
Some jobs in Oracle Fabric Manager can be long running. For example, applying an I/O Profile to many servers can take a significant amount of time. While a job is running, you can cancel it before completion, regardless of what stage the job is in.

Through the Jobs Summary, you can cancel any of the jobs that are still in process. By cancelling a job, you cause it to completely stop. For example, if you apply an I/O Profile to a server, and the job shows as `running` or `pending` in the Job Summary, you can cancel the job to stop the I/O Profile from being applied to the server. Cancelling a job simply stops it. The job is not cleaned up and removed from the Jobs Summary.

Unlike the Undo Jobs function, there is no limit on the type of job that can be cancelled. The only requirement for cancelling a job is that the job state is either running or pending.

To cancel a job, follow this procedure:

Step 1 On the Navigation Frame, select *General->Jobs Status* to display the Jobs Summary. Figure 8 shows the Jobs Summary.



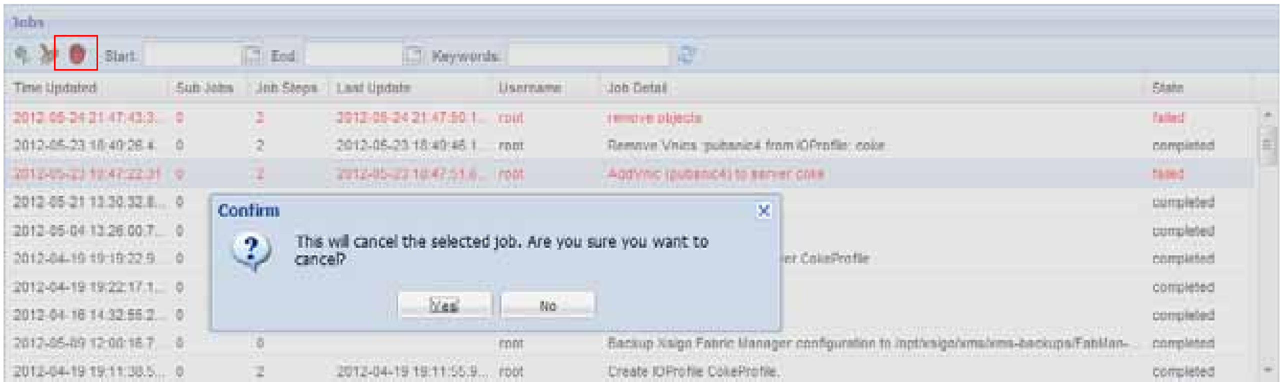
Time Updated	Last Update	Username	Job Detail	State	Detail Status
2012-02-08 11:25:48.42	2012-02-08 11:25:48.62	root	Rescan for new servers	completed	done
2012-02-08 11:33:09.289	2012-02-08 11:33:09.501	root	Rescan for new servers	completed	done
2012-02-08 11:33:53.196	2012-02-08 11:33:54.312	root	Install Plugin xmsperfmgr from local	completed	Job completed successfully
2012-02-08 11:34:57.184	2012-02-08 11:35:05.642	root	Manage directors	completed	Job completed successfully
2012-02-13 15:55:57.887	2012-02-13 15:56:05.947	root	Rescan for new servers	completed	done
2012-02-21 16:10:49.702	2012-02-21 16:10:57.647	root	Rescan for new servers	completed	done
2012-02-22 13:52:21.818	2012-02-22 13:52:28.752	root	Rescan for new servers	completed	done
2012-02-27 17:17:13.969	2012-02-27 17:17:22.357	root	Rescan for new servers	completed	done
2012-02-28 11:19:37.86	2012-02-28 11:19:41.111	root	Manage directors	completed	Job completed successfully
2012-02-29 17:06:46.[illegible]	2012-02-29 17:06:46.[illegible]	root	Install Plugin [illegible] from local	failed	Job is failed

Figure 8 Jobs Summary

Step 2 Select a running or pending job that you want to cancel. You can check the *State* column to verify that the job you want to cancel is either running or pending.

When you select a valid, cancellable job, the ***Cancel Jobs*** button becomes active.

Step 3 When a valid job is selected, click the ***Cancel Jobs*** button.When you click the button, a confirmation dialog is displayed, as shown in Figure 9.



This will cancel the selected job. Are you sure you want to cancel?

Time Updated	Sub Jobs	Job Steps	Last Update	Username	Job Detail	State
2012-05-24 21:47:43.3...	0	2	2012-05-24 21:47:50.1...	root	remove objects	failed
2012-05-23 18:40:26.4	0	2	2012-05-23 18:40:46.1...	root	Remove Vnics :pubanic4 from IOProfile: coke	completed
2012-05-23 18:47:22.31	0	2	2012-05-23 18:47:51.6...	root	AddVnic (pubanic4) to server coke	failed
2012-05-21 13:30:32.8...	0					completed
2012-05-04 13:26:00.7...	0					completed
2012-04-19 19:19:22.5	0				...er CokeProfile	completed
2012-04-19 19:22:17.1...	0					completed
2012-04-16 14:32:56.2...	0					completed
2012-05-09 12:00:16.7	0	0		root	Backup Xsigo Fabric Manager configuration to /opt/xsigo/xms/xms-backups/FabMan-...	completed
2012-04-19 19:11:38.5...	0	2	2012-04-19 19:11:55.9...	root	Create IOProfile CokeProfile.	completed

Figure 9 Jobs Summary — Confirmation of Cancel Jobs

Step 4 On the confirmation dialog, click ***Yes*** to proceed with the Undo function. Allow the undo job to run to completion, which might take some time.

While the job is being undone, the text of the selected job will turn green to indicate the success of the undo.

Step 5 When the undo is complete, check the State column in the Jobs Summary again for a message about the undo function.

Working with Network Clouds

This chapter contains the following topics:

Understanding a Network Cloud

Oracle's Xsigo Fabric Directors contain a set of I/O ports that are connected to your data center network. The network and SAN administrator connect these ports to their Ethernet switches in order to provide I/O resources to the servers.

Each I/O port on the Xsigo system can be thought of as providing access to a set of "clouds." For example, you might have a Network Cloud that provides access to the HR network. As far as the network administrator is concerned, you are connecting wires to the Xsigo I/O ports for the sole purpose of providing the server administrator access to the resources.

The server administrator then needs to connect servers to a set of network resources provided by the network administrators. The server administrator doesn't care what physical Xsigo ports are being connected to as long as the servers have access to the required resources.

Network Clouds can be configured and managed by Network and Administrator roles in Oracle's Xsigo Fabric Manager.

Network QoS Profiles and Network Clouds

If you want a specific Network QoS Profile assigned to the Network Cloud, that specific profile must already exist. If it does not exist, it will not be assignable to the Network Cloud at the time you create the cloud.

As an alternative, Fabric Manager has some commonly used network QoS Profiles that are pre-configured for various network link speeds. These pre-configured Network QoS Profiles use typical CIR and PIR values calculated from the link's total throughput. If you are using pre-configured Network QoS Profiles, make sure that you use a reasonable profile. For example, for a 1 Gigabit Ethernet link, do not select a network QoS profile for a 10 Gigabit Ethernet link (for example, the Network QoS profile named `7g_10g` which has throughput values that are in excess of what the 1 Gigabit link can support).

Network QoS can be configured for a Network Cloud at any of the following times:

- During Network Cloud creation, through the Create Network Cloud wizard.
- After the Network Cloud has already been created, through the Network Cloud Details frame.
- Network QoS can also be changed for a Network Cloud after the Network Cloud has already been created. Changing an assigned Network QoS Profile occurs through the Network Cloud Details frame.

QoS Assignment at Cloud Level and vNIC Level

It is possible to assign Network QoS to a Network Cloud or a vNIC. The following text explains what QoS is applied where:

- If a Network Cloud has a QoS Profile associated with it, a vNIC terminated in the Network Cloud will inherit the Network QoS profile from the Network Cloud.

  In this case, the vNICs inherit the QoS parameters from their respective clouds. This condition is true even if the vNIC has its own QoS Profile associated with it.
- If a Network Cloud has no QoS Profile associated with it, and the vNICs have their own QoS profiles, a vNIC terminated in the Network Cloud will have QoS Profile associated with it.

  In this case, the Network Cloud has no QoS Profile to apply. This situation *does not* automatically apply no QoS to the vNICs. Instead, it causes the cloud to defer to the QoS profiles assigned to the individual vNICs (if any).

  If you intend for no QoS to be applied anywhere for the virtual I/O in a cloud, make sure that no QoS Profile is associated with the Network Cloud, and also that no QoS is associated with the vNIC.

Creating a Network Cloud

When you create a Network Cloud, you assign one or more Ethernet ports or LAGs, plus other network characteristics. When the Network Cloud is attached to an I/O Template, the Network Cloud provides a way for vNICs to connect hosts to the data network when an I/O Profile is deployed to the host. The Network Cloud provides needed network access points with specified characteristics—for example, Network QoS profiles, VLANs, and so on.

A default Network Cloud exists, which contains all the discovered Ethernet ports available to Fabric Manager through the discovered Fabric Director(s). This default Network Cloud is a way to show you the total number of termination points that are under management by Fabric Manager. The total number shown does not decrement when ports are assigned to a specific Network Cloud, since those ports have not been removed from Fabric Manger—they are just reassigned to a different object.

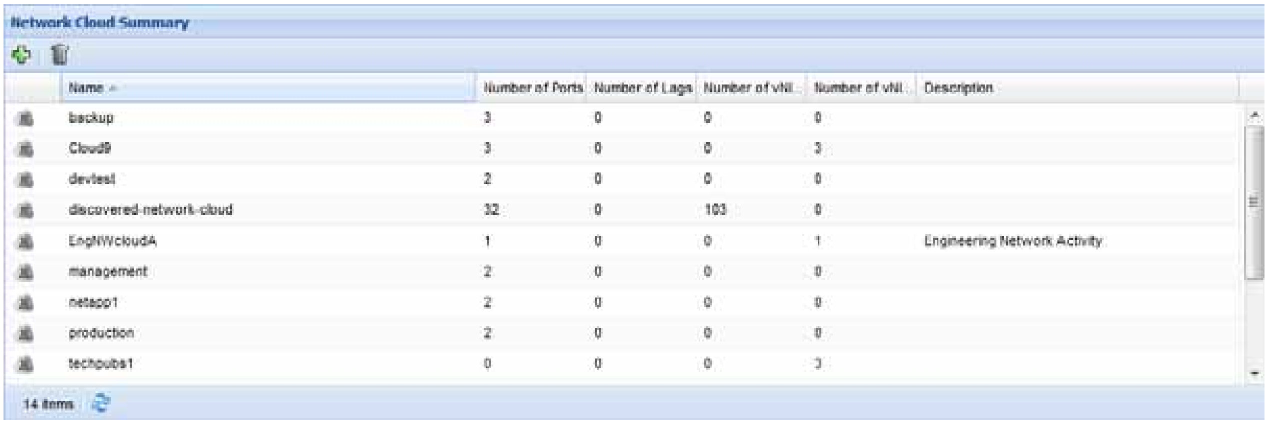
Network Clouds typically are created around some similar theme for the ports or LAGs that are associated with it. For example, a Network Cloud might have ports or LAGs that will provide vNIC connections to a specific domain or specific upstream Ethernet switch, for a specific set of host servers.

Creating a Network Cloud occurs through the Network Cloud option in the Network Resources Manager on the navigation panel.

The following example shows creating a Network Cloud for a single Fabric Director. However, in most cases, Fabric Directors are deployed as redundant pairs, which has a minor difference in the properties you will set for the Network Cloud. For more information about deploying Fabric Director pairs, see Setting the Fabric Director HA Designation for a Network Cloud.

To create a Network Cloud, follow this procedure:

Step 1 On the Navigation panel, select *Network Cloud Manager->Network Clouds* to display the Network Cloud Summary. Figure 1 shows this page.



Network Cloud Summary

Name	Number of Ports	Number of Lags	Number of vNI...	Number of vNI...	Description
backup	3	0	0	0	
Cloud9	3	0	0	3	
devtest	2	0	0	0	
discovered-network-cloud	32	0	103	0	
EngNWcloudA	1	0	0	1	Engineering Network Activity
management	2	0	0	0	
netapp1	2	0	0	0	
production	2	0	0	0	
techpubs1	0	0	0	3	

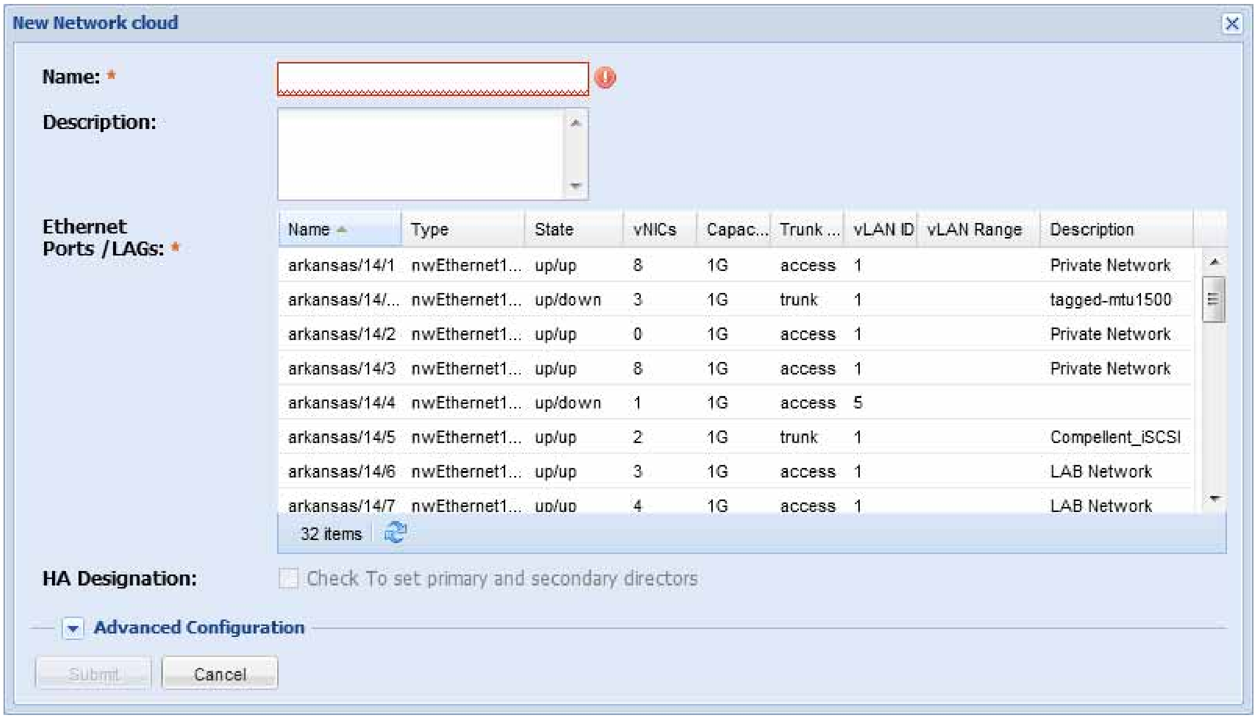
14 items

Figure 1 Network Cloud Summary

Notice the default Network Cloud (discovered-network-cloud) in this example. This example also shows that specific Network Clouds (non-default clouds) are configured.

Adding and deleting Network Clouds occurs through the plus sign and garbage can icons, respectively.

Step 2 Click the plus sign (+) to display the Add a New Network Cloud dialog. Figure 2 shows this dialog.



New Network cloud

Name: *

Description:

Ethernet Ports / LAGs: *

Name	Type	State	vNICs	Capac...	Trunk ...	vLAN ID	vLAN Range	Description
arkansas/14/1	nwEthernet1...	up/up	8	1G	access	1		Private Network
arkansas/14/...	nwEthernet1...	up/down	3	1G	trunk	1		tagged-mtu1500
arkansas/14/2	nwEthernet1...	up/up	0	1G	access	1		Private Network
arkansas/14/3	nwEthernet1...	up/up	8	1G	access	1		Private Network
arkansas/14/4	nwEthernet1...	up/down	1	1G	access	5		
arkansas/14/5	nwEthernet1...	up/up	2	1G	trunk	1		Compellent_iSCSI
arkansas/14/6	nwEthernet1...	up/up	3	1G	access	1		LAB Network
arkansas/14/7	nwEthernet1...	up/up	4	1G	access	1		LAB Network

32 items

HA Designation: □ Check To set primary and secondary directors

Figure 2 New Network Cloud

Step 3 In the *Name* field, enter a name for the Network Cloud that you are creating.

Step 4 As an option, in the *Description* field, enter a description for the Network Cloud that you are creating.

Step 5 From the *Ethernet Ports/LAGs* table, select the port(s) or LAGs that will be used in this Network Cloud. Ports and LAGs are selected when they are highlighted (as shown). Multiple ports and LAGs can be assigned to the same Network Cloud, and multiple Network Clouds can be assigned to the same port(s).

Step 6 If you are deploying two Fabric Directors as a redundant pair, you can use the HA Designation checkbox to specify which Fabric Director is the primary and which Fabric Director is the secondary. For more information about deploying Fabric Director pairs, see Setting the Fabric Director HA Designation for a Network Cloud.

Step 7 When the correct properties have been assigned for the Network Cloud, click ***Submit*** to create the Network Cloud.

Step 8 Check the Network Cloud Summary to verify that the Network Cloud was correctly configured.

Setting the Fabric Director HA Designation for a Network Cloud

In a typical deployment, redundant Fabric Directors are present, and the Network Cloud will be associated with both Fabric Directors. When you create a Network Cloud, Fabric Manager supports a simple and easy way to associate the Network Cloud with two Fabric Directors simultaneously, and also set the connection priority so that one Fabric Director is considered the primary and the other is considered the secondary. When you initially create the cloud, any HA vNICs must be manually connected to the cloud and their primary and secondary status must be manually set. However, after the Network Cloud is initially created, the Fabric Director connection priority is set. Any additional HA pairs that attach to the Network Cloud after the HA designation is made will first attach to the primary Fabric Director and then to the Secondary Fabric Director.

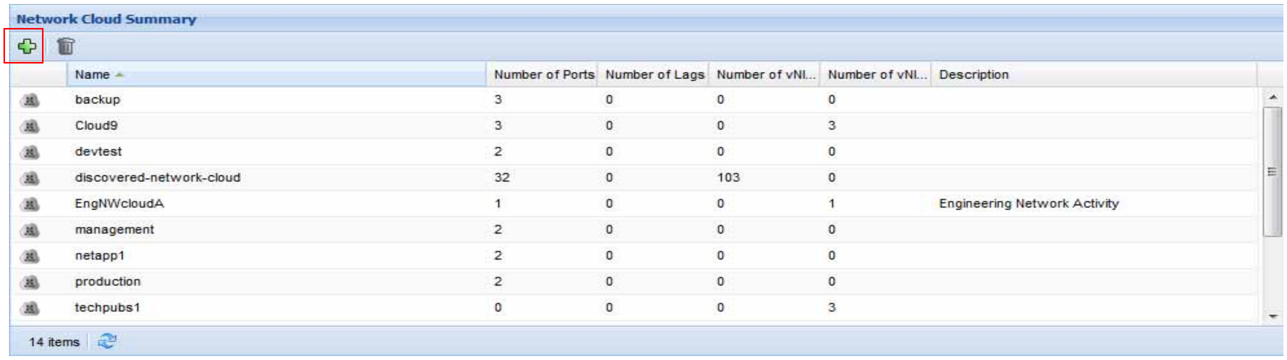
The HA Fabric Director designation is configured when you create the Network Cloud, and is available on the Create Network Cloud dialog.

When a host is discovered or connected to a Fabric Director that is discovered, Fabric Manager will query the Xsigo host drivers on the host for the capability to support HA vNICs. This reporting facilitates the creation of HA vNICs on hosts because some hosts do not support true HA vNICs. For example, ESX servers support NIC Teaming, which requires two individual vNICs instead of one HA vNIC.

- If the host driver reports that HA vNICs are available on the host, a Fabric Manager HA vNIC will create HA vNICs on the server.
- If the host driver reports that HA vNICs are not available on the host, a Fabric Manager HA vNIC will create a pair of single vNICs on the server.

To create a Network Cloud with HA, follow this procedure:

Step 1 Display the Network Cloud Summary (*Network Cloud Manager->Network Clouds*).



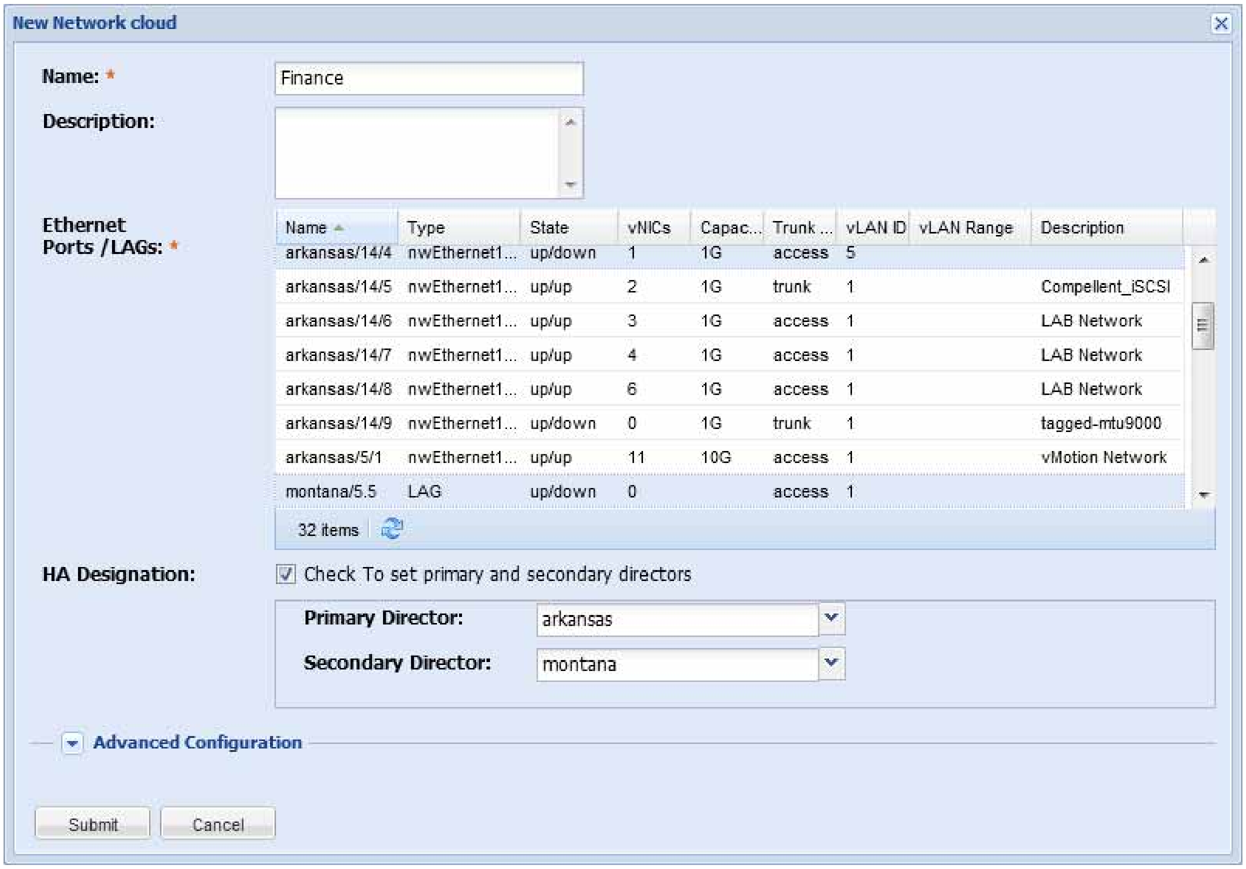
Network Cloud Summary

Name	Number of Ports	Number of Lags	Number of vNI...	Number of vNI...	Description
backup	3	0	0	0	
Cloud9	3	0	0	3	
devtest	2	0	0	0	
discovered-network-cloud	32	0	103	0	
EngNWcloudA	1	0	0	1	Engineering Network Activity
management	2	0	0	0	
netapp1	2	0	0	0	
production	2	0	0	0	
techpubs1	0	0	0	3	

14 items

Figure 3 Network Cloud Summary

Step 2 On the Network Cloud Summary, click the plus sign (+) to display the New Network Cloud dialog. Figure 4 shows this dialog.



New Network cloud

Name: *	Finance
Description:	

Ethernet Ports /LAGs: *

Name	Type	State	vNICs	Capac...	Trunk ...	vLAN ID	vLAN Range	Description
arkansas/14/4	nwEthernet1...	up/down	1	1G	access	5		
arkansas/14/5	nwEthernet1...	up/up	2	1G	trunk	1		Compellent_iSCSI
arkansas/14/6	nwEthernet1...	up/up	3	1G	access	1		LAB Network
arkansas/14/7	nwEthernet1...	up/up	4	1G	access	1		LAB Network
arkansas/14/8	nwEthernet1...	up/up	6	1G	access	1		LAB Network
arkansas/14/9	nwEthernet1...	up/down	0	1G	trunk	1		tagged-mtu9000
arkansas/5/1	nwEthernet1...	up/up	11	10G	access	1		vMotion Network
montana/5.5	LAG	up/down	0		access	1		

32 items

HA Designation: ☑ Check To set primary and secondary directors

Primary Director:	arkansas
Secondary Director:	montana

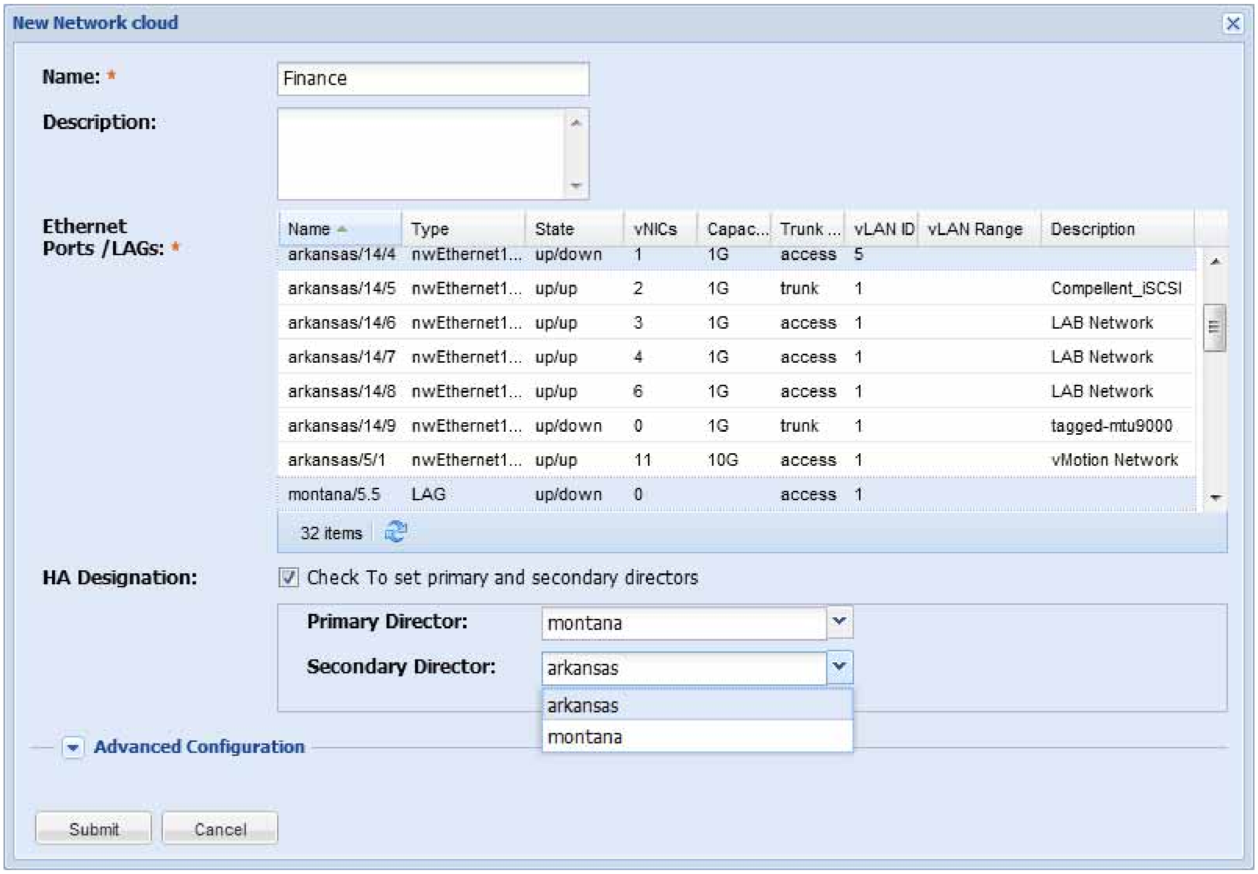
Figure 4 New Network Cloud

Step 3 In the *Name* field, enter a name for the Network Cloud that you are creating.

Step 4 As an option, in the *Description* field, enter a description for the Network Cloud that you are creating.

Step 5 From the *Ethernet Ports/LAGs* table, select at least one port or LAG from each Fabric Director that will be used in the redundant Fabric Director Network Cloud. When one port from two different Fabric Directors are selected, the *HA Designation* checkbox at the bottom of the dialog becomes active.

Step 6 In the *HA Designation* checkbox, click to specify that this is an HA Fabric Director configuration, and also to display the *Primary Director* and *Secondary Director* dropdown menus, as shown in Figure 5.



New Network cloud

Name: *	Finance
Description:	

Ethernet Ports /LAGs: *

Name	Type	State	vNICs	Capac...	Trunk ...	vLAN ID	vLAN Range	Description
arkansas/14/4	nwEthernet1...	up/down	1	1G	access	5		
arkansas/14/5	nwEthernet1...	up/up	2	1G	trunk	1		Compellent_iSCSI
arkansas/14/6	nwEthernet1...	up/up	3	1G	access	1		LAB Network
arkansas/14/7	nwEthernet1...	up/up	4	1G	access	1		LAB Network
arkansas/14/8	nwEthernet1...	up/up	6	1G	access	1		LAB Network
arkansas/14/9	nwEthernet1...	up/down	0	1G	trunk	1		tagged-mtu9000
arkansas/5/1	nwEthernet1...	up/up	11	10G	access	1		vMotion Network
montana/5.5	LAG	up/down	0		access	1		

32 items

HA Designation: ☑ Check To set primary and secondary directors

Primary Director: montana

Secondary Director: arkansas

Figure 5 New Network Cloud — HA Designation

Step 7 From the *Primary Director* dropdown menu, select which of the two Fabric Directors will be the primary. The primary is the Fabric Director to which the primary vNIC in an HA pair is connected first when new HA vNICs are connected to the Network Cloud.

Step 8 From the *Secondary Director* dropdown menu, select which of the two Fabric Directors will be the secondary. The secondary is the Fabric Director to which the secondary vNIC in an HA Pair is connected when new HA vNICs are connected to the Network Cloud.

Step 9 If you want to configure additional properties for the cloud (for example, a VLAN ID or network QoS Profile) continue to Configuring Advanced Features for a Network Cloud. Otherwise, you can complete the configuration of a basic network Cloud by proceeding to Step 10.

Step 10 When the correct properties have been assigned for the Network Cloud, click ***Submit*** to create the Network Cloud.

Step 11 Check the Network Cloud Summary to verify that the Network Cloud was correctly configured.

Configuring Advanced Features for a Network Cloud

Because Network Clouds contain Ethernet ports or LAGs, many standard features that are applicable to network ports and LAGs (for example, Network QoS) are configurable on Network Clouds. Network Clouds support configuration of the following features:

- Network QoS CIR and PIR values. (CBS and PBS values are calculated internally from the CIR and PIR values). The QoS parameters are associated with vNICs in the cloud by either having the cloud assign the Network QoS parameters, or by allowing the vNIC to have its own QoS parameters if the cloud itself has no Network QoS associated with it.
- VLAN properties. Any vNIC VLAN properties are inherited from the Network Cloud with which the vNIC is associated.
- Trunk Mode vNICs
- Private vNICs
- Port Allocation Policy in the Network Cloud

See the following sections for how to configure these features for the Network Cloud.

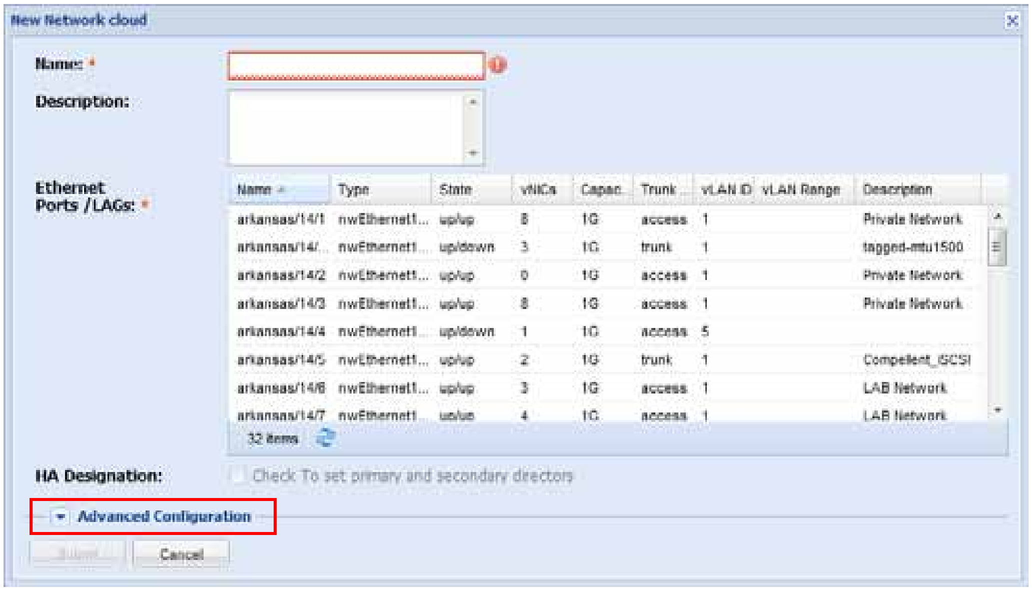
Setting Network QoS on a Network Cloud

Setting Network QoS on a Network Cloud can occur at the cloud level or at the vNIC level. When Network QoS is applied to a Network Cloud, all vNICs associated with the cloud will get the specified CIR and PIR values. If a vNIC also has Network QoS and is added to the Network Cloud, the cloud’s Network QoS takes precedence. For more information about Network QoS and Network Clouds, see Working with Network QoS.

The following procedure assumes that the Network QoS Profile already exists. If it does not, you will need to assign one of the pre-defined Network QoS Profiles that Xsigo has provided.

To configure Network QoS for a Network Cloud, follow this procedure:

Step 1 If the Create a Network Cloud dialog is not already displayed, display it now, as shown in Figure 6.



New Network cloud

Name: *

Description:

Ethernet Ports /LAGs: *

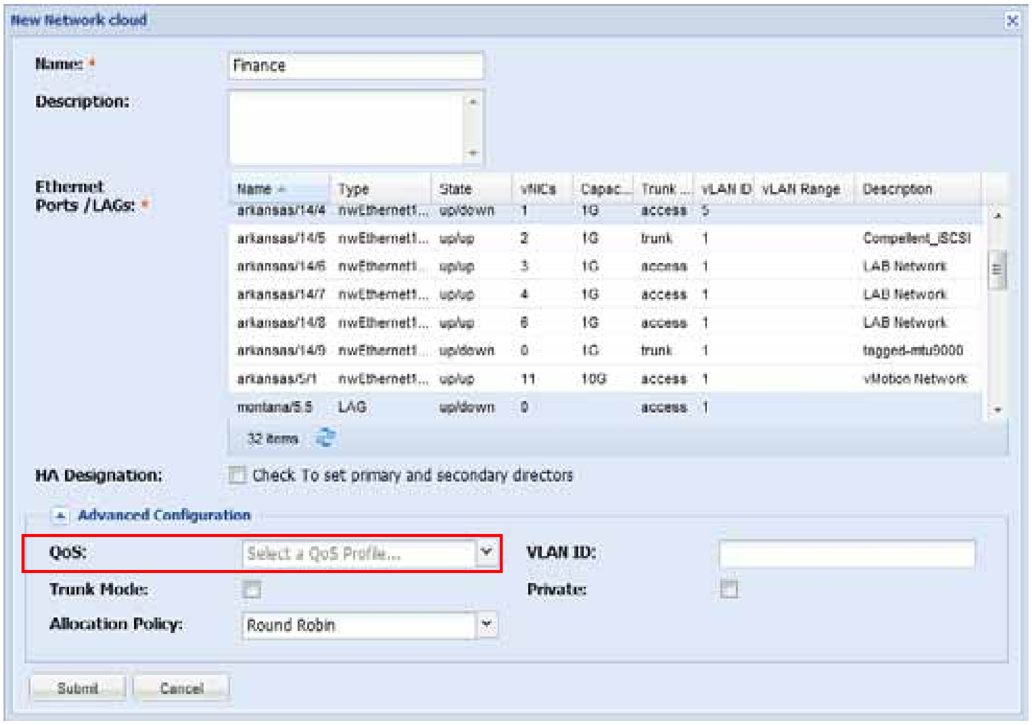
Name	Type	State	vNICs	Capac.	Trunk	vLAN ID	vLAN Range	Description
arkansas/14/1	nwEthernet1...	up/up	8	1G	access	1		Private Network
arkansas/14/...	nwEthernet1...	up/down	3	1G	trunk	1		tagged-mtu1500
arkansas/14/2	nwEthernet1...	up/up	0	1G	access	1		Private Network
arkansas/14/3	nwEthernet1...	up/up	8	1G	access	1		Private Network
arkansas/14/4	nwEthernet1...	up/down	1	1G	access	5		
arkansas/14/5	nwEthernet1...	up/up	2	1G	trunk	1		Compellent_iSCSI
arkansas/14/6	nwEthernet1...	up/up	3	1G	access	1		LAB Network
arkansas/14/7	nwEthernet1...	up/up	4	1G	access	1		LAB Network

32 items

HA Designation: □ Check To set primary and secondary directors

Figure 6 New Network Cloud

Step 2 Click the *Advanced Configuration* dropdown menu to display the additional properties for the Network Cloud. See Figure 7.



New Network cloud

Name: * Finance

Description:

Ethernet Ports /LAGs: *

Name	Type	State	vNICs	Capac...	Trunk ...	vLAN ID	vLAN Range	Description
arkansas/14/4	nwEthernet1...	up/down	1	1G	access	5		
arkansas/14/5	nwEthernet1...	up/up	2	1G	trunk	1		Compellent_iSCSI
arkansas/14/6	nwEthernet1...	up/up	3	1G	access	1		LAB Network
arkansas/14/7	nwEthernet1...	up/up	4	1G	access	1		LAB Network
arkansas/14/8	nwEthernet1...	up/up	6	1G	access	1		LAB Network
arkansas/14/9	nwEthernet1...	up/down	0	1G	trunk	1		tagged-mtu9000
arkansas/5/1	nwEthernet1...	up/up	11	10G	access	1		vMotion Network
montana/5.5	LAG	up/down	0		access	1		

32 items

HA Designation: □ Check To set primary and secondary directors

QoS: Select a QoS Profile...

VLAN ID:

Trunk Mode: □

Private: □

Allocation Policy: Round Robin

Figure 7 Network Cloud Details Frame

Step 3 From the *QoS* dropdown menu, select the new Network QoS Profile for the selected Network Cloud. Figure 7 shows selecting the new QoS Profile.

Step 4 Click ***Submit*** to assign the new Network QoS Profile to the selected Network Cloud. You will be prompted with a confirmation message.

Step 5 Click ***Yes*** to assign the Network QoS profile or ***No*** to abort assigning the Network QoS Profile to the Network Cloud.

Setting a VLAN for a Network Cloud

VLANs are used for traffic isolation and security to prevent some hosts on a network from seeing traffic that is intended for other hosts. When traffic is tagged with a VLAN ID, only the hosts that can transmit or receive packets for that VLAN are able to see and use that traffic.

VLANs can be set for a Network Cloud. When a VLAN is set on the Network Cloud, vNICs added to that cloud inherit the VLAN ID unless additional configuration exists at the port level to enforce different tagging rules.

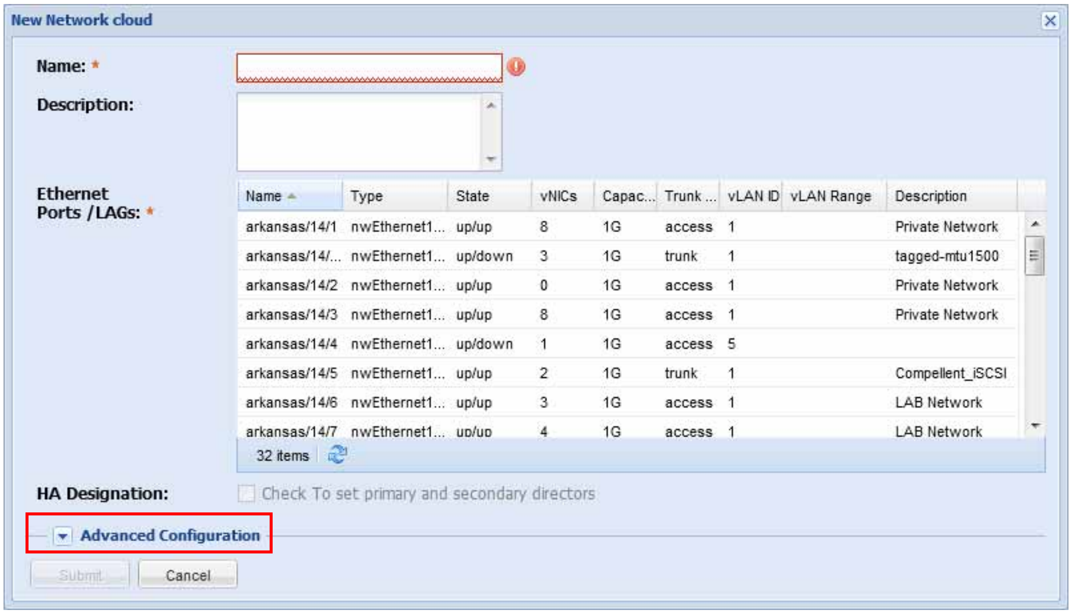
Note

In addition to VLANs on a Network Cloud, you can control the VLAN IDs that are supported on a specific Fabric Director through the Allowed VLAN Range feature. For more information, see Setting the Allowed VLAN Ranges for a Fabric Director.

VLANs can be set for a Network Cloud through the Advanced Configuration dropdown menu on the New Network Cloud dialog. When you set a VLAN on the Network Cloud, it is applied to all ports in the Network Cloud. As a result, when a vNIC is terminated on that Network Cloud it will be assigned to the specified VLAN.

To set a VLAN for a Network Cloud, follow this procedure:

Step 1 If the Create a Network Cloud dialog is not already displayed, display it now, as shown in Figure 8.



New Network cloud

Name: *

Description:

Ethernet Ports /LAGs: *

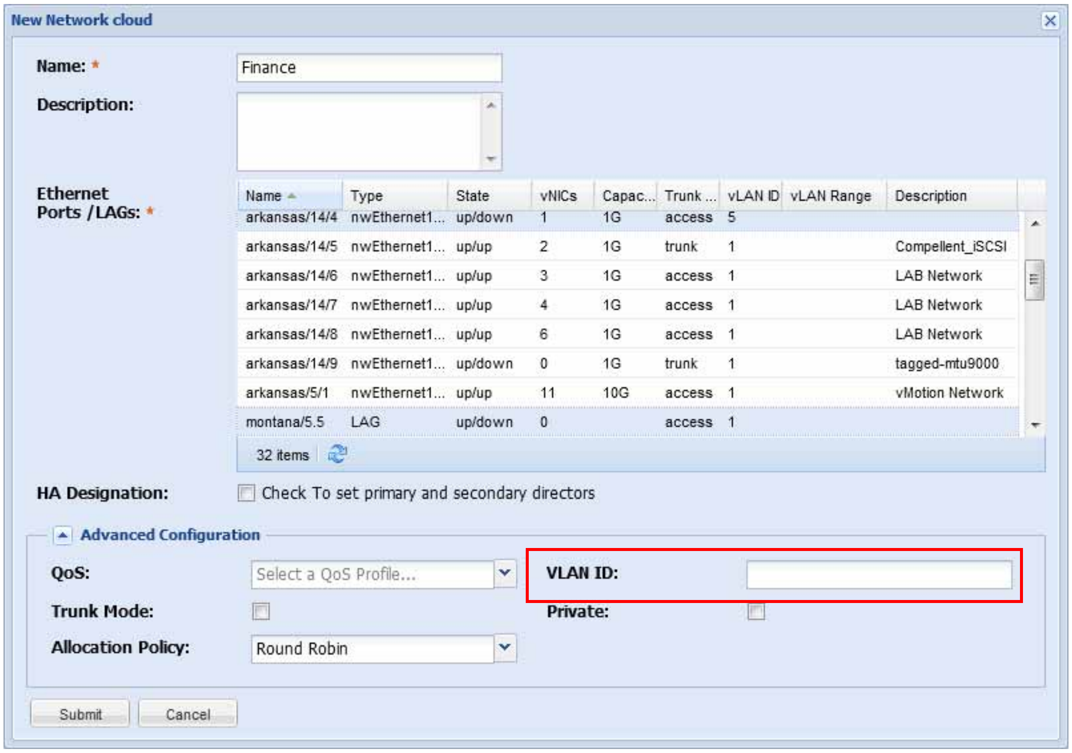
Name	Type	State	vNICs	Capac...	Trunk ...	vLAN ID	vLAN Range	Description
arkansas/14/1	nwEthernet1...	up/up	8	1G	access	1		Private Network
arkansas/14/...	nwEthernet1...	up/down	3	1G	trunk	1		tagged-mtu1500
arkansas/14/2	nwEthernet1...	up/up	0	1G	access	1		Private Network
arkansas/14/3	nwEthernet1...	up/up	8	1G	access	1		Private Network
arkansas/14/4	nwEthernet1...	up/down	1	1G	access	5		
arkansas/14/5	nwEthernet1...	up/up	2	1G	trunk	1		Compellent_iSCSI
arkansas/14/6	nwEthernet1...	up/up	3	1G	access	1		LAB Network
arkansas/14/7	nwEthernet1...	up/up	4	1G	access	1		LAB Network

32 items

HA Designation: □ Check To set primary and secondary directors

Figure 8 New Network Cloud

Step 2 Click the *Advanced Configuration* dropdown menu to display the additional properties for the Network Cloud. See Figure 9.



Name: * Finance

Description:

Ethernet Ports /LAGs: *

Name	Type	State	vNICs	Capac...	Trunk ...	vLAN ID	vLAN Range	Description
arkansas/14/4	nwEthernet1...	up/down	1	1G	access	5		
arkansas/14/5	nwEthernet1...	up/up	2	1G	trunk	1		Compellent_iSCSI
arkansas/14/6	nwEthernet1...	up/up	3	1G	access	1		LAB Network
arkansas/14/7	nwEthernet1...	up/up	4	1G	access	1		LAB Network
arkansas/14/8	nwEthernet1...	up/up	6	1G	access	1		LAB Network
arkansas/14/9	nwEthernet1...	up/down	0	1G	trunk	1		tagged-mtu9000
arkansas/5/1	nwEthernet1...	up/up	11	10G	access	1		vMotion Network
montana/5.5	LAG	up/down	0		access	1		

32 items

HA Designation: □ Check To set primary and secondary directors

Advanced Configuration

QoS: Select a QoS Profile...

VLAN ID:

Trunk Mode: □

Private: □

Allocation Policy: Round Robin

Figure 9 New Network Cloud — Advanced Configuration, VLAN ID

Step 3 In the *VLAN ID* field, set the specific VLAN number which will be applied to the vNICs that are associated with the cloud.

Note

The VLAN ID you set for the Network Cloud must be within the Allowed VLAN Range set for the Fabric Director on which the vNIC(s) are terminated.

Step 4 If the Network Cloud will be supporting vNICs that trunk the VLAN tags, click the *Trunk Mode* checkbox.

Step 5 When the VLAN properties are configured, and any other properties for the Network Cloud, click ***Submit*** to complete the configuration.

Creating Private vNICs on a Network Cloud

By default, when two vNICs are terminated on the same I/O module, Oracle’s Xsigo Fabric Director uses a feature called vNIC-to-vNIC Switching which forwards the traffic between the two vNICs across the I/O module, instead of sending them over the midplane. The vNIC-to-vNIC Switching feature provides better performance for network traffic. However, some situations exist where uncontrolled vNIC-to-vNIC Switching might not be desirable due to security reasons.

Fabric Manager provides a way to add security to vNIC-to-vNIC switching, through a feature called Private vNICs. With Private vNICs, you can add isolation for a set of vNICs, and also provide enhanced compatibility for existing and new methods of external switching. If a vNIC-to-vNIC Switching configuration does not explicitly have one or more vNICs set as a Private vNIC, then those vNICs are assumed to be Public vNICs, which do not support isolation and external switching benefits that Private vNICs do. Specifically, Private vNICs provide the following isolation and switching enhancements:

- A private vNIC can communicate with the Ethernet network and Public vNICs, but it cannot communicate with other Private vNICs.
- If a packet's destination is assigned to a Private vNIC, the packet will be dropped. Packets originating on a private vNIC and destined for another private vNIC will be dropped regardless of whether both vNICs are in the same VLAN.
- Public vNICs can communicate without restriction with the exception of traffic isolation enforced by standard VLANs.
- Packets arriving from private vNICs are dropped or forwarded based on the destination. If the destination is a Public vNIC or the Ethernet network, the packet will be forwarded. Otherwise, it will be dropped. VLAN restrictions will still apply to packets that are forwarded.
- Broadcast or multicast packets are not a special case. They are also not forwarded between Private vNICs.

Note

Private vNICs are not supported with HA vNICs. Configure your Private vNICs as standalone vNICs only. Public vNICs, however, can be configured as HA vNICs.

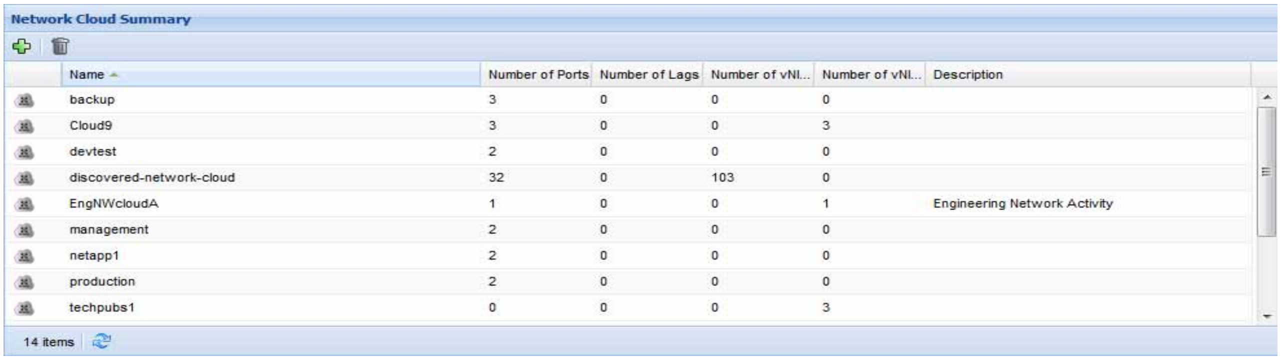
Private vNICs can be specified through the *Private* checkbox, which toggles the *Private* property on (Private vNIC) or off (Public vNIC). The *Private* checkbox is available through the Network Cloud so that all vNICs that attach to the cloud are considered private.

This feature is also settable at the I/O Template level and the vNIC level:

- To set one or more Private vNICs at the I/O Template level, double-click the vNIC on the I/O Template Editor and click the *Private* checkbox as needed. However, any setting configured on an individual vNIC (either Public or Private) will be overridden by the setting at the Network Cloud level. For example, if the vNIC is configured as a Public vNIC, then you move the vNIC to a Network Cloud that is set for Private vNICs, the vNIC will become a Private vNIC after the move completes and the vNIC is terminated on a port in the new Network Cloud.
- To set one or more Private vNICs at the vNIC-level, when the vNIC is deployed to the server, select the server on the Physical Servers page to populate the details frame. Then, click the *vNICs* tab to display the server's vNICs. Then, click the name of the individual vNICs that you want to make into Private vNICs. When the vNIC is displayed, click the *General* tab, then click the ***Edit*** button and mark the *Private* checkbox.

To configure a Network Cloud with Private vNICs, follow this procedure:

Step 1 If the Create a Network Cloud dialog is not already displayed, display it now, as shown in Figure 10.



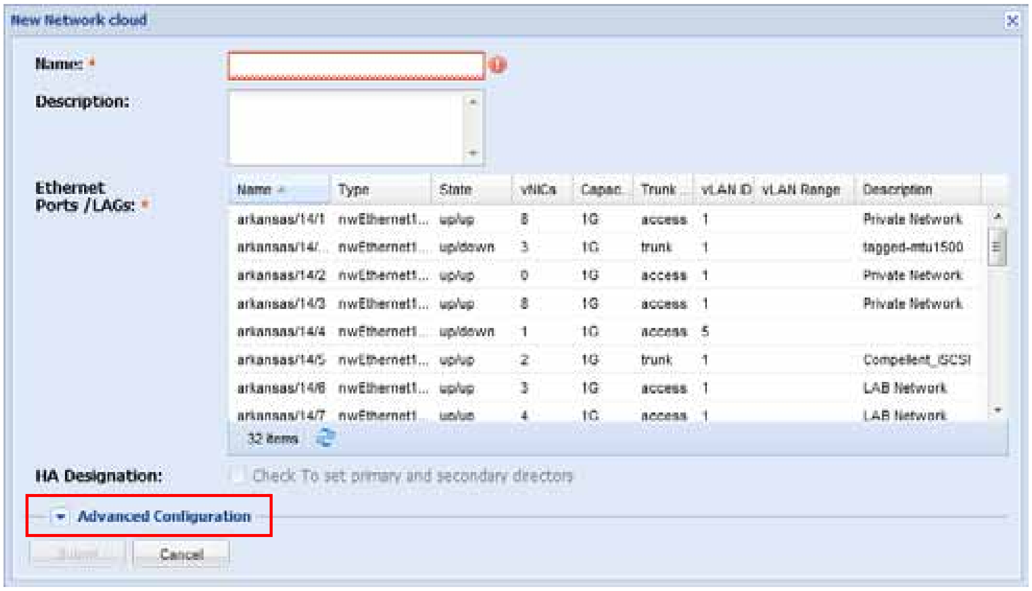
Network Cloud Summary

Name	Number of Ports	Number of Lags	Number of vNI...	Number of vNI...	Description
backup	3	0	0	0	
Cloud9	3	0	0	3	
devtest	2	0	0	0	
discovered-network-cloud	32	0	103	0	
EngNWcloudA	1	0	0	1	Engineering Network Activity
management	2	0	0	0	
netapp1	2	0	0	0	
production	2	0	0	0	
techpubs1	0	0	0	3	

14 items

Figure 10 Network Cloud Summary

Step 2 Click the plus sign (+) to display the New Network Cloud dialog. Figure 11 shows this dialog.



New Network cloud

Name: *

Description:

Ethernet Ports /LAGs: *

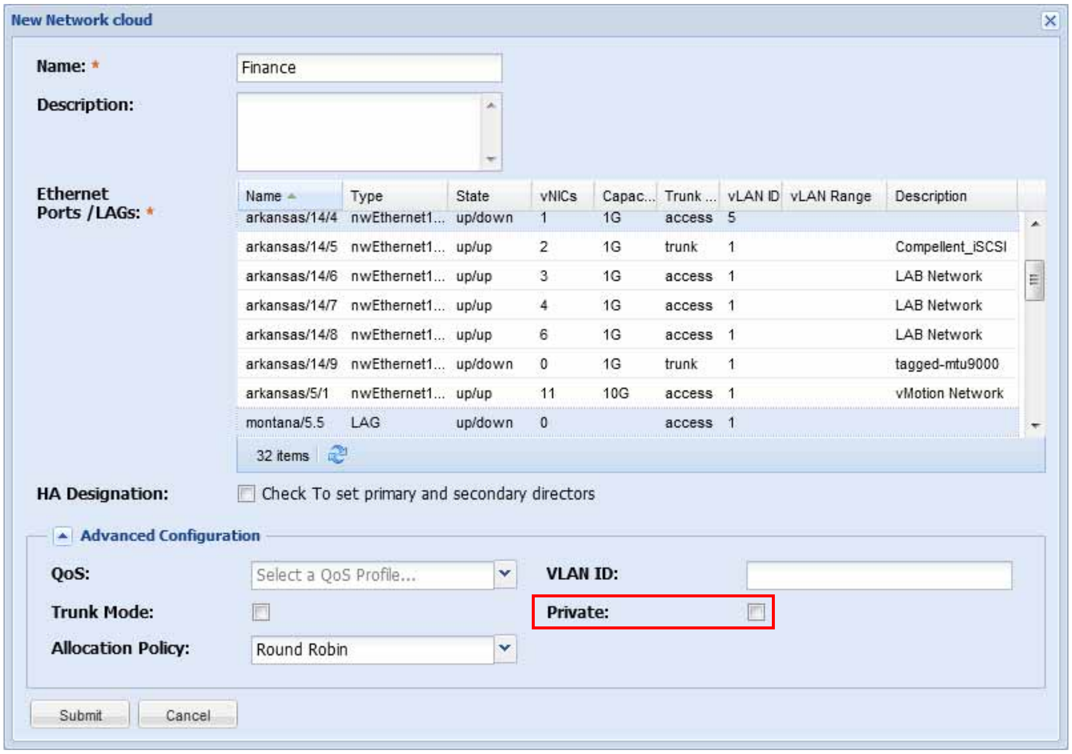
Name	Type	State	vNICs	Capac.	Trunk	vLAN ID	vLAN Range	Description
arkansas/14/1	nwEthernet1...	up/up	8	1G	access	1		Private Network
arkansas/14/...	nwEthernet1...	up/down	3	1G	trunk	1		tagged-mtu1500
arkansas/14/2	nwEthernet1...	up/up	0	1G	access	1		Private Network
arkansas/14/3	nwEthernet1...	up/up	8	1G	access	1		Private Network
arkansas/14/4	nwEthernet1...	up/down	1	1G	access	5		
arkansas/14/5	nwEthernet1...	up/up	2	1G	trunk	1		Compellent_iSCSI
arkansas/14/6	nwEthernet1...	up/up	3	1G	access	1		LAB Network
arkansas/14/7	nwEthernet1...	up/up	4	1G	access	1		LAB Network

32 items

HA Designation: □ Check To set primary and secondary directors

Figure 11 New Network Cloud

Step 3 Click the *Advanced Configuration* dropdown menu to display the additional properties for the Network Cloud. See Figure 12.



New Network cloud

Name: * Finance

Description:

Ethernet Ports /LAGs: *

Name	Type	State	vNICs	Capac...	Trunk ...	vLAN ID	vLAN Range	Description
arkansas/14/4	nwEthernet1...	up/down	1	1G	access	5		
arkansas/14/5	nwEthernet1...	up/up	2	1G	trunk	1		Compellent_iSCSI
arkansas/14/6	nwEthernet1...	up/up	3	1G	access	1		LAB Network
arkansas/14/7	nwEthernet1...	up/up	4	1G	access	1		LAB Network
arkansas/14/8	nwEthernet1...	up/up	6	1G	access	1		LAB Network
arkansas/14/9	nwEthernet1...	up/down	0	1G	trunk	1		tagged-mtu9000
arkansas/5/1	nwEthernet1...	up/up	11	10G	access	1		vMotion Network
montana/5.5	LAG	up/down	0		access	1		

32 items

HA Designation: □ Check To set primary and secondary directors

Advanced Configuration

QoS: Select a QoS Profile...

VLAN ID:

Trunk Mode: □

Private: □

Allocation Policy: Round Robin

Submit Cancel

Figure 12 New Network Cloud — Advanced Configuration, Private vNICs

Step 4 In the *Private* checkbox, click to specify that vNICs terminated on this network cloud are private vNICs. When configured, any vNIC that is terminated on this cloud will not be able to communicate with any public vNICs in any other Network Clouds.

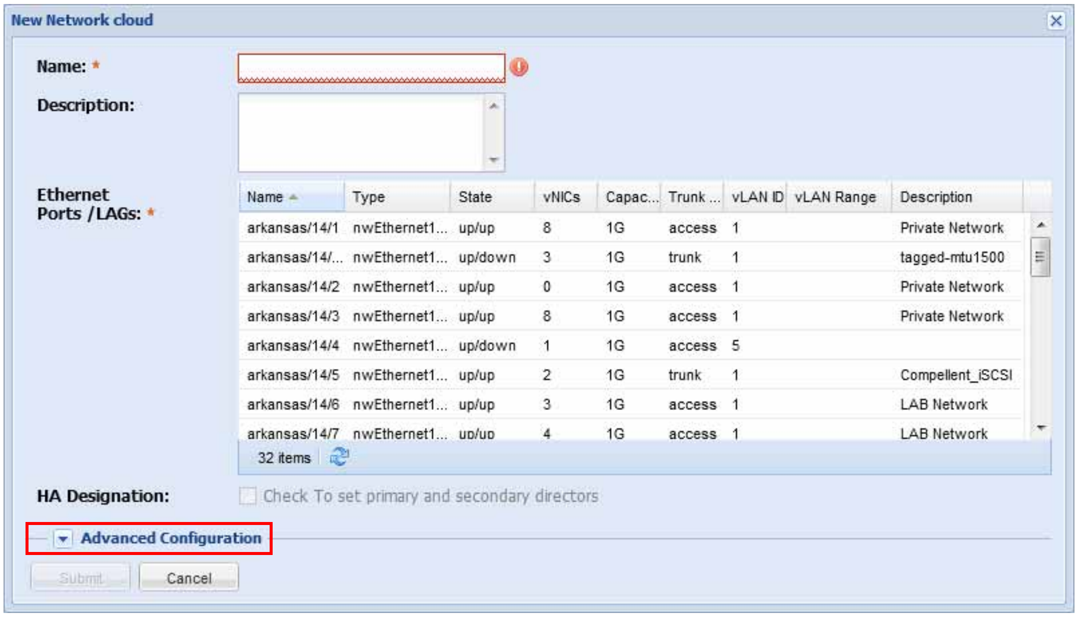
Step 5 When the cloud's properties are specified, click ***Submit*** to complete the configuration.

Setting the Port Allocation Policy

For Network and Storage Clouds, you can set the manner in which ports are allocated to vNICs or vHBAs that connect to the clouds.

To set the port allocation policy for a Network Cloud, follow this procedure:

Step 1 If the Create a Network Cloud dialog is not already displayed, display it now, as shown in Figure 13.



New Network cloud

Name: *

Description:

Ethernet Ports /LAGs: *

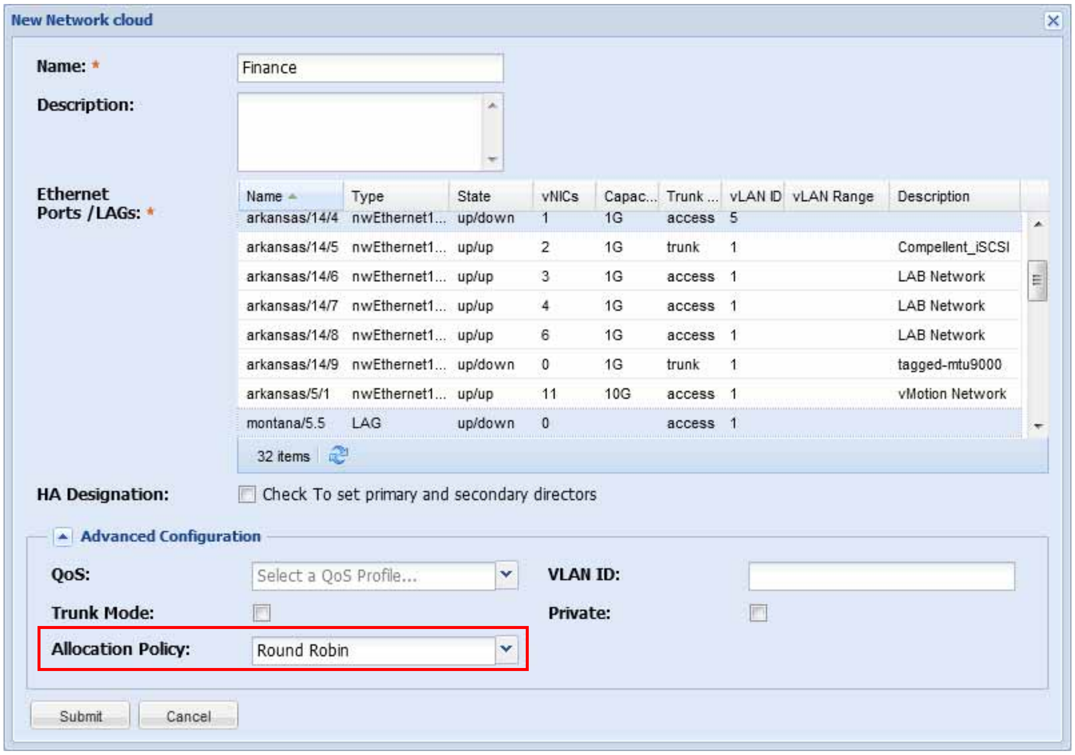
Name	Type	State	vNICs	Capac...	Trunk ...	vLAN ID	vLAN Range	Description
arkansas/14/1	nwEthernet1...	up/up	8	1G	access	1		Private Network
arkansas/14/...	nwEthernet1...	up/down	3	1G	trunk	1		tagged-mtu1500
arkansas/14/2	nwEthernet1...	up/up	0	1G	access	1		Private Network
arkansas/14/3	nwEthernet1...	up/up	8	1G	access	1		Private Network
arkansas/14/4	nwEthernet1...	up/down	1	1G	access	5		
arkansas/14/5	nwEthernet1...	up/up	2	1G	trunk	1		Compellent_iSCSI
arkansas/14/6	nwEthernet1...	up/up	3	1G	access	1		LAB Network
arkansas/14/7	nwEthernet1...	up/up	4	1G	access	1		LAB Network

32 items

HA Designation: □ Check To set primary and secondary directors

Figure 13 New Network Cloud

Step 2 Click the *Advanced Configuration* dropdown menu to display the additional properties for the Network Cloud. See Figure 14.



New Network cloud

Name: * Finance

Description:

Ethernet Ports /LAGs: *

Name	Type	State	vNICs	Capac...	Trunk ...	vLAN ID	vLAN Range	Description
arkansas/14/4	nwEthernet1...	up/down	1	1G	access	5		
arkansas/14/5	nwEthernet1...	up/up	2	1G	trunk	1		Compellent_iSCSI
arkansas/14/6	nwEthernet1...	up/up	3	1G	access	1		LAB Network
arkansas/14/7	nwEthernet1...	up/up	4	1G	access	1		LAB Network
arkansas/14/8	nwEthernet1...	up/up	6	1G	access	1		LAB Network
arkansas/14/9	nwEthernet1...	up/down	0	1G	trunk	1		tagged-mtu9000
arkansas/5/1	nwEthernet1...	up/up	11	10G	access	1		vMotion Network
montana/5.5	LAG	up/down	0		access	1		

32 items

HA Designation: □ Check To set primary and secondary directors

Advanced Configuration

QoS: Select a QoS Profile...

VLAN ID:

Trunk Mode: □

Private: □

Allocation Policy: Round Robin

Figure 14 New Network Cloud — Advanced Configuration, Allocation Policy

Step 3 From the *Allocation Policy* field, select the following policy for how network ports are assigned to vNICs that terminate on the cloud.

- Round Robin, which is a systematic way for ports to be assigned. With round robin allocation, you specify multiple ports in a list of available ports for a Network Cloud. When the list is constructed, you then assign a port as the next available port. When you assign the next available port, it gets a rank that is different than any other port in the available ports list. The port you assign is the next port to be assigned, and after that, any additional vHBAs that are connected to the Network Cloud will receive an Ethernet port based on its rank. For example, assume you create a Network Cloud with Ethernet port 2/1 as the port used to create the cloud. Then, assume you add ports 2/2, 4/1, and 5/1 to the available ports list, and set port 4/1 as the next available port. When new vNICs are connected to the Network Cloud, the first vNIC is connected to port 4/1. After that, additional vNICs are assigned to whichever port has the next lowest rank.

Step 4 When the allocation policy is configured, and any other properties for the Network Cloud, click ***Submit*** to complete the configuration.

Setting Link Aggregation for a Network Cloud

Link Aggregation Groups (LAGs) function the same as physical Ethernet port in the Network Cloud. Virtual NICs can be terminated on a LAG, just as they would be on a physical port. If you are configuring a LAG, it will typically have all ports in the Network Cloud, but the same Network Cloud can have a LAG and one or more physical ports in it. Multiple LAGs can be assigned to the same Network Cloud as long as each LAG complies with the standard LAG guidelines for minimum and maximum number of ports.

To configure LAG for a Network Cloud, follow this procedure. This procedure assumes that the Link Aggregation Groups already exist. If they do not, you will need to create them before assigning them to the Network Cloud. For information about Link Aggregation Groups, see Working with Link Aggregation.

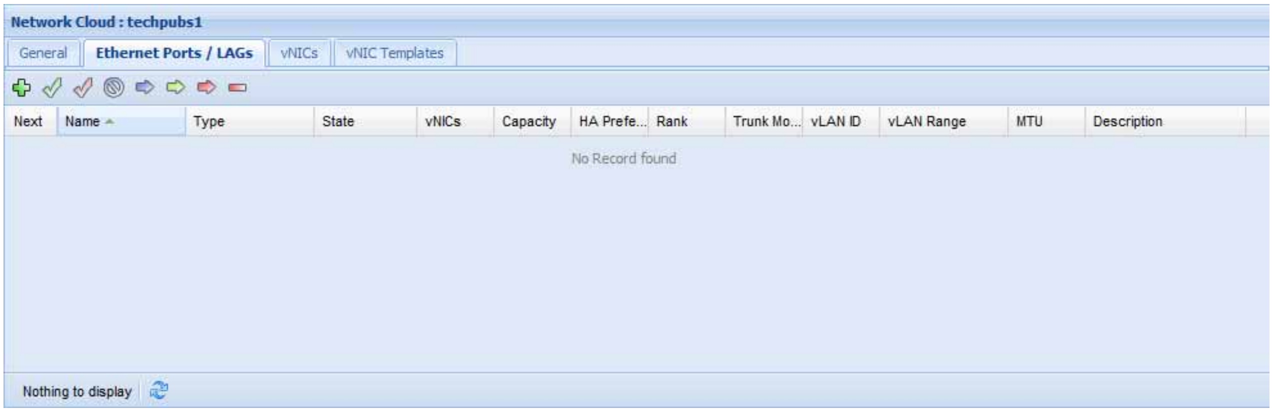
Step 1 Display the Network Cloud Summary (*Network Resources Manager->Network Clouds*).

Step 2 Click the name of the Network Cloud for which you want to assign a Link Aggregation Group (LAG). This step displays the Network Cloud in the details frame.

Step 3 Click the *Ethernet Ports/LAGs* tab to display the LAG currently associated with the Network Cloud.

- If no LAG is currently assigned, you can add a LAG to the Network Cloud.
- If a LAG is currently assigned, you can change the LAG assigned to the Network Cloud, or delete the current LAG from the Network Cloud.

Figure 15 shows an example of a Network Cloud with no LAG assigned.



Next	Name	Type	State	vNICs	Capacity	HA Prefe...	Rank	Trunk Mo...	vLAN ID	vLAN Range	MTU	Description

No Record found

Nothing to display

Figure 15 Network Cloud Details — No LAG Assigned

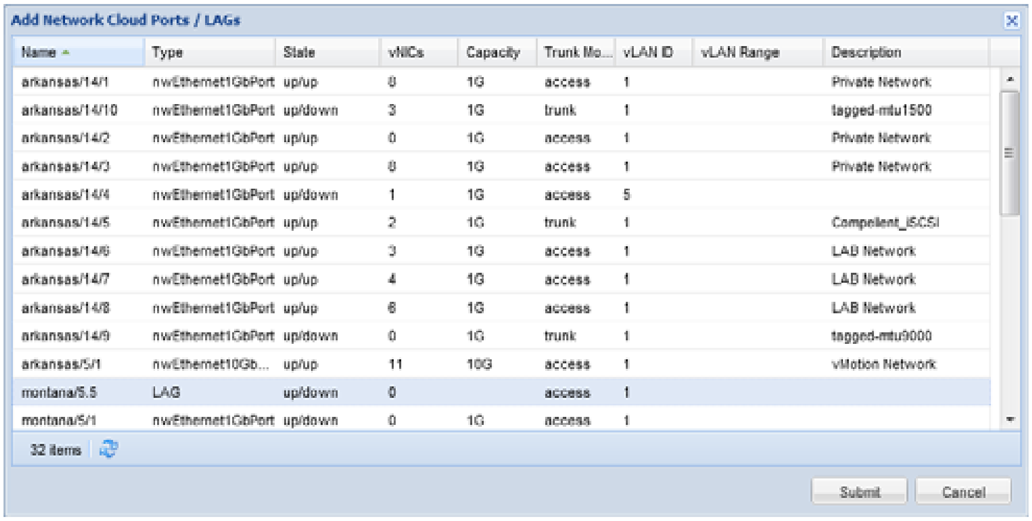
Step 4 Click the plus sign (+) to display the Change Network Cloud LAGs dialog.

Note

To add a LAG, it must already be configured. If it is not yet configured, it is not a selectable item that can be associated with the LAG.

If you are changing the LAG associated with a Network Cloud, select the LAG, click the delete icon (the red dash), then click the plus sign (+) to associate a different LAG with the Network Cloud.

Figure 16 shows the Change Network Cloud LAG dialog.



Add Network Cloud Ports / LAGs

Name	Type	State	vNICs	Capacity	Trunk Mo...	vLAN ID	vLAN Range	Description
arkansas/14/1	nwEthernet1GbPort	up/up	8	1G	access	1		Private Network
arkansas/14/10	nwEthernet1GbPort	up/down	3	1G	trunk	1		tagged-mtu1500
arkansas/14/2	nwEthernet1GbPort	up/up	0	1G	access	1		Private Network
arkansas/14/3	nwEthernet1GbPort	up/up	8	1G	access	1		Private Network
arkansas/14/4	nwEthernet1GbPort	up/down	1	1G	access	5		
arkansas/14/5	nwEthernet1GbPort	up/up	2	1G	trunk	1		Compellent_iSCSI
arkansas/14/6	nwEthernet1GbPort	up/up	3	1G	access	1		LAB Network
arkansas/14/7	nwEthernet1GbPort	up/up	4	1G	access	1		LAB Network
arkansas/14/8	nwEthernet1GbPort	up/up	6	1G	access	1		LAB Network
arkansas/14/9	nwEthernet1GbPort	up/down	0	1G	trunk	1		tagged-mtu9000
arkansas/5/1	nwEthernet10Gb...	up/up	11	10G	access	1		vMotion Network
montana/5.5	LAG	up/down	0		access	1		
montana/5/1	nwEthernet1GbPort	up/down	0	1G	access	1		

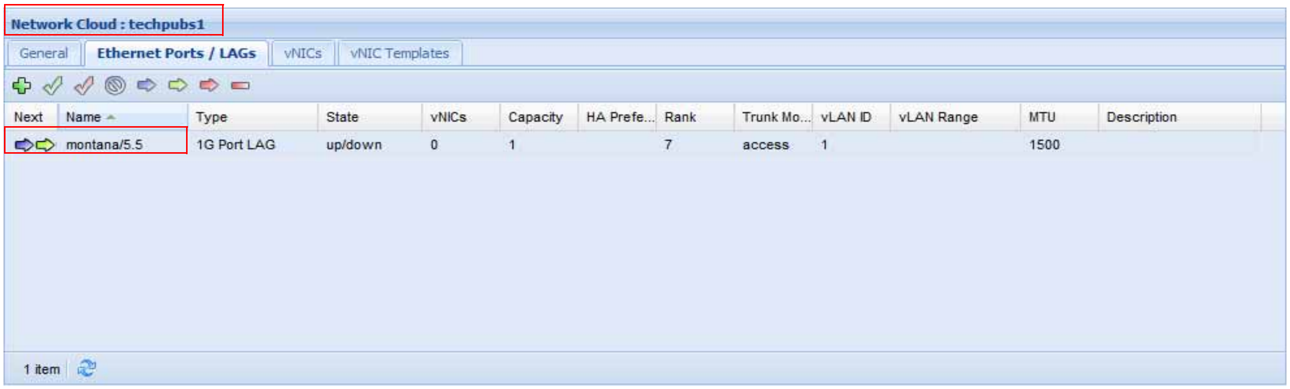
32 items

Figure 16 Network Cloud Details — Select the LAG for the Network Cloud

Step 5 Click the LAG you want to assign to the Network Cloud. The LAG is selected when it is highlighted, as shown.

Step 6 Click ***Submit*** to assign the LAG to the Network Cloud in Fabric Manager.

Step 7 Check the *Ethernet Ports/LAG* tab to verify that the LAG was assigned. Figure 17 shows an example of a LAG assigned to a Network Cloud.



Network Cloud : techpubs1

Next	Name	Type	State	vNICs	Capacity	HA Prefe...	Rank	Trunk Mo...	vLAN ID	vLAN Range	MTU	Description
	montana/5.5	1G Port LAG	up/down	0	1		7	access	1		1500	

1 item

Figure 17 Network Cloud Details — LAG Assigned to Network Cloud

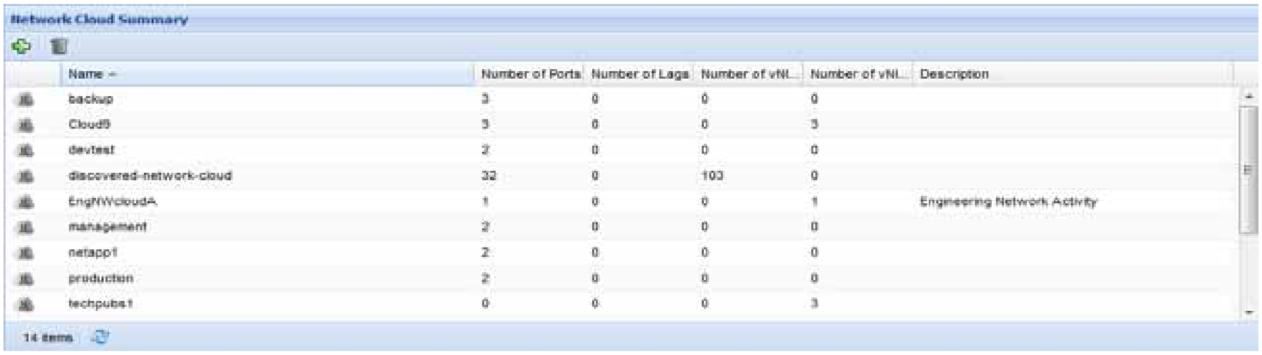
Displaying Network Clouds

Network Clouds are displayed in the summary and details frames of the work panel. Each frame provides different levels of information about the configured Network Clouds.

Displaying Summary Information for Network Clouds

The Network Cloud Summary is a table of all the configured Network Clouds, including the default Network Cloud (discovered-network-cloud). Additional, detailed information about each Network Cloud is contained in the Network Cloud Details frame, which is located directly below the Network Cloud Summary.

Figure 18 shows the Network Cloud Summary.



Network Cloud Summary

Name	Number of Ports	Number of Lags	Number of vNI...	Number of vNI...	Description
backup	3	0	0	0	
Cloud9	3	0	0	3	
devtest	2	0	0	0	
discovered-network-cloud	32	0	103	0	
EngNWcloudA	1	0	0	1	Engineering Network Activity
management	2	0	0	0	
netapp1	2	0	0	0	
production	2	0	0	0	
techpubs1	0	0	0	3	

14 items

Figure 18 Network Cloud Summary

Table 1 shows the field contained in the Network Cloud Summary and explains what each one means.

Table 1 Contents of the Network Cloud Summary

Field	Indicates
Name	The name of each configured Network Cloud.
Number of Ports	The number of Ethernet ports in the Network Cloud. This number is the total of all ports, regardless of whether they are up or down.
Number of LAGs	The number of link aggregation groups (LAGs) in the Network Cloud. This number is the total of all LAGs configured, not the total number of ports in LAGs.
Number of vNICs	The total number of vNICs that are connected to the Network Cloud.
Number of vNIC Templates	The total number of I/O Templates that are associated with each Network Cloud.
Description	The description string (if any) that was applied to the Network Cloud. If this field is blank, either no description string was specified when the Network Cloud was created, or the Network Cloud was originally created with a description string, but the Network Cloud was later edited and the description string was removed.

Displaying Detailed Information for Network Clouds

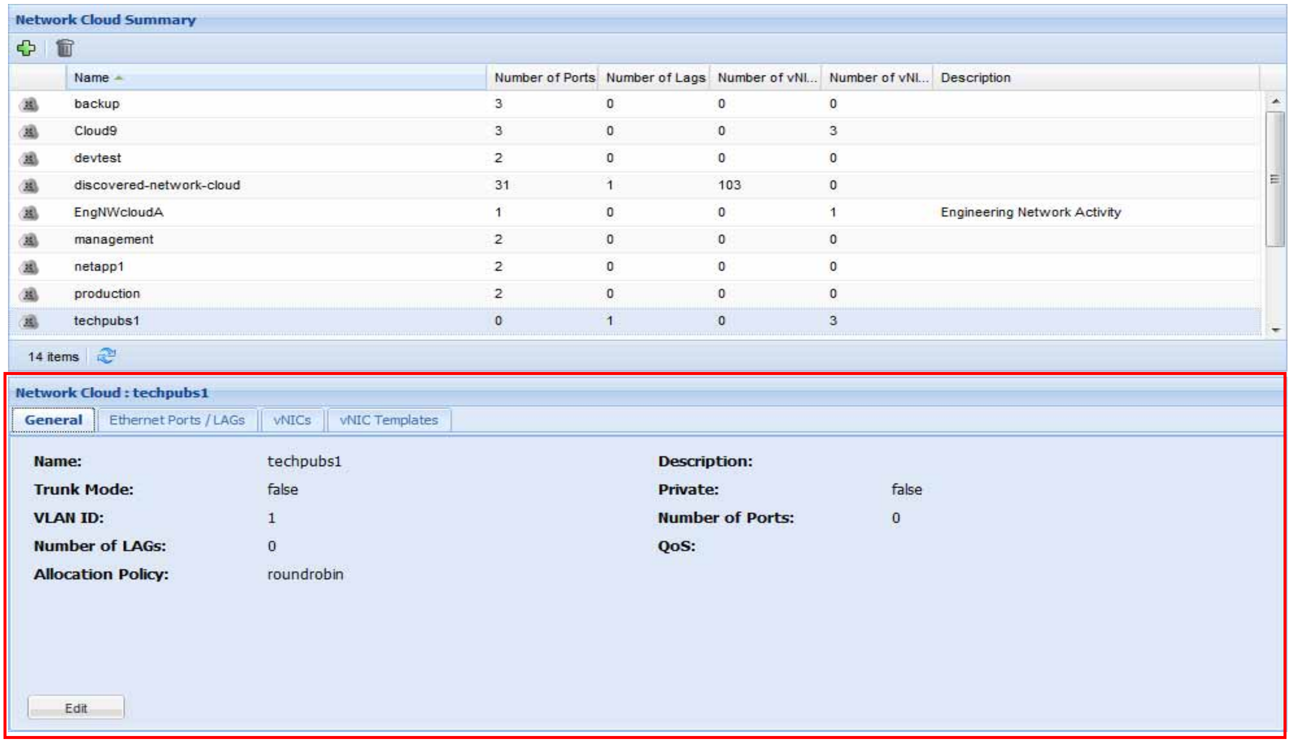
The Network Cloud Details frame is a section of the work panel that is located below the Network Cloud Summary. The Network Cloud Details frame is typically a list of fields for a selected Network Cloud, a list of Ethernet ports or LAGs contained in the Network Cloud, or a list of fields for a selected Ethernet port in the Network Cloud.

The Network Cloud Details frame enables you to display additional, detailed information for a single Network Cloud including the default Network Cloud (`discovered-network-ports`). For non-default Network Clouds, you can use the Network Cloud Details frame to edit various aspects of the cloud itself, or the components of it. The Network Cloud Details frame has the following controls, which are common on most details frames for features throughout the entire Fabric Manager interface:

- add and delete buttons, a plus sign and a red dash, respectively
- tabs, which logically organized additional information about the contents of the details frame
- an ***Edit*** button, which unlocks editable parts of the details frame so that you can set or change information elements for the contents of the details frame

To use the Network Cloud Details frame, you must first select a configured cloud from the Network Cloud Summary. By selecting a cloud from the summary, you set the focus of the Network Cloud Details frame. When the cloud is selected in the summary, you will see its details displayed in the Details frame.

Figure 19 shows the Network Cloud Details frame. Notice that the details frame is contextual, so that it displays detailed information for the item selected in the Network Cloud Summary.



Name	Number of Ports	Number of Lags	Number of vNI...	Number of vNI...	Description
backup	3	0	0	0	
Cloud9	3	0	0	3	
devtest	2	0	0	0	
discovered-network-cloud	31	1	103	0	
EngNWcloudA	1	0	0	1	Engineering Network Activity
management	2	0	0	0	
netapp1	2	0	0	0	
production	2	0	0	0	
techpubs1	0	1	0	3	

Name:	techpubs1	**Description:**	
Trunk Mode:	false	**Private:**	false
VLAN ID:	1	**Number of Ports:**	0
Number of LAGs:	0	**QoS:**	
Allocation Policy:	roundrobin		

Figure 19 Network Cloud Details Frame

Through the Network Cloud Details frame, you can also see information about the Ethernet Ports or LAGs that are associated with the specific cloud.

Editing Network Cloud Properties

Through the Network Cloud Details frame, you can edit parameters associated with the Network Cloud without having to completely redefine the cloud. When you edit the Network Cloud's properties, the new properties take effect as soon as you save them, and the properties are applied to the vNICs terminated in the cloud.

Note

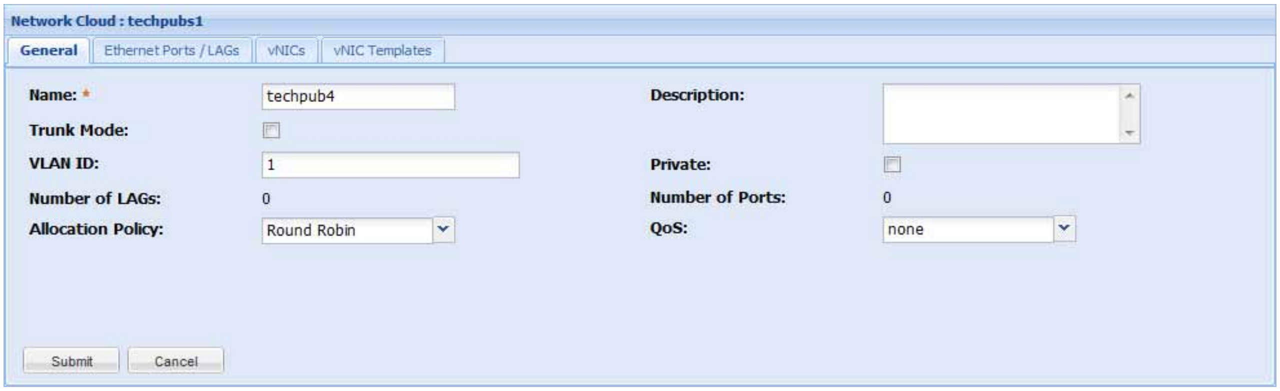
Anytime you edit a Network Cloud to make changes, it is a best practice to manually push those changes to the vNICs associated with that cloud. For more information, see Pushing Cloud Changes to an I/O Template's vNICs

To edit the Network Cloud properties, follow this procedure:

Step 1 Display the Network Cloud Summary.

Step 2 Click a configured Network Cloud to highlight it. When the cloud is highlighted, the Network Cloud Details frame is populated with the details for the selected Network Cloud, as shown in Figure 19.

Step 3 Click the ***Edit*** button to unlock the editable fields, as shown in Figure 20.



Network Cloud : techpubs1

Name: *	techpub4	Description:	
Trunk Mode:	□		
VLAN ID:	1	Private:	□
Number of LAGs:	0	Number of Ports:	0
Allocation Policy:	Round Robin	QoS:	none

Figure 20 Network Cloud General Tab — Editing Network Cloud Properties

Step 4 Make the appropriate changes. Editable fields are:

- Name, for renaming the Network Cloud after it has been created.
- Description, for specifying an optional description string for the cloud.
- Trunk Mode, for vNICs in the cloud that are, or will be, participating in a VLAN.
- VLAN ID, for vNICs in the cloud that are, or will be, participating in a VLAN.
- Private, which is a checkbox that toggles the state of Private vNIC on or off for the Network Cloud.
- Allocation Policy, for specifying how Ethernet ports get attached to vNICs that are configured in the cloud.

- QoS, for setting or changing the Network QoS Policer Profile associated with the vNICs in the Network Cloud. You can also use this dropdown menu to remove cloud-level QoS by depopulating any assigned Network QoS Profile from the field.

Step 5 When the Network Cloud changes are complete, click ***Save***.

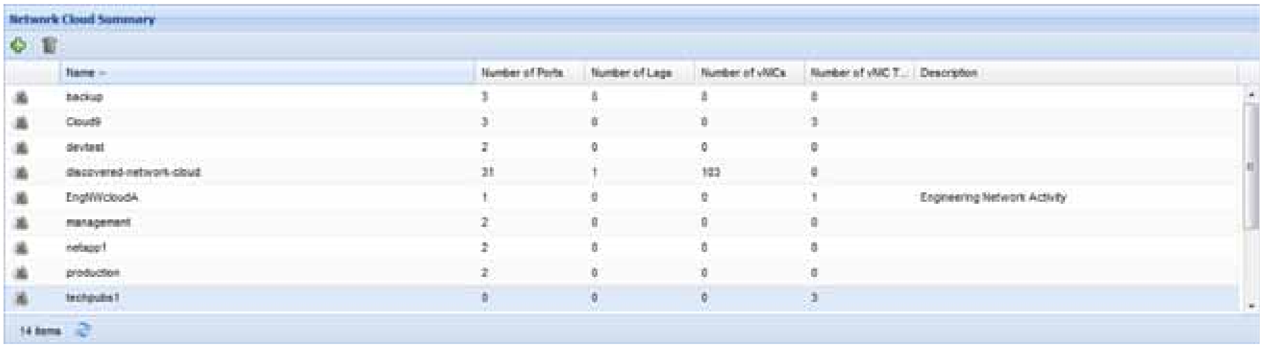
Renaming a Network Cloud

Fabric Manager supports renaming a Network Cloud without having to completely delete and recreate the entire Network Cloud. When the Network Cloud is renamed, all other properties for the Network Cloud are retained, including the ports and vNICs associated with the cloud. As an option, you can also set or change the description for the Network Cloud.

You can rename a Network Cloud through the Network Cloud Details frame. To rename the Network Cloud, follow this procedure:

Step 1 On the Navigation Frame, select *Network Cloud Manager->Network Clouds*.

Step 2 Select a Network Cloud to populate the details frame with its properties as shown in Figure 21.



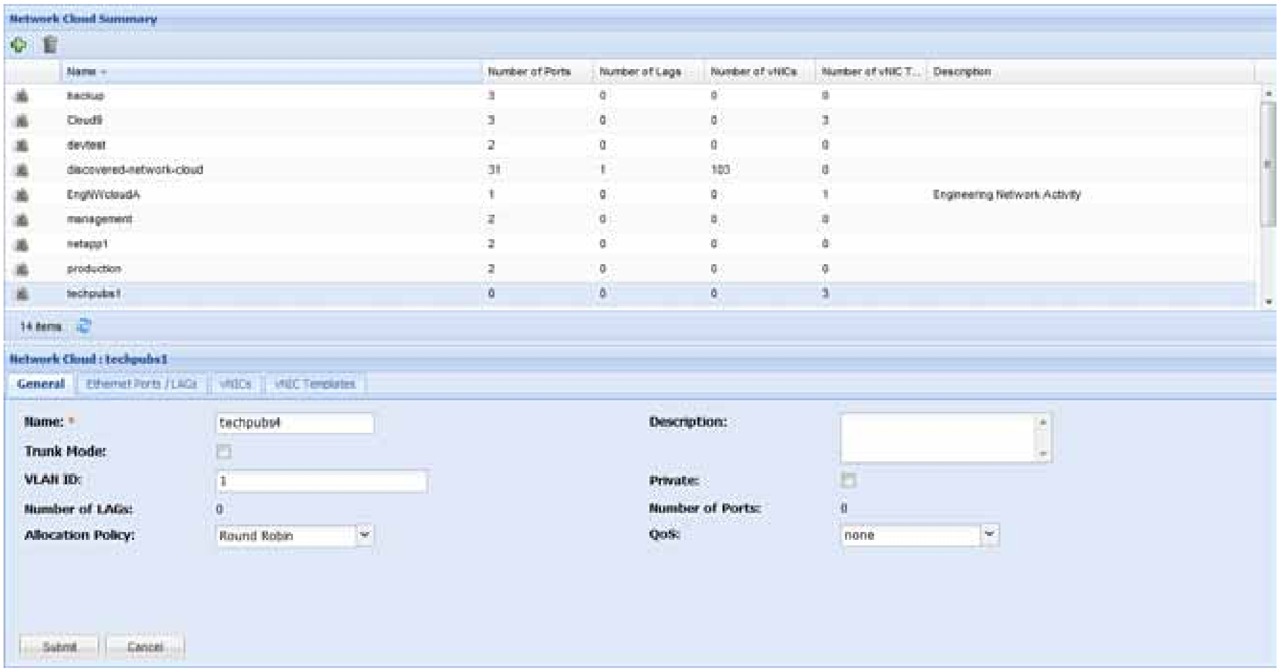
Network Cloud Summary

Name	Number of Ports	Number of Lags	Number of vNICs	Number of vNIC T...	Description
backup	3	0	0	0	
Cloud9	3	0	0	3	
devtest	2	0	0	0	
discovered-network-cloud	31	1	103	0	
EngNWcloudA	1	0	0	1	Engineering Network Activity
management	2	0	0	0	
netapp1	2	0	0	0	
production	2	0	0	0	
techpubs1	0	0	0	3	

14 items

Figure 21 Network Cloud Summary

Step 3 Click the ***Edit*** button to edit the properties of the selected Network Cloud, as shown in Figure 22.



Network Cloud Summary

	Name	Number of Ports	Number of Lags	Number of vNICs	Number of vNIC T...	Description
	backup	3	0	0	0	
	Cloud8	3	0	0	3	
	devtest	2	0	0	0	
	discovered-network-cloud	31	1	103	0	
	EngNWcloudA	1	0	0	1	Engineering Network Activity
	management	2	0	0	0	
	netapp1	2	0	0	0	
	production	2	0	0	0	
	techpubs1	0	0	0	3	

14 items

Network Cloud : techpubs1

Name: * techpubs4

Trunk Mode: □

VLAN ID: 1

Number of LAGs: 0

Allocation Policy: Round Robin

Description:

Private: □

Number of Ports: 0

QoS: none

Figure 22 Network Cloud Summary — Editing Details to Rename Network Cloud

Step 4 In the *Name* field, enter the new name for the Network Cloud.

Step 5 As an option, you also can set or change the description for the selected Network Cloud.

Step 6 As an option, you also can set or change any of the other editable fields on the details frame.

Step 7 When the new name has been specified for the Network Cloud, click ***Submit***.

Pushing Cloud Changes to an I/O Template’s vNICs

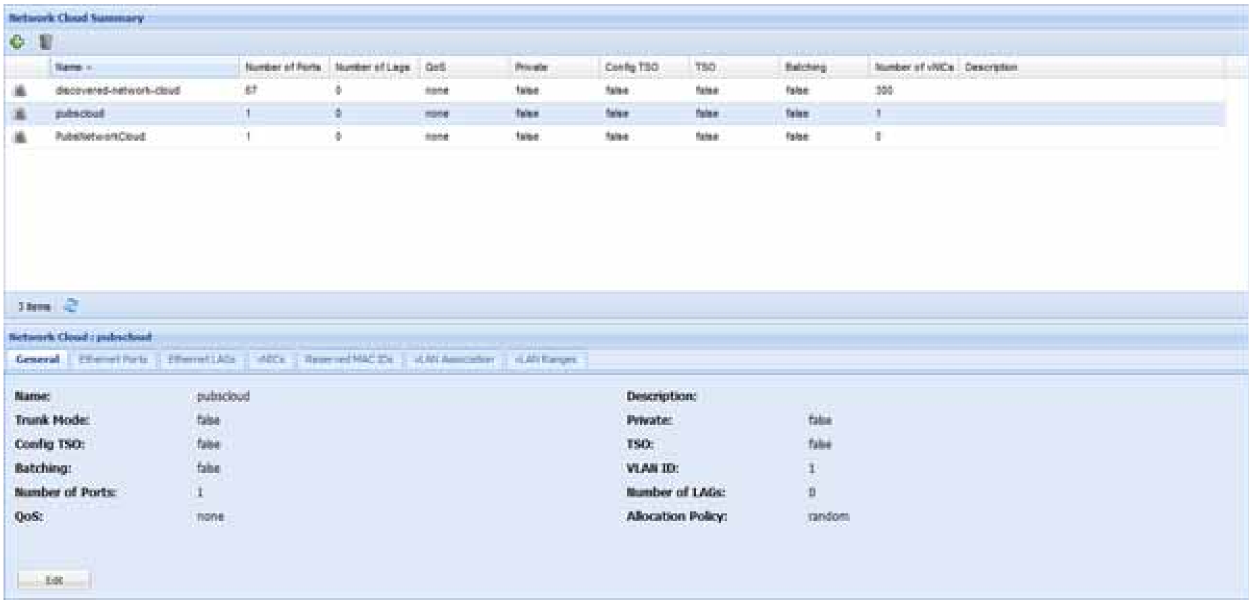
When you configure an I/O Template, you reference Network or Storage Clouds for the termination of the vNICs and vHBAs that connect the host server. These clouds are external to the template, and they are controlled through a different workflow. Because the cloud(s) and the templates are separate entities, any updates on a cloud must be explicitly forced to the I/O Template. Conceptually, this is intuitive because you are changing a cloud, you are not actually changing anything within the template itself.

If you need to change a cloud property, and that cloud is associated with an I/O Template, be aware that the change you make is not automatically updated in the I/O Template that is using that cloud. However, you can push changes in a Network or Storage Cloud to the I/O Template that is using that cloud by using the ***Re-Apply Cloud Changes to vNIC*** button for Network Clouds or the ***Re-Apply Cloud Changes to vHBA*** button for Storage Clouds.

To reapply Storage Cloud changes to vNICs in a template, follow this procedure:

Step 1 Select *Network Cloud Manager->Network Clouds* to display the Network Cloud Summary.

Step 2 Select the Network Cloud for which you want to make changes. This step populates the details frame with information about the selected Network Cloud. See Figure 23.



Network Cloud Summary

Name	Number of Ports	Number of Lags	QoS	Private	Config TSO	TSO	Batching	Number of vNICs	Description
discovered-network-cloud	67	0	none	false	false	false	false	300	
pubscloud	1	0	none	false	false	false	false	1	
PubsNetworkCloud	1	0	none	false	false	false	false	0	

3 items

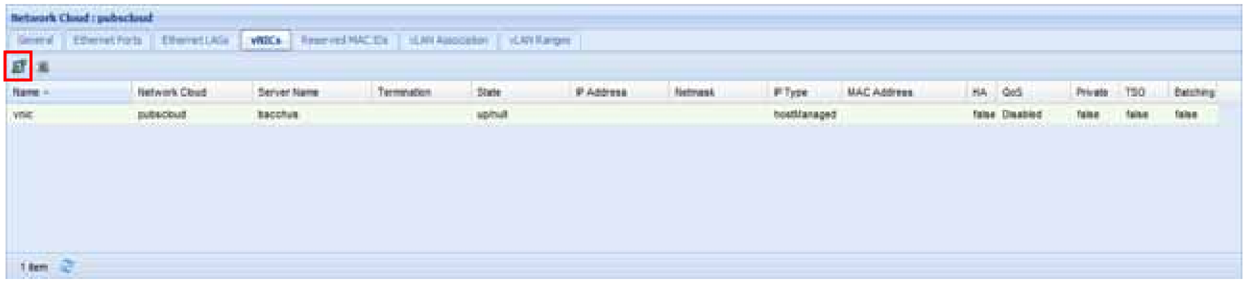
Network Cloud : pubscloud

Name:	pubscloud	Description:	
Trunk Mode:	false	Private:	false
Config TSO:	false	TSO:	false
Batching:	false	VLAN ID:	1
Number of Ports:	1	Number of LAGs:	0
QoS:	none	Allocation Policy:	random

Figure 23 Network Cloud Details Frame

Step 3 In the Cloud Details frame, click the *vNICs* tab.

Step 4 On the *vNICs* tab, select the vNIC(s) you want to receive the Network Cloud Changes. This step activates the ***Re-Apply Cloud Changes to vNIC*** button as shown in Figure 24.



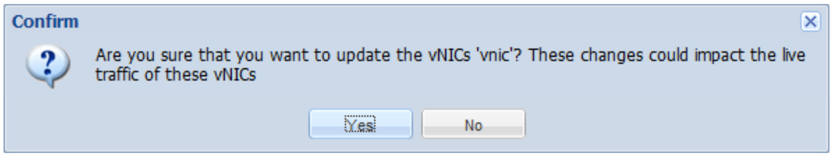
Network Cloud : pubscloud

Name	Network Cloud	Server Name	Termination	State	IP Address	Netmask	IP Type	MAC Address	HA	QoS	Private	TSO	Batching
vnic	pubscloud	bacchus		up/null			hostManaged		false	Disabled	false	false	false

1 item

Figure 24 Applying Network Cloud Changes to a vNIC in a Template

Step 5 Click the button to apply the changes to the selected vNIC(s). When you do so, a confirmation dialog is displayed. See Figure 25.



Confirm

Are you sure that you want to update the vNICs 'vnic'? These changes could impact the live traffic of these vNICs

Figure 25 Confirming the Network Cloud Changes to a vNIC in a Template

Step 6 Click ***Yes*** to make the changes. When you do, the Storage Cloud changes are pushed to the vHBA.

Displaying the Ethernet Ports or LAGs in a Network Cloud

Each Network Cloud contains one or more Ethernet ports (or LAGs) that provide the termination point for vNICs connected to the cloud. For each Network Cloud, you can display a list of all the Ethernet ports or LAGs in a particular cloud. In addition to displaying the ports or LAGs in the cloud, you can:

- remove Ethernet ports (or LAGs) from the Network Cloud
- control the port allocation policy for each Ethernet port (or LAG) in the Network Cloud.

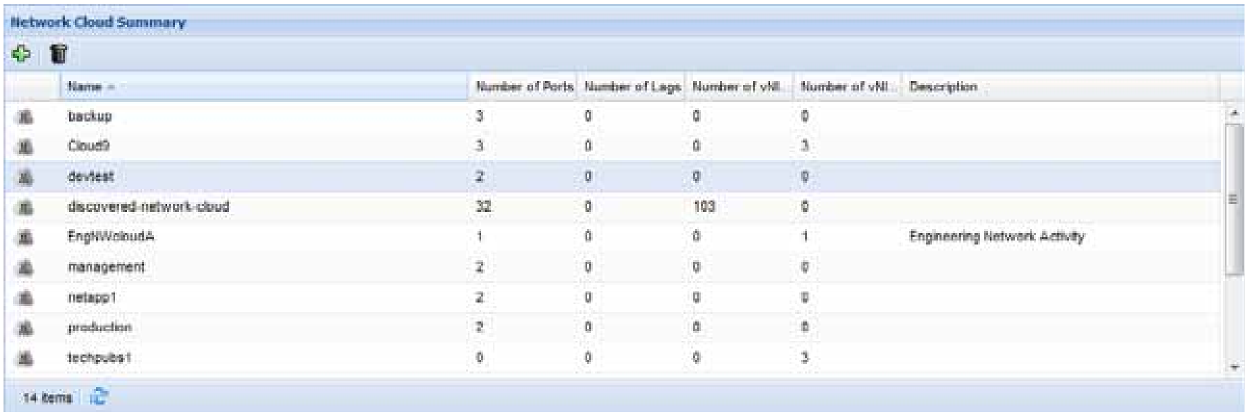
Note

Ethernet ports are listed in a modified ascending order. So, for example, port `iowa1/1` is listed before port `iowa2/1` as expected. However, port `iowa1/10` and `iowa11/1` would also be listed before port `iowa2/1`.

Due to the listing order in the *Ethernet Ports/LAGs* tab, you will need to pay attention to which port you select as the next available by moving the arrows around. For example, if you want the round robin policy to start with port `iowa1/1` and the next port to be assigned as port `iowa1/2`, you cannot just move the arrow to the next port down in the list because this might be port `iowa11/1` (not `iowa1/2`). Without paying close attention to the listing order, you might accidentally assign the wrong port(s). As a result, the round robin policy will operate correctly, but do so based on the incorrect ports you inadvertently assigned.

To display the Ethernet ports, follow this procedure:

Step 1 On the Navigation Frame, select *Network Cloud Manager->Network Clouds*. Figure 26 shows the Network Cloud summary.



Network Cloud Summary

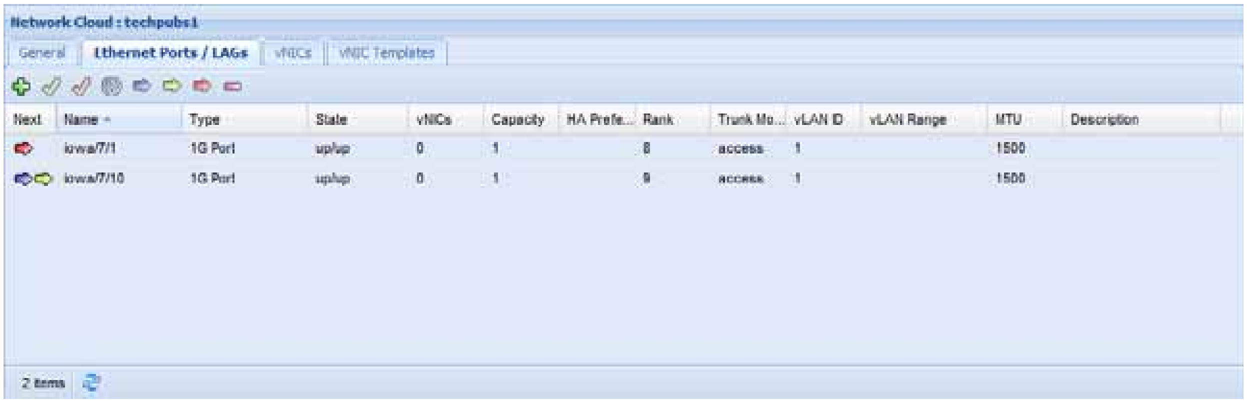
Name	Number of Ports	Number of Lags	Number of vNI...	Number of vNI...	Description
backup	3	0	0	0	
Cloud9	3	0	0	3	
devtest	2	0	0	0	
discovered-network-cloud	32	0	103	0	
EngNWcloudA	1	0	0	1	Engineering Network Activity
management	2	0	0	0	
netapp1	2	0	0	0	
production	2	0	0	0	
techpubs1	0	0	0	3	

14 items

Figure 26 network Cloud Summary

Step 2 Select a Network Cloud to populate the details frame with its properties.

Step 3 Click the *Ethernet Ports/LAGs* tab to display the Fibre Channel ports associated with the Storage Cloud as shown in Figure 27.



Network Cloud : techpubs1

Next	Name	Type	State	vNICs	Capacity	HA Prefe...	Rank	Trunk Mo...	vLAN ID	vLAN Range	MTU	Description
	iowa/7/1	1G Port	up/up	0	1		8	access	1		1500	
	iowa/7/10	1G Port	up/up	0	1		9	access	1		1500	

2 items

Figure 27 Network Cloud Details Frame — *Ethernet Ports/LAG* Tab

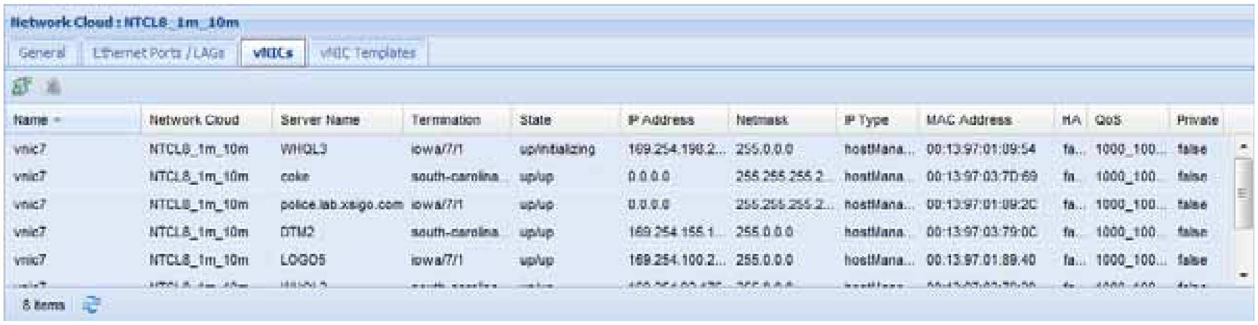
Displaying the vNICs Associated with a Network Cloud

When vNICs are either associated with an I/O Profile or deployed to a host server, those vNICs are displayed through the *vNICs* tab on the Network Cloud details frame. The *vNICs* tab displays only vNICs that are actually deployed on a host server, not the vNICs that are connected to a Network Cloud. As a result, it is possible that the vNICs tab is empty even though a Network Cloud actually has vNICs connected to it.

To display the vNICs associated with a Network Cloud, follow this procedure:

Step 1 Display the Network Cloud Details frame.

Step 2 Click the *vNICs* tab as shown in Figure 28.



Network Cloud : NTCL8_1m_10m

Name	Network Cloud	Server Name	Termination	State	IP Address	Netmask	IP Type	MAC Address	HA	QoS	Private
vnic7	NTCL8_1m_10m	WHQL3	iowa/7/1	up/initializing	169.254.190.2...	255.0.0.0	hostMana...	00:13:97:01:09:54	fa...	1000_100...	false
vnic7	NTCL8_1m_10m	coke	south-carolina...	up/up	0.0.0.0	255.255.255.2...	hostMana...	00:13:97:03:7D:69	fa...	1000_100...	false
vnic7	NTCL8_1m_10m	police.lab.xsigo.com	iowa/7/1	up/up	0.0.0.0	255.255.255.2...	hostMana...	00:13:97:01:09:2C	fa...	1000_100...	false
vnic7	NTCL8_1m_10m	DTM2	south-carolina...	up/up	169.254.155.1...	255.0.0.0	hostMana...	00:13:97:03:79:0C	fa...	1000_100...	false
vnic7	NTCL8_1m_10m	LOGOS	iowa/7/1	up/up	169.254.100.2...	255.0.0.0	hostMana...	00:13:97:01:89:40	fa...	1000_100...	false

8 items

Figure 28 Network Cloud Details — *vNICs* Tab

Applying Network Cloud Changes to vNICs in the Cloud

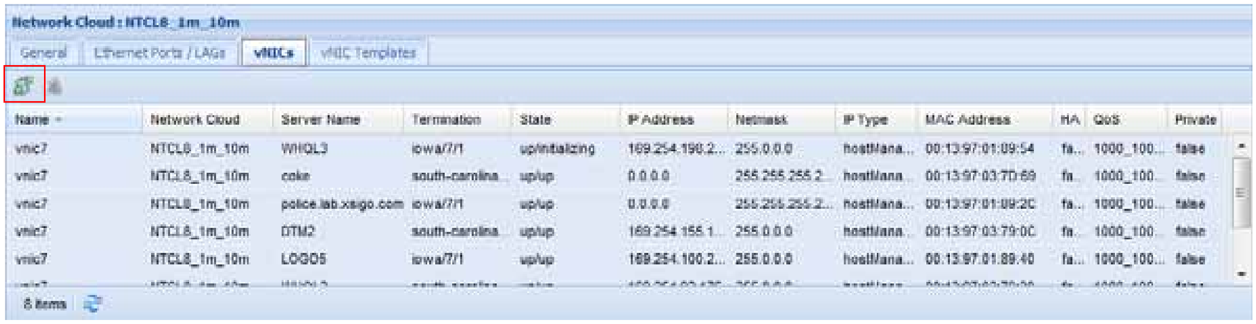
Properties from the Network Cloud can be inherited by the vNICs that attach to that cloud. For example, VLAN IDs and Network QoS profiles are properties for the Network Cloud that can be inherited by the vNICs that attach to it. For more information, see Understanding a Network Cloud.

If a Network Cloud's properties have been edited after vNICs are attached. The new properties for the Network Cloud are not automatically inherited by the currently attached vNICs. Instead, you must manually push those changes to the vNICs that are currently attached to the cloud. New vNICs that are attached after the cloud's properties were changed will receive the new properties, but currently connected vNICs do not receive the new cloud properties until you apply those changes. You can apply network cloud changes to currently attached vNICs by using the ***Apply Network Cloud changes*** button on the Network Cloud details frame.

To apply changed cloud properties to currently attached vNICs, follow this procedure:

Step 1 Display the Network Cloud details frame.

Step 2 Click the *vNICs* tab as shown in Figure 29.



Network Cloud : NTCL8_1m_10m

Name	Network Cloud	Server Name	Termination	State	IP Address	Netmask	IP Type	MAC Address	HA	QoS	Private
vnic7	NTCL8_1m_10m	WHQL3	iowa/7/1	up/initializing	169.254.190.2...	255.0.0.0	hostMana...	00:13:97:01:09:54	fa...	1000_100...	false
vnic7	NTCL8_1m_10m	coke	south-carolina...	up/up	0.0.0.0	255.255.255.2...	hostMana...	00:13:97:03:7D:69	fa...	1000_100...	false
vnic7	NTCL8_1m_10m	police.lab.xsigo.com	iowa/7/1	up/up	0.0.0.0	255.255.255.2...	hostMana...	00:13:97:01:09:2C	fa...	1000_100...	false
vnic7	NTCL8_1m_10m	DTM2	south-carolina...	up/up	169.254.155.1...	255.0.0.0	hostMana...	00:13:97:03:79:0C	fa...	1000_100...	false
vnic7	NTCL8_1m_10m	LOGO5	iowa/7/1	up/up	169.254.100.2...	255.0.0.0	hostMana...	00:13:97:01:89:40	fa...	1000_100...	false

Figure 29 Network Cloud Details — *vNICs* Tab

Step 3 Select the vNIC to which you want to push the Network Cloud changes. This step activates the ***Apply Cloud Changes to vNICs*** button.

Step 4 Click the ***Apply Cloud Changes to vNICs*** button to push all the new Network Cloud properties to the currently selected vNICs.

After a brief period of time, the vNICs have the new cloud properties.

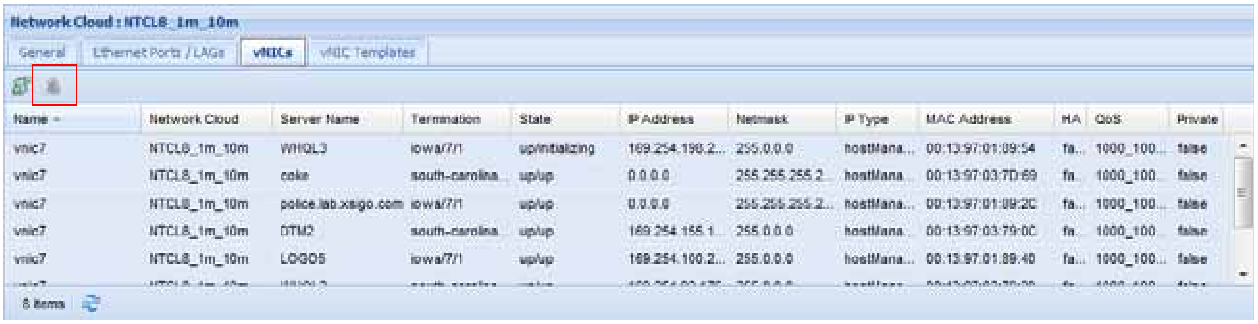
Terminating vNICs in a Network Cloud on Another vNIC Cloud

Some management tasks might require you to move a vNIC to a different Network Cloud. For example, if you need to run diagnostics on an Ethernet port, or perhaps service an I/O Module. In such cases, if other Network Clouds are available and have available Ethernet ports, you can change the termination of a vNIC from one cloud to another through Fabric Manager. If you change the termination of a vNIC with live traffic, a service interruption will occur.

To terminate a vNIC on another Network Cloud, follow this procedure:

Step 1 Display the Network Cloud details frame.

Step 2 Click the *vNICs* tab as shown in Figure 30.



Network Cloud : NTCL8_1m_10m

Name	Network Cloud	Server Name	Termination	State	IP Address	Netmask	IP Type	MAC Address	HA	QoS	Private
vnic7	NTCL8_1m_10m	WHQL3	iowa/7/1	up/initializing	169.254.198.2...	255.0.0.0	hostMana...	00:13:97:01:09:54	fa...	1000_100...	false
vnic7	NTCL8_1m_10m	coke	south-carolina...	up/up	0.0.0.0	255.255.255.2...	hostMana...	00:13:97:03:7D:69	fa...	1000_100...	false
vnic7	NTCL8_1m_10m	police.lab.xsigo.com	iowa/7/1	up/up	0.0.0.0	255.255.255.2...	hostMana...	00:13:97:01:09:2C	fa...	1000_100...	false
vnic7	NTCL8_1m_10m	DTM2	south-carolina...	up/up	169.254.155.1...	255.0.0.0	hostMana...	00:13:97:03:79:0C	fa...	1000_100...	false
vnic7	NTCL8_1m_10m	LOGOS	iowa/7/1	up/up	169.254.100.2...	255.0.0.0	hostMana...	00:13:97:01:89:40	fa...	1000_100...	false

8 items

Figure 30 Network Cloud Details — *vNICs* Tab

Step 3 Select the vNIC in the Network Cloud you want to terminate on a different Network Cloud. This step activates the ***Terminate vNICs on another Cloud*** button.

Step 4 Click the ***Terminate vNICs on another Cloud*** button to push all the new Network Cloud properties to the currently selected vNICs.

Step 5 From the resulting dialog, select the Network Cloud on which you want to terminate the selected vNIC. This step activates the ***Submit*** button.

Step 6 Click ***Submit*** to reterminate the selected vNIC.

After a brief period of time, the vNIC are terminated on available Gigabit Ethernet ports in the new Network Cloud.

Displaying the vNIC Templates Associated with a Network Cloud

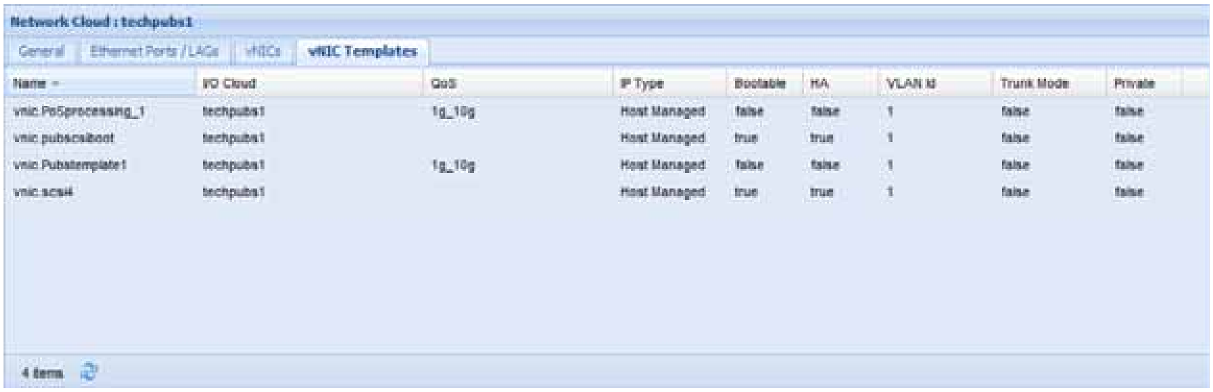
Network Clouds are part of I/O Templates, which in turn, are used in creating the I/O Profiles that are deployed to servers. Through the *vNIC Templates* tab, Oracle's Xsigo Fabric Manager supports a way of seeing all the vNIC Templates that are associated with a specific Network Cloud. This tab shows the association between vNICs in a template and the I/O Cloud regardless of the state of the vNIC being bound or not.

The *vNIC Templates* tab shows information only. You cannot manage the vNIC Templates associated with a specific Network Cloud.

To display the vNIC Templates for a specific Network Cloud, follow this procedure:

Step 1 Display the Network Cloud details frame.

Step 2 Click the vNIC Templates tab as shown in Figure 31.



Name	I/O Cloud	QoS	IP Type	Bootable	HA	VLAN Id	Trunk Mode	Private
vnic.PoSprocessing_1	techpubs1	1g_10g	Host Managed	false	false	1	false	false
vnic.pubscsiboot	techpubs1		Host Managed	true	true	1	false	false
vnic.Pubstemplate1	techpubs1	1g_10g	Host Managed	false	false	1	false	false
vnic.scsi4	techpubs1		Host Managed	true	true	1	false	false

4 items

Figure 31 Network Cloud Details — *vNIC Templates* Tab

Working with Storage Clouds

This chapter contains the following topics:

Understanding Storage Clouds

Oracle's Xsigo Fabric Directors contain a set of I/O ports that are connected to your data center SAN. The SAN administrator connects these ports to their Fibre Channel switches in order to provide I/O resources to the servers.

Each I/O port on the Xsigo system can be thought of as providing access to a set of "clouds". For example, you might have a Storage Cloud that is zoned to give access to a set of LUNs used by HR. As far as the storage administrator is concerned, you are connecting wires to the Xsigo I/O ports for the sole purpose of providing the server administrator access to the resources.

The server administrator then needs to connect the servers to a set of storage resources provided by the storage administrators. The server administrator doesn't care what physical Xsigo ports are being connected to as long as the servers have access to the required resources.

Storage Clouds can be configured and managed by Storage and Administrator roles.

SAN QoS Profiles and Storage Clouds

If you want a specific SAN QoS Profile assigned to a Storage Cloud, that specific profile must already exist. If it does not exist, it will not be assignable to the Storage Cloud at the time you create the cloud.

Oracle's Xsigo Fabric Manager has some commonly used SAN QoS Profiles that are pre-configured for various Fibre Channel link speeds. These pre-configured SAN QoS Profiles use typical CIR and PIR values calculated from the link's total throughput. If you are using pre-configured SAN QoS Profiles, make sure that you use a reasonable profile.

SAN QoS can be configured for a Storage Cloud at any of the following times:

- During Storage Cloud creation, through the Create Storage Cloud wizard.
- After the Storage Cloud has already been created, through the Storage Cloud Details frame.
- SAN QoS can also be changed for a Storage Cloud after the Storage Cloud has already been created. Changing an assigned SAN QoS Profile occurs through the Storage Cloud Details frame.

For information about SAN QoS Profiles, see Working with SAN QoS.

QoS Assignment at Cloud Level and vHBA Level

It is possible to assign SAN QoS to a Storage Cloud or a vHBA. The following text explains where and how QoS get applied:

- If a Storage Cloud has a QoS Profile associated with it, a vHBA terminated in the Storage Cloud will inherit the Storage QoS Profile from the Storage Cloud.

  In this case, the vHBAs inherit the QoS parameters from their respective clouds. This condition is true even if the vHBA has its own QoS Profile associated with it.

- If a Storage Cloud has no QoS Profile associated with it, and the vHBAs have their own QoS profiles, a vHBA terminated in the Storage Cloud will have the QoS profile associated with it.

  In this case, the Storage Cloud has no QoS Profile to apply. This situation *does not* automatically apply no QoS to the vHBAs. Instead, it causes the cloud to defer to the QoS profiles assigned to the individual vHBAs (if any).

  If you intend for no QoS to be applied anywhere for the virtual I/O in a cloud, make sure that no QoS Profile is associated with the Storage Cloud, and also that no QoS is associated with the vHBA.

Creating a Storage Cloud

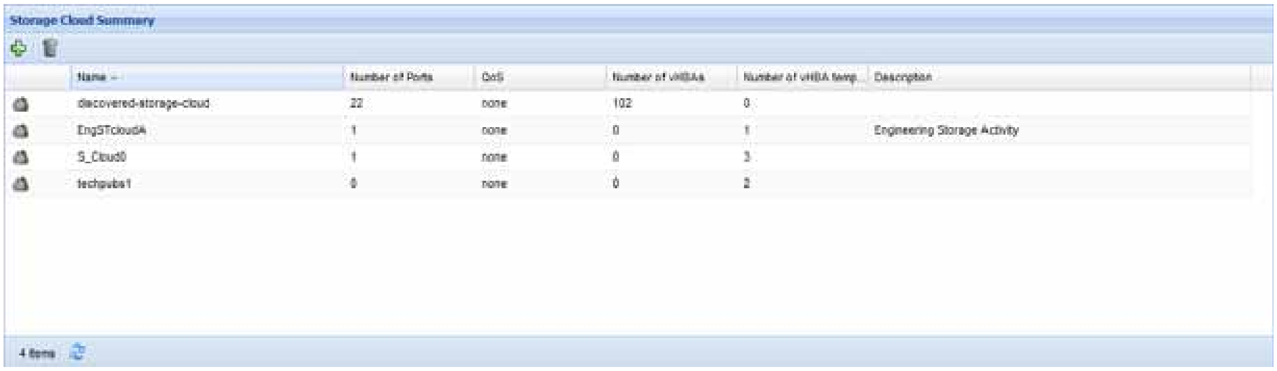
When you create a Storage Cloud, you associate one or more Fibre Channel ports that have been assigned to a Fibre Channel switch with the cloud. Other SAN characteristics (such as SAN QoS) are also associated with the Storage Cloud. When the Storage Cloud is attached to an I/O Template, the Storage Cloud eventually provides a way for hosts to attach to the storage network after an I/O Profile containing the Storage Cloud is pushed to the hosts. The Storage Cloud provides needed storage access points with specified characteristics—for example, SAN QoS.

A default Storage Cloud exists, which contains all the discovered Fibre Channel ports available to Fabric Manager through the discovered Fabric Director(s). This default Storage Cloud is a way to show you the total number of termination points that are under management by Fabric Manager. The total number shown does not decrement when ports are assigned to a specific Storage Cloud, since those ports have not been removed from Fabric Manger—they are just reassigned to a different object.

Storage Clouds typically are created around some similar theme for the Fibre Channel ports that are associated with it. For example, a Storage Cloud might have ports that provide vHBA connections to a specific zone or controller, for a specific set of host servers.

Creating a Storage Cloud occurs through the *Storage Clouds* option in the Storage Resources Manager on the navigation panel. To create a Storage Cloud, follow this procedure:

Step 1 On the Navigation panel, select *Storage Resource Manager->Storage Clouds* to display the Storage Cloud Summary. Figure 1 shows this page.



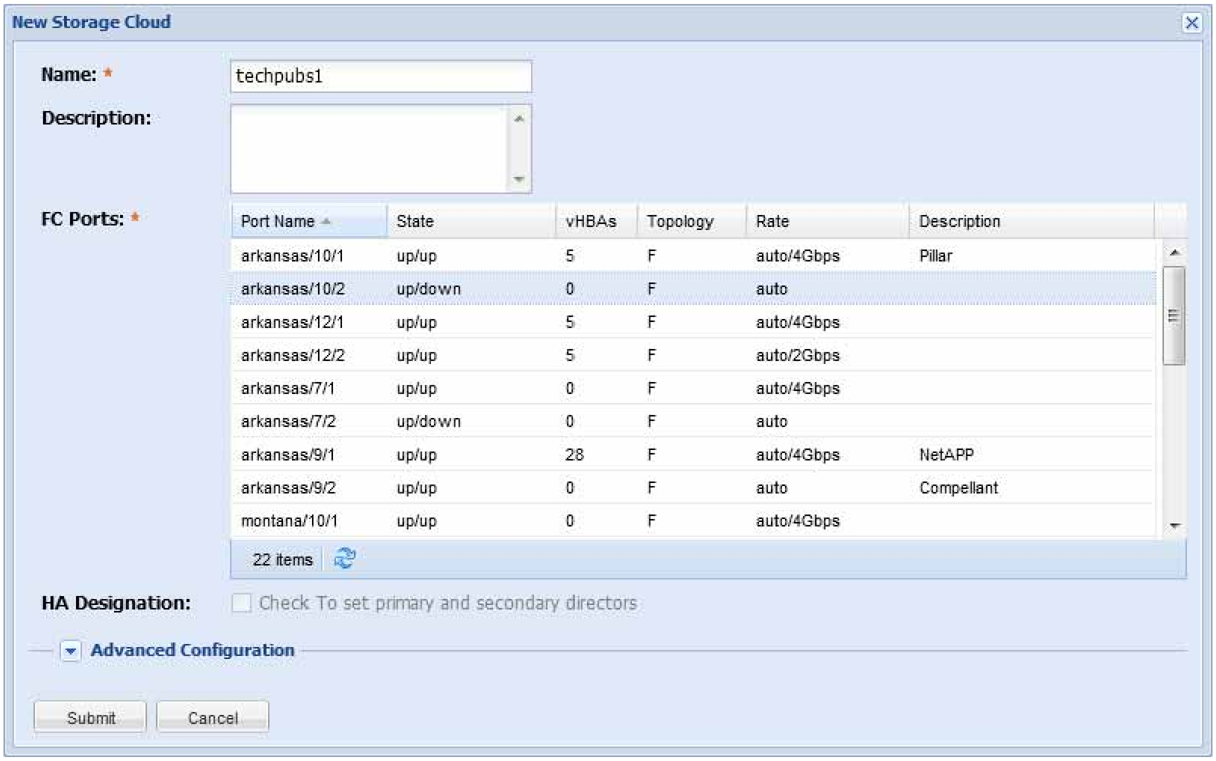
Name	Number of Ports	QoS	Number of vHBAs	Number of vHBA temp...	Description
discovered-storage-cloud	22	none	102	0	
EngSTcloudA	1	none	0	1	Engineering Storage Activity
S_Cloud0	1	none	0	3	
techpubs1	0	none	0	2	

Figure 1 Storage Cloud Summary

Notice the default Storage Cloud (discovered-storage-cloud) in this example. This example also shows that specific Storage Clouds (non-default clouds) are configured.

Adding and deleting Storage Clouds occurs through the plus sign and garbage can icons, respectively.

Step 1 Click the plus sign (+) to display the Create a New Storage Cloud dialog. Figure 2 shows this dialog.



Name: * techpubs1

Description:

FC Ports: *

Port Name	State	vHBAs	Topology	Rate	Description
arkansas/10/1	up/up	5	F	auto/4Gbps	Pillar
arkansas/10/2	up/down	0	F	auto	
arkansas/12/1	up/up	5	F	auto/4Gbps	
arkansas/12/2	up/up	5	F	auto/2Gbps	
arkansas/7/1	up/up	0	F	auto/4Gbps	
arkansas/7/2	up/down	0	F	auto	
arkansas/9/1	up/up	28	F	auto/4Gbps	NetAPP
arkansas/9/2	up/up	0	F	auto	Compellant
montana/10/1	up/up	0	F	auto/4Gbps	

22 items

HA Designation: □ Check To set primary and secondary directors

Figure 2 Create a New Storage Cloud

Step 2 In the *Name* field, enter a name for the Storage Cloud that you are creating.

Step 3 As an option, in the *Description* field, enter a description for the Storage Cloud that you are creating.

Step 4 From the *FC Ports* table, select the port(s) that will be used in this Storage Cloud. Ports are selected when they are highlighted. Multiple ports can be assigned to the same Storage Cloud, and multiple Storage Clouds can be assigned to the same port(s).

Step 5 When the correct properties have been assigned for the Storage Cloud, click ***Submit*** to create the Storage Cloud. When you click ***Submit***, a dialog is briefly displayed that informs you that Fabric Manager client and server are exchanging data.

Step 6 Check the Storage Cloud Summary to verify that the Storage Cloud was successfully created.

Configuring Features in the Storage Cloud

Because Storage Clouds contain Fibre Channel ports, many standard features that are applicable to physical FC ports (for example, SAN QoS) are configurable on Storage Clouds. Storage Clouds support configuration of the following features:

- SAN QoS
- Port Allocation Policy

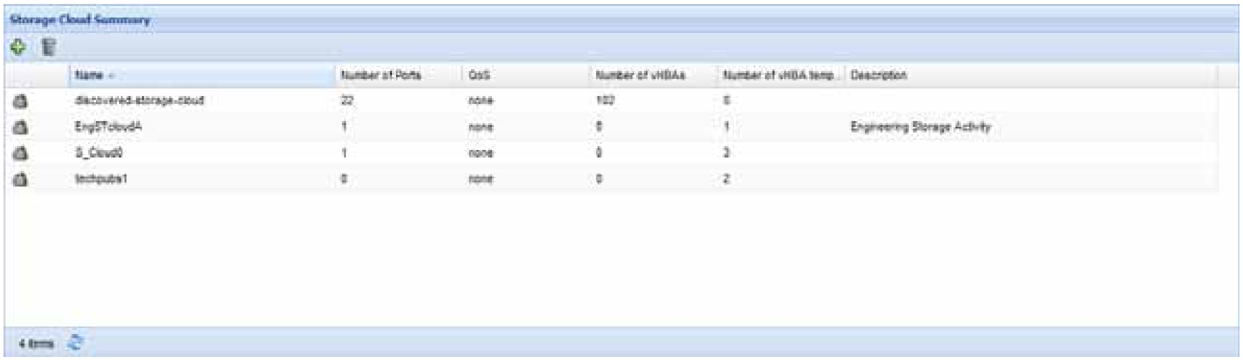
See the following sections for how to configure these features for the Storage Cloud.

Setting SAN QoS on a Storage Cloud

Setting Storage QoS on a Storage Cloud can occur at the cloud level or on the vHBA level. When SAN QoS is applied to a Storage Cloud, all vHBAs associated with the cloud will get the specified CIR value. If a vHBA also has SAN QoS and is added to the Storage Cloud, the cloud's SAN QoS takes precedence. For more information about SAN QoS and Storage Clouds, see Working with SAN QoS.

To configure SAN QoS for a Storage Cloud, follow this procedure. This procedure assumes that the SAN QoS Profile already exists. If it does not, you will need to create the SAN QoS Profile.

Step 1 Display the Storage Cloud Summary (*Storage Resources Manager->Storage Clouds*). Figure 3 shows the Storage Cloud Summary.



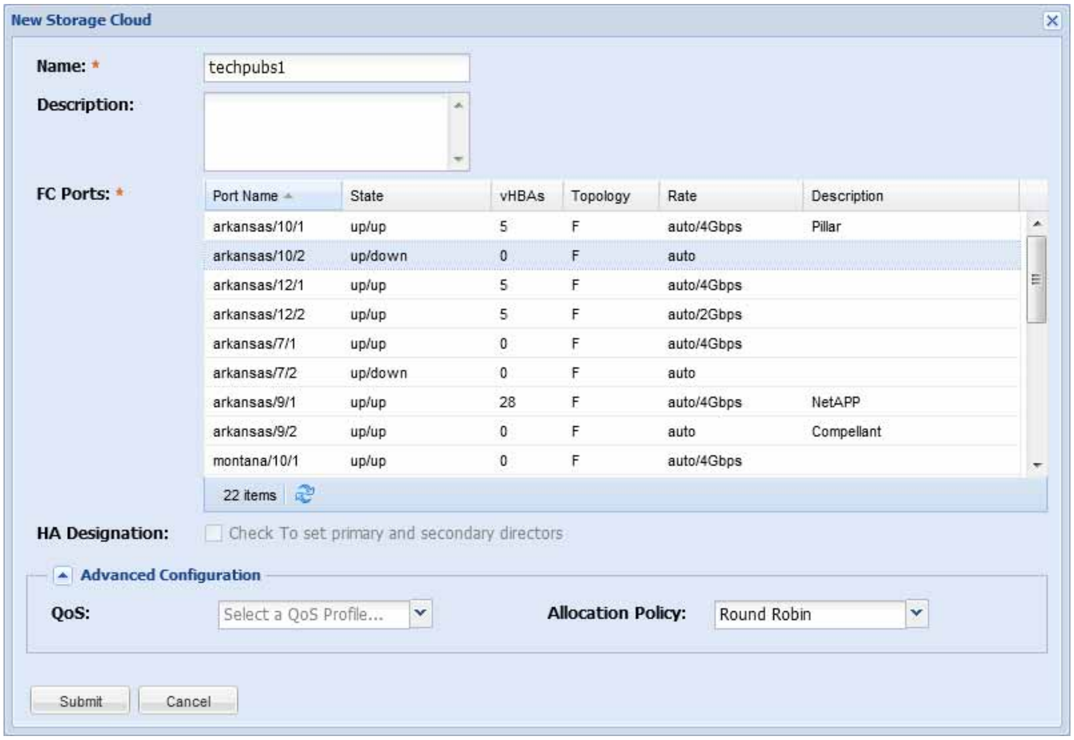
Storage Cloud Summary

Name	Number of Ports	QoS	Number of vHBAs	Number of vHBA temp...	Description
discovered-storage-cloud	22	none	102	6	
EngSTcloudA	1	none	0	1	Engineering Storage Activity
S_Cloud0	1	none	0	3	
techpubs1	0	none	0	2	

4 items

Figure 3 Storage Cloud Summary

Step 2 Click the plus sign to display the New Storage Cloud dialog. Figure 4.



New Storage Cloud

Name: * techpubs1

Description:

FC Ports: *

Port Name	State	vHBAs	Topology	Rate	Description
arkansas/10/1	up/up	5	F	auto/4Gbps	Pillar
arkansas/10/2	up/down	0	F	auto	
arkansas/12/1	up/up	5	F	auto/4Gbps	
arkansas/12/2	up/up	5	F	auto/2Gbps	
arkansas/7/1	up/up	0	F	auto/4Gbps	
arkansas/7/2	up/down	0	F	auto	
arkansas/9/1	up/up	28	F	auto/4Gbps	NetAPP
arkansas/9/2	up/up	0	F	auto	Compellant
montana/10/1	up/up	0	F	auto/4Gbps	

22 items

HA Designation: □ Check To set primary and secondary directors

Advanced Configuration

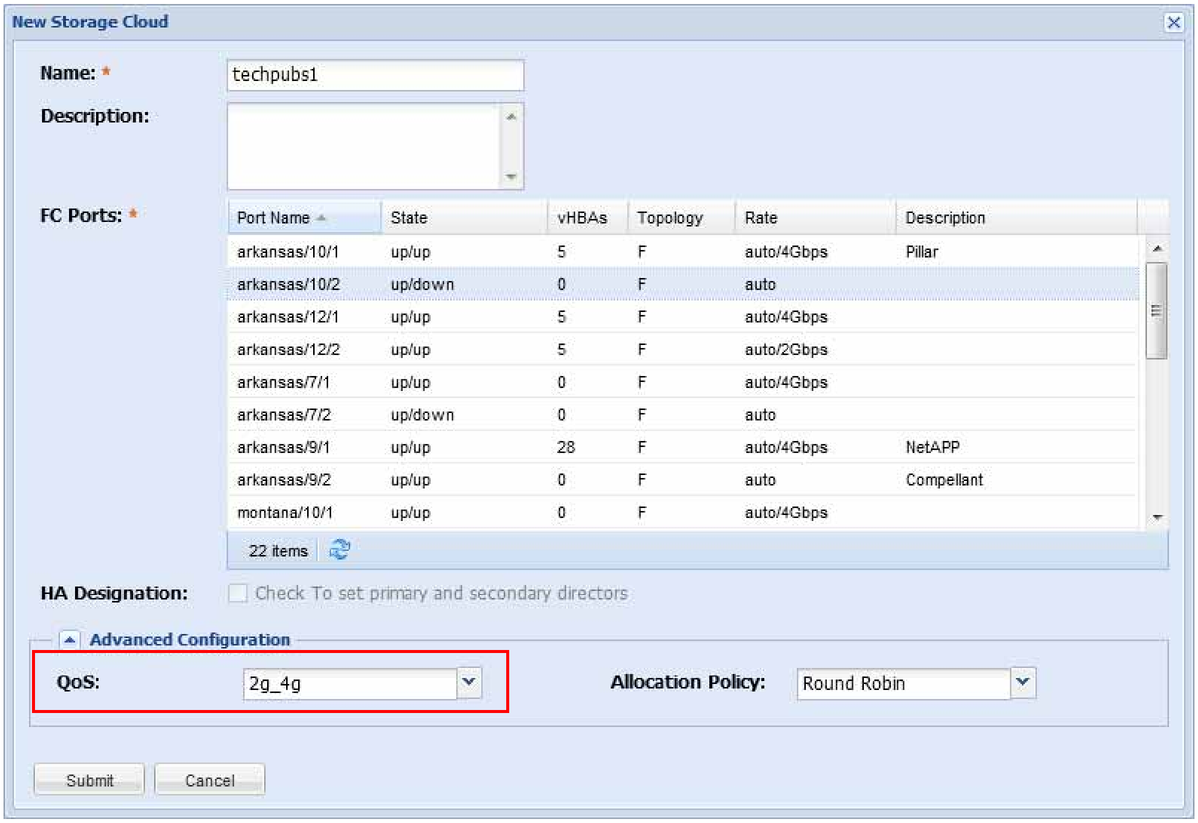
QoS: Select a QoS Profile...

Allocation Policy: Round Robin

Figure 4 New Storage Cloud

Step 3 Select at least one fibre channel port for creating the Storage Cloud.

Step 4 On the New Storage Cloud dialog, click the *Advanced Configuration* button to display the QoS dropdown menu as shown in Figure 5.



Name: * techpubs1

Description:

FC Ports: *

Port Name	State	vHBAs	Topology	Rate	Description
arkansas/10/1	up/up	5	F	auto/4Gbps	Pillar
arkansas/10/2	up/down	0	F	auto	
arkansas/12/1	up/up	5	F	auto/4Gbps	
arkansas/12/2	up/up	5	F	auto/2Gbps	
arkansas/7/1	up/up	0	F	auto/4Gbps	
arkansas/7/2	up/down	0	F	auto	
arkansas/9/1	up/up	28	F	auto/4Gbps	NetAPP
arkansas/9/2	up/up	0	F	auto	Compellant
montana/10/1	up/up	0	F	auto/4Gbps	

22 items

HA Designation: ☐ Check To set primary and secondary directors

Advanced Configuration

QoS: 2g_4g

Allocation Policy: Round Robin

Figure 5 New Storage Cloud, QoS Dropdown Menu

In this example, a new SAN QoS Profile configured for 2 Gbps of CIR and 4 Gbps Mbps of PIR (2g_4g) is being applied to the Storage Cloud.

Step 5 Click ***Submit*** to assign the new SAN QoS Profile to the selected Storage Cloud. You will be prompted with a confirmation message. Click ***Yes*** to assign the SAN QoS profile or ***No*** to abort assigning the SAN QoS Profile to the Storage Cloud.

Step 6 Check the QoS field of the Storage Cloud Details Frame to verify that the correct SAN QoS Policy is assigned.

Setting an Allocation Policy for a Storage Cloud

An allocation policy determines how ports are assigned from the Storage Cloud to any vHBA that is connected to the cloud. In order for the port to be allocated, it must already be configured in the Storage Cloud. Multiple ports can be configured in a Storage Cloud, and ports from different Fibre Channel modules, and even different Oracle Fabric Directors, can be configured in the same Storage Cloud.

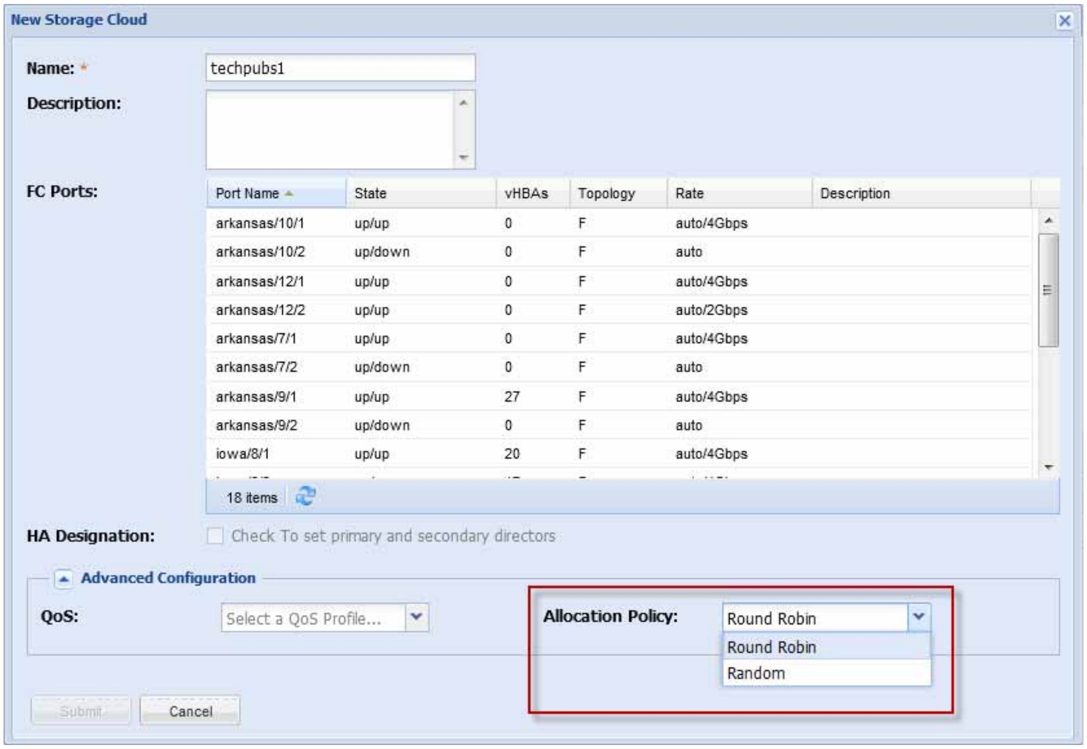
The following allocation policy exists:

- Round Robin, which is a systematic way for ports to be assigned. With round robin allocation, you specify multiple ports in a list of available ports for a Storage Cloud. When the list is constructed, you then assign a port as the next available port. When you assign the next available port, it gets a rank that is different than any other port in the available ports list. The port you assign is the next port to be assigned, and after that, any additional vHBAs that are connected to the Storage Cloud will receive a fibre channel port based on its rank. For example, assume you create a Storage Cloud with fibre channel port 2/1 as the port used to create the cloud. Then, assume you add ports 2/2, 4/1, and 5/1 to the available ports list, and set port 4/1 as the next available port. When new vHBAs are connected to the Storage Cloud, the first vHBA is connected to port 4/1. After that, additional vHBAs are assigned to whichever port has the next lowest rank.

To set an allocation policy for a storage cloud, follow this procedure:

Step 1 If you have not already done so, create a Storage Cloud with at least one fibre channel port in it, as documented in Creating a Storage Cloud.

Step 2 When the Storage Cloud is created, click the *Advanced Configuration* button to display the Allocation Policy dropdown menu.



New Storage Cloud

Name: * techpubs1

Description:

FC Ports:

Port Name	State	vHBAs	Topology	Rate	Description
arkansas/10/1	up/up	0	F	auto/4Gbps	
arkansas/10/2	up/down	0	F	auto	
arkansas/12/1	up/up	0	F	auto/4Gbps	
arkansas/12/2	up/up	0	F	auto/2Gbps	
arkansas/7/1	up/up	0	F	auto/4Gbps	
arkansas/7/2	up/down	0	F	auto	
arkansas/9/1	up/up	27	F	auto/4Gbps	
arkansas/9/2	up/down	0	F	auto	
iowa/8/1	up/up	20	F	auto/4Gbps	

18 items

HA Designation: □ Check To set primary and secondary directors

Advanced Configuration

QoS: Select a QoS Profile...

Allocation Policy: Round Robin

Figure 6 New Storage Cloud

Step 3 From the Allocation Policy dropdown menu, select the method you want to use to allocate fibre channel ports from the Storage Cloud:

- Round Robin allocates port in the cloud by rotating through the unallocated fibre channel ports in a systematic way starting from the port you select when you create the Storage Cloud. When using round robin port allocation, you will need to select a list of the ports available in the round robin queue. When the list is specified, anytime a vHBA is connected to the Storage Cloud, Fabric Manager will step through the list and allocate the next available port based on numerical value of the port’s slot. For example, For example, assume the following ports are available in the Storage

Cloud: port 2 in slot 2, port 1 in slot 4, and port 2 in slot 9. When new vHBAs are connected to the Storage Cloud, the first vHBA will be terminated on port 2 slot 2, the next vHBA will be connected to port 1 in slot 4, and the last vHBA will be terminated on port 2 in slot 9.

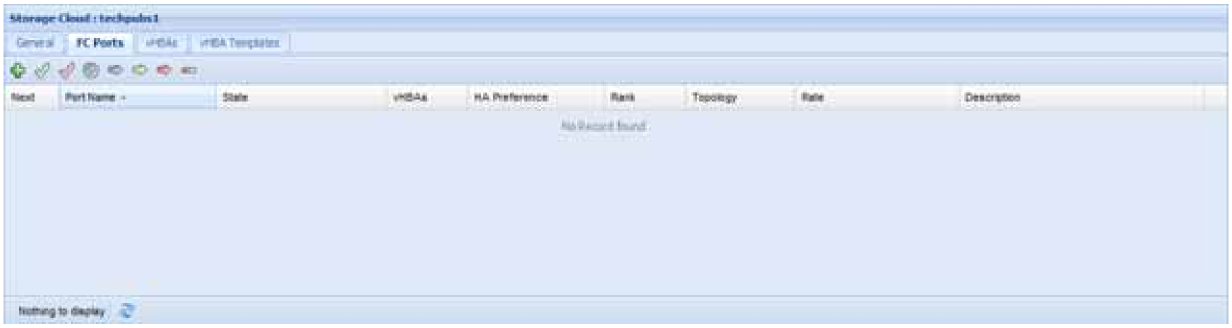
Note

A port can only belong to one Storage Cloud. As a result, make sure that the ports in your round robin list are not also part of another Storage Cloud.

Step 4 When the Allocation Policy is selected, click ***Submit*** to create the Storage Cloud.

Step 5 On the Storage Cloud Summary, select the Storage Cloud you just created. When you do so, the details frame will contain additional information about the selected Storage Cloud.

Step 6 Click the *FC Ports* tab to display the list of fibre channel ports in the Storage Cloud.



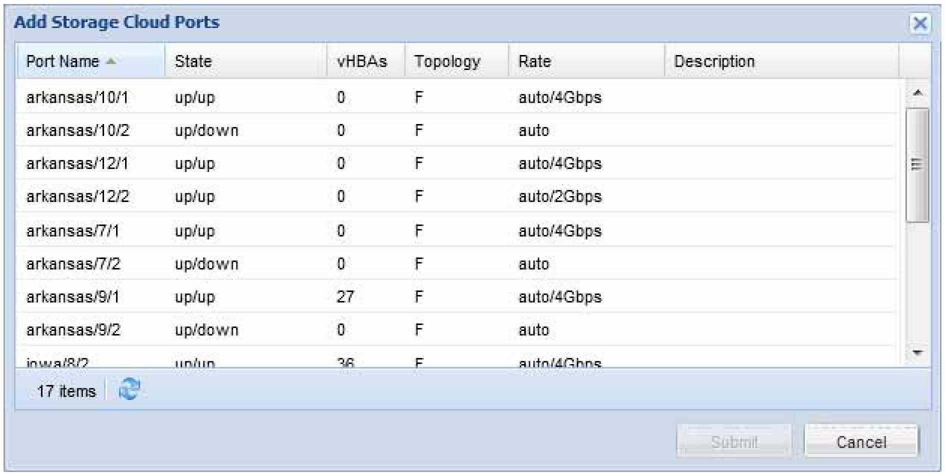
Next	Port Name	State	vHBAs	HA Preference	Rank	Topology	Rate	Description

No Record found

Nothing to display

Figure 7 Storage Cloud Details Frame — FC Ports Tab

Step 7 Click the plus sign (+) to display the Add Storage Cloud Ports dialog, as shown in Figure 8.



Port Name	State	vHBAs	Topology	Rate	Description
arkansas/10/1	up/up	0	F	auto/4Gbps	
arkansas/10/2	up/down	0	F	auto	
arkansas/12/1	up/up	0	F	auto/4Gbps	
arkansas/12/2	up/up	0	F	auto/2Gbps	
arkansas/7/1	up/up	0	F	auto/4Gbps	
arkansas/7/2	up/down	0	F	auto	
arkansas/9/1	up/up	27	F	auto/4Gbps	
arkansas/9/2	up/down	0	F	auto	
iowa/8/2	up/up	36	F	auto/4Gbps	

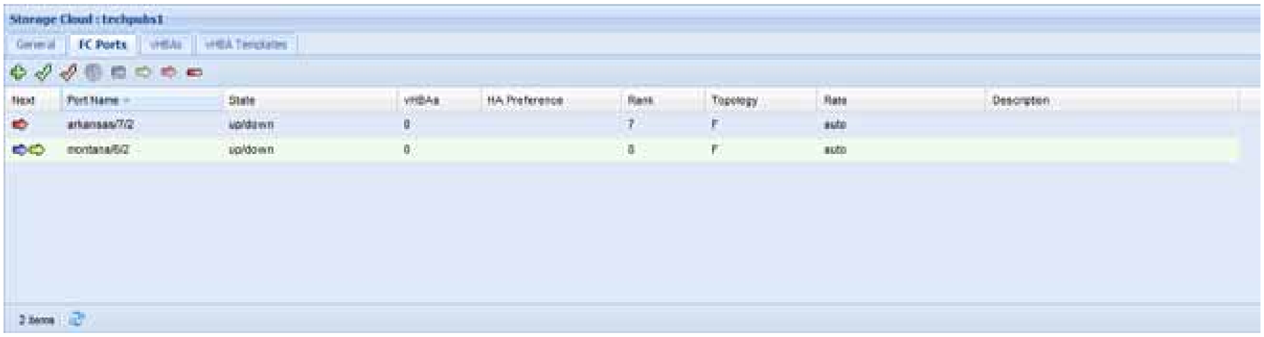
17 items

Figure 8 Add Storage Cloud Ports Dialog

Step 8 Select the port(s) that you want to add to the list of ports. When you do, the ***Submit*** button becomes active.

Step 9 Click ***Submit*** to add the selected ports to the list.

Step 10 After the correct storage ports have been added to the Storage Cloud, click the blue arrow on the toolbar to set the next available port in the list.



Next	Port Name	State	vHBAs	HA Preference	Rank	Topology	Rate	Description
	arkansas/7/2	up/down	0		7	F	auto	
	montana/6/2	up/down	0		8	F	auto	

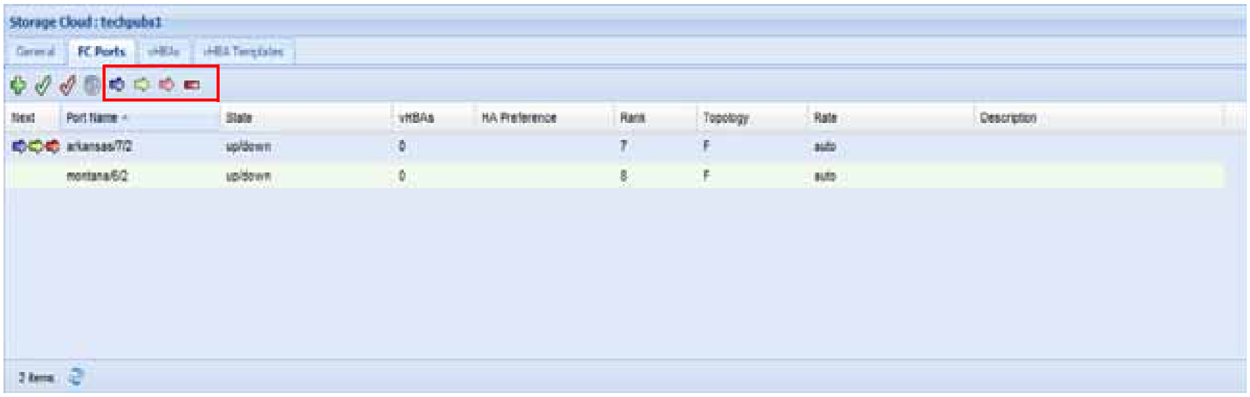
Figure 9 Storage Cloud Details Frame — Next Port for Round Robin Algorithm

After the next available port is selected, Fabric Manager will begin the round robin queue from that port, and assign fibre channel ports in ascending numerical order based on the *Rank* field. You can set the rank by specifying the next port for each port in the list. When each "next port" is specified, it gets a unique rank number, which is used in selecting the next available port in the round robin algorithm.

Step 11 When all ports in the list are selected, click ***Submit*** to finalize the list. It is a good idea to double check the rank associated with each port in the list because this is the criteria used by the round robin algorithm. Ports with lower ranks are assigned before ports with higher ranks.

Changing the Port Priority for a Storage Cloud

The port priority for a storage cloud can be changed by selecting a different option from the toolbar on the ***FC Ports*** tab, as shown in Figure 10.



Next	Port Name	State	vHBAs	HA Preference	Rank	Topology	Rate	Description
	arkansas/7/2	up/down	0		7	F	auto	
	montana/6/2	up/down	0		8	F	auto	

Figure 10 FC Ports Tab, Port Priority Options

This toolbar contains the following buttons for setting port priority:

- ***Mark the next port to be assigned*** (the blue arrow). This option is available for standalone vHBAs (non-HA/non-multipath).
- ***Mark the next primary port to be assigned*** (the green arrow). This option is available only for HA/multipath vHBAs.
- ***Mark the next secondary port to be assigned*** (the red arrow). This option is available only for HA/multipath vHBAs.

If the available ports list has only one port, and the port priority is set incorrectly, you might need to delete the port list, then recreate it. You can delete ports from the port availability list by selecting the port you want to delete, then clicking the red dash.

Note

Fibre Channel ports are listed in a modified ascending order. So, for example, port `iowa1/1` is listed before port `iowa 2/1` as expected. However, port `iowa1/10` and `iowa11/1` would also be listed before port `iowa2/1`.

Due to the listing order in the *FC Ports* tab, you will need to pay attention to which port you select as the next available by moving the arrows around. For example, if you want the round robin policy to start with port `iowa1/1` and the next port to be assigned as port `iowa2/1`, you cannot just move the arrow to the next port down in the list because this might be port `iowa11/1` (not `iowa1/2`). Without paying close attention to the listing order, you might accidentally assign the wrong port(s). As a result, the round robin policy will operate correctly, but do so based on the incorrect ports you inadvertently assigned.

To change the port priority in the list, follow this procedure:

Step 1 Select the port for which you want to set or change the port priority. The port is selected when it is highlighted in the *FC Ports* tab. You will also notice that the port priority toolbar buttons become active.

Step 2 Click the appropriate button to set the port priority for the selected port:

- For non-HA/non-multipath vHBAs, only the blue arrow is valid.
- For HA/multipath vHBAs, use the green arrow to set the port to be assigned as the primary port for the vHBA. Then, use the red arrow to set the port that will be next assigned as the secondary vHBA.

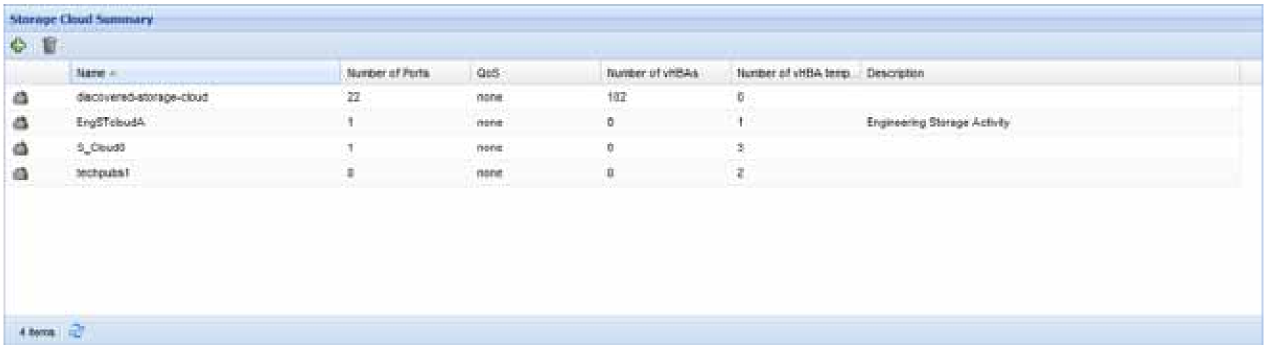
Displaying Storage Clouds

Storage Clouds are displayed in the summary and details frame of the work panel, which provide information about the configured Storage Clouds.

Displaying Summary Information for Storage Clouds

The Storage Cloud Summary is a table of all the configured Storage Clouds, including the default Storage Cloud (discovered-storage-cloud). Additional, detailed information about each Storage Cloud is contained in the Storage Cloud Details frame, which is located directly below the Storage Cloud Summary.

Figure 11 shows the Storage Cloud Summary.



Storage Cloud Summary

Name	Number of Ports	QoS	Number of vHBAs	Number of vHBA temp...	Description
discovered-storage-cloud	22	none	102	0	
EngSTcloudA	1	none	0	1	Engineering Storage Activity
5_Cloud3	1	none	0	3	
techpubs1	8	none	0	2	

4 items

Figure 11 Storage Cloud Summary

Table 1 shows the field contained in the Storage Cloud Summary and explains what each one means.

Table 1 Contents of the Storage Cloud Summary

Field	Indicates
Name	The name of each configured Storage Cloud.
Number of Ports	The number of Fibre Channel Ports in the Storage Cloud. This number is the total of all ports, regardless of whether they are up or down.
QoS	The name of any SAN QoS Profile associated with the Storage Cloud. If no SAN QoS is configured, this field indicates “none”. If a SAN QoS Profile is configured for the Storage Cloud, the name indicates the CIR and PIR values. For example, a QoS Profile named 125M_250M indicates 125 Mbps of CIR and 250 Mbps of PIR.

Table 1 (continued) Contents of the Storage Cloud Summary

Field	Indicates
Number of vHBAs	The total number of vHBAs connected to the Storage Cloud.
Number of vHBA Templates	The total number of vHBAs in I/O Templates that are associated with the Storage Cloud.
Description	The description string (if any) that was applied to the Storage Cloud. If this field is blank, either no description string was specified when the Storage Cloud was created, or the Storage Cloud was originally created with a description string, but the Storage Cloud was later edited and the description string was removed.

Displaying Detailed Information for Storage Clouds

The Storage Cloud Details frame is a section of the work panel that is located below the Storage Cloud Summary. The Storage Cloud Details frame is typically a list of fields for a selected Storage Cloud, a list of FC ports contained in the Storage Cloud, or a list of fields for a selected FC port in the Storage Cloud.

The Storage Cloud Details frame enables you to display additional, detailed information for a single Storage Cloud including the default Storage Cloud (discovered-storage-ports). For non-default Storage Clouds, you can use the Storage Cloud Details frame to edit various aspects of the cloud itself, or the components of it. The Storage Cloud Details has the following controls, which are common on most details frames for features throughout the entire Fabric Manager interface:

- add and delete buttons, a plus sign and a red dash, respectively
- tabs, which logically organize additional information about the contents of the details frame
- an ***Edit*** button, which unlocks editable parts of the details frame so that you can set or change information elements for the contents of the details frame

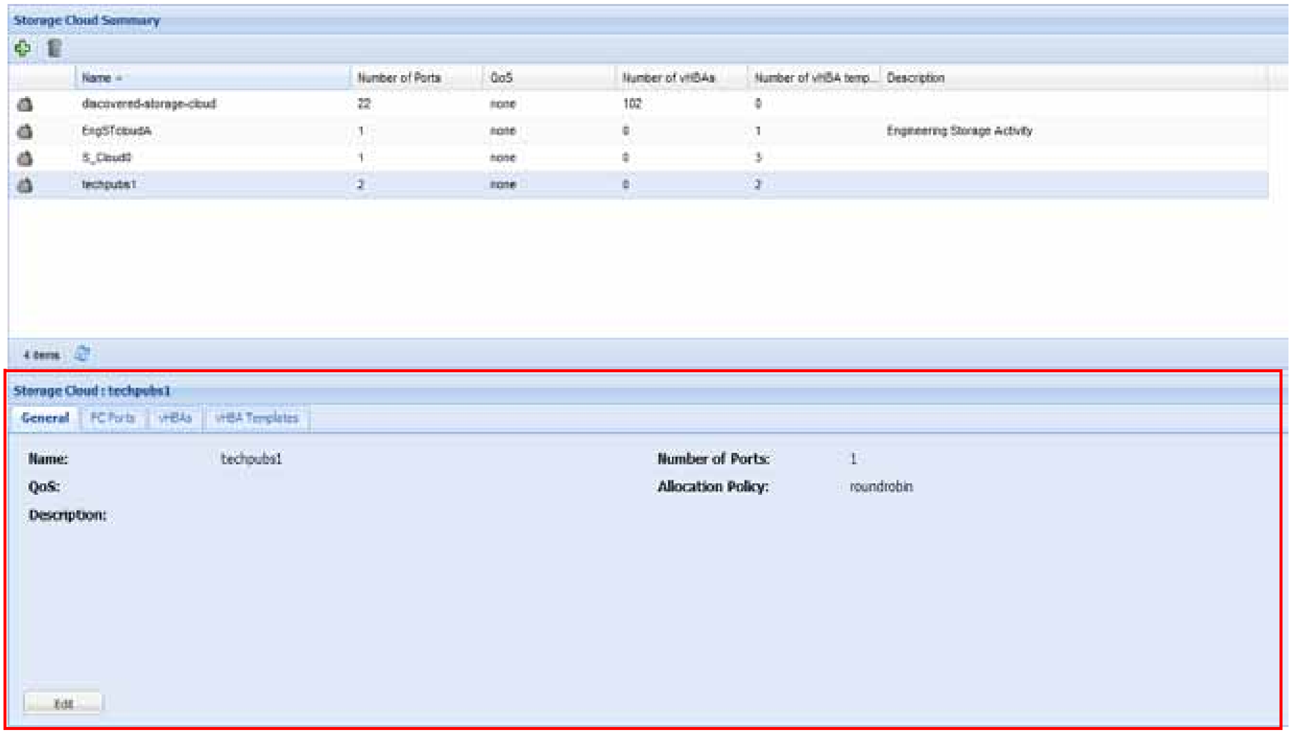
To use the Storage Cloud Details frame, you must first select a configured cloud from the Storage Cloud Summary. By selecting a cloud from the summary, you set the focus of the Storage Cloud Details frame. When the cloud is selected in the summary, you will see its details displayed in the Details frame.

Through the Storage Cloud details frame, you can edit properties for the Storage Cloud.

Note

Anytime you edit a Storage Cloud to make changes, it is a best practice to manually push those changes to the vHBAs that are associated with that cloud. For more information, see Pushing Cloud Changes to vHBAs in an I/O Template.

Figure 12 shows the Storage Cloud Details frame. Notice that the details frame is contextual, so that it displays detailed information for the item selected in the Storage Cloud Summary.



Name	Number of Ports	QoS	Number of vHBAs	Number of vHBA temp...	Description
discovered-storage-cloud	22	none	102	0	
EngSTcloudA	1	none	0	1	Engineering Storage Activity
S_Cloud0	1	none	0	3	
techpubs1	2	none	0	2	

Name: techpubs1

QoS:

Description:

Number of Ports: 1

Allocation Policy: roundrobin

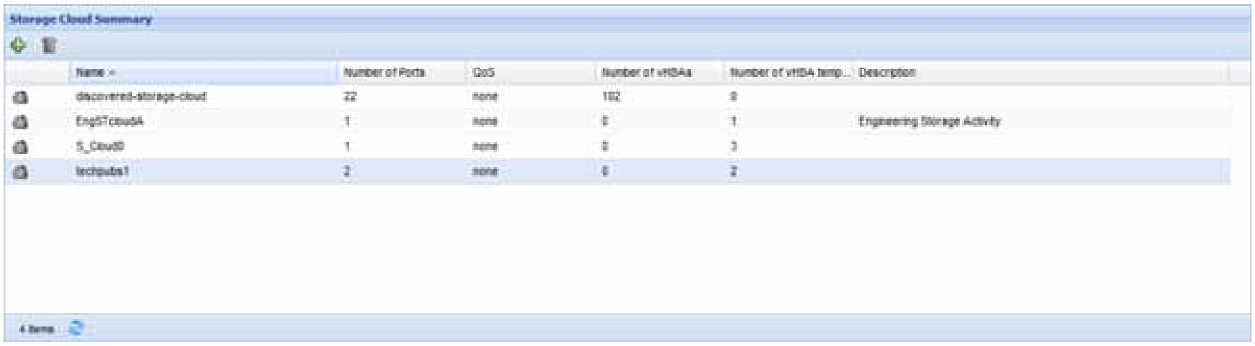
Figure 12 Storage Cloud Details Frame

Renaming a Storage Cloud

Fabric Manager supports renaming a Storage Cloud, which enables you to change the name without having to completely delete and recreate the entire Storage Cloud. When the Storage Cloud is renamed, all other properties for the Storage Cloud are retained, including the ports and vHBAs associated with the cloud. As an option, you can also set or change the description for the Storage Cloud.

You can rename the Storage Cloud through the Storage Cloud Details frame. To rename the Storage Cloud, follow this procedure:

Step 1 On the Navigation Frame, select *Storage Cloud Manager->Storage Clouds*. Figure 13 shows the Storage Cloud summary.



Storage Cloud Summary

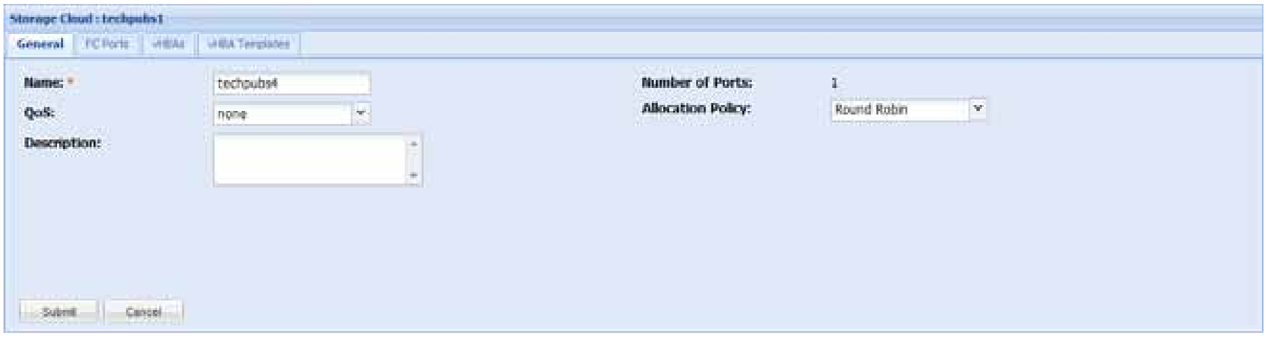
	Name	Number of Ports	QoS	Number of vHBAs	Number of vHBA temp...	Description
	discovered-storage-cloud	22	none	102	0	
	EngSTcloudA	1	none	0	1	Engineering Storage Activity
	S_Cloud0	1	none	0	3	
	techpubs1	2	none	0	2	

4 items

Figure 13 Storage Cloud Summary

Step 2 Select a Storage Cloud to populate the details frame with its properties.

Step 3 Click the ***Edit*** button to edit the properties of the selected Storage Cloud, as shown in Figure 14.



Storage Cloud : techpubs1

Name: * techpubs4

QoS: none

Description:

Number of Ports: 1

Allocation Policy: Round Robin

Figure 14 Storage Cloud Summary — Editing Details to Rename Storage Cloud

Step 4 In the *Name* field, enter the new name for the Storage Cloud.

Step 5 As an option, you also can set or change the description for the selected Storage Cloud.

Step 6 As an option, you also can set or change any of the other editable fields on the details frame.

Step 7 When the new name has been specified for the Storage Cloud, click ***Submit***.

Pushing Cloud Changes to vHBAs in an I/O Template

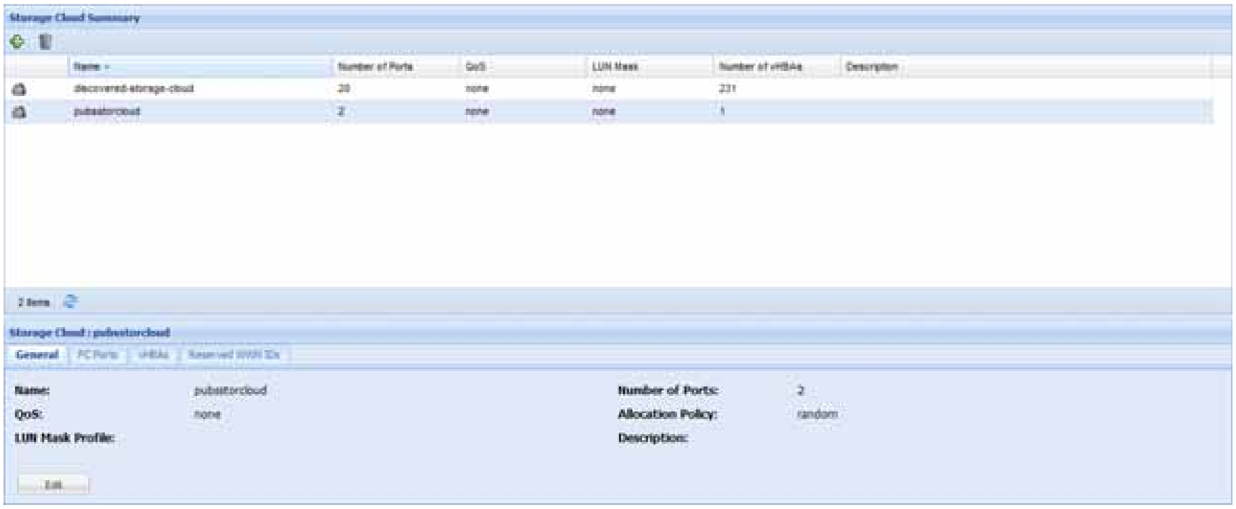
When you configure an I/O Template, you reference Storage Clouds for the termination of the vHBAs that connect the host server. These clouds are external to the template, and they are controlled through a different workflow. Because the cloud(s) and the templates are separate entities, any updates on a cloud must be explicitly forced to the I/O Template. Conceptually, this is intuitive because you are changing a cloud, you are not actually changing anything within the template itself.

If you need to change a cloud property, and that cloud is associated with an I/O Template, be aware that the change you make is not automatically updated in the I/O Template that is using that cloud. However, you can push changes in a Network or Storage Cloud to the I/O Template that is using that cloud by using the ***Re-Apply Cloud Changes to vHBA*** button for Storage Clouds.

To reapply Storage Cloud changes to vHBAs in a template, follow this procedure:

Step 1 Select *Storage Cloud Manager->Storage Clouds* to display the Storage Cloud Summary.

Step 2 Select the Storage Cloud for which you want to make changes. This step populates the details frame with information about the selected Storage Cloud as shown in Figure 15.



Storage Cloud Summary

Name	Number of Ports	QoS	LUN Mask	Number of vHBAs	Description
discovered-storage-cloud	20	none	none	231	
pubstorcloud	2	none	none	1	

2 items

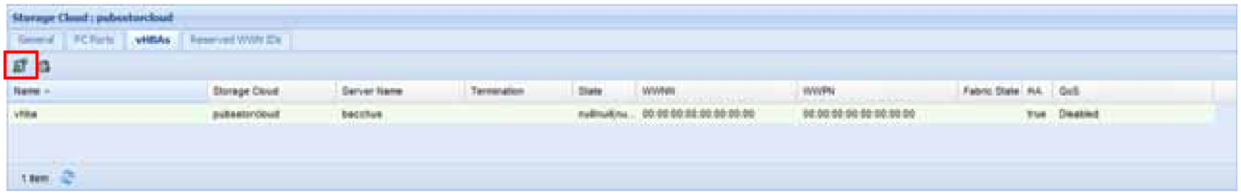
Storage Cloud : pubstorcloud

Name: pubstorcloud
QoS: none
LUN Mask Profile:
Number of Ports: 2
Allocation Policy: random
Description:

Figure 15 Storage Cloud Details Frame

Step 3 In the Cloud Details frame, click the *vHBAs* tab.

Step 4 On the *vHBAs* tab, select the vHBA you want to receive the Storage Cloud changes. This step activates the ***Re-Apply Cloud Changes to vHBA*** button as shown in Figure 16.



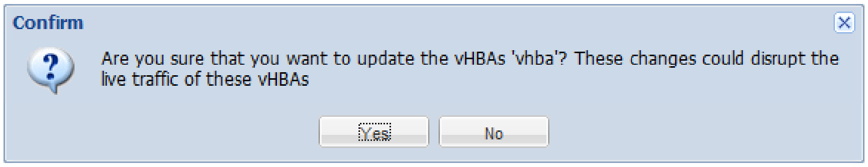
Storage Cloud : pubstorcloud

Name	Storage Cloud	Server Name	Termination	State	WWNN	WWPN	Fabric State	HA	QoS
vhba	pubstorcloud	bacchus		null/null/nu...	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00		true	Disabled

1 item

Figure 16 Applying Storage Cloud Changes to a vHBA

Step 5 Click the button to apply the changes to the vHBA in the template. When you do so, a confirmation dialog is displayed. See Figure 17.



Confirm

Are you sure that you want to update the vHBAs 'vhba'? These changes could disrupt the live traffic of these vHBAs

Figure 17 Confirming the Storage Cloud Changes to a vHBA in a Template

Step 6 Click ***Yes*** to make the changes. When you do, the Storage Cloud changes are pushed to the vHBA.

Displaying the Fibre Channel Ports in a Storage Cloud

Each Storage Cloud contains one or more Fibre Channel ports that provide the termination point for vHBAs connected to the cloud. For each Storage Cloud, you can display a list of all the Fibre Channel ports in a particular cloud. In addition to displaying the ports in the cloud, you can:

- remove Fibre Channel ports from the Storage Cloud
- control the port allocation policy for each Fibre Channel port in the Storage Cloud

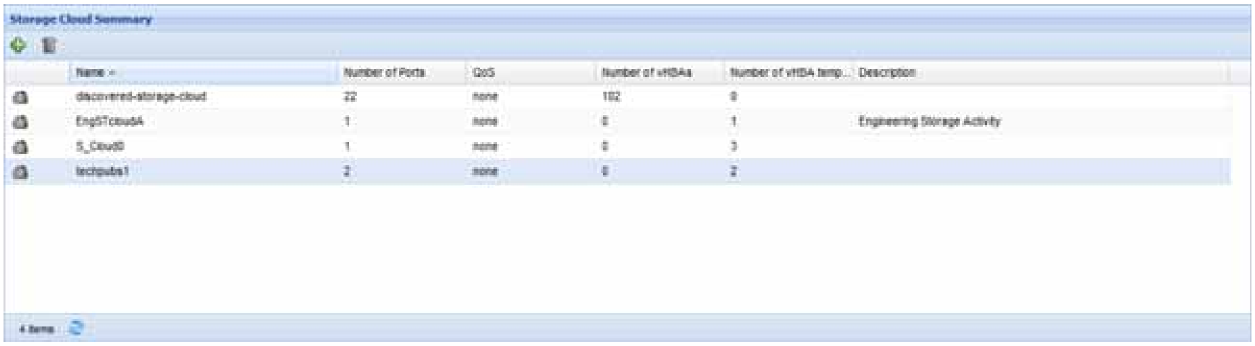
Note

Fibre Channel ports are listed in a modified ascending order. So, for example, port `iowa1/1` is listed before port `iowa 2/1` as expected. However, port `iowa1/10` and `iowa11/1` would also be listed before port `iowa2/1`.

Due to the listing order in the *FC Ports* tab, you will need to pay attention to which port you select as the next available by moving the arrows around. For example, if you want the round robin policy to start with port `iowa1/1` and the next port to be assigned as port `iowa2/1`, you cannot just move the arrow to the next port down in the list because this might be port `iowa11/1` (not `iowa1/2`). Without paying close attention to the listing order, you might accidentally assign the wrong port(s). As a result, the round robin policy will operate correctly, but do so based on the incorrect ports you inadvertently assigned.

To display the Fibre Channel ports, follow this procedure:

Step 1 On the Navigation Frame, select *Storage Cloud Manager->Storage Clouds*. Figure 18 shows the Storage Cloud summary.



Storage Cloud Summary

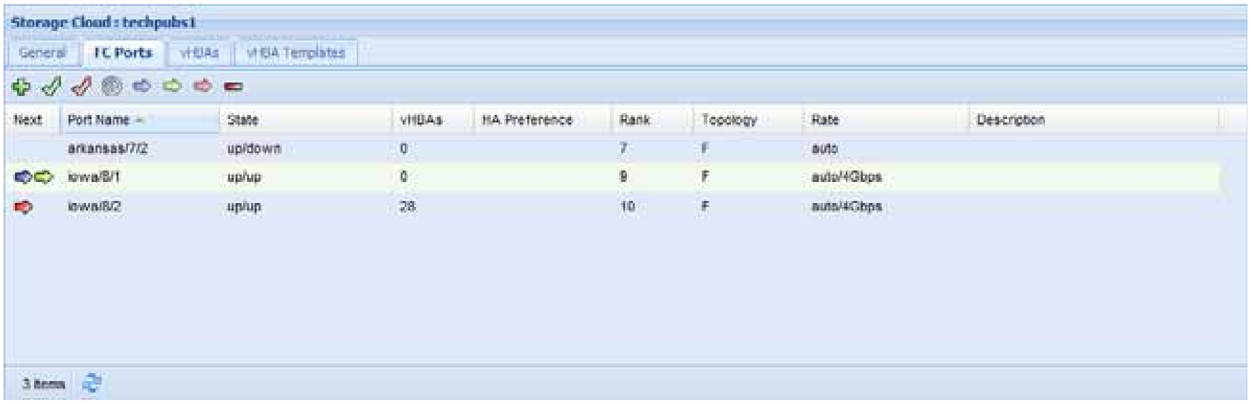
Name	Number of Ports	QoS	Number of vHBAs	Number of vHBA temp...	Description
discovered-storage-cloud	22	none	102	0	
EngSTcloudA	1	none	0	1	Engineering Storage Activity
S_Cloud0	1	none	0	3	
techpubs1	2	none	0	2	

4 items

Figure 18 Storage Cloud Summary

Step 2 Select a Storage Cloud to populate the details frame with its properties.

Step 3 Click the *FC Ports* tab to display the Fibre Channel ports associated with the Storage Cloud as shown in Figure 19.



Storage Cloud : techpubs1

Next	Port Name	State	vHBAs	HA Preference	Rank	Topology	Rate	Description
	arkansas/7/2	up/down	0		7	F	auto	
➡ ➡	iowa/8/1	up/up	0		9	F	auto/4Gbps	
➡	iowa/8/2	up/up	28		10	F	auto/4Gbps	

3 items

Figure 19 Storage Cloud Details — *FC Ports* Tab

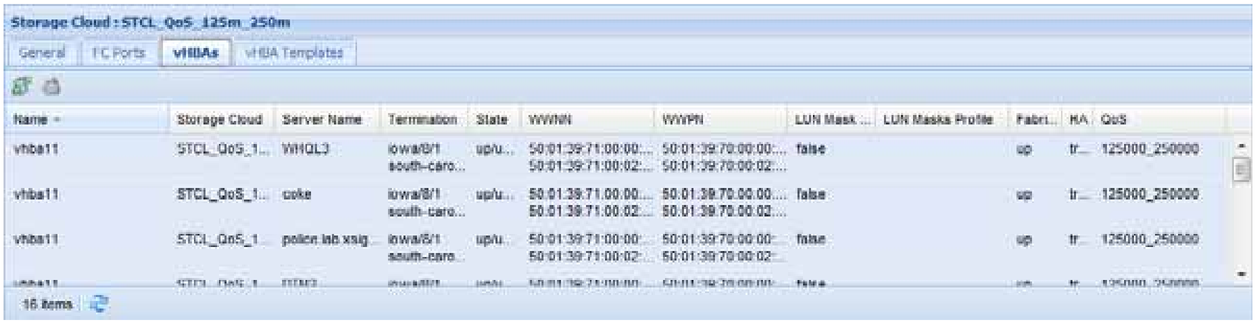
Displaying the vHBAs Associated with a Storage Cloud

When vHBAs are either associated with an I/O Profile or deployed to a host server, those vHBAs are displayed through the *vHBAs* tab on the Storage Cloud details frame. The *vHBAs* tab displays only vHBAs that are actually used in an I/O Profile regardless of whether or not the I/O Profile is connected to a host server, not the vHBAs that are connected to a Storage Cloud. As a result, it is possible that the *vHBAs* tab is empty even though a Storage Cloud actually has vHBAs connected to it.

To display the vHBAs associated with a Storage Cloud, follow this procedure:

Step 1 Display the Storage Cloud Details frame.

Step 2 Click the *vHBAs* tab as shown in Figure 20.



Storage Cloud : STCL_QoS_125m_250m

Name	Storage Cloud	Server Name	Termination	State	WWNN	WWPN	LUN Mask ...	LUN Masks Profile	Fabri...	HA	QoS
vhba11	STCL_QoS_1...	WHQL3	iowa/8/1 south-caro...	up/u...	50:01:39:71:00:00:... 50:01:39:71:00:02:...	50:01:39:70:00:00:... 50:01:39:70:00:02:...	false		up	tr...	125000_250000
vhba11	STCL_QoS_1...	coke	iowa/8/1 south-caro...	up/u...	50:01:39:71:00:00:... 50:01:39:71:00:02:...	50:01:39:70:00:00:... 50:01:39:70:00:02:...	false		up	tr...	125000_250000
vhba11	STCL_QoS_1...	police lab xsig...	iowa/8/1 south-caro...	up/u...	50:01:39:71:00:00:... 50:01:39:71:00:02:...	50:01:39:70:00:00:... 50:01:39:70:00:02:...	false		up	tr...	125000_250000

16 items

Figure 20 Storage Cloud Details — *vHBAs* Tab

Applying Storage Cloud Changes to vHBAs in the Cloud

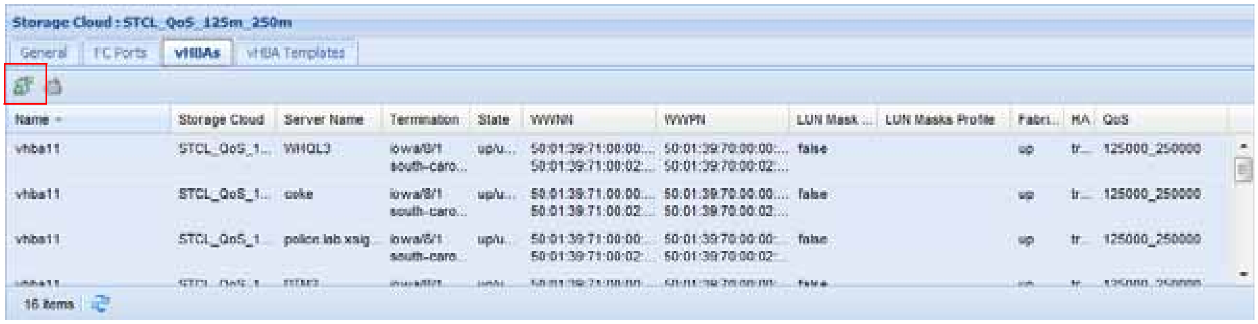
Properties from the Storage Cloud can be inherited by the vHBAs that attach to that cloud. For example, LUN Masks and SAN QoS profiles are properties for the Storage Cloud that can be inherited by the vHBAs that attach to it. For more information, see Understanding Storage Clouds.

If a Storage Cloud's properties have been edited after vHBAs are attached. The new properties for the Storage Cloud are not automatically inherited by the currently attached vHBAs. Instead, you must manually push those changes to the vHBAs that are currently attached to the cloud. New vHBAs that are attached after the cloud's properties were changed will receive the new properties, but currently connected vHBAs do not receive the new cloud properties until you apply those changes. You can apply Storage Cloud changes to currently attached vHBAs by using the ***Apply Storage Cloud changes*** button on the Storage Cloud details frame.

To apply changed cloud properties to currently attached vHBAs, follow this procedure:

Step 1 Display the Storage Cloud details frame.

Step 2 Click the *vHBAs* tab as shown in Figure 21.


Storage Cloud : STCL_QoS_125m_250m

Name	Storage Cloud	Server Name	Termination	State	WWNN	WWPN	LUN Mask ...	LUN Masks Profile	Fabri...	HA	QoS
vhba11	STCL_QoS_1...	WHQL3	iowa/8/1 south-caro...	up/u...	50:01:39:71:00:00:... 50:01:39:71:00:02:...	50:01:39:70:00:00:... 50:01:39:70:00:02:...	false		up	tr...	125000_250000
vhba11	STCL_QoS_1...	coke	iowa/8/1 south-caro...	up/u...	50:01:39:71:00:00:... 50:01:39:71:00:02:...	50:01:39:70:00:00:... 50:01:39:70:00:02:...	false		up	tr...	125000_250000
vhba11	STCL_QoS_1...	pollen.lab.xsig...	iowa/8/1 south-caro...	up/u...	50:01:39:71:00:00:... 50:01:39:71:00:02:...	50:01:39:70:00:00:... 50:01:39:70:00:02:...	false		up	tr...	125000_250000

16 items

Figure 21 Storage Cloud Details — *vHBAs* Tab

Step 3 Select the vHBA to which you want the Storage Cloud's changes pushed. This step activates the ***Apply Cloud Changes to vHBAs*** button.

Step 4 Click the ***Apply Cloud Changes to vHBAs*** button to push all the new Storage Cloud properties to the currently selected vHBA.

After a brief period of time, the vHBA has the new cloud properties.

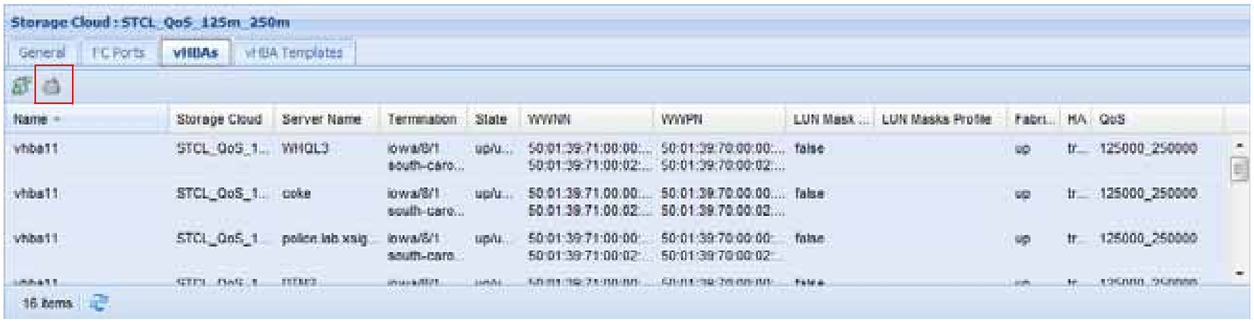
Terminating vHBAs in a Storage Cloud on Another Storage Cloud

Some management tasks might require you to move a vHBA to a different Storage Cloud. For example, if you need to run diagnostics on a Fibre Channel port, or perhaps service an I/O Module. In such cases, if other Storage Clouds are available and have available Fibre Channel ports, you can change the termination of a vHBA from one cloud to another through Fabric Manager. If you change the termination of a vHBA with live traffic, a service interruption will occur.

To terminate a vHBA on another Storage Cloud, follow this procedure:

Step 1 Display the Storage Cloud details frame.

Step 2 Click the *vHBAs* tab as shown in Figure 22.



Storage Cloud : STCL_QoS_125m_250m

Name	Storage Cloud	Server Name	Termination	State	WWNN	WWPN	LUN Mask ...	LUN Masks Profile	Fabri...	HA	QoS
vhba11	STCL_QoS_1...	WHQL3	iowa/8/1 south-caro...	up/u...	50:01:39:71:00:00:... 50:01:39:71:00:02:...	50:01:39:70:00:00:... 50:01:39:70:00:02:...	false		up	tr...	125000_250000
vhba11	STCL_QoS_1...	coke	iowa/8/1 south-caro...	up/u...	50:01:39:71:00:00:... 50:01:39:71:00:02:...	50:01:39:70:00:00:... 50:01:39:70:00:02:...	false		up	tr...	125000_250000
vhba11	STCL_QoS_1...	pollen lab xsig...	iowa/8/1 south-caro...	up/u...	50:01:39:71:00:00:... 50:01:39:71:00:02:...	50:01:39:70:00:00:... 50:01:39:70:00:02:...	false		up	tr...	125000_250000
vhba11	STCL_QoS_1...	[illegible]	iowa/8/1	up/u...	50:01:39:71:00:00:...	50:01:39:70:00:00:...	false		up	tr...	125000_250000

16 items

Figure 22 Storage Cloud Details — *vHBAs* Tab

Step 3 Select the vHBA that you want to terminate on a different Storage Cloud. This step activates the ***Terminate vHBAs on another Cloud*** button.

Step 4 Click the ***Terminate vHBAs on another Cloud*** button to change the vHBA to a new Storage Cloud.

Step 5 From the resulting dialog, select the Storage Cloud on which you want to terminate the selected vHBA. This step activates the ***Submit*** button.

Step 6 Click ***Submit*** to reterminate the selected vHBAs.

After a brief period of time, the vHBAs are terminated on available Fibre Channel ports in the new Storage Cloud.

Displaying the vHBA Templates Associated with a Storage Cloud

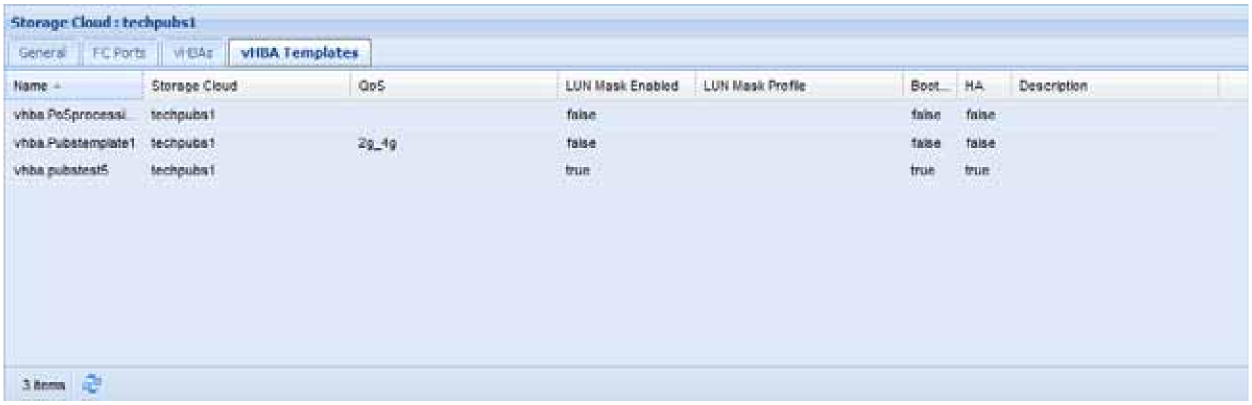
Storage Clouds are part of I/O Templates, which in turn, are used in creating the I/O Profiles that are deployed to servers. Through the *vHBAs Templates* tab, Oracle's Xsigo Fabric Manager supports a way of seeing all the vHBA Templates that are associated with a specific Storage Cloud. This tab shows the association between vHBAs in a template and the Storage Cloud regardless of the state of the vHBAs being bound or not.

The *vNIC Templates* tab shows information only. You cannot manage the vNIC Templates associated with a specific Storage Cloud.

To display the vHBA Templates for a specific Storage Cloud, follow this procedure:

Step 1 Display the Storage Cloud details frame.

Step 2 Click the *vHBA Templates* tab as shown in Figure 23.



Storage Cloud : techpubs1

Name	Storage Cloud	QoS	LUN Mask Enabled	LUN Mask Profile	Boot...	HA	Description
vhba.PoSprocessi...	techpubs1		false		false	false	
vhba.Pubstemplate1	techpubs1	2g_4g	false		false	false	
vhba.pubstest5	techpubs1		true		true	true	

Figure 23 Storage Cloud Details — *vHBA Templates* Tab

Working with Default Gateways

This chapter documents the following topics:

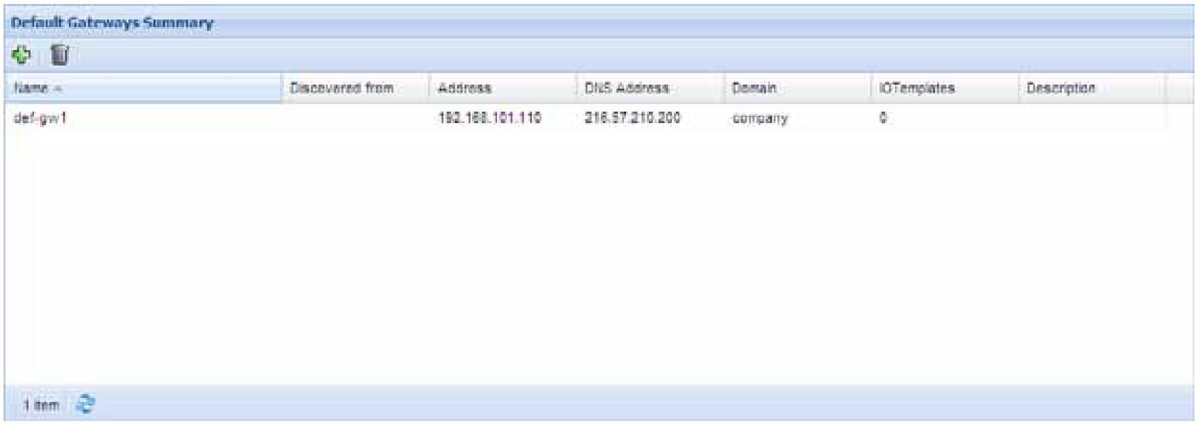
- Understanding Default Gateways
- Displaying Default Gateways
- Creating Default Gateways
- Deleting a Default Gateway

Understanding Default Gateways

A default gateway allows host servers to forward packets with unknown destination addresses off of the server’s local network. When this feature is configured, the Oracle Fabric Director gets a pool of default gateways for all the servers attached to the Fabric Director, and with this pool of default gateways the Fabric Director can support forwarding packets to and from the various networks that hosts use. Each Default Gateway must be manually specified for it to be added to the Default Gateways Summary.

Displaying Default Gateways

Through the Default Gateways Summary, you can display or configure one or more default gateways, which enables host servers to forward unknown packets to vNICs. Each Default Gateway configured in Oracle’s Xsigo Fabric Manager is displayed through the Default Gateways Summary. Figure 1 shows the Default Gateways Summary.



Default Gateways Summary

Name	Discovered from	Address	DNS Address	Domain	IOTemplates	Description
def-gw1		192.168.101.110	216.57.210.200	company	0	

1 item

Figure 1 Default Gateways Summary

Notice that default gateways can be configured or deleted through the Default Gateways Summary.

Table 1 shows the contents of the Default Gateways Summary, and explains what each field means.

Table 1 Contents of the Default Gateways Summary

Field...	Indicates...
Name	The default gateway’s name.
Discovered From	The name or IP address of the Fabric Director from which the default gateway was discovered.
Address	The gateway router’s IP address. The default address is 0.0.0.0.
DNS Address	The DNS server’s IP address. The default address is 0.0.0.0.

Table 1 (continued) Contents of the Default Gateways Summary

Field...	Indicates...
Domain	The domain in which the default gateway is configured.
I/O Templates	The number of I/O Templates that are assigned to hosts that are using each default gateway.
Description	The optional description assigned to the default gateway.

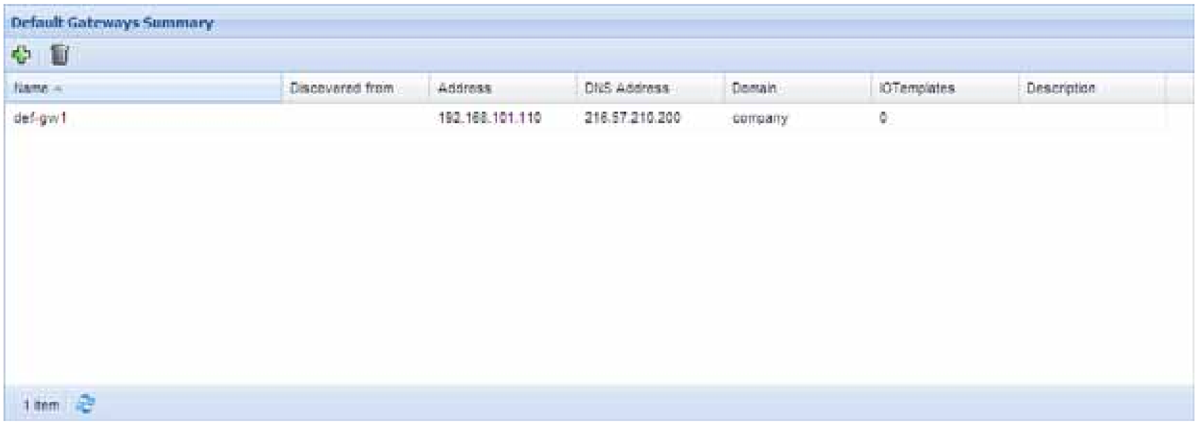
Creating Default Gateways

A default gateway is configured for each host server network attached to the Fabric Director. By doing, you specify the default gateway address for all host servers on that network, and packets will be forwarded off of the server networks as needed.

Default gateways are configured manually, and if you want a specific default gateway assigned to a specific server(s), you can associate the default gateway with an I/O Template, create an I/O Profile from the I/O Template, then deploy that I/O Profile to the server.

Default gateway creation is supported through the Create Default Gateway dialog. To create a default gateway, follow this procedure:

Step 1 On the navigation frame, select Default Gateways to display the Default Gateways summary.



Default Gateways Summary

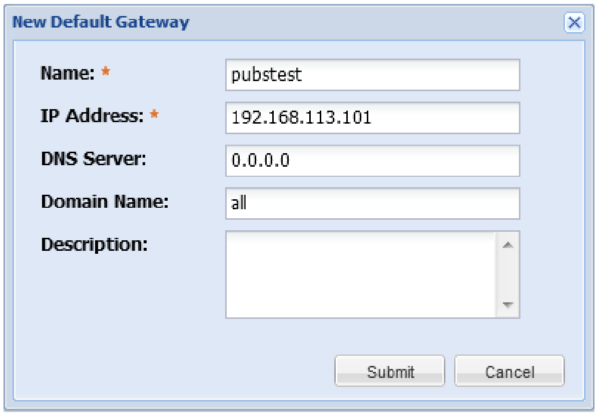
Name	Discovered from	Address	DNS Address	Domain	IOTemplates	Description
def-gw1		192.168.101.110	216.57.210.200	company	0	

1 item

Figure 2 Default Gateways Summary

Notice that you can add or delete default gateways by using the plus sign and garbage can icons, respectively.

Step 2 Click the plus sign to display the Create Default Gateway dialog. Figure 3 shows this dialog.



New Default Gateway

Name: * pubstest

IP Address: * 192.168.113.101

DNS Server: 0.0.0.0

Domain Name: all

Description:

Figure 3 New Default Gateway Dialog

Step 3 In the *Name* field, enter the name you are assigning to the default gateway.

Step 4 In the *IP Address* field, enter the IP Address of the default gateway.

Step 5 In the *DNS Address* field, enter either the IP address or the fully qualified name of the DNS server for the default gateway.

Step 6 In the *Domain Name* field, enter the name of the domain in which the default gateway is configured.

Step 7 As an option, in the *Description* field, enter a short description for the default gateway.

Step 8 Click ***Submit*** to configure the default gateway information. A confirmation dialog is displayed to verify that you want to configure the default gateway.

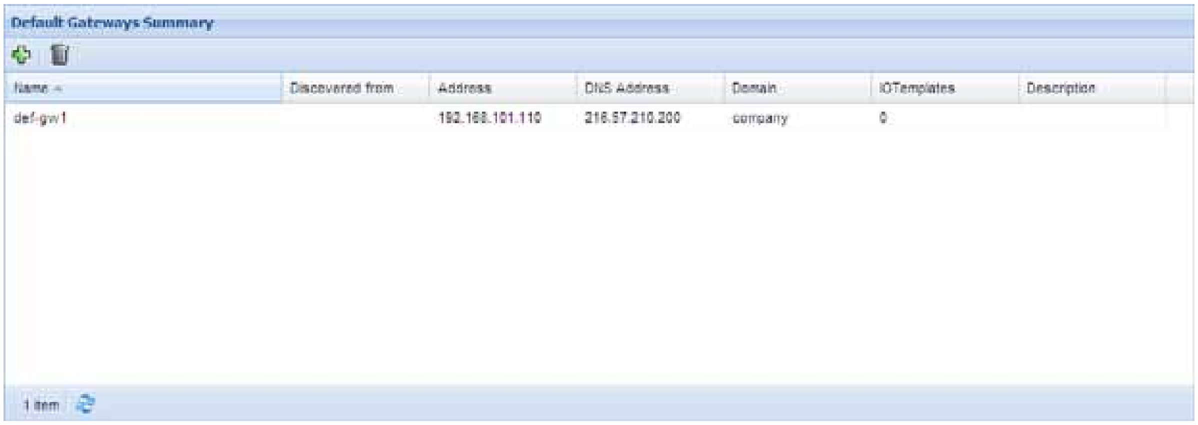
Step 9 On the confirmation dialog, click ***Yes***.

Deleting a Default Gateway

Any default gateway that is configured on an Oracle Fabric Director can be deleted through the Default Gateways Summary. When a default gateway is deleted, the vNICs can no longer forward traffic to destinations on a subnet that is different than the server where the vNIC is deployed.

To delete a default gateway, follow this procedure:

Step 1 On the navigation frame, select Default Gateways to display the Default Gateway summary.



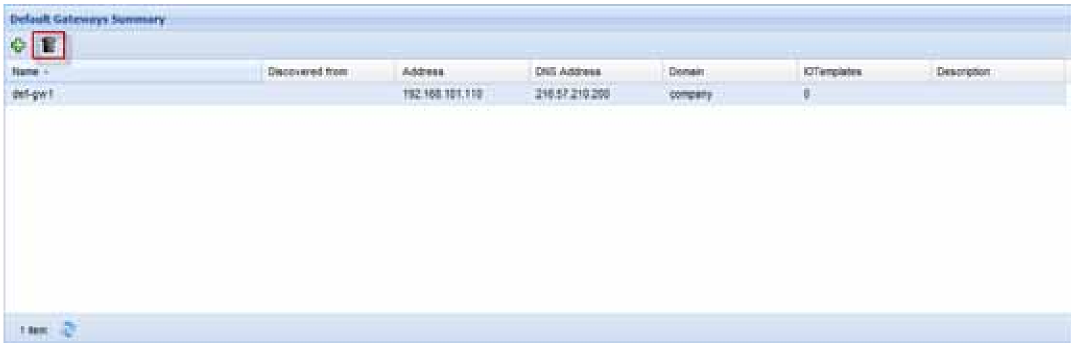
Default Gateways Summary

Name	Discovered from	Address	DNS Address	Domain	IOTemplates	Description
def-gw1		192.168.101.110	216.57.210.200	company	0	

1 item

Figure 4 Default Gateways Summary

Step 2 On the Default Gateways Summary, select the click the default gateway(s) that you want to delete, then click the garbage can icon as shown in Figure 5.



Default Gateways Summary

Name	Discovered from	Address	DNS Address	Domain	IOTemplates	Description
def-gw1		192.168.101.110	216.57.210.200	company	0	

1 item

Figure 5 Deleting A Default Gateway

When you click the garbage can icon, a confirmation dialog is displayed to verify that you want to delete the default gateway.

Step 3 On the confirmation dialog, click ***Yes*** delete the selected default gateway.

Working with the Fabric Director

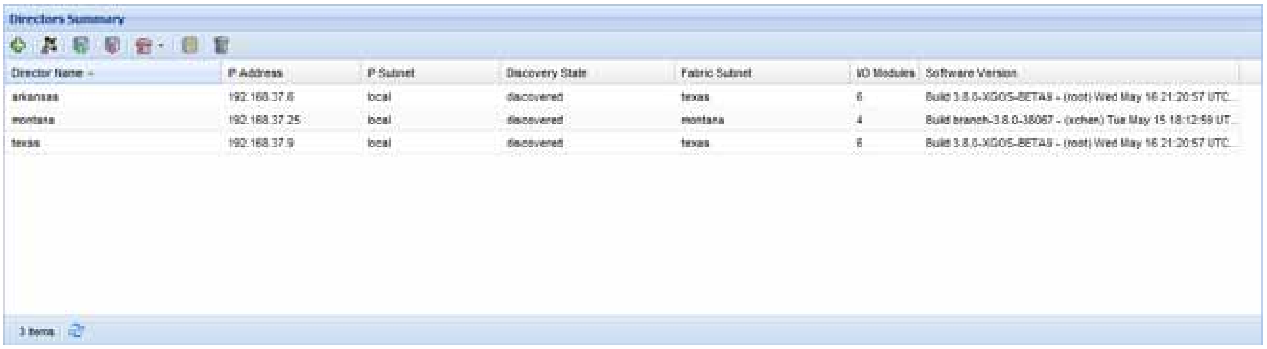
This chapter documents the following topics:

- Displaying All Managed Directors in the Network
- Scanning for Fabric Directors
- Discovering Fabric Directors with Fabric Manager
- Displaying Fabric Director Details
- Unmanaging a Fabric Director
- Backing Up and Restoring a Fabric Director Configuration
- Performing Tech Support Functions on the Fabric Director
- Collecting Xsigo Log Files

Displaying All Managed Directors in the Network

Information about the Oracle Fabric Director chassis (VP780 and VP560) that are managed through Oracle's Xsigo Fabric Manager is contained on the Directors Summary. Through the Directors Summary, you can select a specific chassis and display more details for it by using the Fabric Director Details frame. For more information about Fabric Director Details, see Displaying Fabric Director Details.

The Directors Summary is available through the navigation panel by clicking *Fabric Directors->Fabric Directors*. Figure 1 shows the Directors Summary.



Directors Summary

Director Name	IP Address	IP Subnet	Discovery State	Fabric Subnet	I/O Modules	Software Version
arkansas	192.168.37.6	local	discovered	texas	6	Build 3.8.0-XGOS-BETA9 - (root) Wed May 16 21:20:57 UTC...
montana	192.168.37.25	local	discovered	montana	4	Build branch-3.8.0-38067 - (xchen) Tue May 15 18:12:59 UT...
texas	192.168.37.9	local	discovered	texas	6	Build 3.8.0-XGOS-BETA9 - (root) Wed May 16 21:20:57 UTC...

3 items

Figure 1 Directors Summary Page

Table 1 explains the contents of the Directors Summary.

Table 1   Contents of the Directors Summary

Column	Contains
Director Name	The name of each managed Fabric Director in the network. The name is a link to the Details frame for the chassis. For more information about the Fabric Director Details frame, see Displaying Fabric Director Details.
IP Address	The chassis IP address of each managed Fabric Director.
IP Subnet	The IP subnet on which each Fabric Director is discovered. The subnet is either a name (for example, "local") or displayed in dotted decimal notation.

Table 1 (continued) Contents of the Directors Summary

Column	Contains
Discovery State	The Fabric Director’s current state in Fabric Manager. The state takes in the format `state1/state2`. Valid states include: • Discovered • Unmanaged • Upgrading • Up/Initializing • Up/Indeterminate • Up/VersionMismatch • Up/HostControlPathDown • Up/Down • Up/Up
Discovery State	The state of the discovery process while chassis are being discovered and added to the Fabric Manager management framework.
Fabric Subnet	Indicates the name or InfiniBand ID of the Fabric Director that is the master node, which provides the Infiniband subnet. If this value is the same as the Fabric Director’s name, that Fabric Director is providing the IB subnet manager. If this value is different than the Fabric Director’s name, the IB subnet manager in use is provided by the device named in this field. It is possible that a Fabric Director named in the Fabric Subnet field that is not managed by Fabric Manager is providing subnet manager functionality for a Fabric Director that is managed by Fabric Manager.
I/O Modules	The total number of I/O Modules installed in each chassis.
Software Version	The version of Oracle’s XgOS currently installed on each managed chassis.

Scanning for Fabric Directors

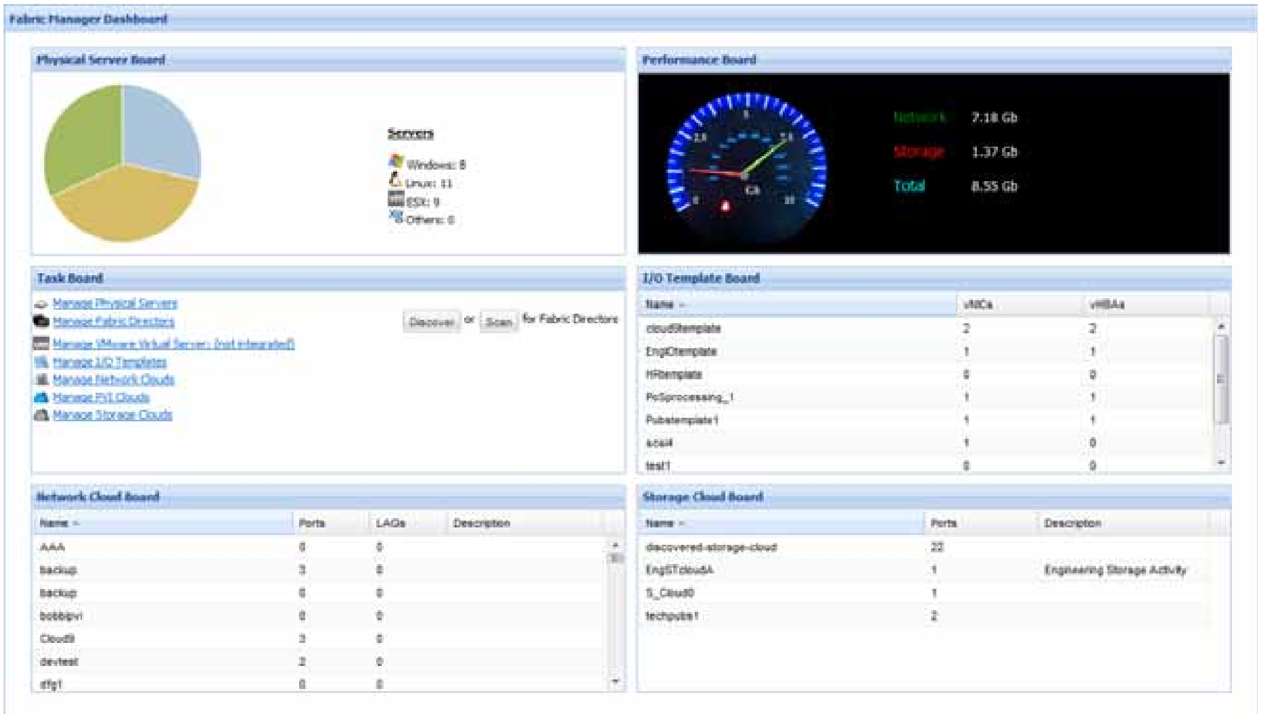
Before discovering one or more Fabric Directors, you can perform a scan process that queries for Fabric Directors in the network. The scan broadcasts to the Fabric Director’s management IP address, and listens for a response. The query and acknowledgement occurs over the discovery subnet, and can occur for Fabric Directors on the local network, or through a proxy Fabric Director on a remote network. (For more information about discovery subnets, see Working with Discovery Subnets.) When a Fabric Director responds, the management IP address is learned and added to the Directors Summary Page.

When a scan occurs, the listed Fabric Directors are not actually added to Fabric Manager for management. Instead, they are simply listed as available. The responding Fabric Directors are put into a list of all the Fabric Directors in the network that can be managed through Fabric Manager.

You can also scan through the ***Scan*** button on the Fabric Manager on the Overview page’s Common Tasks section.

To scan for Fabric Directors, follow this procedure

Step 1 Select *General->Dashboard* to display the Fabric Manager Dashboard. Figure 2 shows the Dashboard.



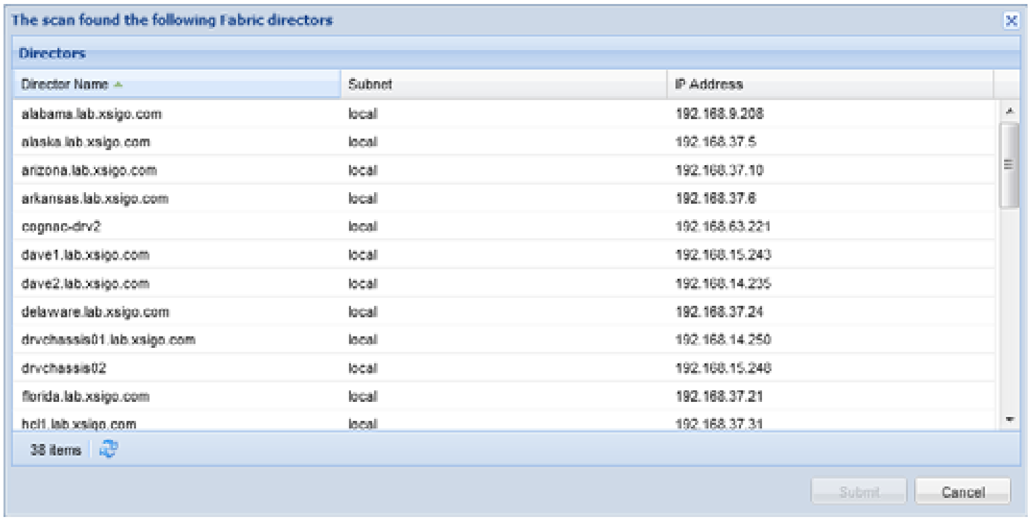
Name	vNICs	vHBAs
cloudStemplate	2	2
EngICtemplate	1	1
HRtemplate	0	0
PoSprocessing_1	1	1
Pubstemplate1	1	1
scsi4	1	0
test1	0	0

Name	Ports	LAGs	Description
AAA	0	0	
backup	3	0	
backup	0	0	
bobbipvi	0	0	
Cloud9	3	0	
devtest	2	0	
dfg1	0	0	

Name	Ports	Description
discovered-storage-cloud	22	
EngSTcloudA	1	Engineering Storage Activity
S_Cloud0	1	
techpubs1	2	

Figure 2 Fabric Manager Dashboard

Step 2 On the Task Board, click the ***Scan...*** button to display the results of the Fabric Director scan. Figure 3 shows the results.



The scan found the following Fabric directors

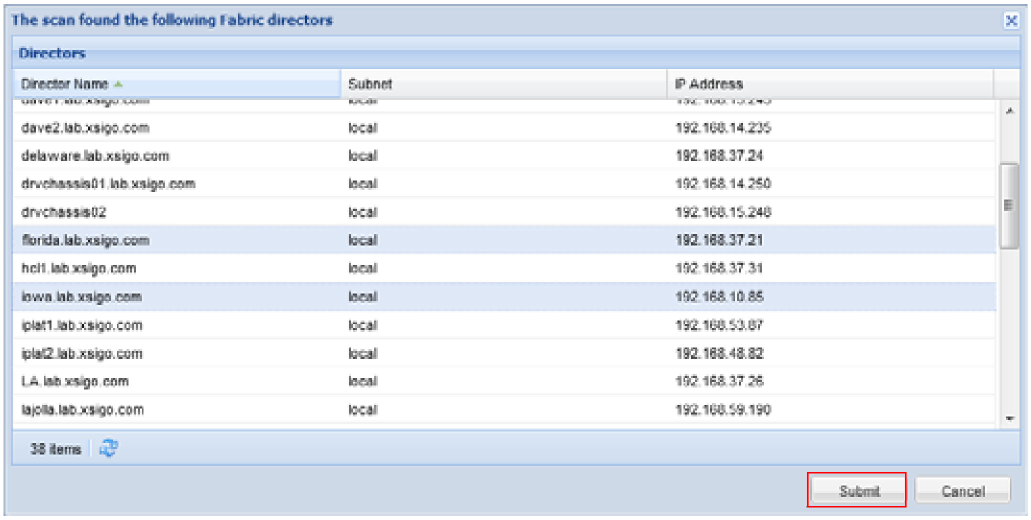
Directors

Director Name	Subnet	IP Address
alabama.lab.xsigo.com	local	192.168.9.208
alaska.lab.xsigo.com	local	192.168.37.5
arizona.lab.xsigo.com	local	192.168.37.10
arkansas.lab.xsigo.com	local	192.168.37.8
cognac-drv2	local	192.168.63.221
dave1.lab.xsigo.com	local	192.168.15.243
dave2.lab.xsigo.com	local	192.168.14.235
delaware.lab.xsigo.com	local	192.168.37.24
drvchassis01.lab.xsigo.com	local	192.168.14.250
drvchassis02	local	192.168.15.248
florida.lab.xsigo.com	local	192.168.37.21
hcl1.lab.xsigo.com	local	192.168.37.31

38 items

Figure 3 Fabric Directors Scan Results

Step 3 You can discover one or more of the scanned Fabric Directors by selecting the Fabric Director(s) in the table, and clicking ***Submit*** as shown in Figure 4.



The scan found the following Fabric directors

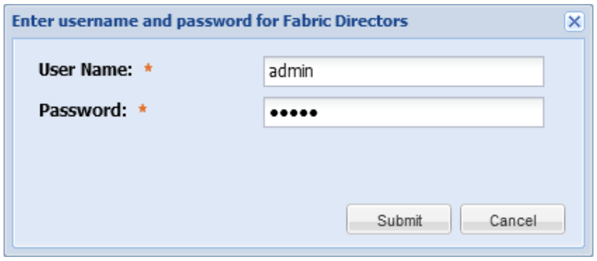
Directors

Director Name	Subnet	IP Address
dave2.lab.xsigo.com	local	192.168.14.235
delaware.lab.xsigo.com	local	192.168.37.24
drvchassis01.lab.xsigo.com	local	192.168.14.250
drvchassis02	local	192.168.15.248
florida.lab.xsigo.com	local	192.168.37.21
hcl1.lab.xsigo.com	local	192.168.37.31
iowa.lab.xsigo.com	local	192.168.10.85
iplat1.lab.xsigo.com	local	192.168.53.87
iplat2.lab.xsigo.com	local	192.168.48.82
LA.lab.xsigo.com	local	192.168.37.26
lajolla.lab.xsigo.com	local	192.168.59.190

38 items

Figure 4 Discovering Fabric Directors through Scan Display

When you click the ***Submit*** button, the Login dialog is displayed, as shown in Figure 5.



User Name: * admin

Password: * ●●●●●

Figure 5 Login Dialog for Discovering a Fabric Director

Step 4 In the *User Name* field, enter a valid user that can log in to the Fabric Director as an administrator. The user account must be able to login to the Fabric Director to be able to add the Fabric Director to Fabric Manager.

Step 5 In the *Password* field, enter the password for the user account entered in the *User Name* field.

Step 6 Click ***Submit*** to discover the scanned Fabric Director and add it to Fabric Manager. When the Fabric Director is successfully added to Fabric Manager, you can begin configuring and managing Xsigo virtual I/O and its features.

Discovering Fabric Directors with Fabric Manager

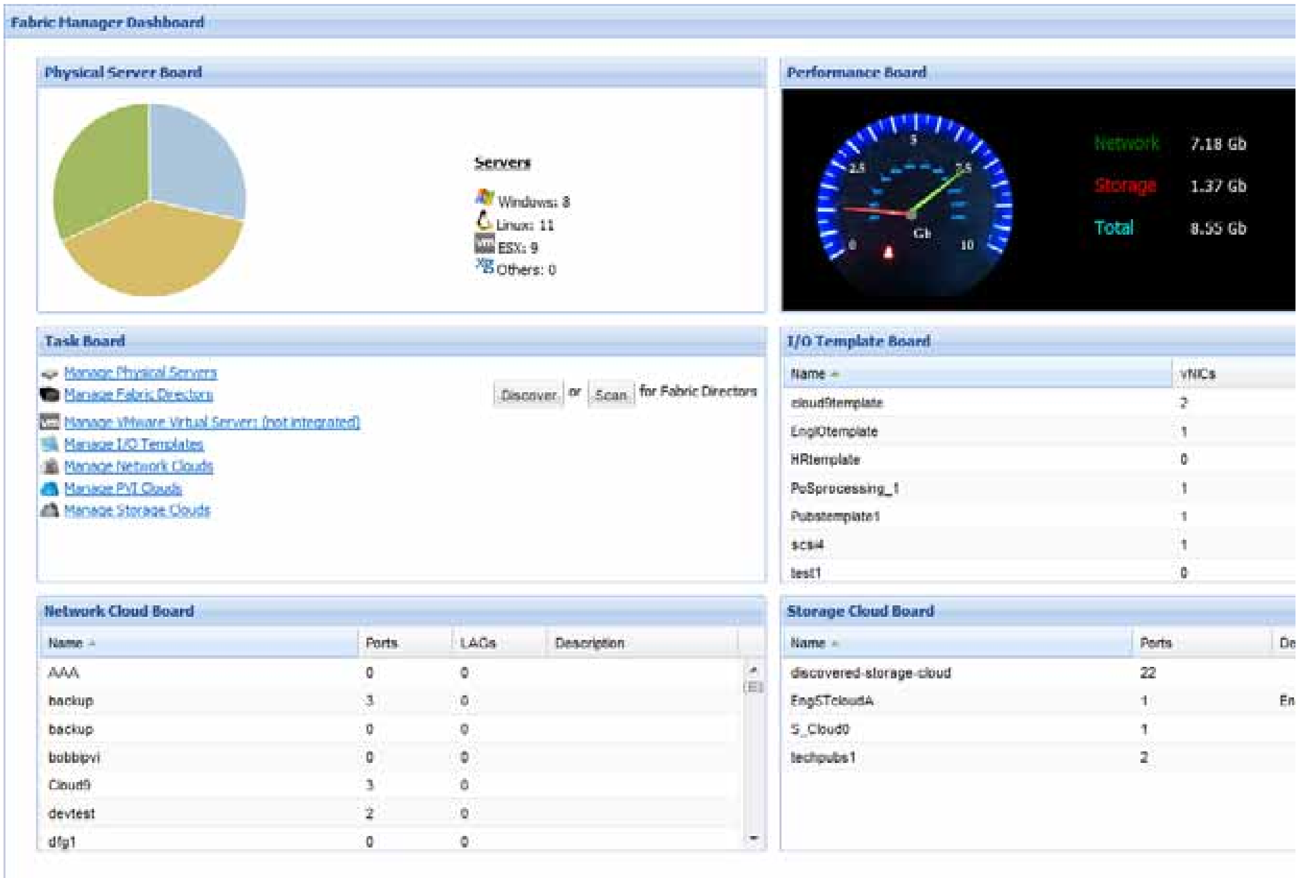
When Fabric Directors are added to the network, they are discovered through either their chassis IP address or host name, and then added to Fabric Manager. The process of discovery actually adds the Fabric Director into Fabric Manager so that a discovered Fabric Director is one that is actively being managed by Fabric Manager. This is different than a scanned Fabric Director, which simply provides a list of known Fabric Directors that can be managed.

When discovery occurs, the Fabric Manager server communicates with the Fabric Director’s system control processor (SCP) to learn about the Fabric Director, take an inventory of each Fabric Director’s hardware, learn the software version installed and the virtual resources configured on the Fabric Director (if any). After a Fabric Director is discovered, Fabric Manager adds it to the Directors Summary. After the Fabric Director is displayed in the Directors Summary, it can be managed through Fabric Manager.

Fabric Manager requires the management IP address to open a communication path for learning the Fabric Director contents. Do not use a vNIC IP address for discovery.

To discover a Fabric Director, follow this procedure:

Step 1 Select *General->Dashboard* to display the Fabric Manager Dashboard. Figure 6 shows the Dashboard.



Fabric Manager Dashboard

Physical Server Board

Servers

Windows: 8
Linux: 11
ESX: 9
Others: 0

Performance Board

Network	7.18 Gb
Storage	1.37 Gb
Total	8.55 Gb

Task Board

- Manage Physical Servers
- Manage Fabric Directors
- Manage VMware Virtual Servers (not integrated)
- Manage I/O Templates
- Manage Network Clouds
- Manage PVI Clouds
- Manage Storage Clouds

Discover or Scan for Fabric Directors

I/O Template Board

Name	vNICs
cloud9template	2
EngIOtemplate	1
HRtemplate	0
PoSprocessing_1	1
Pubstemplate1	1
scsi4	1
test1	0

Network Cloud Board

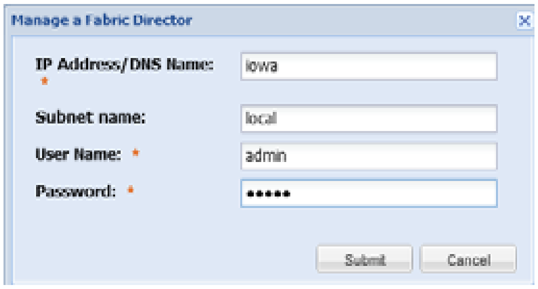
Name	Ports	LAGs	Description
AAA	0	0	
backup	3	0	
backup	0	0	
bobbipvi	0	0	
Cloud9	3	0	
devtest	2	0	
dfg1	0	0	

Storage Cloud Board

Name	Ports	De
discovered-storage-cloud	22	
Eng5TcloudA	1	En
S_Cloud0	1	
techpubs1	2	

Figure 6 Fabric Manager Dashboard

Step 2 On the Task Board, click the ***Discover...*** button. The Manage Fabric Director dialog is displayed as shown in Figure 7.



Manage a Fabric Director

IP Address/DNS Name: *	iowa
Subnet name:	local
User Name: *	admin
Password: *	●●●●●

Figure 7 Discover Fabric Director — Manage Fabric Director

Step 3 In the *IP Address/DNS Name* field, enter the Fabric Director’s IP address or name.

Step 4 In the *Subnet Name* field, enter name of the subnet on which the Fabric Director you want to discover is currently located. By default, the subnet is the local subnet.

Step 5 In the *User Name*, specify the admin account that you will use to log in to the Fabric Director for the purpose of discovering it. The user name can be anything, but by default it is administrator, root, or xsigoadmin.

Step 6 In the *Password* field, enter the password for the user name that you specified in the preceding field.

Step 7 When the Fabric Director discovery information is complete, click ***Submit*** to discover the Fabric Director.

Displaying Fabric Director Details

In addition to the Directors Summary, Fabric Manager contains a Directors details frame where additional information is contained. The Directors Details frame is available through the Directors Summary by clicking a chassis name. When you click the chassis name, the Director details frame is populated with information about the selected Fabric Director.

Fabric Manager supports inventorying and managing both Oracle's VP780 and the VP560., and Fabric Director details are available for both models. There are some minor hardware differences between the VP780 and VP560, such as a smaller form factor and fewer I/O modules in the VP560, which is a two rack-unit Fabric Director.

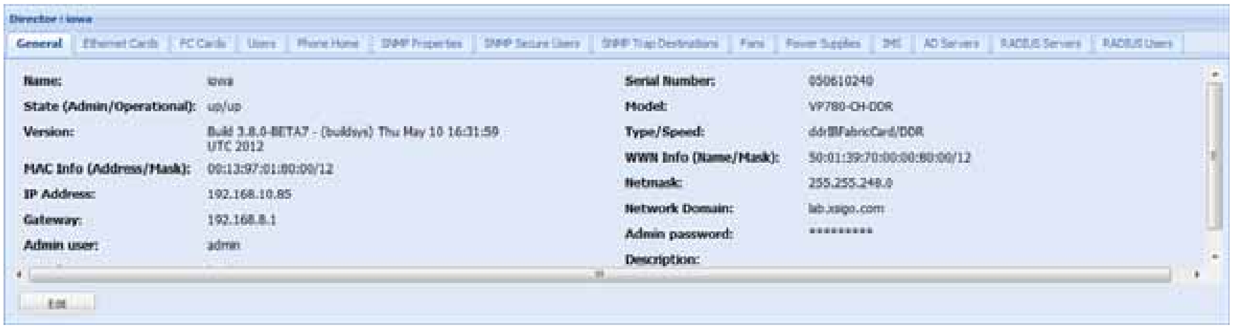
The Directors details frame shows information about a single Fabric Director. The Directors details frame is separated into tabs, which arrange different types of chassis information into sections. Some tabbed pages have additional tables and controls that allow more in-depth configuration and management of a single Fabric Director. The Directors Details frame contains tabs for:

- Displaying General Information About the Fabric Director
- Displaying Ethernet Cards
- Displaying Fibre Channel Cards
- Displaying Chassis Users
- Displaying Phone Home Information
- Displaying SNMP Properties
- Displaying SNMP Secure Users
- Displaying SNMP Trap Destinations
- Displaying Fan Information
- Displaying Power Supply Information
- Displaying IMS Properties
- Displaying Active Directory Properties
- Displaying RADIUS Servers
- Displaying RADIUS Users

It is important to understand that Fabric Manager has many of the same types of information as the Fabric Director. However, when you display this information through the Fabric Director, the information is relevant only to the context of that particular Fabric Director.

Displaying General Information About the Fabric Director

The Fabric Director’s *General* tab contains some basic, top-level information about the Fabric Director, its Fabric type and speed, non-I/O Module hardware inventory, management interface, location, and so on. Figure 8 shows the Fabric Director’s *General* tab.



Name: iowa
State (Admin/Operational): up/up
Version: Build 3.8.0-BETA7 - (buildsys) Thu May 10 16:31:59 UTC 2012
MAC Info (Address/Mask): 00:13:97:01:80:00/12
IP Address: 192.168.10.85
Gateway: 192.168.8.1
Admin user: admin

Serial Number: 050610240
Model: VP780-CH-DDR
Type/Speed: ddrIBFabricCard/DDR
WWN Info (Name/Mask): 50:01:39:70:00:00:80:00/12
Netmask: 255.255.248.0
Network Domain: lab.xsigo.com
Admin password: *********
Description:

Figure 8 Fabric Director Details Frame — General

Table 2 Contents of the General Tab

Column	Contains
Name	The name of each fan unit in the chassis. Each fan unit contains more than one fan, so the fan named 1/1 is for fan unit 1, fan 1 and the fan named 1/2 is for fan unit 1, fan 2 and so on.
Serial Number	The unique serial number assigned to the Fabric Director.
State (Admin/Operational)	The current administrative and operational state of the Fabric Director. The administrative is state is the state that the Fabric Director should be in, and the operational state is what state the Fabric Director actually is in.
Model	The model number of the Fabric Director.
Version	The current version of XgOS operating system software running on the Fabric Director.
MAC Info (Name/Mask)	The beginning MAC address available in the Fabric Director’s embedded MAC address pool. The mask bits determine how many MAC addresses can be assigned from the Fabric Director’s MAC address pool. For example, `/12` indicates that 12 bits worth of addresses can be assigned incrementally starting with the MAC address listed.
WWN Info (Name/Mask)	The beginning WWN number available in the Fabric Director’s embedded WWN pool. The mask bits determine how many WWN numbers can be assigned from the Fabric Director’s WWN pool. For example, `/12` indicates that 12 bits worth of addresses can be assigned incrementally starting with the WWN number listed.

Table 2 (continued) Contents of the General Tab

Column	Contains
Netmask	The network mask assigned to the Fabric Director’s management address.
IP Address	The Fabric Director’s management address.
Network Domain	The network domain in which the Fabric Director is currently deployed.
Gateway	The IP address of the Fabric Director’s gateway switch or router.
Admin Password	The currently assigned administrator password for accessing the Fabric Director. For security purposes, the password is displayed as a series of asterisks (*****).
Admin User	The user name of the currently assigned admin user.
Description	An optional string that helps to describe the Fabric Director.
IP Subnet	The IP subnet for the Fabric Director.

Displaying Ethernet Cards

Each Fabric Director supports Ethernet I/O modules that are the underlying physical connectivity to the IP network. These hardware modules then support the creation of vNICs for virtual IP connectivity. The following I/O modules are supported in each Fabric Director:

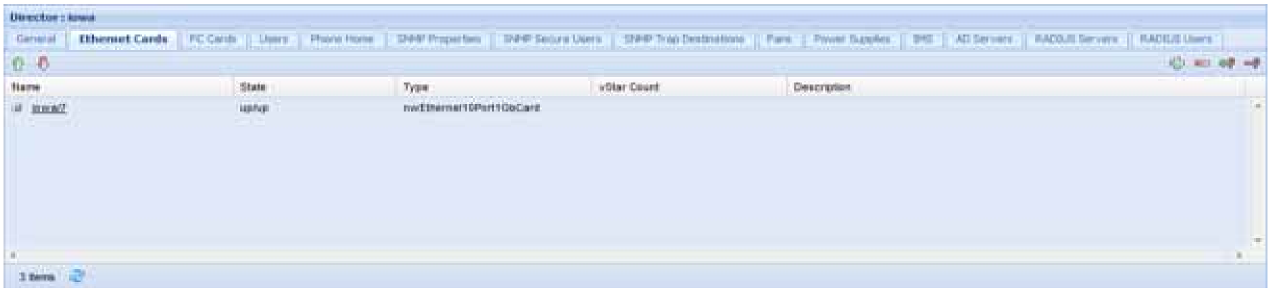
- 10 Gig Ethernet module (10 GE), which supports 1 physical link at 10 Gbps.
- 4-Port 10 Gig Ethernet module (4-Port 10 GE), which support 4 physical links at 10 Gbps per link.
- 10-Port Gig Ethernet module (10-Port GE), which supports 10 individual physical links at 1 Gbps.

For more information about the Fabric Director’s I/O modules, see the *XgOS Hardware and Drivers Installation Guide*.

In addition, some hardware-specific features, such as Link Aggregation Groups (LAGs) are supported through the Ethernet Cards page. For information, see Working with Link Aggregation.

When a Fabric Director is discovered by Fabric Manager, the Fabric Director’s I/O Modules are inventoried. The I/O Module information for the Ethernet card is displayed through the *Ethernet Cards* tab on the Director Details frame.

Figure 9 shows the *Ethernet Cards* tab.



Name	State	Type	vStar Count	Description
iowa/7	up/up	nwEthernet10Port1GbCard		

Figure 9 Directors Details Frame — Ethernet Cards

Table 3 Contents of the FC Cards Tab

Column	Contains
Name	The name of each Ethernet card that is inventoried in the Fabric Director. Each I/O card is named with the format `chassis/slot`, so the card texas/1 is the Ethernet card in slot 1 of the "Texas" chassis. If a module contains a termination port supporting a vNIC, the module is expandable and collapsible to display its configured Ethernet ports. Ethernet port information is also shown for any port that is terminating a vNIC. The port is named with the format `chassis/slot/port`, so the port texas/1/1 is the Ethernet port 1, on slot 1, of the "Texas" chassis.
State	The current state of the Ethernet card. The state is displayed as administrative state/operational state. Ethernet cards in up/up state are operating correctly.
Type	The type of Ethernet card installed in the Fabric Director: The following modules are supported: • 10 Gig Ethernet module (10 GE), which supports 1 physical link at 10 Gbps. In the *Type* field, Fabric Manager displays this module appears as `nwEthernet1Port10GBCardEthIB` • 4-Port 10 Gig Ethernet module (4-Port 10 GE), which support 4 physical links at 10 Gbps per link. In the *Type* field, this module appears as `nwEthernet4Port10GbCardEthIB` • 10-Port Gig Ethernet module (10-Port GE), which supports 10 individual physical links at 1 Gbps. In the Type, field, this module appears as `nwEthernet10Port1GbCardEthIB`
vStar Count	The total number of virtual resources configured on each port on the Ethernet card.
Description	An optional description field for the Ethernet Card.

Notice that the *Ethernet Card* tab has a list of individual modules, which is expandable to the port level. On the port level, additional features are available, such as general properties, Ethernet properties for the port (for example, MTU size), and Allowed VLAN Range.

Setting the Allowed VLAN Ranges for a Fabric Director

By default, the allowable VLAN range is from 1 to 4095. However, you can set a custom range of VLANs on the port so that only the VLAN-tagged packets within the specified range are allowed to ingress or egress the port. Traffic that has a VLAN tag not in the specified range is blocked from ingress or egress on the port.

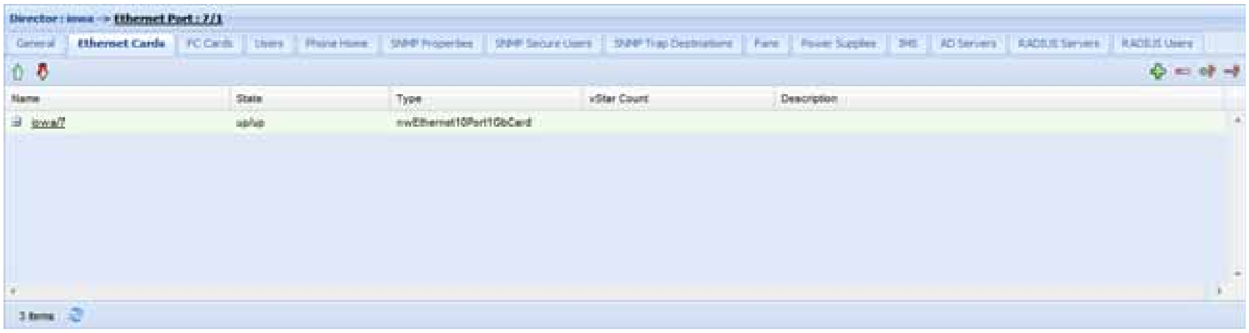
You can set or change the allowed VLAN range for the port through the *Allowed VLANs* tab at the port level of the Ethernet Card Details Frame.

To set the allowed VLAN range for a specific Fabric Director, follow this procedure:

Step 1 Select *Fabric Directors->Fabric Directors* to display the Director Summary page.

Step 2 Select the Fabric Director for which you want to set the Allowed VLAN range by clicking the Fabric Director in the summary. This step populates the details frame with information for that Fabric Director.

Step 3 On the details frame, click the *Ethernet Cards* tab to display each Ethernet module in the selected chassis. Figure 10 shows an example of the *Ethernet Cards* tab.

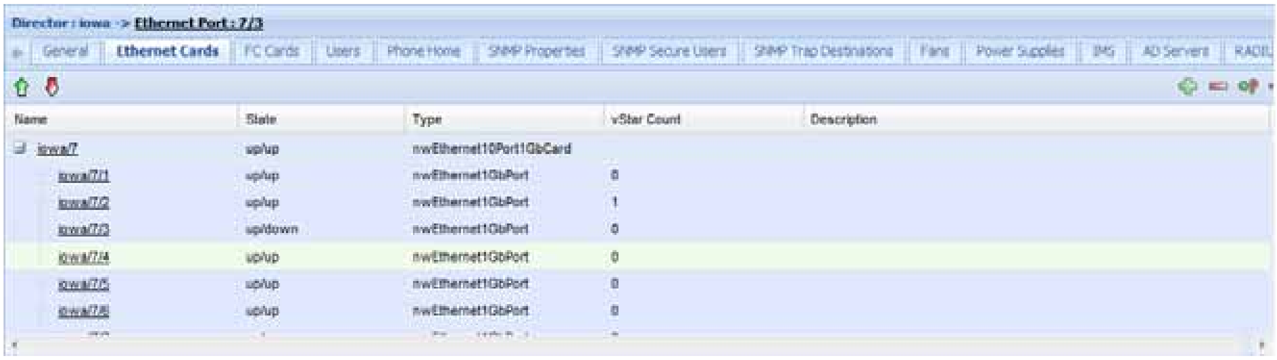


Director : iowa -> Ethernet Port : 7/1

Name	State	Type	vStar Count	Description
iowa/7	up/up	nwEthernet10Port1GbCard		

Figure 10 Fabric Director Details — Ethernet Card Tab

Step 4 Click the plus sign for the card on which you want to set the VLAN range. This step expands the card to display individual ports as shown in Figure 11.



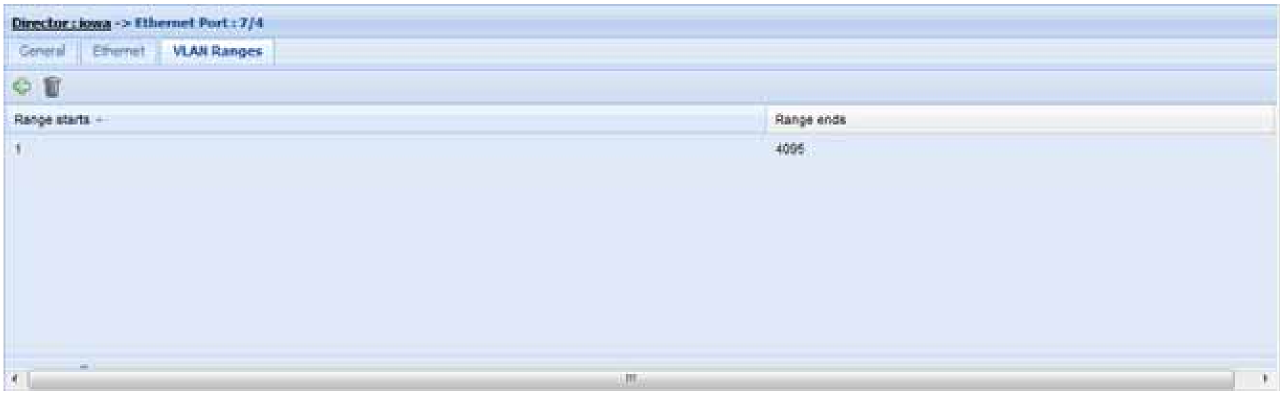
Director : iowa -> Ethernet Port : 7/3

Name	State	Type	vStar Count	Description
iowa/7	up/up	nwEthernet10Port1GbCard		
iowa/7/1	up/up	nwEthernet1GbPort	0	
iowa/7/2	up/up	nwEthernet1GbPort	1	
iowa/7/3	up/down	nwEthernet1GbPort	0	
iowa/7/4	up/up	nwEthernet1GbPort	0	
iowa/7/5	up/up	nwEthernet1GbPort	0	
iowa/7/6	up/up	nwEthernet1GbPort	0	

Figure 11 Fabric Director Details — Ethernet Card Tab

Step 5 Click the port (which is indented under the card) to display the port properties in the details frame.

Step 6 Click the *VLAN Ranges* tab, as shown in Figure 12.

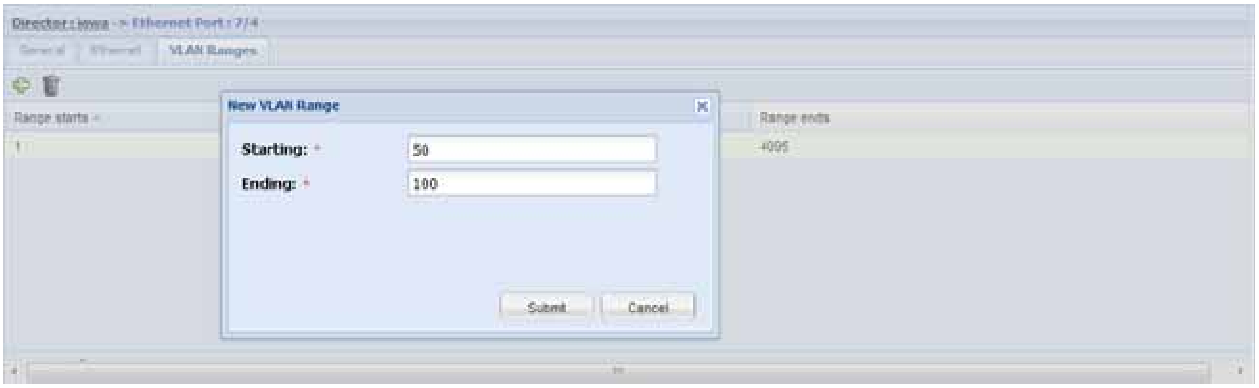


Director : iowa -> Ethernet Port : 7/4

Range starts	Range ends
1	4095

Figure 12 Fabric Director Details — VLAN Range Tab

Step 7 Click the plus sign (+) to display the New VLAN Range dialog as shown in Figure 13.



New VLAN Range

Starting: * 50

Ending: * 100

Figure 13 Fabric Director Details — New VLAN Range Dialog

Step 8 In the *Starting* field, enter the first VLAN ID that you want to be available.

Step 9 In the *Ending* field, enter the last VLAN ID you want to be available.

Step 10 When the Allowed VLAN Range is configured, click ***Submit***.

Displaying Fibre Channel Cards

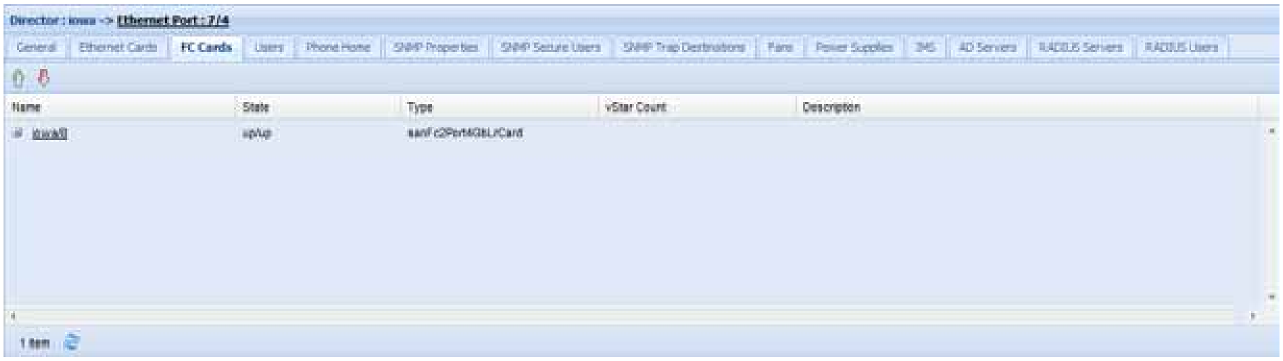
Each Fabric Director supports Fiber Channel modules that are the underlying physical connectivity to an FC SAN. These hardware modules then support the creation of vHBAs for host servers' SAN connectivity. The Fabric Director supports the following Fibre Channel cards:

- the Line Rate Fibre Channel module (2x4 FC Line Rate card). This module supports 2 Fibre Channel port pairs (one transmit port of 4 Gbps and one receive port at 4 Gbps for each port pair) for a total of 8 Gbps per module.
- the 8 Gbps Line Rate Channel module (2x8 FC Line Rate card). This module supports 2 Fibre Channel port pairs (one transmit port of 8 Gbps and one receive port at 8 Gbps for each port pair) for a total of 8 Gbps (full line rate) for each port pair.

For more information about the Fabric Director I/O modules, see the *XgOS Hardware and Drivers Installation Guide*.

When a Fabric Director is discovered by Fabric Manager, the Fabric Director's I/O Modules are inventoried. The I/O Module information for the Fibre Channel card is displayed through the *FC Cards* tab on the Director Details frame.

Figure 14 shows the *FC Cards* tab.



Director : iowa -> Ethernet Port : 7/4

Name	State	Type	vStar Count	Description
iowa/8	up/up	sanFc2Port4GbLrCard		

Figure 14 Directors Details Frame — FC Cards

Table 4 Contents of the FC Cards Tab

Column	Contains
Name	The name of each Fibre Channel card that is inventoried in the Fabric Director. Each I/O card is named with the format `chassis/slot`, so the card texas/1 is the Fibre Channel card in slot 1 of the "Texas" chassis. If a module contains a termination port supporting a vHBA, the module is expandable and collapsible to display its configured FC ports. Fibre Channel port information is also shown for any port that is terminating a vHBA. The port is named with the format `chassis/slot/port`, so the port texas/1/1 is the FC port 1, on slot 1, of the "Texas" chassis.
State	The current state of the Fibre Channel card. The state is displayed as administrative state/operational state. Fibre Channel cards in up/up state are operating correctly.
Type	The type of Fibre Channel card installed in the Fabric Director. The following modules are supported: • the Line Rate Fibre Channel module, which supports 2 Fibre Channel port pairs (one transmit port of 4 Gbps and one receive port at 4 Gbps for each port pair) for a total of 8 Gbps per module. In the Type field, this module appears as `sanFc2Port4GbLrCard` • the 8 Gbps Line Rate Fibre Channel module, which supports 2 Fibre Channel port pairs (one transmit port of 8 Gbps and one receive port at 8 Gbps for each port pair) for a total of 8 Gbps (full line rate) for each port pair. In the Type field, this module appears as `sanFc2Port8GbLrCardEthIB`
vStar Count	The total number of virtual resources configured on each port on the FC card.
Description	An optional description field for the FC Card.

Displaying Chassis Users

Fabric Manager supports local user accounts. Local user accounts are local because they are independent accounts that exist on individual Fabric Directors.

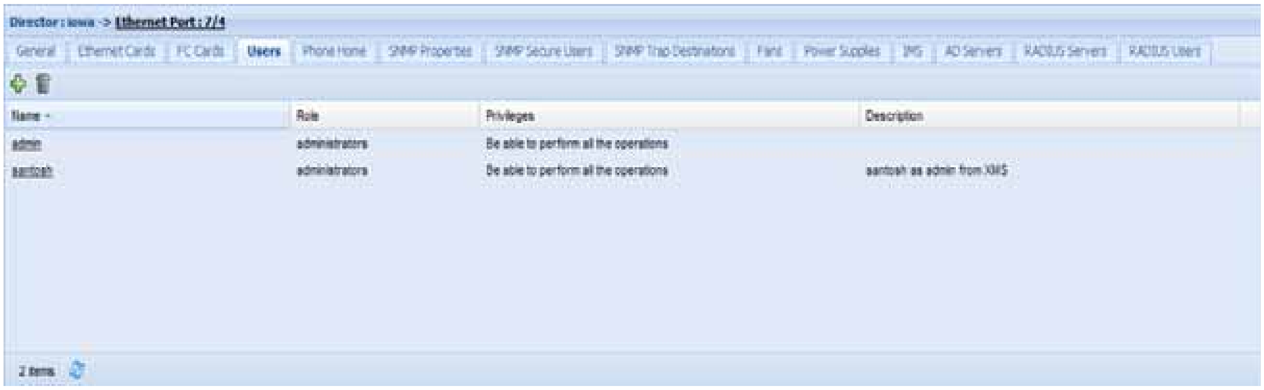
Typically, a local user account is mapped into a role group. That role group provides the permissions for what objects the user can and cannot write to. When a user account is assigned to a role, the conditions are created for what actions the user can perform, and what objects the user can configure, change, or manage.

It is possible to create a local user without assigning the user to a specific role group. In this case, the user is assigned to the "operator" role group by default. The operator role group is the most restrictive. It provides read-only access.

All users have a role group—either a role group that is explicitly assigned to the user, or the operator role group that is assigned by default.

At the Fabric Director level, local user accounts are used. You can manage local user accounts through the *Users* tab on the Directors Details frame.

Figure 15 shows the *Users* tab.



Director : iowa -> Ethernet Port : 7/4

Name	Role	Privileges	Description
admin	administrators	Be able to perform all the operations	
santosh	administrators	Be able to perform all the operations	santosh as admin from XMS

2 items

Figure 15 Director Details Frame — Users

You can add local users to the Fabric Director by clicking the plus sign, and you can delete a configured user by selecting it in the *Users* tab, then clicking the garbage can icon.

Configuring Local Users

Local user accounts define what users can log in to the Fabric Director and what privileges that user has while logged in.

To configure local user accounts, follow this procedure:

Step 1 On the *Users* tab, click the plus sign to display the Create a New User dialog.

Step 2 In the *User Name* field, enter the name for the local user account that you are creating.

Step 3 As an option, in the *Description* field, enter an alphanumeric character string that describes the user account.

Step 4 From the *Roles* dropdown menu, select the appropriate role for the user account. The user's privileges on the Fabric Director are a result of the role that is assigned to the user account. Table 5 shows the roles and summarizes what privileges belong to each role.

Table 5 Roles

Role	Priviliges for...
operator	read access to Fabric Director features
network	vNIC configuration and managment, Network QoS

Table 5 (continued) Roles

Role	Priviliges for...
storage	vHBA configuration and management, SAN QoS
server	compute resource configuration and management
administrator	full admin responsibilities

Step 5 When the user account is configured, click ***Submit***.

Step 6 Check the *Users* tab to verify the user account is configured correctly.

Displaying Phone Home Information

The Xsigo Phone Home feature supports periodically transmitting the following information to Xsigo Technical Support:

- the contents of selected log files
- the output of the **`show tech-support`** command from the XgOS CLI

By transmitting this information, Xsigo Technical Support can proactively look for and diagnose potential problems without requiring you to collect data, package it, and transmit it Xsigo Systems.

No sensitive customer data is gathered and transmitted to Xsigo. To ensure that private information is kept safe, the Xsigo Phone Home feature provides ways to:

- send a copy of the information to an internal website for auditing purposes
- remove private data, such as IP addresses, from the data sent to Xsigo Customer Support

Also, the data is transmitted in an encrypted form so that it cannot easily be read.

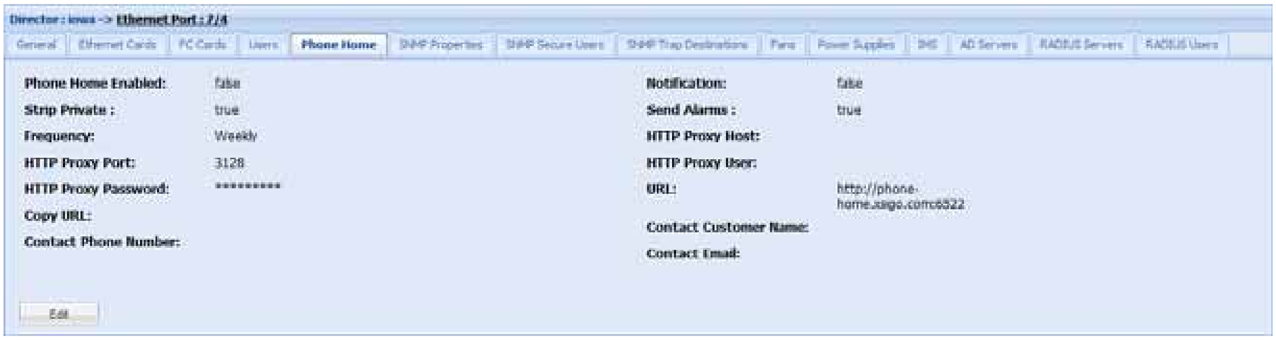
Table 6 shows defaults for Phone Home. Most of these parameters are determined through the Xsigo First Boot script which automatically runs when you install the Fabric Director for the first time.

Table 6 Xsigo Phone Home Defaults

Phone Home Parameter	Default
proxy	Xsigo Phone Home communication occurs to port 3128.
notify	No notification when Xsigo Phone Home communication occurs
strip-private	IP addresses are removed from the Xsigo Phone Home information and replaced with a `<privip:x>` string—for example, `<privip:1>` `<privip:2>`
mode	Periodic, transmissions occur as scheduled by you

However, you can customize the Phone Home properties and transmission schedules through the *Phone Home* tab of the Fabric Directors Details frame.

Figure 16 show the *Phone Home* tab.



Phone Home Enabled:	false	Notification:	false
Strip Private :	true	Send Alarms :	true
Frequency:	Weekly	HTTP Proxy Host:	
HTTP Proxy Port:	3128	HTTP Proxy User:	
HTTP Proxy Password:	*********	URL:	http://phone-home.xsigo.com:6522
Copy URL:		Contact Customer Name:	
Contact Phone Number:		Contact Email:	

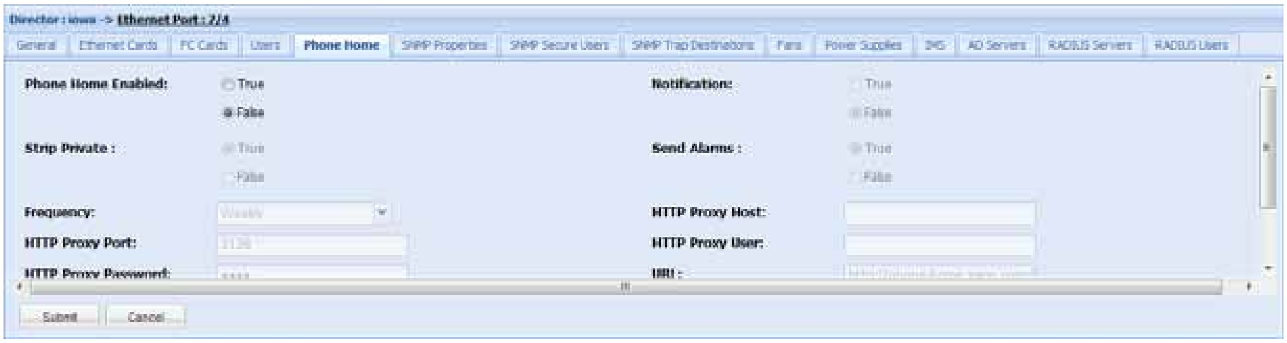
Figure 16 Director Details Frame — Phone Home

To edit the Phone Home properties, follow this procedure:

Step 1 Display the Directors Details frame by selecting *Fabric Directors->Fabric Directors*.

Step 2 On the Directors Details frame, click the *Phone Home* tab to display the Phone Home properties configured on the Fabric Director.

Step 3 On the *Phone Home* tab, click the ***Edit*** button to unlock the editable phone home parameters as shown in Figure 17.



Phone Home Enabled:	○ True ● False	Notification:	○ True ● False
Strip Private :	● True ○ False	Send Alarms :	● True ○ False
Frequency:	Weekly	HTTP Proxy Host:	
HTTP Proxy Port:	3128	HTTP Proxy User:	
HTTP Proxy Password:	****	URL :	

Figure 17 Editable Phone Home Tab

Step 4 As needed, enable or disable scheduled transmission of phone home data:

- True to enable scheduled transmission.
- False to disable scheduled transmission.

Step 5 From the *Notification* section, determine whether you want Xsigo Technical Support to contact you whenever Phone Home information is received:

- *True* causes Xsigo to contact the person in the Contact Name field by any method listed in the Contact Phone Number or Contact Email fields.
- *False* causes Xsigo to not contact you, even if contact information exists in the Phone Home configuration.

Step 6 From the *Strip Private* section, select whether you want private IP address information removed from the Phone Home information:

- *True* causes the IP address information to be represented with `<privip:X>` labels.
- *False* causes your IP addresses to be visible in the Phone Home information.

Step 7 From the *Send Alarms* section, select whether you want Phone Home information sent whenever a major alarm is raised in the network:

- *True* causes the Phone Home information to be sent whenever a major alarm occurs.
- *False* causes Phone Home information to be transmitted as configured, and major alarms will not trigger a Phone Home message.

Step 8 From the *Frequency* dropdown menu, select the periodicity at which the Fabric Director will transmit Phone Home data.

Step 9 If you are configuring HTTP Proxy, in the *HTTP Proxy Host* field, enter the name of the HTTP Proxy Host.

Step 10 If you are configuring HTTP Proxy, in the *HTTP Proxy Port* field, enter the port number on which the HTTP Proxy will communicate Phone Home information. By default, port 3128 is used, but you can set any other port that is not supporting a service.

Step 11 If you are configuring HTTP Proxy, in the *HTTP Proxy User* field, enter the user name for the HTTP Proxy.

Step 12 In the *URL* field, enter the URL of where the Phone Home information will be sent. By default, this field contains the default site for Xsigo Technical Support.

Step 13 In the *Copy To URL* field, enter the URL of an audit server in your network to which you want a copy of any Phone Home message sent.

Step 14 In the *Contact Customer Name* field, enter the name of someone on site that manages the Fabric Director. This person is who Xsigo will contact if the “Notifications” section is set to “True” and a Phone Home message is received.

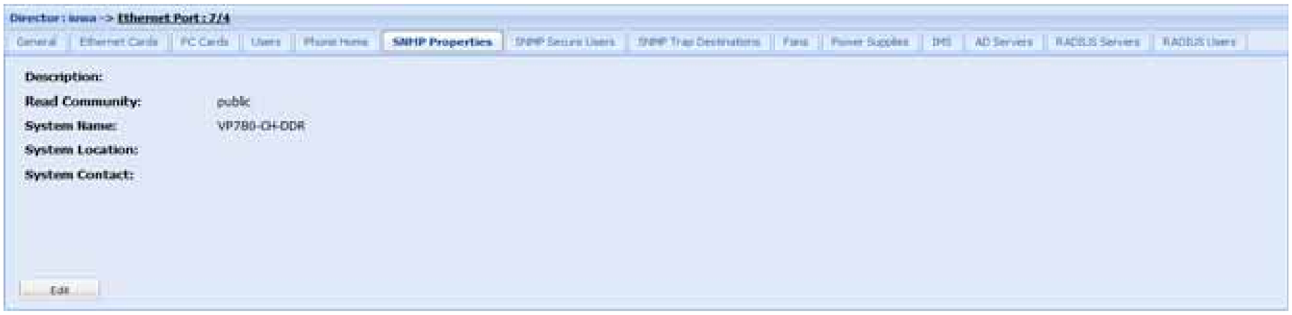
Step 15 In the *Contact Customer Phone* field, enter the phone number (if any) for the person named in the *Contact Customer Name* field.

Step 16 In the *Contact Customer Email* field, enter the email address (if any) for the person named in the *Contact Customer Name* field.

Step 17 Click ***Save*** to configure Phone Home on the Fabric Director.

Displaying SNMP Properties

Fabric Manager tracks general properties for SNMP on each Fabric Director. These properties are available through the *SNMP Properties* tab on the Fabric Directors Details frame. Figure 18 shows this tab.



Director : iowa -> Ethernet Port : 7/4

Description:
Read Community: public
System Name: VP780-CH-DDR
System Location:
System Contact:

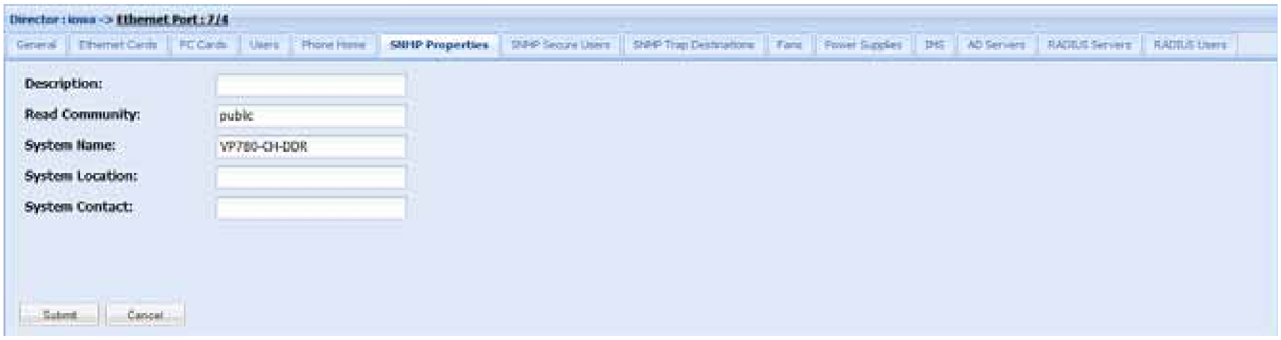
Figure 18 Director Details Frame — SNMP Properties

You can also edit the SNMP Properties to set or change current values. To edit the SNMP properties, follow this procedure:

Step 1 Display the Directors Details frame by selecting *Fabric Directors->Fabric Directors*.

Step 2 On the Directors Details frame, click the *SNMP Properties* tab to display the configured SNMP properties.

Step 3 On the *SNMP Properties* tab, click ***Edit*** button to unlock the editable SNMP properties as shown in Figure 19.



Director : iowa -> Ethernet Port : 7/4

Description:
Read Community: public
System Name: VP780-CH-DDR
System Location:
System Contact:

Figure 19 Editable SNMP Properties Tab

Step 4 Edit the SNMP fields as needed, then click ***Submit***.

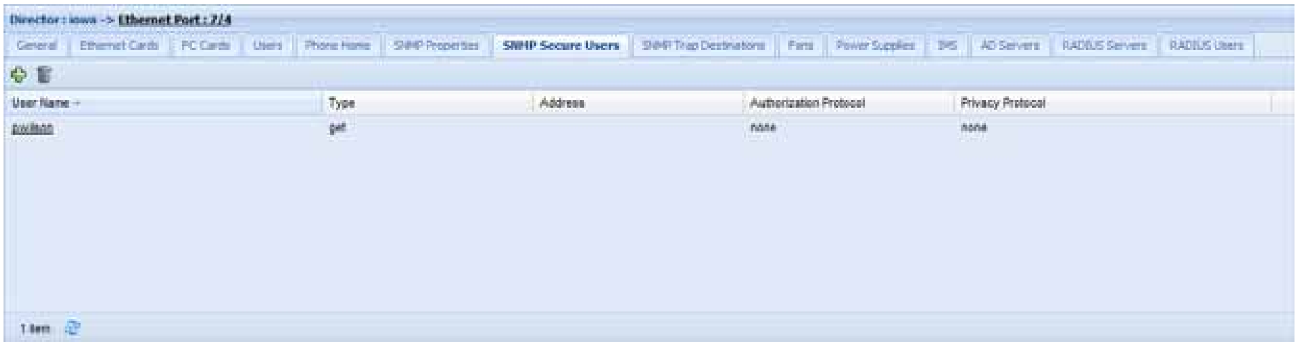
Step 5 Check the *SNMP Properties* tab to verify that the correct properties are configured.

Displaying SNMP Secure Users

Fabric Manager supports Secure SNMP. If you are configuring Secure SNMP, you must configure the SNMP user and password which the security algorithms will use as inputs. When the user name and password are specified, you can select the type of security to use. As an option, you can use simple password authentication by not specifying any security parameters.

SNMP secure users for each Fabric Director are available through the *SNMP Secure Users* tab of the Fabric Directors Details frame.

Figure 20 shows the *SNMP Secure Users* tab.



Director : iowa -> Ethernet Port : 7/4

User Name	Type	Address	Authorization Protocol	Privacy Protocol
paulkan	get		none	none

1 item

Figure 20 Director Details Frame — SNMP Secure Users

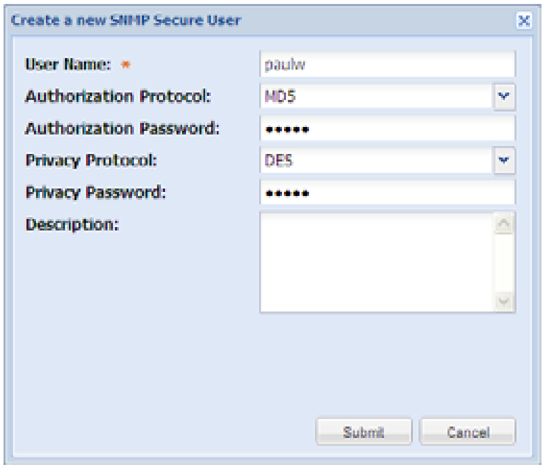
You can also add SNMP secure users by clicking the plus sign, or delete secure users by selecting one or more of them in the *SNMP Secure Users* tab, then clicking the garbage can icon.

To add SNMP Secure Users to a Fabric Director, follow this procedure:

Step 1 Display the Directors Details frame by selecting *Fabric Directors->Fabric Directors*.

Step 2 On the Directors Details frame, click the *SNMP Secure Users* tab to display the trap destinations configured on the Fabric Director.

Step 3 On the *SNMP Secure Users* tab, click the plus sign to display the Create a New SNMP Secure User dialog. Figure 21 shows this dialog.



Create a new SNMP Secure User

User Name: * paulw
Authorization Protocol: MD5
Authorization Password: •••••
Privacy Protocol: DES
Privacy Password: •••••
Description:

Figure 21 Create a New SNMP Secure User

Step 4 In the *User Name* field, enter the username that will be used to log in to the trap destination.

Step 5 From the *Authorization Protocol* dropdown menu, select the type of authorization that will be used for logging in to the trap destination:

- None for no authorization
- MD5 to use MD5 hashing algorithm
- SHA to use Secure Hashing Algorithm

Step 6 In the *Authorization Password* field, enter the password that will be used by the SNMP secure user.

Step 7 From the *Privacy Protocol* dropdown menu, select the protocol to be used:

- None for no authorization
- DES to use Data Encryption Standard

Step 8 In the *Privacy Password* field, enter the password that will be used.

Step 9 As an option, in the *Description* field, enter an optional description string for this secure user.

Displaying SNMP Trap Destinations

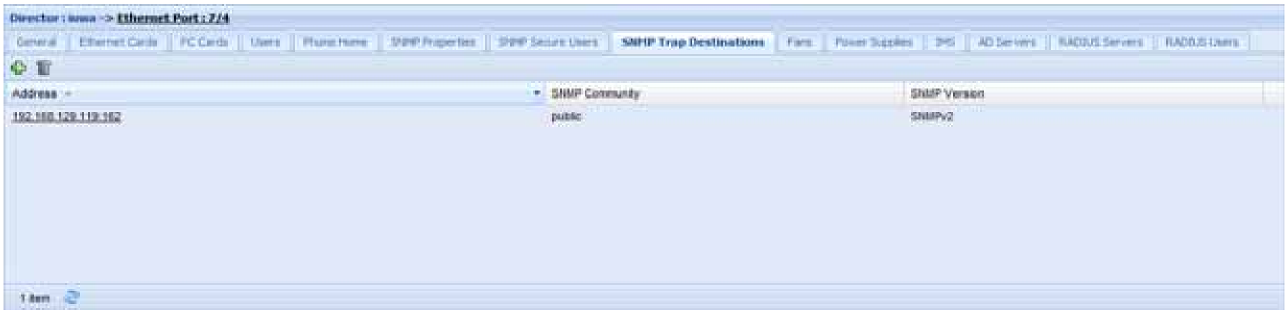
Fabric Manager supports simple network management protocol (SNMP). The Xsigo implementation of SNMP supports SNMPv1, v2,and v3. Get, getnext, and getbulk operations are all supported. Set operations are not supported. Community strings are read only. Some standard Enterprise MIBs as well as Xsigo proprietary MIBs are supported.

Through SNMP you can configure trap hosts (trap destinations) that will receive events and errors if they occur. Fabric Manager supports configuring SNMP variables also, such as system ID strings.

To configure SNMP trap destinations, follow this procedure:

Step 1 Display the Directors Details frame by selecting *Fabric Directors->Fabric Directors*.

Step 2 On the Directors Details frame, click the *SNMP Trap Destinations* tab to display the trap destinations configured on the Fabric Director. Figure 22 shows this tab.



Address	SNMP Community	SNMP Version
192.168.129.119:162	public	SNMPv2

Figure 22 Director Details Frame — SNMP Trap Destinations

Configuring SNMP Trap Destinations

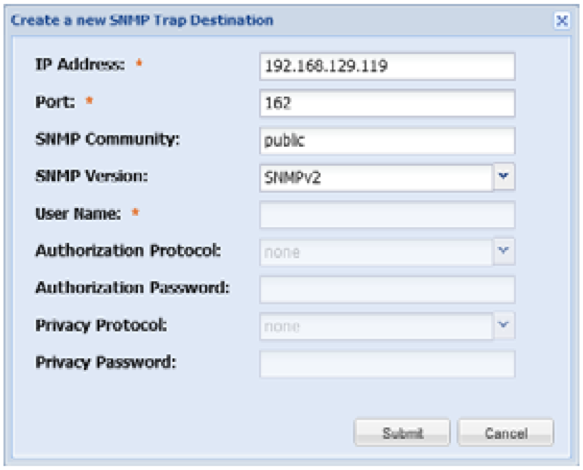
You can use the *SNMP Trap Destinations* tab to add or delete trap destinations. Add trap destinations by clicking the plus sign, or delete configured trap destinations by selecting one or more of them, then clicking the garbage can icon.

To add an SNMP trap destination, follow this procedure:

Step 1 Display the Directors Details frame by selecting *Fabric Directors->Fabric Directors*.

Step 2 On the Directors Details frame, click the *SNMP Trap Destinations* tab to display the trap destinations configured on the Fabric Director.

Step 3 On the *SNMP Trap Destinations* tab, click the plus sign to display the Create a New SNMP Trap Destination dialog. Figure 23 shows this dialog.



Create a new SNMP Trap Destination

IP Address: *	192.168.129.119
Port: *	162
SNMP Community:	public
SNMP Version:	SNMPv2
User Name: *	
Authorization Protocol:	none
Authorization Password:	
Privacy Protocol:	none
Privacy Password:	

Figure 23 Create a New SNMP Trap Destination

Step 4 In the *IP Address* field, enter the network address of the trap destination in dotted decimal notation.

Step 5 In the *Port* field, specify the port number on which traps will be sent to the trap destination. By default, port 162 is used, but you can set another port as long as it is not supporting other traffic. Valid ports are in the range of 1 to 65535.

Step 6 In the *SNMP Community* field, enter the read community string for the trap destination.

Step 7 From the *SNMP Version* dropdown menu, select the version of SNMP is in use in your network:

- SNMPv2
- SNMPv3

Step 8 In the *User Name* field, enter the username that will be used to log in to the trap destination.

Step 9 In the *Authorization Protocol* dropdown menu, select the type authorization that will be used for logging in to the trap destination:

- None for no authorization
- MD5 to use MD5 hashing algorithm
- SHA to use Secure Hashing Algorithm

Step 10 In the *Authorization Password* field, enter the password that will be used by the user specified in *User Name*.

Step 11 From the *Privacy Protocol* dropdown menu, select the protocol to be used:

- None for no authorization
- DES to use Data Encryption Standard

Step 12 In the *Privacy Password* field, enter the password that will be used.

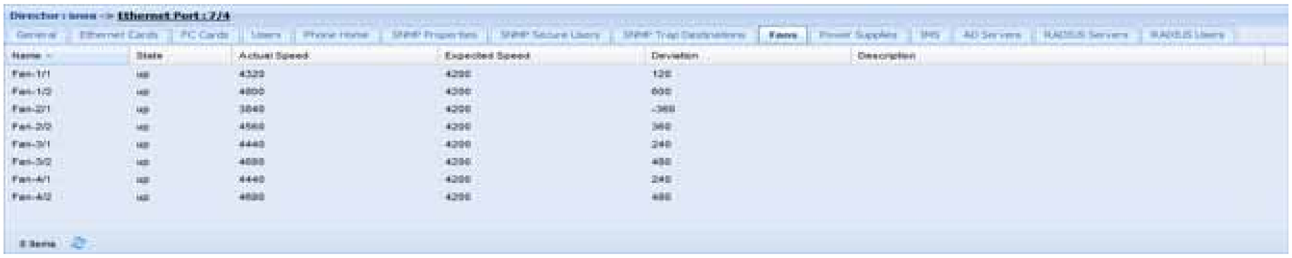
Displaying Fan Information

When a Fabric Director is managed by Fabric Manager, each Fabric Director registers its hardware information with the Fabric Manager server. Part of the hardware information that Fabric Manager monitors is the fan state. Each Fabric Director has built-in fans for cooling.

Fabric Manager tracks the operational state of the fans and if an error is detected, an alarm is posted. Fans are monitored for operational states, such as:

- operational, up/up
- non-operational, up/down
- unknown, indeterminate, which can occur if the fan is operating but not supplying proper cooling to the Fabric Director.

The fan information is available through the *Fans* tab on the Directors Details frame. Figure 24 shows the *Fans* tab.



Name	State	Actual Speed	Expected Speed	Deviation	Description
Fan-1/1	up	4320	4200	120	
Fan-1/2	up	4800	4200	600	
Fan-2/1	up	3840	4200	-360	
Fan-2/2	up	4560	4200	360	
Fan-3/1	up	4440	4200	240	
Fan-3/2	up	4680	4200	480	
Fan-4/1	up	4440	4200	240	
Fan-4/2	up	4680	4200	480	

8 items

Figure 24 Director Details Frame — Fans

Table 7 shows the contents of the *Fans* tab and explains what each field means.

Table 7 Contents of the Fans Tab

Column	Contains
Name	The name of each fan unit in the chassis. Each fan unit contains more than one fan, so the fan named 1/1 is for fan unit 1, fan 1 and the fan named 1/2 is for fan unit 1, fan 2 and so on.
State	The current state of the fan. The state is displayed as administrative state/operational state. Fans in up/up state are operating correctly.
Actual Speed	The actual speed in RPMs of each fan.

Table 7 (continued) Contents of the Fans Tab

Column	Contains
Expected Speed	The expected speed of the fan based on internal calculations.
Deviation	The difference between the actual speed and the expected speed. This number can be a positive number if a fan is spinning faster than expected, or a negative number if the fan is spinning slower than expected.
Description	An optional description for each fan.

Displaying Power Supply Information

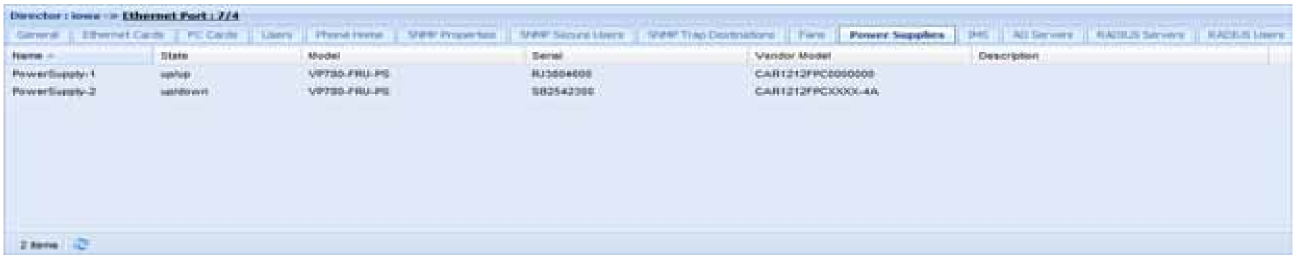
When a Fabric Director is managed by Fabric Manager, each Fabric Director registers its hardware information with the Fabric Manager server. Part of the hardware information that Fabric Manager monitors is the power supply state. The number of power supplies (PSUs) is different depending on the model of Fabric Director:

- Oracle’s VP780 two built-in PSUs that condition facility power, numbered one and two.
- Oracle’s VP560 has two built-in PSUs, numbered one and two

Fabric Manager tracks the operational state of the PSUs and if an error is detected, an alarm is posted. Fans are monitored for operational states, such as:

- operational, up/up
- non-operational, up/down
- unknown, indeterminate, which can occur if the PSU is operating, but not at proper speed.

The PSU information is available on the *Power Supplies* tab of the Directors Details frame. Figure 25 shows the *Power Supplies* tab.



Director : iowa -> Ethernet Port : 7/4

Name	State	Model	Serial	Vendor Model	Description
PowerSupply-1	up/up	VP780-FRU-PS	RJ3604600	CAR1212FPC0000000	
PowerSupply-2	up/down	VP780-FRU-PS	SB2542300	CAR1212FPCXXXX-4A	

2 items

Figure 25 Director Details Frame — Power Supplies

Table 8 shows the contents of the *Power Supplies* tab and explains what each field means.

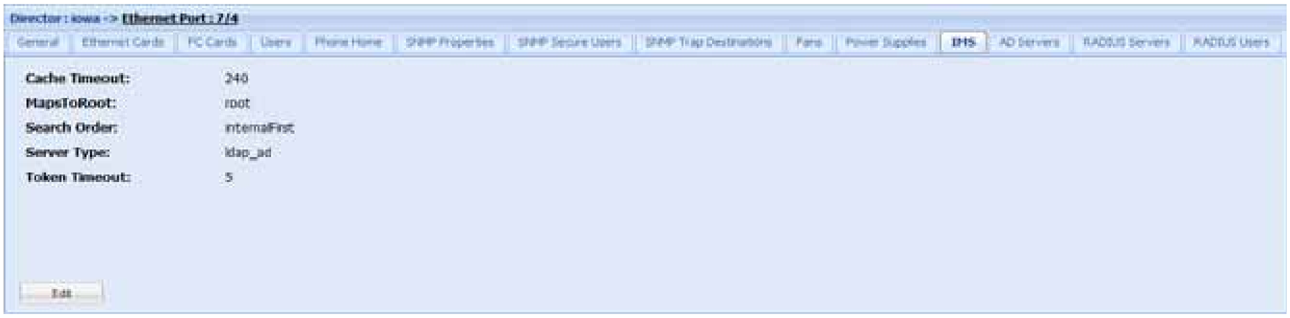
Table 8 Contents of the Power Supplies Tab

Column	Contains
Name	The name of each power supply unit (PSU) in the chassis. Each chassis contains two power supplies that are redundant and load share when both are operating. If one fails, the Fabric Director can operate on one PSU.
State	The current state of the PSU. The state is displayed as administrative state/operational state. PSUs in up/up state are operating correctly.
Model	The Xsigo model number for each PSU.
Serial	The Xsigo serial number associated with each PSU.
Vendor Model	The PSUs model number assigned by the fan manufacturer.
Description	An optional description field for the PSU.

Displaying IMS Properties

The Xsigo Identity Management System (IMS) uses some general parameters for synchronizing information between the Fabric Manager Server and an external authentication system, such as an Active Directory or RADIUS server. Although the IMS properties have sensible default values, you might need to set more appropriate values for your network. You can set the IMS properties for Fabric Manager through the *IMS* tab on the Directors Details frame.

Figure 26 shows the *IMS* tab.



Cache Timeout: 240
MapsToRoot: root
Search Order: internalFirst
Server Type: ldap_ad
Token Timeout: 5

Figure 26 Director Details Frame — IMS

Default parameters are displayed, but you can set or change individual parameters by clicking the ***Edit*** button to unlock the editable options.

Table 9 shows the contents of the *IMS* tab, and explains the tab’s contents.

Table 9 Contents of the IMS Tab

Field...	Means...
Cache Timeout	Specifies the periodicity of flushing the IMS Cache on the Fabric Manager Server and resynchronizing with the external authentication server. The IMS Cache is encrypted and contains user name, password, and role(s) for all configured users. Can be set to a value between 1 and 1440 minutes. The default is 240 minutes, and setting the *Cache Timeout* to zero (0) disables cache flushing and resynchronization.
Maps To Root	Specifies where the user account information is located on the authentication server. The location is typically where you configure your users and groups. For Active Directory, you will typically enter `users`. The default is `root`.
Search Order	Specifies which IMS entity is checked first for user account information: • *InternalFirst* sets the IMS to look at the IMS Server's local users and groups first. If user account information is not found in the internal IMS, then check an external IMS (for example, the AD Server). • *ExternalFirst* sets the IMS to look at the external IMS server first (for example, the AD Server) for user and groups information. If user account information is not found in the external IMS, then check the IMS Server's local users database. These two options are not mutually exclusive, and their use is determined by where user accounts are—either on the Fabric Director or on the AD server. In cases where a user account is configured on both the Fabric Director's internal IMS and an external IMS (the AD Server), the roles and user privileges on the Fabric Director are used.
Server Type	Specifies the type of external authentication is currently in use. • For AD configuration, this setting is not optional. It must be set to *ldap_ad*. • For RADIUS authentication, this value must be *RADIUS*.
Token Timeout	Specifies the amount of time that the IMS will wait for authentication to occur before timing out. When a log in attempt occurs, the authentication token is sent to the AD Server or domain controller. This field allows you specify how long the AD Server (or domain controller) will hold the token before closing the login attempt. Valid values are from 1 to 1440 seconds. The default is 5 seconds. Setting the value to zero (0) disables the time out and allows the login attempt to remain in progress indefinitely.

Displaying Active Directory Properties

This section documents how to configure a Fabric Director in an AD authentication model by using Fabric Manager so that members of an AD group can log into the Fabric Director after they are authenticated. When you perform the procedure in this section, you will use Fabric Manager to specify the Fabric Director(s) and other properties associated with AD, such as the AD server IP (or host name), the authentication method and so on. When the Fabric Director is integrated into the AD environment, users will be able to log in to the Fabric Director through `ssh` or other methods and undergo AD authentication.

Fabric Manager supports an internal identity management system (IMS) for users and roles, but also supports external IMS functionality through LDAP, Active Directory, Simple Password, or Kerberos authentication.

- Simple password authentication provides a basic level of security. An encrypted database of user names and passwords exists on the AD server. When a user logs in through Fabric Manager, that user is challenged by the IMS (AD) server to provide valid user name and password. When the user enters valid information, the user name and password are sent “in the clear” to the server which looks up the user name and password in the list. If the user name and password are present, the user’s credentials are sent. With simple password authentication, the user name and password as well as other content are sent in clear text.
- Kerberos authentication relies on some of the generic Active Directory settings, but also requires additional parameters that are greyed out if you are doing simple password authentication through AD. As a result, you will need to have the generic AD parameters configured, just like with simple password, but the authentication type will be changed to Kerberos. When Kerberos is selected, the AD server configuration wizard unlocks the Kerberos parameters.

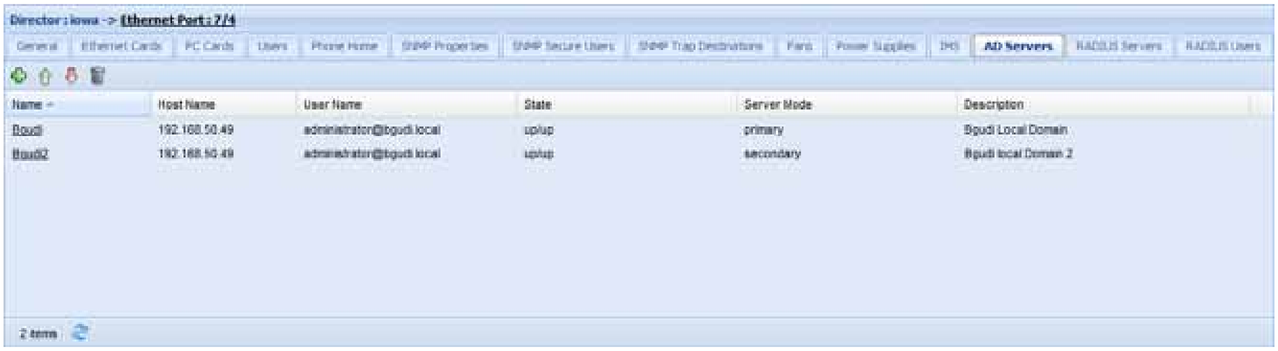
On the AD server, users and roles must be configured. Roles can be defined on the AD server in either of the following ways:

- *Legacy*, the Xsigo roles (`administrators`, `operators`, `network`, `storage`, `server,` and `no-access)` and can be prefaced with “`xg-`” for example, `xg-administrators`). Using the “`xg-`” prefix was required, but no longer is. Using “`xg-`” is still supported so that you do not need to delete and recreate the user accounts and roles on the AD server. However, if you do have existing groups that use the “`xg-`” prefix, you will need to create a group mapping to map them to the role(s) on the Fabric Manager.
- *Group Mapping*, the users can be mapped to Fabric Manager RBAC roles through a group mapping. The group mapping allows groups and roles to be created on the AD servers without the “`xg-`” prefix. Then, on Fabric Manager, the group can be mapped into Fabric Manager’s RBAC roles. Through the group mapping, the groups can be mapped into different roles, and users in a mapped group can then have multiple roles. Group mappings can be set up at either the Fabric Manager and Fabric Director level or at the individual domain level. For more information, see Mapping Users in External Groups Into Fabric Manager.

For additional information about how to configure users on an Active Directory server, see documentation that accompanied your AD server.

In Fabric Manager, additional properties must be configured that reference, or point to, the AD server in your network. These properties are documented in the following section.

Figure 27 shows the *AD Servers* tab.



Name	Host Name	User Name	State	Server Mode	Description
Bgudi	192.168.50.49	administrator@bgudi.local	up/up	primary	Bgudi Local Domain
Bgudi2	192.168.50.49	administrator@bgudi.local	up/up	secondary	Bgudi local Domain 2

Figure 27 Director Details Frame — AD Servers

Through the *AD Servers* tab, you can add a new AD Server for a Fabric Director, or you can delete a configured AD server by selecting it in the *AD Servers* tab, then clicking the garbage can icon. You can also control the state of a selected AD server by bringing it up by clicking the up arrow, or bringing the AD server down by clicking the down arrow.

Configuring AD Properties for Fabric Manager

In addition to configuring the Active Directory server, you must configure a set of parameters in Fabric Manager that specify the AD server in use in your network. These AD properties are configurable for up to two AD servers, a primary and a secondary. You can configure the AD properties for Fabric Manager through the *AD Servers* tab.

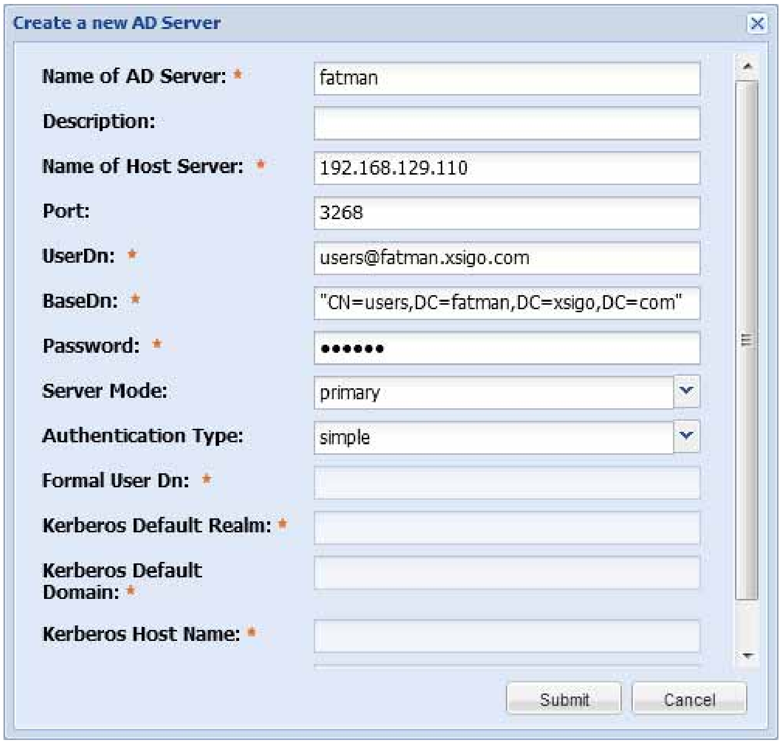
To configure AD properties for Fabric Manager, follow this procedure:

Step 1 Display the Directors Summary *Fabric Directors->Fabric Directors*.

Step 2 Select the Fabric Director for which you want to configure the AD Server. This step displays the Fabric Director in the Directors Summary.

Step 3 In the Directors Summary, click the *AD Servers* tab, as shown in Figure 28.

Step 4 On the *AD Servers* tab, click the plus sign to display the Create a new AD Server dialog. Figure 28 shows this dialog.



Create a new AD Server

Name of AD Server: *	fatman
Description:	
Name of Host Server: *	192.168.129.110
Port:	3268
UserDn: *	users@fatman.xsigo.com
BaseDn: *	"CN=users,DC=fatman,DC=xsigo,DC=com"
Password: *	●●●●●●
Server Mode:	primary
Authentication Type:	simple
Formal User Dn: *	
Kerberos Default Realm: *	
Kerberos Default Domain: *	
Kerberos Host Name: *	

Figure 28 Create a New AD Server Dialog

Step 5 In the *Name of AD Server* field, enter the name of the AD server in your network. The AD server name can be a nickname, alias, or other name that is not a fully qualified domain name (non-FQDN).

Step 6 As an option, in the *Description* field, you can provide an alphanumeric string that describes the AD server that you are configuring.

Step 7 In the *Name of Host Server* field, enter the name of the host through which one or more users will be authenticating. The host server name must be a fully qualified domain name (FQDN).

Step 8 As an option, in the *Port* field, enter the number of a particular port you want the Fabric Manager Server and Active Directory to use for communication. By default, port 3268 is used.

If you specify a non-default port, the port you specify must be dedicated specifically to the Fabric Manager Server and AD server. The port you specify cannot be used for any other traffic or service.

Step 9 In the *User DN* field, enter the user domain name for the AD server. The user DN is a string that consists of:

- user name
- the “at” sign (@)
- the host server name as an FQDN

For example, users@fatman.xsigo.com (as shown) is a validly formed user DN

Step 10 In the *Base DN* field, enter the base domain name that the server will be using. The base DN is a string of all the individual components of the domain name plus the `DC=` prefix to indicate each domain component of the domain name. Each user DN string has the following syntax requirements:

- the entire user DN string must be enclosed in quotation marks
- the user DN string cannot contain any blank spaces
- each domain component in the Base DN must separated by a comma

For example, `"DC=pubstest,DC=xsigo,DC=com"` (as shown) is a properly formed Base DN.

Step 11 In the *Password* field enter the password for the server that you are configuring. This password is used to log in from the host server to the AD server.

Note

The User DN, Base DN, and password combine to form a “blob” of account information and a pointer to the location of the account. The account information “blob” is sent to the AD server, which performs authentication and authorization, gets the user’s group membership and credentials, and responds to the Fabric Manager Server with role information.
Because the blob is sent to the AD server:
- the user account and user account group membership must already be present on the AD server. By following this procedure, the account should already have been created on the AD server
- the user logging in must be a member of the appropriate group (for example, `xg-administrators`).

Step 12 As an option, from the *Server Mode* dropdown menu, select whether the server instance you are configuring is the primary or secondary AD server. The Xsigo IMS implementation supports setting a primary and secondary server. Select the appropriate value for your network:

- *Primary*—The primary server is where the user login is attempted first. If the primary AD server is available, it will always be used for user authentication and authorization. *Primary* is the default value. Only one primary server is allowed in each AD configuration.
- *Secondary*—For redundancy, you can also specify a secondary AD server, which will be used if the primary AD server cannot respond. The secondary server will perform authentication and authorization as long as the primary server is offline.

Tip

For redundancy, Xsigo suggests configuring a primary AD server, and a secondary AD server that is a separate physical server.

Step 13 As an option, from the *Authentication Type* dropdown menu, select the type of authentication that will be used for this user:

- Simple, for simple password authentication, which is the default.
- Kerberos, if Kerberos authentication will be used as the IMS.

At this point, simple password authentication parameters are complete. Proceed to Step 19.

Additional parameters exist on this step of the wizard for Kerberos authentication. If you are configuring Kerberos authentication on the AD server, continue to Step 14.

Step 14 In the *Formal User DN* field, enter the user domain name that the server will be processing. The Formal User DN is a string consisting of:

- user name
- the “at” sign (`@`)
- the host server name as an FQDN

For example, pubs@pubstest.xsigo.com (as shown) is a valid Formal User DN.

Step 15 In the *Kerberos Default Realm* field, enter the default realm name that the server will be using. The Kerberos Default Realm is a string of all the individual components of the default realm plus the `DC=` prefix to indicate each individual component of the default realm string. Each default realm string has the following syntax requirements:

- the entire default realm string must be enclosed in quotation marks
- the entire default realm string cannot contain any blank spaces
- each component of the default realm string must separated by a comma

For example, `“DC=pubstest,DC=xsigo,DC=com”` (as shown) indicates a valid Kerberos Default Realm.

Step 16 In the *Kerberos Default Domain* field, enter the base domain name that the server will be using. This string consists of the minimum domain components of the realm for which the AD server will be authenticating through Kerberos. For example, xsigo.com is a valid default domain.

Step 17 In the *Kerberos Host Name* field, enter the name of the host server through which one or more users will be authenticating. The host server name must be a fully qualified domain name (FQDN).

Step 18 As an option, in the *Kerberos Host Port* field, enter the number of a particular port you want the Fabric Manager Server and Active Directory to use for communication. By default, port 88 is used.

If you specify a non-default port, the port you specify must be open and available to the Fabric Manager Server and AD Server. The port you specify cannot be used for any other traffic or service.

Step 19 When the AD server properties are configured, click ***Submit*** to configure the AD server.

Step 20 Check the *AD Servers* tab to verify that the AD Server is configured for the Fabric Director.

Displaying RADIUS Servers

RADIUS authentication is supported in Fabric Manager. When you configure RADIUS, you are specifying parameters that do the following:

- point to the specific RADIUS server that Fabric Manager can use
- allow the Fabric Manager Server to login to the RADIUS database so that users in the RADIUS database are authenticated and authorized through the RADIUS server.

The Xsigo implementation of RADIUS supports authentication and authorization and is based on RFC 2138. No Xsigo proprietary attributes currently exist. Xsigo's RADIUS support does not support accounting. For information about installing and configuring the RADIUS server, see the documentation that accompanied your RADIUS server.

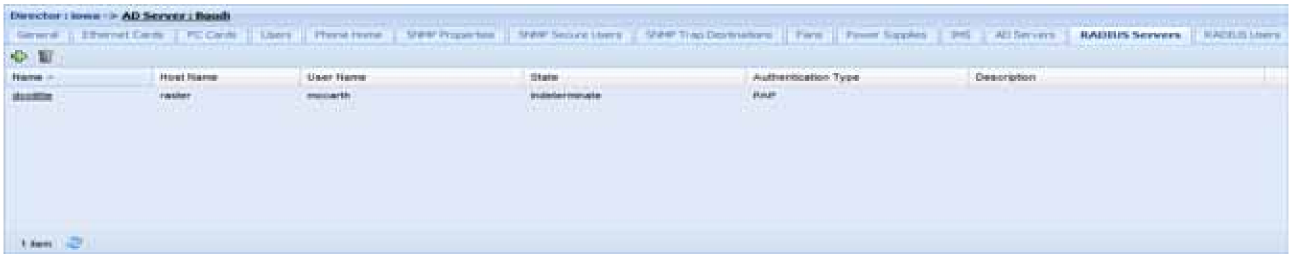
Be aware that you will need to configure specific RADIUS users in the Fabric Manager GUI. These users are different than the local users on the Fabric Director, and options specific to each user must be set. Additional information about configuring RADIUS users exists in the following section.

RADIUS users are required as part of configuring the RADIUS server for Fabric Manager. As a result, you must configure the RADIUS users before configuring the RADIUS server.

Caution

When configuring RADIUS, be aware that you must edit the RADIUS Clients database to include the Fabric Director, and Fabric Manager Server that will be using RADIUS for authentication and authorization.

RADIUS server information is contained in the *RADIUS Servers* tab of the Directors Details frame. Figure 29 shows the *RADIUS Servers* tab.



Name	Host Name	User Name	State	Authentication Type	Description
doolittle	raster	mccarth	indeterminate	PAP	

Figure 29 Director Details Frame — RADIUS Servers

You can configure a RADIUS server for Fabric Manager by clicking the plus sign, or delete a configured RADIUS server by selecting it on the RADIUS Servers tab, then clicking the garbage can icon.

Configuring RADIUS Servers for Fabric Manager

When configured, RADIUS servers handle authorization and authentication of users logging in to the Fabric Manager or Fabric Directors. To provide RADIUS functionality, you must configure some parameters in Fabric Manager that reference the particular RADIUS server that will be used. You can configure one or more RADIUS servers for your network, through the *RADIUS Servers* tab in the Directors Details frame.

When configuring a RADIUS Server for use by Fabric Manager, be aware that you must also configure RADIUS user entries which have some prerequisites. For more information, see Displaying RADIUS Users. RADIUS users must be created before configuring the RADIUS server for Fabric Manager, so make sure to create all RADIUS user accounts first. See Configuring RADIUS Users.

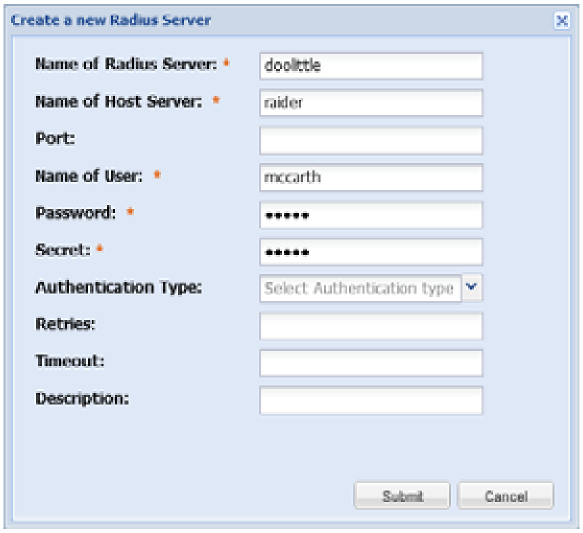
To configure RADIUS Servers for Fabric Manager, follow this procedure:

Step 1 If RADIUS users have not been configured yet, create them now as documented in Configuring RADIUS Users. When the correct RADIUS user accounts are created, continue with this procedure.

Step 2 Display the Directors Details frame by clicking *Fabric Directors->Fabric Directors*, then selecting the Fabric Director for which you want to configure a RADIUS Server.

Step 3 In the Directors Details frame, click the *RADIUS Servers* tab, as shown in Figure 29.

Step 4 Click the plus sign to display the Create a New RADIUS Server dialog. Figure 30 shows this dialog.



Create a new Radius Server

Name of Radius Server: *	doolittle
Name of Host Server: *	raider
Port:	
Name of User: *	mccarth
Password: *	•••••
Secret: *	•••••
Authentication Type:	Select Authentication type
Retries:	
Timeout:	
Description:	

Figure 30 Create a New RADIUS Server Dialog

Step 5 In the *Name of Radius Server* field, enter the name of the RADIUS server in your network. The RADIUS server name can be a nickname, alias, or other name that is not a fully qualified domain name (non-FQDN).

Step 6 In the *Name of Host Server* field, enter the name of the host through which one or more users will be authenticating. The host server name must be a fully qualified domain name (FQDN).

Step 7 As an option, in the *Port* field, enter the number of a particular port you want the Fabric Manager Server and RADIUS Server to use for communication. By default, port 3268 is used.

If you specify a non-default port, the port you specify must be dedicated specifically to the Fabric Manager Server and RADIUS server. The port you specify cannot be used for any other traffic or service.

Step 8 In the *Name of User* field, enter the name of the user(s) that will be authenticated by RADIUS when they log in to Fabric Manager. This user name is the RADIUS user name that you configured in the preceding section.

Note

The named users must exist in the RADIUS users database to be allowed to authenticate. If a RADIUS user has not been created for each person who will log in to Fabric Manager, you must cancel the Create a New RADIUS Server wizard and add their RADIUS user accounts now.

Step 9 In the *Password* field, enter that password that the user will be required to enter in order to log in. This password will be checked as part of the RADIUS authentication.

Step 10 In the *Secret* field, enter the RADIUS secret password, which is used between the Fabric Manager Server and the RADIUS server to allow the Fabric Manager Server to log in to the RADIUS for the purpose of handing off user names for authentication and authorization.

Step 11 From the *Authentication* type dropdown menu, select the type of authentication that the RADIUS user will be enforcing for the user:

- PAP (password authentication protocol), which is a simple password authentication method. PAP is the default authentication protocol.
- CHAP (challenge handshake authentication protocol), which is a method of combining the user’s password with a computation, and comparing that to information that the user enters when the RADIUS challenges the user. CHAP is the more secure authentication protocol of the two.

Step 12 As an option, in the *Retries* field, you can enter the number of retires that can occur between the Fabric Manager Server and the RADIUS server. Enter a number between 0 and 100. The default is 3 retries. Zero (0) sets no retry, so any failed connection attempt between the Fabric Manager Server and the RADIUS server halts the authentication attempt.

Each unsuccessful log in attempt between the Fabric Manager Server and the RADIUS server causes a retry (if the retry value is greater than 0), and the number specified in the *Retries* field is the maximum number of retries before authentication is aborted. The default value is 3 retries.

Step 13 As an option, you can enter the *Timeout* value (in seconds) for log in attempts between the Fabric Manager Server and the RADIUS server. Enter a number between 0 and 120. The default is 3 seconds. Zero (0) sets no timeout value, and causes a failed log in attempt to abort the log in attempt.

If a login attempt between the Fabric Manager Server and the RADIUS server is hung or slow, the attempt will remain alive for the length of the timeout. If the timeout value is met without a successful log in, the log in attempt is aborted.

Step 14 As an option, in the *Description* field, you can provide an alphanumeric string that describes the AD server that you are configuring.

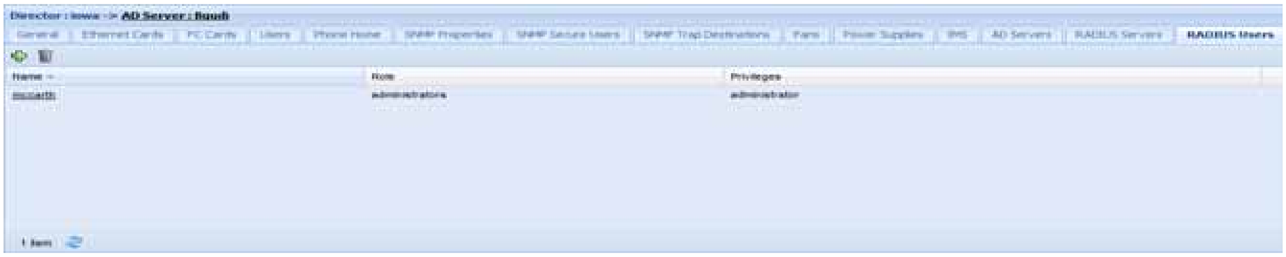
Step 15 When the RADIUS configuration has been specified, click ***Submit*** to create the instance of the RADIUS Server in Fabric Manager.

Step 16 Check the *RADIUS Servers* tab to verify that the RADIUS server was configured correctly.

Displaying RADIUS Users

RADIUS users must exist in the RADIUS users database in order for authentication to occur for each user. The RADIUS user name must match the name of the user who will log in to Fabric Manager for RADIUS authentication to successfully occur. If there is a mismatch between the user name used at Fabric Manager login and the user name in the RADIUS database, authentication will not complete and the user will not be allowed to log in to Fabric Manager.

Figure 31 shows the *RADIUS Users* tab.



Name	Role	Privileges
mccarth	administrators	administrator

Figure 31 Directors Details Frame — RADIUS Users

You can add a new RADIUS user by clicking the plus sign, and you can delete a configured RADIUS user by selecting it in the *RADIUS Users* tab, then clicking the garbage can icon.

Configuring RADIUS Users

RADIUS users must exist in the RADIUS users database in order for authentication to occur for each user. The RADIUS user name must match the name of the user who will log in to Fabric Manager for RADIUS authentication to successfully occur. If there is a mismatch between the user name used at Fabric Manager login and the user name in the RADIUS database, authentication will not complete and the user will not be allowed to log in to Fabric Manager.

RADIUS users must be created before configuring the RADIUS server for Fabric Manager, so make sure to create all RADIUS user accounts first.

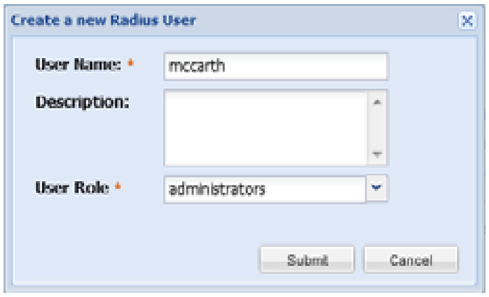
RADIUS users can be created through Fabric Manager by using the RADIUS Users list. As an alternative, you can edit the `raddb/users` file and add the users through a command-line session. Be aware that if a user name is not configured in the RADIUS users database, or if there is a mismatch between the RADIUS users user name and the name used to log in to Fabric Manager, authentication will fail. If RADIUS users are not yet configured, configure them now.

To configure RADUS Users, follow this procedure:

Step 1 Display the Directors Details frame by selecting *Fabric Directors->Fabric Directors*, then selecting the Fabric Director for which you want to configure a RADIUS user.

Step 2 In the Directors Details frame, click the *RADIUS Users* tab, as shown in Figure 31.

Step 3 Click the plus sign to display the Create a New RADIUS User dialog. Figure 32 shows this dialog.



Create a new Radius User

User Name: * mccarth

Description:

User Role * administrators

Figure 32 Create a New RADIUS Server

Step 4 In the *User Name* field, enter the name of the user who will log in to Fabric Manager. The user name must exactly match the name you enter. This name will be passed to the RADIUS server, written to its users database, and will be checked against the user name that is entered when someone attempts to log in to Fabric Manager.

Step 5 As an option, in the *Description* field, you can enter an alphanumeric sting that describes the user you are creating.

Step 6 From the *User Role* dropdown menu, select the role that the user will be granted when authentication occurs. Select from the following roles:

- administrators
- network
- operators
- server
- storage

Step 7 When the RADIUS user properties have been configured, click ***Submit***.

Step 8 Check the *RADIUS Users* tab to verify that the RADIUS user was correctly configured.

Unmanaging a Fabric Director

At any time, you can unmanage a Fabric Director in Fabric Manager. Unmanaging a Fabric Director is intended to be used only when the Fabric Director is no longer going to be managed by Fabric Director. Xsigo recommends that unmanaging a Fabric Director is not used for any purpose other than permanently removing a Fabric Director from Fabric Manager.

Note

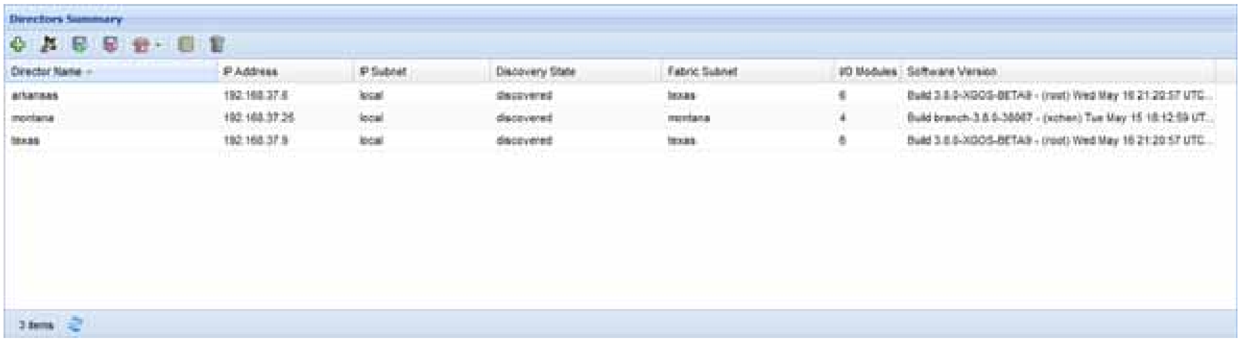
Unmanaging Fabric Directors is not to be used for clearing errors or transient states (for example, if a large job is running for a long time, and you want to “force quit” the job), unless you are otherwise directed to do so by Xsigo personnel.

When a Fabric Director is unmanaged, then remanaged within a reasonable amount of time, the Fabric Manager database retains selected configuration information (for example, port associations in clouds, vNIC and vHBA terminations, and so on). As a result, when the Fabric Director is remanaged, the general rule is that this information is put back into Fabric Manager after the Fabric Director has returned to `up/up` state when it is remanaged.

However, there are some exceptions to this rule. Domains contain their own secured objects—Fabric Directors, users, I/O modules and so on. If a domain has secured objects assigned to it, and the Fabric Manager that controlling those secured items is unmanaged, when the Fabric Manager is managed again, the secured objects are not automatically put back into their original domain(s). For more information, see Working with Domains.

To unmanage a Fabric Director, follow this procedure:

Step 1 Display the Fabric Director summary by selecting *Fabric Directors->Fabric Directors*. Figure 33 show the Directors Summary.



Directors Summary

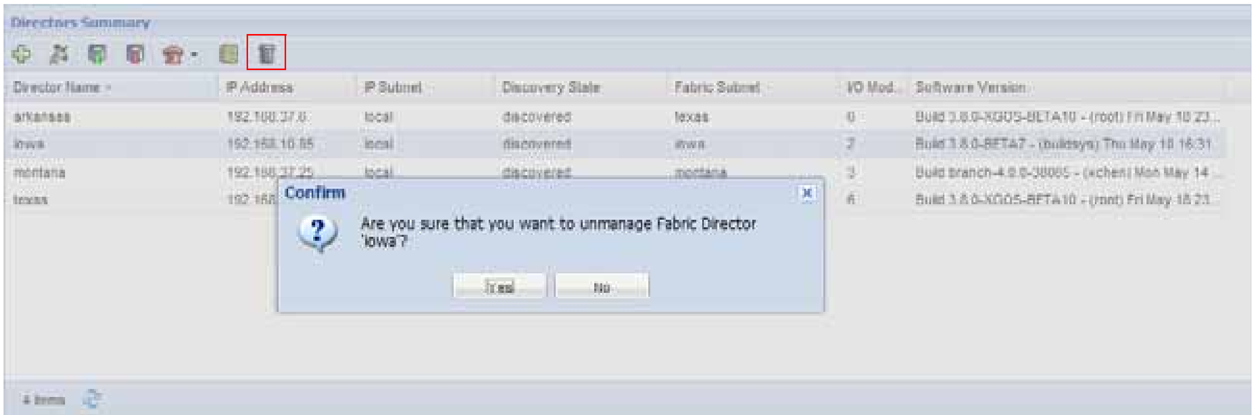
Director Name	IP Address	IP Subnet	Discovery State	Fabric Subnet	I/O Modules	Software Version
arkansas	192.168.37.6	local	discovered	texas	6	Build 3.8.0-XGOS-BETA9 - (root) Wed May 16 21:20:57 UTC...
montana	192.168.37.26	local	discovered	montana	4	Build branch-3.8.0-38087 - (xchen) Tue May 15 18:12:59 UT...
texas	192.168.37.9	local	discovered	texas	6	Build 3.8.0-XGOS-BETA9 - (root) Wed May 16 21:20:57 UTC...

3 items

Figure 33 Directors Summary

Step 2 Select the Fabric Director that you want to unmanage. This step activates the ***Unmanage*** button (garbage can) on the Director Summary toolbar.

Step 3 Click ***Unmanage*** to remove the selected Fabric Director from Fabric Manager. When you click ***Unmanage***, a confirmation is displayed.



Directors Summary

Director Name	IP Address	IP Subnet	Discovery State	Fabric Subnet	I/O Mod...	Software Version
arkansas	192.168.37.6	local	discovered	texas	6	Build 3.8.0-XGOS-BETA10 - (root) Fri May 18 23...
iowa	192.168.10.65	local	discovered	iowa	2	Build 3.8.0-BETA7 - (buildsys) Thu May 10 16:31
montana	192.168.37.25	local	discovered	montana	3	Build branch-4.0.0-38005 - (xchen) Mon May 14 ...
texas	192.168				6	Build 3.8.0-XGOS-BETA10 - (root) Fri May 18 23...

Confirm

Are you sure that you want to unmanage Fabric Director 'iowa'?

Figure 34 Unmanaging a Fabric Director

Step 4 Click ***Yes*** on the confirmation dialog to complete unmanaging the Fabric Director.

Backing Up and Restoring a Fabric Director Configuration

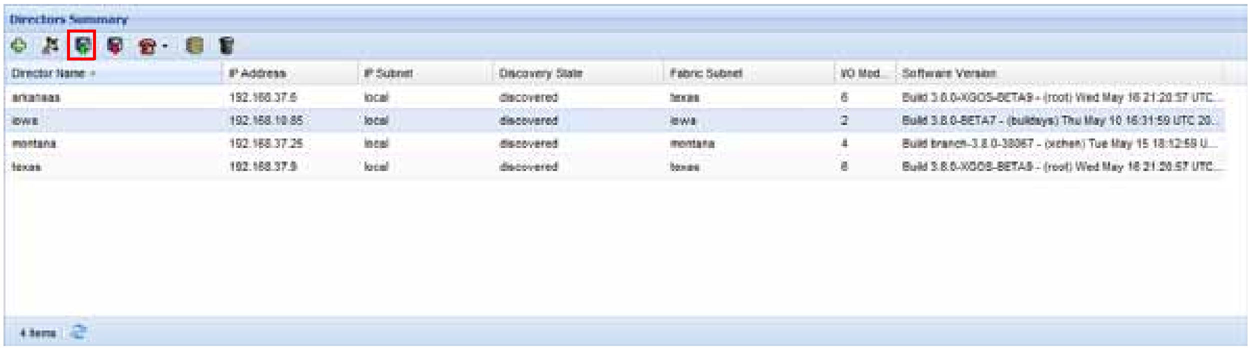
As a best practice, you should be running scheduled backups of the Fabric Director. By doing so, you have the ability to replace parts of the Fabric Director (or in more serious situations, the entire Fabric Director itself) while still keeping the virtual I/O configuration.

As an alternative to scheduled backups, you can use on-demand backups which you must manually start. While scheduled backups are preferred because the operate automatically, on-demand backups are also useful for capturing the Fabric Director configuration as long as you are consistent with manually taking the on-demand backups.

In situations where you need to replace the Fabric Director and want to save the current configuration through Fabric Manager, use this procedure, which requires that you have a Fabric Director configuration saved prior to the need to replace the Fabric Director:

Step 1 Display the Directors Summary page by selecting *Fabric Directors->Fabric Directors.*

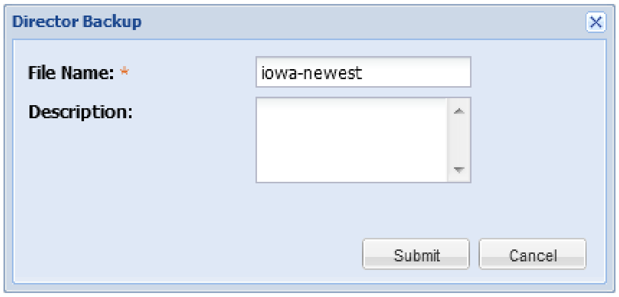
Step 2 On the Fabric Director Summary, select the Fabric Director that you want to backup, and click the ***Backup Configuration from Selected Fabric Directors*** button as shown in Figure 35.



Director Name	IP Address	IP Subnet	Discovery State	Fabric Subnet	I/O Mod...	Software Version
arkansas	192.168.37.6	local	discovered	texas	6	Build 3.8.0-XGOS-BETA9 - (root) Wed May 16 21:20:57 UTC...
iowa	192.168.10.85	local	discovered	iowa	2	Build 3.8.0-BETA7 - (buildsys) Thu May 10 16:31:59 UTC 20...
montana	192.168.37.25	local	discovered	montana	4	Build branch-3.8.0-38067 - (xchen) Tue May 15 18:12:59 U...
texas	192.168.37.9	local	discovered	texas	8	Build 3.8.0-XGOS-BETA9 - (root) Wed May 16 21:20:57 UTC...

Figure 35 Directors Summary — Backup the Configuration of Selected Fabric Directors

Step 3 When you click the button, the Director Backup dialog is displayed. See Figure 36.



File Name: * iowa-newest

Description:

Figure 36 Director Backup

Step 4 In the *File Name* field, enter a name for the configuration that you are saving.

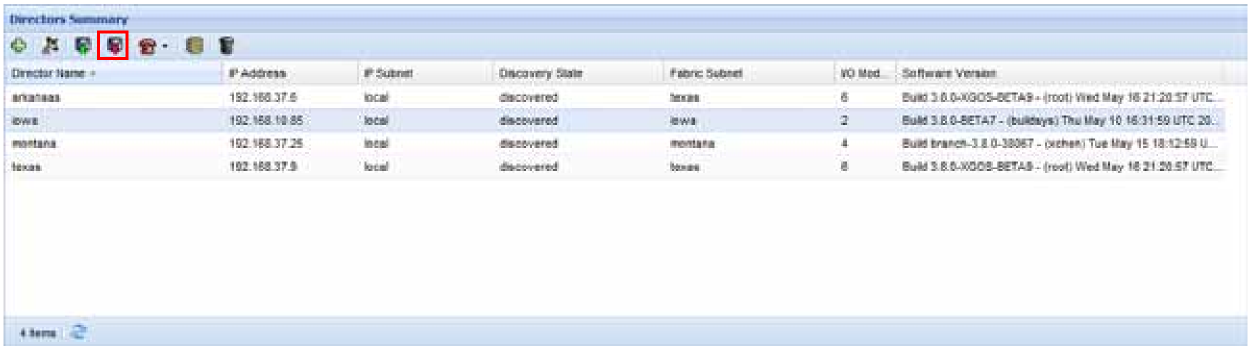
Step 5 Click ***Submit*** to save the selected Fabric Director's configuration to the file you just named.

Step 6 Make the necessary repairs or replacements to the Fabric Director.

Step 7 When the Fabric Director has recovered from the errored state, log in to Fabric Manager again.

Step 8 Display the Directors Summary page by selecting *Fabric Directors->Fabric Directors*.

Step 9 On the Fabric Director Summary, select the Fabric Director that you want to backup, and click the ***Restore a Configuration Back to the Selected Fabric Directors*** button as shown in Figure 35.



Director Name	IP Address	IP Subnet	Discovery State	Fabric Subnet	I/O Mod...	Software Version
arkansas	192.168.37.6	local	discovered	texas	6	Build 3.8.0-XGOS-BETA9 - (root) Wed May 16 21:20:57 UTC...
iowa	192.168.10.85	local	discovered	iowa	2	Build 3.8.0-BETA7 - (buildsys) Thu May 10 16:31:59 UTC 20...
montana	192.168.37.25	local	discovered	montana	4	Build branch-3.8.0-38067 - (xichen) Tue May 15 18:12:58 U...
texas	192.168.37.9	local	discovered	texas	8	Build 3.8.0-XGOS-BETA9 - (root) Wed May 16 21:20:57 UTC...

Figure 37 Directors Summary — Restore the Configuration of Selected Fabric Directors

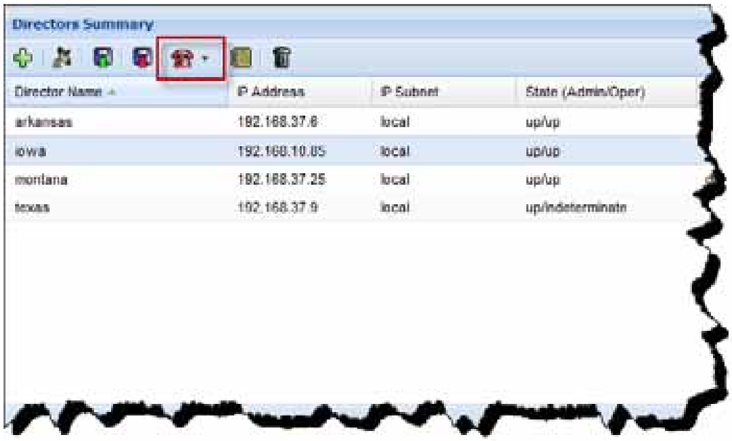
Performing Tech Support Functions on the Fabric Director

For each Fabric Director managed by Fabric Manager, you can perform a selected number of troubleshooting functions, including:

- Collecting Tech Support Information
- Sending an On-Demand Phone Home Message to Xsigo Support
- Snoozing Phone Home for a Window of Time

Because these functions are available for each Fabric Director, if you have two Fabric Directors in your environment, you might need to perform the troubleshooting function on both Fabric Directors to get the information you need.

Each of these features is supported through the ***Technical Support Actions*** toolbar button on the Directors Summary, as shown in Figure 38.



Director Name	IP Address	IP Subnet	State (Admin/Oper)
arkansas	192.168.37.8	local	up/up
iowa	192.168.10.85	local	up/up
montana	192.168.37.25	local	up/up
texas	192.168.37.9	local	up/indeterminate

Figure 38 Directors Summary — Tech Support Functions Toolbar Button

Collecting Tech Support Information

The Fabric Director can prepare specific information for Xsigo Technical Support services to diagnose. Through Fabric Manager, you can trigger the Fabric Director to prepare and gather the information contained in tech support logs, and transmit that information to Xsigo Support. Collecting tech support information occurs from one Fabric Director at a time, so if you have HA Fabric Directors on a shared fabric, you might need to collect the tech support information twice—once for each Fabric Director. This function in Fabric Manager operates the same as the **`set system tech-support`** command in Oracle’s XgOS CLI.

Typically, you will collect the tech support information when directed to do so by Xsigo Support, but you can collect this information at any time it is needed.

Note

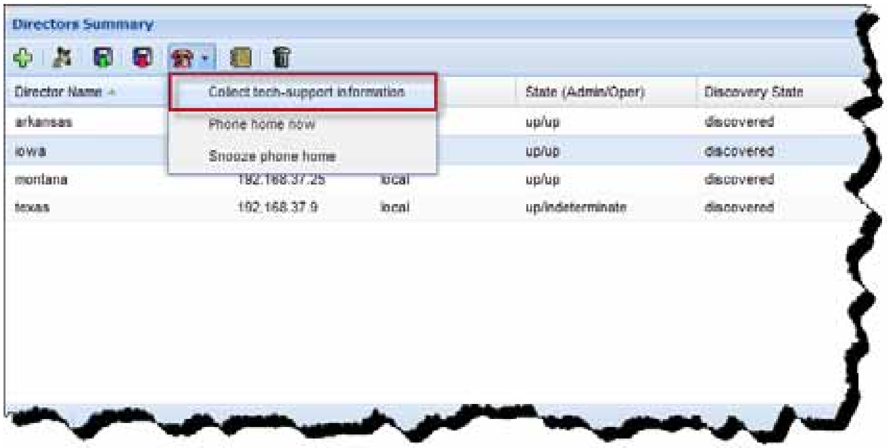
Collecting the tech support information can take a considerable amount of time based on the amount of data that will be collected. Please be patient and allow this function to complete.

To collect the tech support information from a Fabric Director, follow this procedure:

Step 1 On the navigation panel, select *Fabric Directors->Fabric Directors* to display the Directors Summary.

Step 2 Click the ***Tech Support Actions*** toolbar button to display the dropdown menu.

Step 3 Select *Collect tech-support information*, as shown in Figure 39.

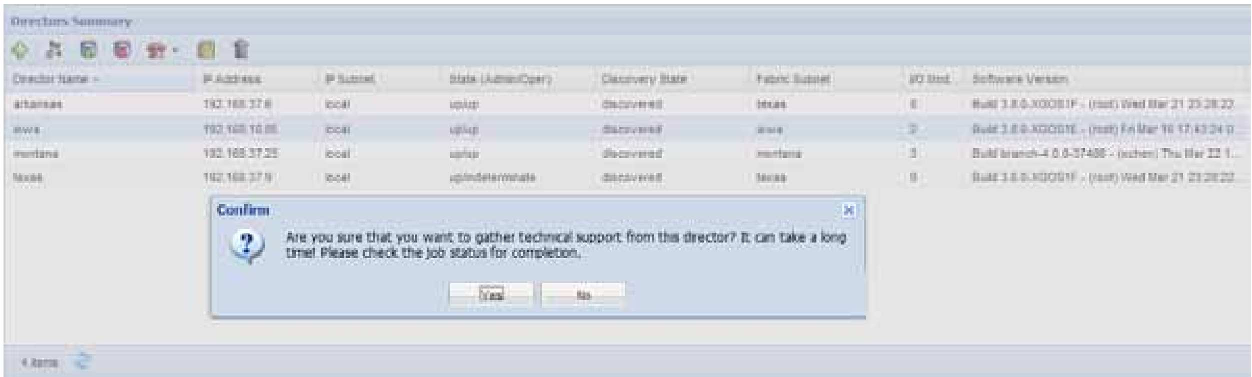


Directors Summary

Director Name ▲			State (Admin/Oper)	Discovery State
arkansas			up/up	discovered
iowa			up/up	discovered
montana	192.168.37.25	local	up/up	discovered
texas	192.168.37.9	local	up/indeterminate	discovered

Figure 39 Tech Support Functions — Phone Home Now

Step 4 When you select *Collect tech-support information*, you are prompted with a confirmation dialog, as shown in Figure 40.



Directors Summary

Director Name ▲	IP Address	IP Subnet	State (Admin/Oper)	Discovery State	Fabric Subnet	I/O Slot	Software Version
arkansas	192.168.37.6	local	up/up	discovered	texas	6	Build 3.8.0-XGOS1F - (root) Wed Mar 21 23:28:22
iowa	192.168.10.85	local	up/up	discovered	iowa	2	Build 3.8.0-XGOS1E - (root) Fri Mar 16 17:43:24 0...
montana	192.168.37.25	local	up/up	discovered	montana	3	Build branch-4.0.0-37488 - (xchen) Thu Mar 22 1...
texas	192.168.37.9	local	up/indeterminate	discovered	texas	8	Build 3.8.0-XGOS1F - (root) Wed Mar 21 23:28:22...

Confirm

Are you sure that you want to gather technical support from this director? It can take a long time! Please check the job status for completion.

Figure 40 Collect Tech Support Information Confirmation Dialog

Step 5 Read the confirmation message, and click ***Yes*** to begin gathering the information.

Step 6 When directed to do so by Xsigo Support, send the information to Xsigo Support.

Sending an On-Demand Phone Home Message to Xsigo Support

Phone Home information can be set up to occur on a regular schedule, but you can also send a Phone Home message to Xsigo Support whenever you need to by sending an on-demand phone home message. This type of phone home message provides the same information to Xsigo Support as a scheduled phone home, and an on-demand phone home message also uses the same parameters. For example, if `Strip Private` is set for scheduled phone home messages, no private IP addresses will be sent in the on-demand phone home message either. For information about setting up Phone Home parameters, see Displaying Phone Home Information.

Typically, a Phone Home Now message is sent when Xsigo Support directs you to do so, but you can send a Phone Home message without Xsigo explicitly telling you to.

Note

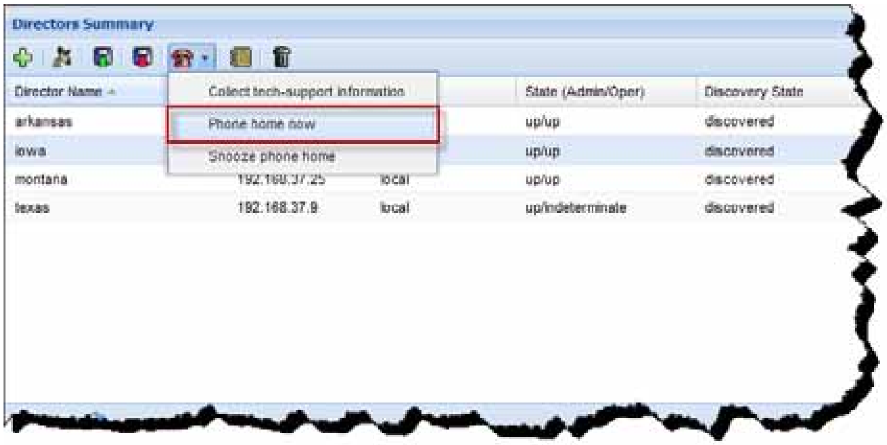
Sending a Phone Home message to Xsigo Support creates a secure HTTP message. This message varies in size, but based on the information gathered from the Fabric Director, can be very large. Please be patient and allow the Phone Home message to complete.

To send an on-demand phone home message to Xsigo Support, follow this procedure:

Step 1 On the navigation panel, select *Fabric Directors->Fabric Directors* to display the Directors Summary.

Step 2 Click the ***Tech Support Actions*** toolbar button to display the dropdown menu.

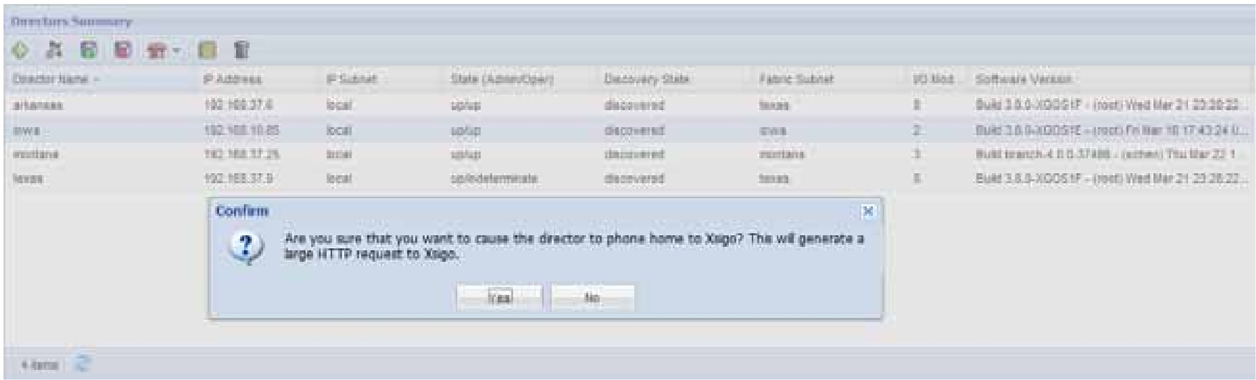
Step 3 Select *Phone Home Now*, as shown in Figure 41.



Director Name			State (Admin/Oper)	Discovery State
arkansas			up/up	discovered
iowa			up/up	discovered
montana	192.168.37.25	local	up/up	discovered
texas	192.168.37.9	local	up/indeterminate	discovered

Figure 41 Tech Support Functions — Phone Home Now

Step 4 When you select *Phone Home Now*, you are prompted with a confirmation dialog, as shown in Figure 42.



Directors Summary

Director Name	IP Address	IP Subnet	State (Admin/Oper)	Discovery State	Fabric Subnet	I/O Mod	Software Version
arkansas	192.168.37.6	local	up/up	discovered	texas	8	Build 3.8.0-XGOS1F - (root) Wed Mar 21 23:20:22...
iowa	192.168.10.85	local	up/up	discovered	iowa	2	Build 3.8.0-XGOS1E - (root) Fri Mar 16 17:43:24 U...
montana	192.168.37.25	local	up/up	discovered	montana	3	Build branch-4.0.0-37486 - (scheri) Thu Mar 22 1...
texas	192.168.37.9	local	up/indeterminate	discovered	texas	6	Build 3.8.0-XGOS1F - (root) Wed Mar 21 23:28:22...

Confirm

Are you sure that you want to cause the director to phone home to Xsigo? This will generate a large HTTP request to Xsigo.

Figure 42 Phone Home Now Confirmation Dialog

Step 5 Read the confirmation message, then click ***Yes*** to send the Phone Home message to Xsigo Support.

Step 6 If needed, follow up with Xsigo Support to verify that they received the Phone Home message.

Snoozing Phone Home for a Window of Time

For scheduled Phone Home, you can temporarily halt the scheduled transmission of Phone Home information through the use of the snooze feature. The snooze feature lasts for a customizable amount of time from 10 minutes to two days. During the snooze interval, no scheduled phone messages occur. After the snooze interval expires, the scheduled Phone Home messages resume transmission at their regularly scheduled time. During the snooze interval, you can still send on-demand Phone Home messages. (See Sending an On-Demand Phone Home Message to Xsigo Support if needed).

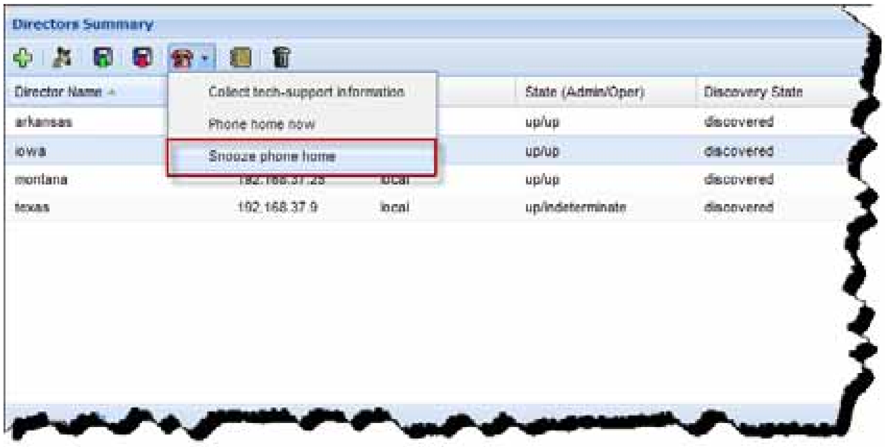
Snoozing Phone Home occurs on one Fabric Director at a time, so you might need to use this feature twice if you have an HA Fabric Director environment—once for each of the Fabric Directors. Typically, Phone Home is snoozed by Xsigo Support's request, for example, while they are diagnosing Phone Home messages that have already been sent. However, you can snooze phone home at any time for any reason.

To snooze Phone Home, follow this procedure:

Step 1 On the navigation panel, select *Fabric Directors->Fabric Directors* to display the Directors Summary.

Step 2 Click the ***Tech Support Actions*** toolbar button to display the dropdown menu.

Step 3 Select *Snooze Phone Home*, as shown in Figure 43.



Director Name			State (Admin/Oper)	Discovery State
arkansas			up/up	discovered
iowa			up/up	discovered
montana	192.168.37.25	local	up/up	discovered
texas	192.168.37.9	local	up/indeterminate	discovered

Figure 43 Tech Support Functions Toolbar — Snooze Phone Home

Step 4 When you select Snooze Phone Home, the Snooze Phone Home dialog is displayed as shown in Figure 44.

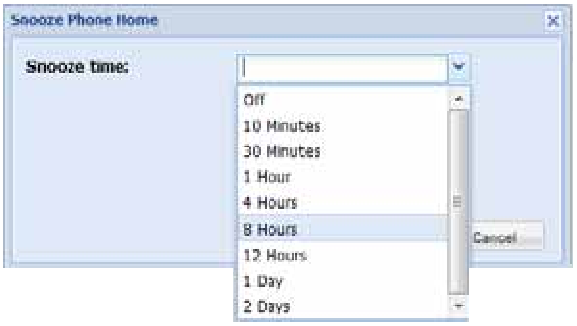


Figure 44 Snooze Phone Home Interval Time

Step 5 From the *Snooze Time* dropdown menu, select the amount of time from 10 minutes to 2 days that you want to snooze the scheduled phone home messages.

Step 6 When the snooze time is selected, click ***Submit*** to set Phone Home into snooze mode.

Collecting Xsigo Log Files

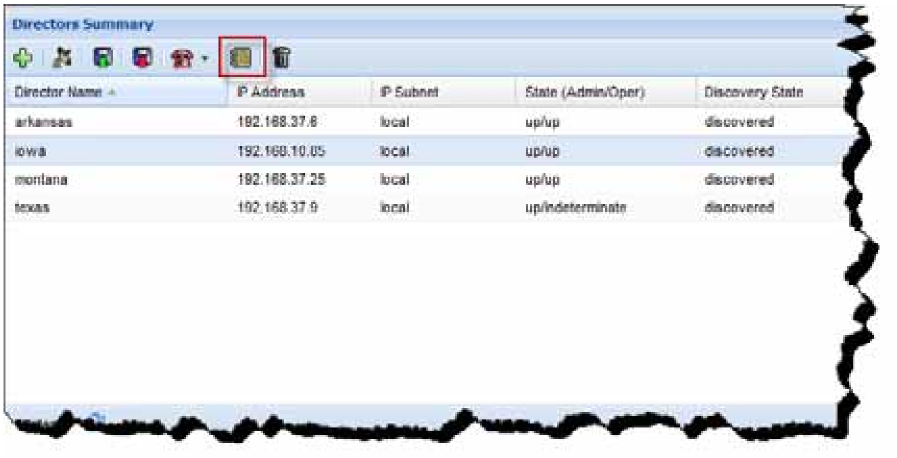
Oracle’s Xsigo Fabric Manager supports collecting a subset of the log files from a Fabric Director. Typically, collecting log files is done at Xsigo Support’s request, but it can be done at any time. Depending on the amount of data in a Fabric Director’s log files, collecting the log files can take a considerable amount of time. Please be patient and allow the process to run to completion.

Collecting log files from a Fabric Director is supported on one Fabric Director at a time. In an HA Fabric Director environment, you might need to run this operation twice—once for each Fabric Director. This procedure is supported through the ***Collect Log Files from Selected Fabric Director*** toolbar button on the Directors Summary.

To collect all Xsigo log files, follow this procedure:

Step 1 On the navigation panel, select *Fabric Directors->Fabric Directors* to display the Directors Summary.

Step 2 Click the ***Collect Log Files from Selected Fabric Director*** toolbar button, as shown in Figure 45.

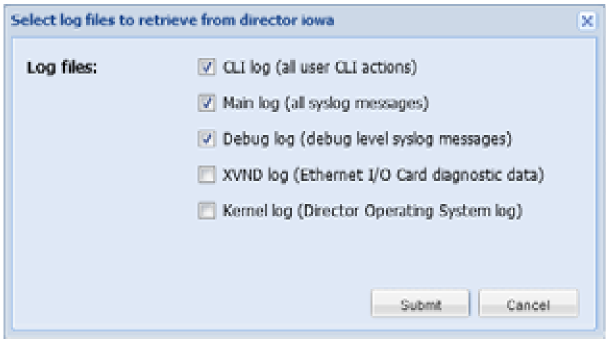


Directors Summary

Director Name ▲	IP Address	IP Subnet	State (Admin/Oper)	Discovery State
arkansas	192.168.37.6	local	up/up	discovered
iowa	192.168.10.05	local	up/up	discovered
montana	192.168.37.25	local	up/up	discovered
texas	192.168.37.9	local	up/indeterminate	discovered

Figure 45 Directors Summary Toolbar — Collect Log Files from Selected Fabric Director Button

When you click the ***Collect Log Files from Selected Fabric Director*** button, the Select Log Files to Retrieve dialog is displayed, as shown in Figure 46.



Select log files to retrieve from director iowa

Log files:

☑ CLI log (all user CLI actions)

☑ Main log (all syslog messages)

☑ Debug log (debug level syslog messages)

☐ XVND log (Ethernet I/O Card diagnostic data)

☐ Kernel log (Director Operating System log)

Figure 46 Select Log Files To Retrieve Dialog

Step 3 From the *Log Files* checkboxes, select whichever log file(s) you want to gather from the selected Oracle Fabric Director.

Step 4 When the correct log files are selected, click ***Submit*** to gather the log files.

Step 5 When directed to do so by Xsigo Support, send the files to Xsigo Support for diagnostics.

Working with I/O Templates

This chapter contains the following topics:

Note

Even though I/O Templates can be used to configure a single physical server, they are most useful when deploying virtual connectivity to multiple servers. Be aware that if you use I/O Templates to define the virtual connectivity for one or more servers, the I/O Template is only the first half of provisioning the server with the needed connectivity. After creating an I/O Template, you must then create an I/O Profile. The I/O Profile, which is derived from an I/O Template, is the object in Oracle's Xsigo Fabric Manager that you use to actually connect the vNICs and vHBAs in an I/O Template to the physical server. For information about I/O Profiles, see Working with I/O Profiles.

Understanding I/O Templates

An I/O Template is a Fabric Manager feature that allows the server administrator to create the shape of the I/O for a set of servers. Different servers have different I/O requirements. For example, a server that will be used by the engineering department may require access to a couple of Network Clouds and a Storage Cloud, but a server that is used by Finance may only require access to the internet.

By setting up an I/O Template, the server administrator is building a way to deploy a set of servers with the desired I/O requirements. An I/O Template specifies a blueprint (or general configuration) for a server, which you can use for servers of a similar type or that need the same connectivity. For example, for servers that require HA network connections and multipathed storage connections, you could create one I/O Template that provides these connections. It is important to note that the I/O Template is not directly applied to a server. Instead, the I/O Template simply defines the type and number of connections for a server. The I/O Template is then used as an input to another Fabric Manager object called an *I/O Profile*. The I/O Profile is derived from the I/O Template, and it is the I/O Profile that is deployed to the server to push the vNICs and vHBAs to that host. For more information about I/O Profiles, see Working with I/O Profiles.

As part of creating an I/O Template, you will be using a Network Cloud, a Storage Cloud, or both. You will find it helpful if your Network and Storage Clouds are already created before building I/O Templates.

Creating an I/O Template

An I/O Template must be created by you with information that is pertinent to your network. Xsigo does not provide pre-configured I/O Templates.

Creating an I/O Template can occur by either adding a new I/O Template and building it from scratch, or when at least one I/O Template exists, copying that I/O Template and editing it as needed.

This section documents creating a new I/O Template from scratch. For information about editing a configured I/O Template, see Editing an I/O Template.

When you create a new I/O Template, you are essentially creating an empty container that you add building blocks to until the I/O Template has the connectivity and virtual resources required for your network. For example, creating a new I/O Template might consist of the following phases:

- naming the I/O Template
- adding a Network Cloud and a Storage Cloud (building blocks)
- editing the network and Storage Clouds to support specific features (for example, Network and SAN QoS Profiles)
- adding one or more vNICs and vHBAs (more building blocks)
- editing the vNICs and vHBAs with specific Ethernet and Fibre Channel properties
- connecting the vNIC to the Network Cloud, and connecting the vHBA to the Storage Cloud
- saving the named I/O Template, and deploying it to one or more host servers

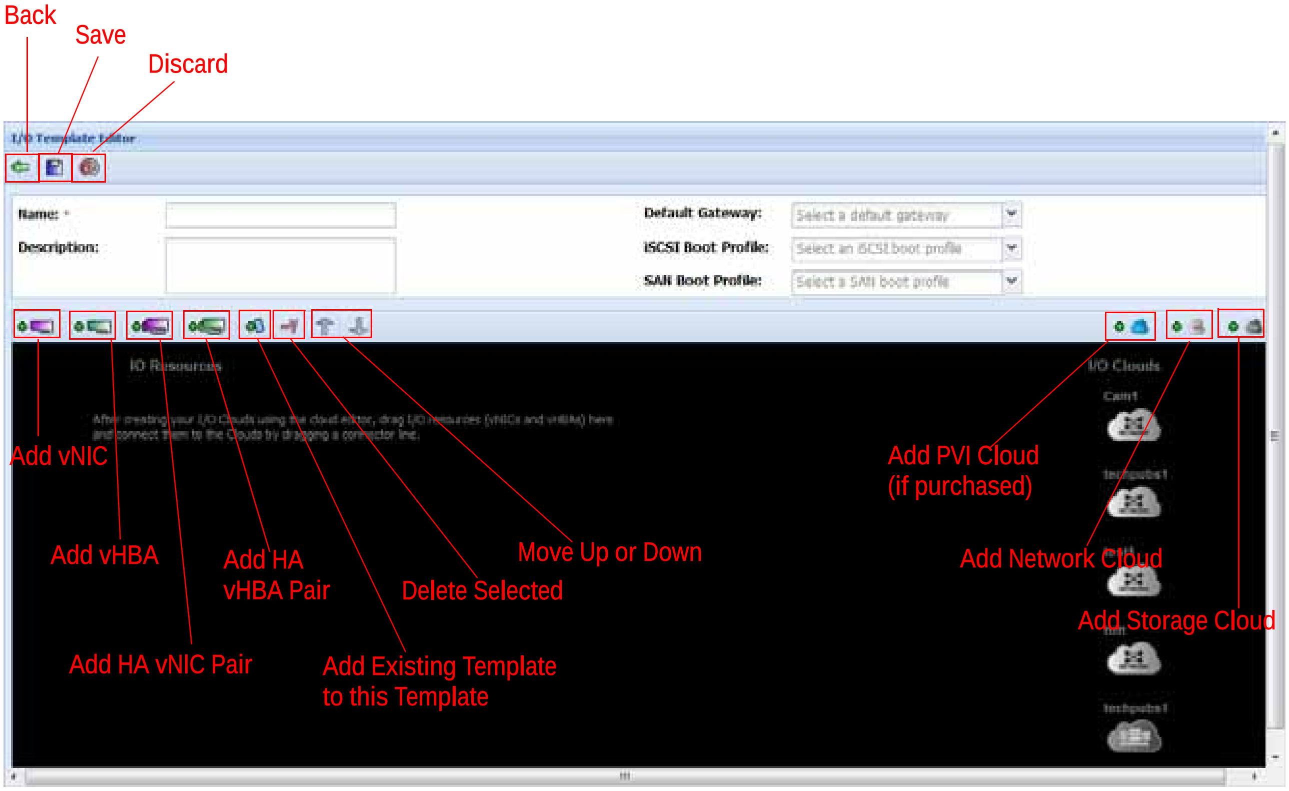
Creating an I/O Template is supported through the I/O Template Editor, which has two main frames:

- The top frame is for general properties of the I/O Template—for example, name and description.
- The bottom frame is the work area where the I/O Template’s building blocks are assembled and the bulk of the work occurs. The bottom frame also has two specific parts:
  - — I/O Resources, which is where vNICs and vHBAs are added as building blocks to the I/O Template.

— I/O Clouds, which is where Network and Storage Clouds are added as building blocks to the overall I/O Template.

Each area (the top frame, I/O Resources in the bottom frame, and I/O Clouds in the bottom frame) has a group of buttons that control those parts of the I/O Template editor.

Figure 1 shows the I/O Template Editor and indicates the controls available in the I/O Template.



After creating your I/O Clouds using the cloud editor, drag I/O resources (vNICs and vHBAs) here and connect them to the Clouds by dragging a connector line.

Figure 1 I/O Template Editor

You can add a new I/O Template by clicking the plus sign, and you can delete the currently displayed I/O Template by clicking the ***Discard*** icon.

Creating a New I/O Template

Creating an I/O Template is supported through the I/O Template Editor, which is a work space that allows adding building blocks to the empty I/O Template. Because the I/O Template Editor is a work space, you can add, delete, and make changes as needed without impacting the Fabric Manager or Oracle Xsigo Fabric Director. Fabric Manager does not save the in-progress I/O Template configuration at intervals during the configuration, and Fabric Manager also does not automatically save the finished configuration. To save the configuration when it is complete, you must explicitly click the ***Save*** icon.

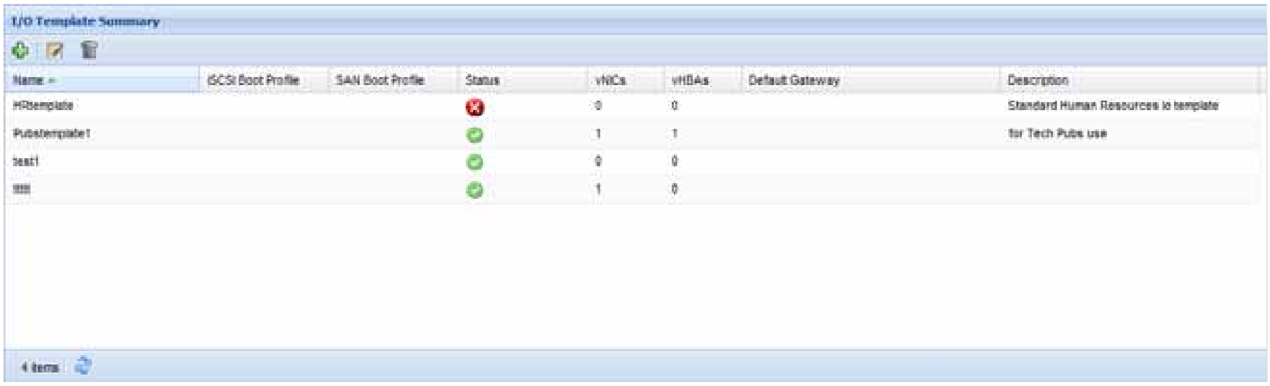
The I/O Template Editor is accessible from the navigation panel by selecting *Server Resource Manager->I/O Templates*.

Tip

You will find it helpful if the following elements are already created before building I/O Templates.
* server boot profiles (SAN Boot Profiles or iSCSI Boot Profiles)
* default gateways
* Network QoS Profiles
* Storage QoS Profiles

To create a new I/O Template, follow this procedure:

Step 1 Display the I/O Template Summary by selecting *Server Resource Manager->I/O Templates*. Figure 2 shows the I/O Template Summary.



I/O Template Summary

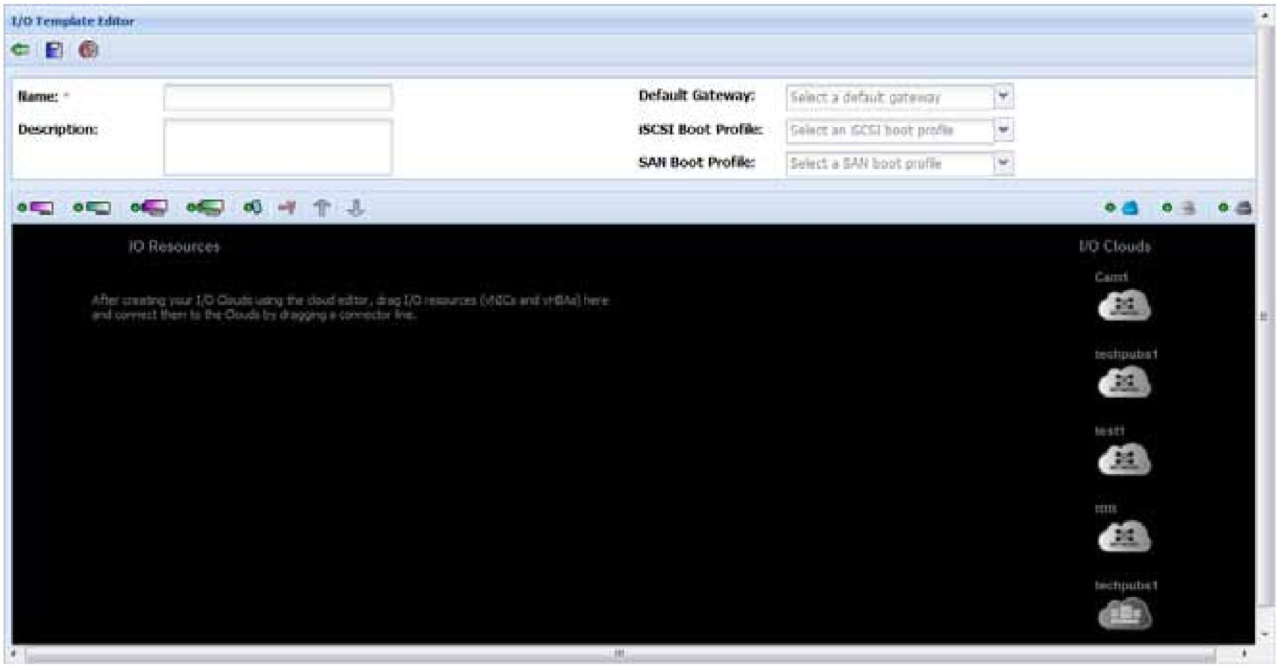
Name	iSCSI Boot Profile	SAN Boot Profile	Status	vNICs	vHBAs	Default Gateway	Description
HRtemplate			✗	0	0		Standard Human Resources io template
Pubstemplate1			✓	1	1		for Tech Pubs use
test1			✓	0	0		
tttt			✓	1	0		

4 items

Figure 2 I/O Template Summary

You can add a new I/O Template by clicking the plus sign, and you can delete a configured I/O Template by selecting it in the I/O Template Summary, then clicking the garbage can icon.

Step 2 Click the plus sign to display the I/O Template Editor. Figure 3 shows the I/O Template Editor.



I/O Template Editor

Name: *

Description:

Default Gateway: Select a default gateway

iSCSI Boot Profile: Select an iSCSI boot profile

SAN Boot Profile: Select a SAN boot profile

IO Resources

After creating your I/O Clouds using the cloud editor, drag I/O resources (vNICs and vHBAs) here and connect them to the Clouds by dragging a connector line.

I/O Clouds

Figure 3 I/O Template Editor

Step 3 In the *Name* field, enter an alphanumeric string that names the I/O Template that you are creating.

Step 4 As an option, in the *Description* field, enter an alphanumeric string that describes the I/O Template that you are creating.

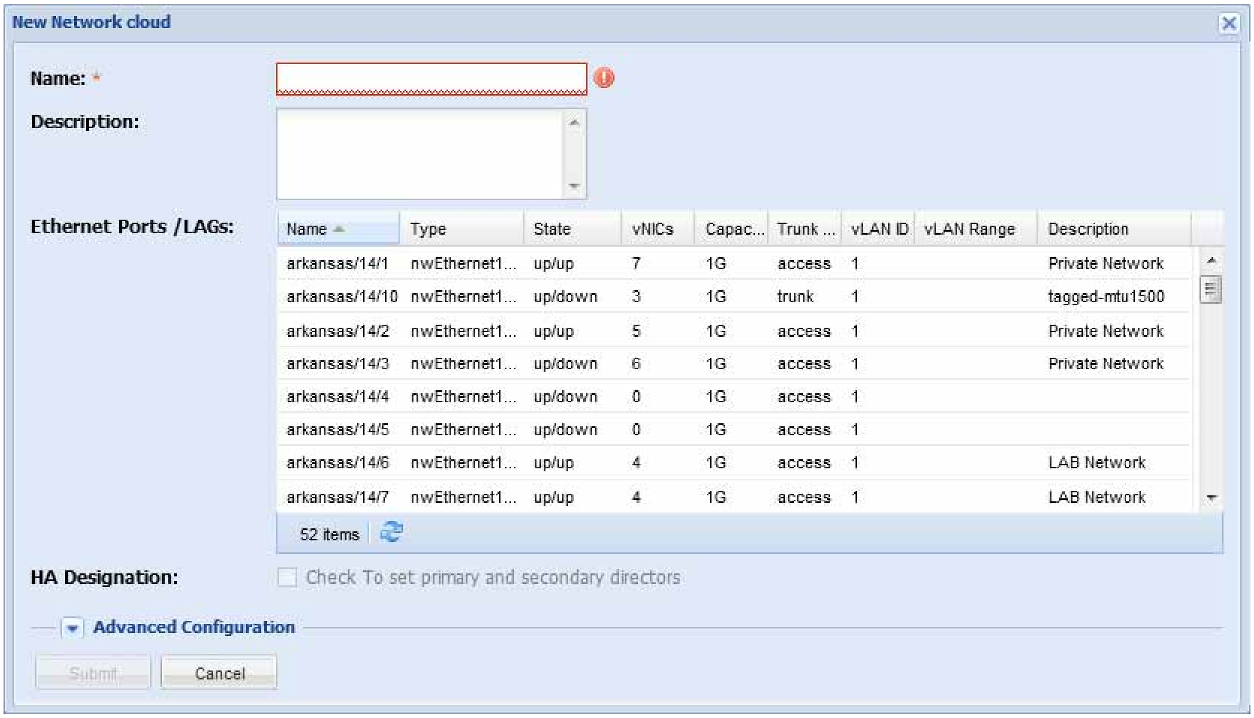
Step 5 From the *Default Gateway* dropdown menu, select the default gateway for the I/O Template. The default gateway must already be created in Fabric Manager for it to be a selectable item on the dropdown menu.

Step 6 If the hosts using this I/O Template will be booting up through iSCSI boot, from the *iSCSI Boot Profile* dropdown menu, select the iSCSI Boot Profile for the I/O Template. The iSCSI Boot Profile must already be created in Fabric Manager for it to be a selectable item on the dropdown menu.

Step 7 If the hosts using this I/O Template will be booting up through SAN boot, from the *SAN Boot Profile* dropdown menu, select the SAN Boot Profile for the I/O Template. The SAN Boot Profile must already be created in Fabric Manager for it to be a selectable item on the dropdown menu.

Adding Network Clouds to the I/O Template

Step 8 Click the ***Add Network Cloud*** button to display the New Network Cloud dialog. Figure 4 shows this dialog. For this procedure, only one Network Cloud is being assigned, but you can assign multiple Network Clouds to the same I/O Template.



New Network cloud

Name: *

Description:

Ethernet Ports /LAGs:

Name	Type	State	vNICs	Capac...	Trunk ...	vLAN ID	vLAN Range	Description
arkansas/14/1	nwEthernet1...	up/up	7	1G	access	1		Private Network
arkansas/14/10	nwEthernet1...	up/down	3	1G	trunk	1		tagged-mtu1500
arkansas/14/2	nwEthernet1...	up/up	5	1G	access	1		Private Network
arkansas/14/3	nwEthernet1...	up/down	6	1G	access	1		Private Network
arkansas/14/4	nwEthernet1...	up/down	0	1G	access	1		
arkansas/14/5	nwEthernet1...	up/down	0	1G	access	1		
arkansas/14/6	nwEthernet1...	up/up	4	1G	access	1		LAB Network
arkansas/14/7	nwEthernet1...	up/up	4	1G	access	1		LAB Network

52 items

HA Designation: □ Check To set primary and secondary directors

Figure 4 Add a New Network Cloud Dialog

Step 9 In the *Name* field, enter an alphanumeric string that names the Network Cloud that you are creating.

Step 10 As an option, in the *Description* field, enter an alphanumeric string that describes the Network Cloud that you are creating.

Step 11 From the *Ethernet Ports* table, select the port(s) that will be used in this Network Cloud. Ports are selected when they are highlighted. Multiple ports can be assigned to the same Network Cloud, and multiple Network Clouds can be assigned to the same port(s).

Note

If you are creating a Network Cloud that will be terminating an HA vNIC, you must have at least two separate Ethernet ports in the Network Cloud. You can use standard key combinations (for example, ***CTRL*** + click) to select multiple ports. For more information about creating an I/O Template for an HA vNIC, see Creating an HA vNIC Template.

Step 12 As an option, if two Fabric Directors will be deployed as a high availability pair, you can set the HA designation for each Fabric Director by using the *HA Designation* check box. The HA designation determines the first and second Fabric Director to which any HA objects in Fabric Manager will connect. The primary Fabric Director is where the primary HA object connects first, and the secondary Fabric Director is where the secondary HA object connects second. For additional information, see Setting the Fabric Director HA Designation for a Network Cloud.

At this point, you can create a basic Network Cloud, or you can specify advanced configuration parameters for the Network Cloud.

- To create the basic cloud, proceed to Figure 13.

- To specify advanced parameters for the Network Cloud, proceed to Specifying Advanced Properties for the Network Cloud.

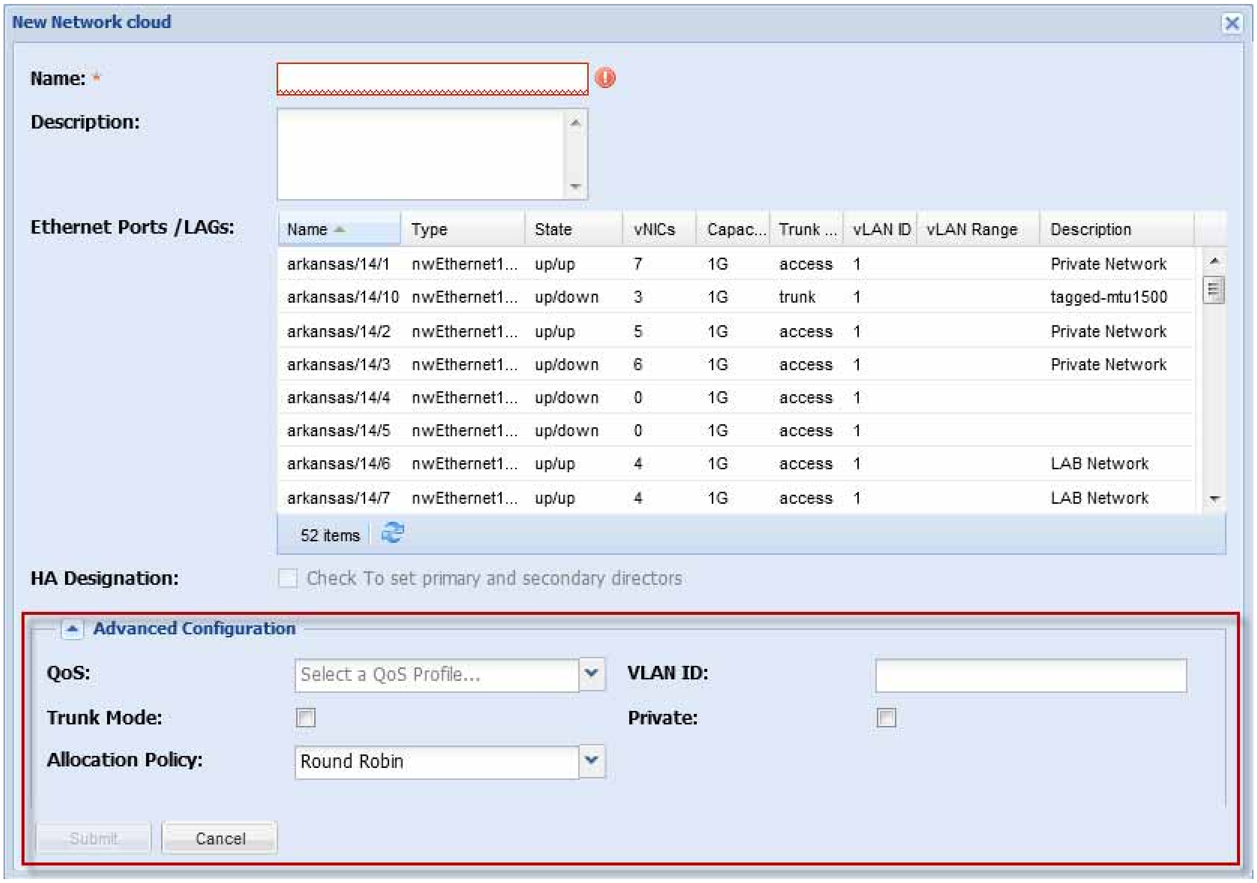
Step 13 To complete the configuration of a basic Network Cloud, click ***Submit***.

Specifying Advanced Properties for the Network Cloud

Advanced properties are available for the Network Cloud. Advanced properties give you additional control and customization of the vNICs that are available to servers. With advanced properties, you can enable powerful features like VLANs, or traffic shaping features like Network QOS. While these properties are not required for the basic configuration of a vNIC to carry traffic, they are useful for more complex deployments.

To specify advanced properties, follow this procedure:

Step 14 Click the ***Advanced Configuration*** button to display the advanced properties for the Network Cloud. See Figure 5.



New Network cloud

Name: *

Description:

Ethernet Ports /LAGs:

Name	Type	State	vNICs	Capac...	Trunk ...	vLAN ID	vLAN Range	Description
arkansas/14/1	nwEthernet1...	up/up	7	1G	access	1		Private Network
arkansas/14/10	nwEthernet1...	up/down	3	1G	trunk	1		tagged-mtu1500
arkansas/14/2	nwEthernet1...	up/up	5	1G	access	1		Private Network
arkansas/14/3	nwEthernet1...	up/down	6	1G	access	1		Private Network
arkansas/14/4	nwEthernet1...	up/down	0	1G	access	1		
arkansas/14/5	nwEthernet1...	up/down	0	1G	access	1		
arkansas/14/6	nwEthernet1...	up/up	4	1G	access	1		LAB Network
arkansas/14/7	nwEthernet1...	up/up	4	1G	access	1		LAB Network

52 items

HA Designation: □ Check To set primary and secondary directors

Advanced Configuration

QoS: Select a QoS Profile...

VLAN ID:

Trunk Mode: □

Private: □

Allocation Policy: Round Robin

Figure 5 New Network Cloud Dialog — Advanced Configuration

Step 15 From the *QoS* dropdown menu, if the vNICs in the Network Cloud will require QoS, select the Network QoS profile that will be applied to the Network Cloud. The Network Cloud must already exist for it to be a selectable object. If you do not see the Network QoS Profile you want to assign, verify that it exists.

Step 16 If the vNICs that connect to the Network Cloud will all be in the same VLAN, in the *VLAN ID* field, enter the VLAN number.

Step 17 In the *Trunk Mode* checkbox, if the Network Cloud will be supporting trunk-mode VLANs, click the checkbox.

Step 18 As an option, if you want the vNICs that connect to the Network Cloud to be private vNICs, click the *Private* checkbox. Private vNICs are used for Xsigo's vNIC-to-vNIC switching to provide add isolation for a set of vNICs, and also provide enhanced compatibility for existing and new methods of external switching.

Step 19 From the *Allocation Policy* dropdown menu, select how the Network Cloud will be applied to the host server when the cloud gets deployed. Select:

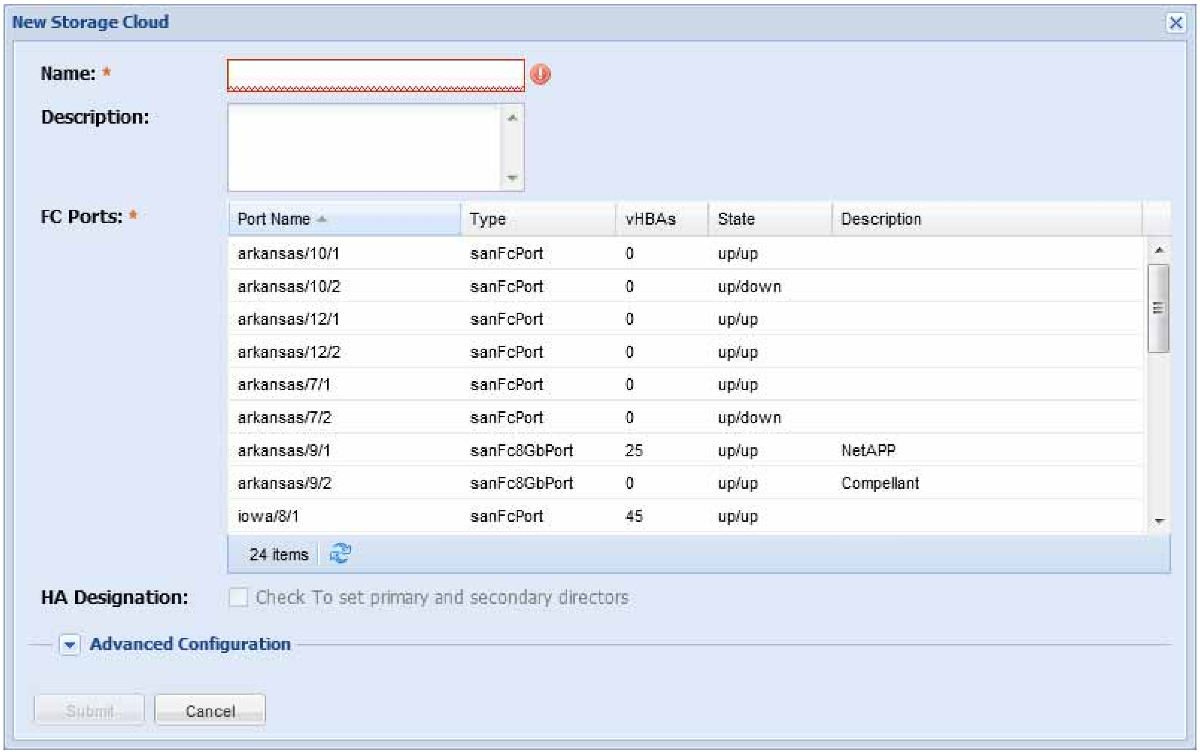
- *Round Robin*, which is a systematic way for ports to be assigned. With round robin allocation, you specify multiple ports in a list of available ports for a Network Cloud. When the list is constructed, you then assign an Ethernet port as the next available port. When you assign the next available port, it gets a rank that is different than any other port in the available ports list. The port you assign is the next port to be assigned, and after that, any additional vNICs that are connected to the Network Cloud will receive an Ethernet port based on its rank. For example, assume you create a Network Cloud with Ethernet port 2/1 as the port used to create the cloud. Then, assume you add ports 2/2, 4/1, and 5/1 to the available ports list, and set port 4/1 as the next available port. When new vNICs are connected to the Network Cloud, the first vNIC is connected to port 4/1. After that, additional vNICs are assigned to whichever port has the next lowest rank.

Step 20 When the correct properties have been assigned for the Network Cloud, click ***Submit*** to create the Network Cloud.

Step 21 Check the I/O Template Editor to verify that the Network Cloud was added correctly.

Adding Storage Clouds to the Template

Step 22 Click the ***Add Storage Cloud*** button to display the New Storage Cloud dialog. Figure 6 shows this dialog. For this procedure, only one Storage Cloud is being assigned, but you can assign multiple Storage Clouds to the same I/O Template.



Port Name	Type	vHBAs	State	Description
arkansas/10/1	sanFcPort	0	up/up	
arkansas/10/2	sanFcPort	0	up/down	
arkansas/12/1	sanFcPort	0	up/up	
arkansas/12/2	sanFcPort	0	up/up	
arkansas/7/1	sanFcPort	0	up/up	
arkansas/7/2	sanFcPort	0	up/down	
arkansas/9/1	sanFc8GbPort	25	up/up	NetAPP
arkansas/9/2	sanFc8GbPort	0	up/up	Compellant
iowa/8/1	sanFcPort	45	up/up	

Figure 6 Add a New Storage Cloud Dialog

Step 23 In the *Name* field, enter a name for the Storage Cloud that you are creating.

Step 24 As an option, in the *Description* field, enter a description for the Storage Cloud that you are creating.

Step 25 From the *FC Ports* table, select the port(s) that will be used in this Storage Cloud. Ports are selected when they are highlighted. Multiple ports can be assigned to the same Storage Cloud, and multiple Storage Clouds can be assigned to the same port(s).

Note

If you are creating a Storage Cloud that will be terminating an HA vHBA, you must have at least two separate Fibre Channel ports in the Storage Cloud. You can use standard key combinations (for example, ***CTRL*** + click) to select multiple ports. For more information about creating an I/O Template for an HA vHBA, see Creating an HA vHBA Template.

Step 26 As an option, if two Fabric Directors will be deployed as a high availability pair, you can set the HA designation for each Fabric Director by using the *HA Designation* check box. The HA designation determines the first and second Fabric Director to which any HA objects in Fabric Manager will connect. The primary Fabric Director is where the primary HA object connects first, and the secondary Fabric Director is where the secondary HA object connects second. For additional information, see Setting the Fabric Director HA Designation for a Network Cloud.

At this point, you can create a basic Storage Cloud, or you can specify advanced configuration parameters for the Network Cloud.

- To create the basic cloud, proceed to Step 27.
- To specify advanced parameters for the Storage Cloud, proceed to Specifying Advanced Properties for the Storage Cloud.

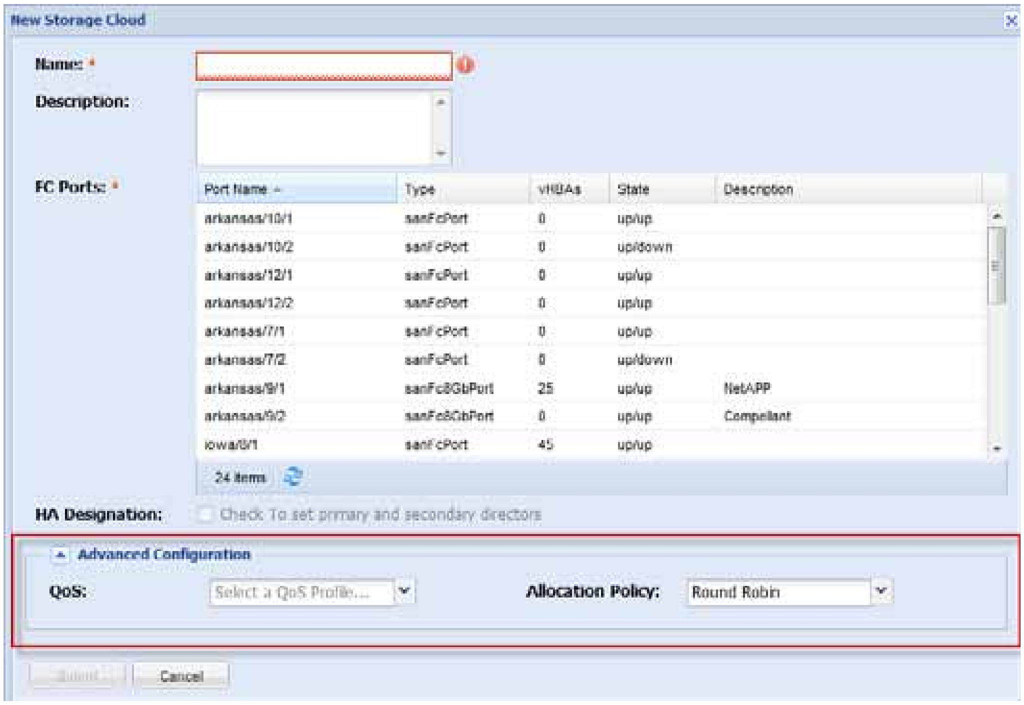
Step 27 To complete the configuration of a basic Storage Cloud, click ***Submit***.

Specifying Advanced Properties for the Storage Cloud

Advanced properties are available for the Storage Cloud. Advanced properties give you additional control and customization of the vHBAs that are available to servers. With advanced properties, you can enable traffic shaping features like SAN QOS. While these properties are not required for the basic configuration of a vNIC to carry traffic, they are useful for more complex deployments.

To specify advanced properties for a Storage Cloud, follow this procedure:

Step 28 Click the ***Advanced Configuration*** button to display the advanced properties for the Storage Cloud. See Figure 7.



New Storage Cloud

Name: *

Description:

FC Ports: *

Port Name	Type	vHBAs	State	Description
arkansas/10/1	sanFcPort	0	up/up	
arkansas/10/2	sanFcPort	0	up/down	
arkansas/12/1	sanFcPort	0	up/up	
arkansas/12/2	sanFcPort	0	up/up	
arkansas/7/1	sanFcPort	0	up/up	
arkansas/7/2	sanFcPort	0	up/down	
arkansas/9/1	sanFc8GbPort	25	up/up	NetAPP
arkansas/9/2	sanFc8GbPort	0	up/up	Compellant
iowa/8/1	sanFcPort	45	up/up	

24 items

HA Designation: □ Check To set primary and secondary directors

Advanced Configuration

QoS: Select a QoS Profile...

Allocation Policy: Round Robin

Figure 7 New Storage Cloud Dialog — Advanced Configuration

Step 29 From the *QoS* dropdown menu, if the vHBAs in the Storage Cloud will require QoS, select the SAN QoS profile that will be applied to the Storage Cloud (if any).

Step 30 From the *Allocation Policy* dropdown menu, select how the Network Cloud will be applied to the host server when the cloud gets deployed. Select:

- Round Robin, which is a systematic way for ports to be assigned. With round robin allocation, you specify multiple ports in a list of available ports for a Storage Cloud. When the list is constructed, you then assign a port as the next available port. When you assign the next available port, it gets a rank that is different than any other port in the available ports list. The port you assign is the next port to be assigned, and after that, any additional vHBAs that are connected to the Storage Cloud will receive a fibre channel port based on its rank. For example, assume you create a Storage Cloud with fibre channel port 2/1 as the port used to create the cloud. Then, assume you add ports 2/2, 4/1, and 5/1 to the available ports list, and set port 4/1 as the next available port. When new vHBAs are connected to the Storage Cloud, the first vHBA is connected to port 4/1. After that, additional vHBAs are assigned to whichever port has the next lowest rank.

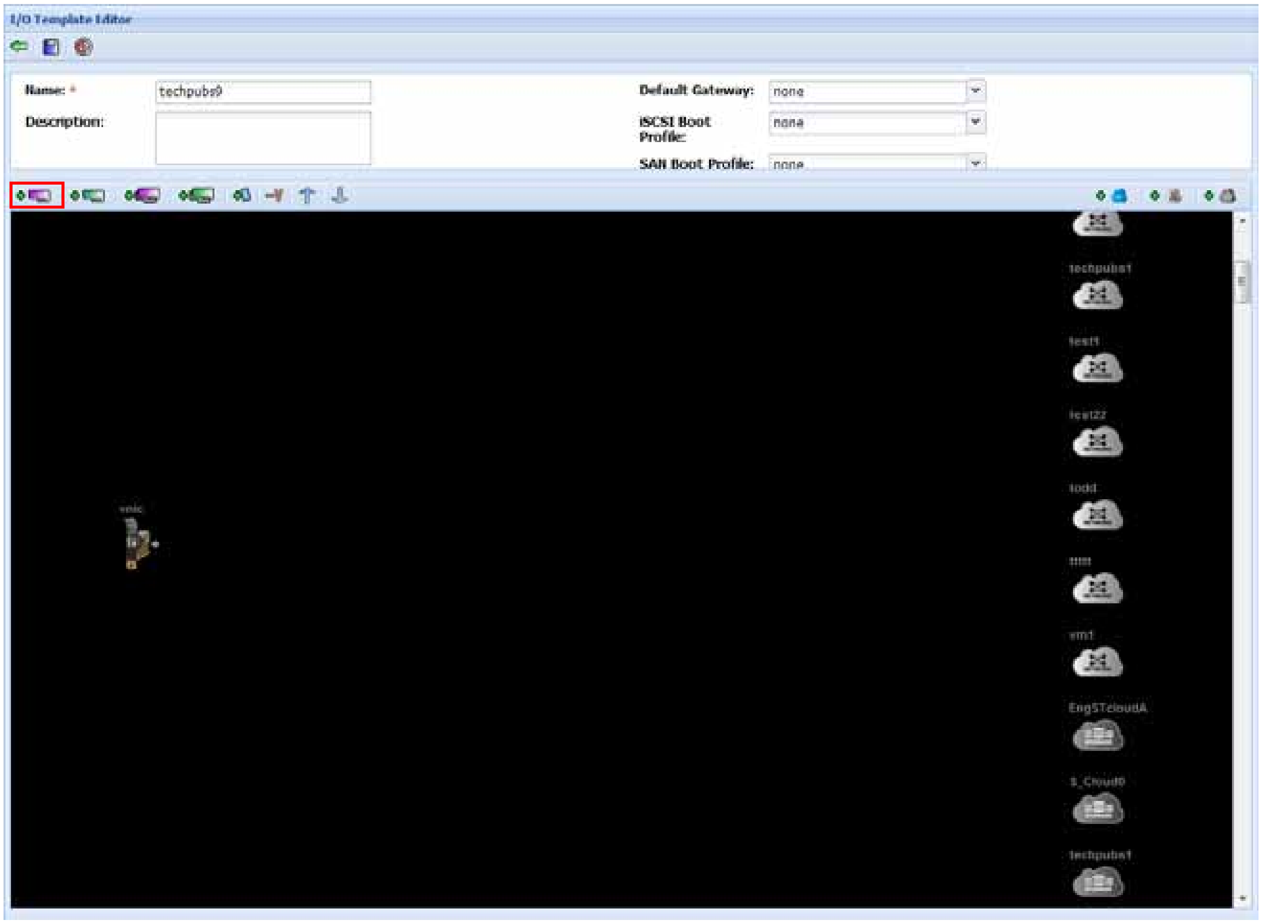
Step 31 When the correct properties have been assigned for the Storage Cloud, click ***Submit*** to create the Storage Cloud. When you click ***Submit***, a dialog is briefly displayed that informs you that Fabric Manager client and server are exchanging data.

Step 32 Check the I/O Template Editor to verify that the Storage Cloud was added correctly.

Adding vNICs to the I/O Template

Continue the main workflow for creating an I/O Template by adding one or more vNICs to the I/O Template:

Step 33 Click the ***Add vNIC*** button to add an instance of a vNIC to the I/O Template Editor, as shown in Figure 8. This procedure only adds one, but you can add as many vNICs to the I/O Template as needed.



Name: * techpubs9

Description:

Default Gateway: none

iSCSI Boot Profile: none

SAN Boot Profile: none

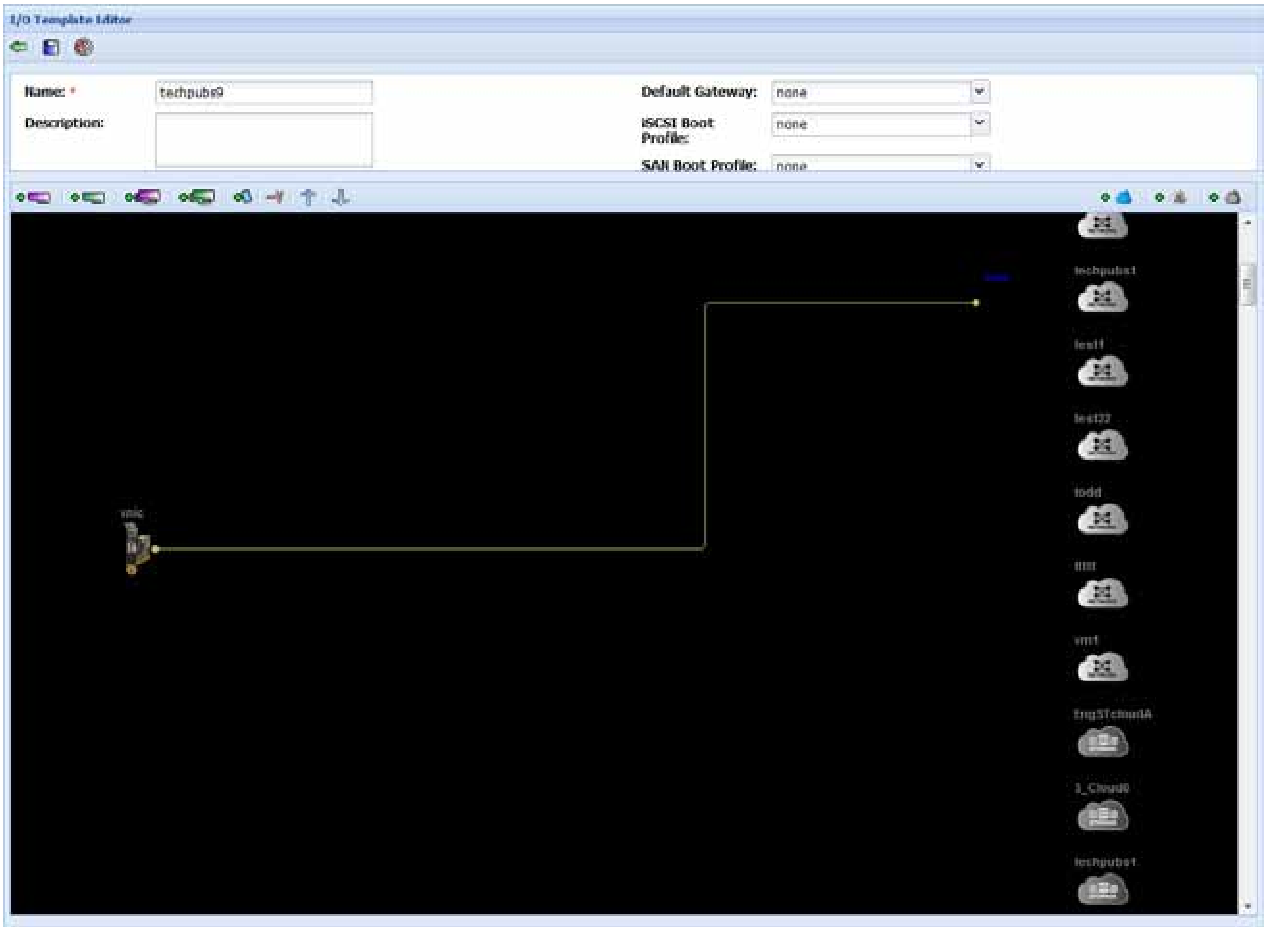
Figure 8 I/O Template Editor — Adding a vNIC to the Pending Template

Step 34 When the vNIC is added to the I/O Template Editor’s work space, click and drag a connection from the vNIC to the correct Network Cloud, as shown in Figure 9.

This step creates a vNIC with default parameters and terminates it on a Network Cloud. You will want to edit the vNIC parameters.

Note

This step does not provide the virtual I/O connection to the host server. It simply creates a vNIC and terminates it on a port in the Network Cloud. The vNIC will not be pushed to the host server until the I/O Template is saved, and after that an I/O Profile is created from the I/O Template, and then that I/O Profile is connected to a server.



I/O Template Editor

Name: * techpubs9

Description:

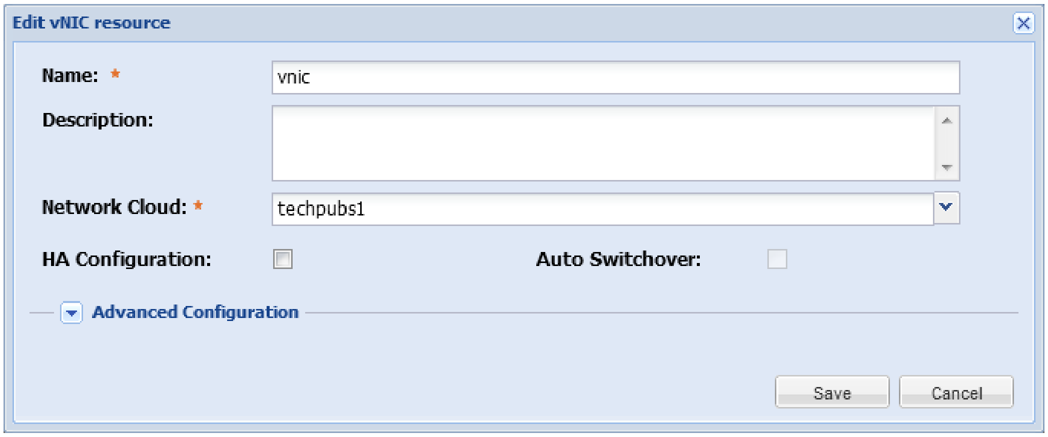
Default Gateway: none

iSCSI Boot Profile: none

SAN Boot Profile: none

Figure 9 I/O Template Editor — Connecting a vNIC to a Network Cloud

Step 35 When the vNIC is connected to the Network Cloud, double click the vNIC icon in the work space to display the Edit vNIC Resource dialog and set or change vNIC properties as needed. Figure 10 shows the Edit vNIC Resource dialog.



Name: * vnic

Description:

Network Cloud: * techpubs1

HA Configuration: □ Auto Switchover: □

Figure 10 Edit vNIC Resource

Step 36 In the *Name* field, set or change the vNIC name.

Step 37 As an option, in the *Description* field, enter an alphanumeric string that describes the vNIC.

Step 38 As needed, from the *Network Cloud* dropdown menu, select the Network Cloud to which the vNIC will belong.

Note

Because you have already connected the vNIC to the Network Cloud by clicking and dragging a connection from the vNIC icon to the cloud icon, you should not need to do this step. However, you can use the Network Cloud dropdown menu to change the vNIC's termination to a different cloud if needed.

Step 39 If the vNIC will be one of an HA vNIC pair, click the *HA Configuration* checkbox. This checkbox toggles, so clicking multiple times alternatively sets and unsets the HA configuration flag for the vNIC.

Note

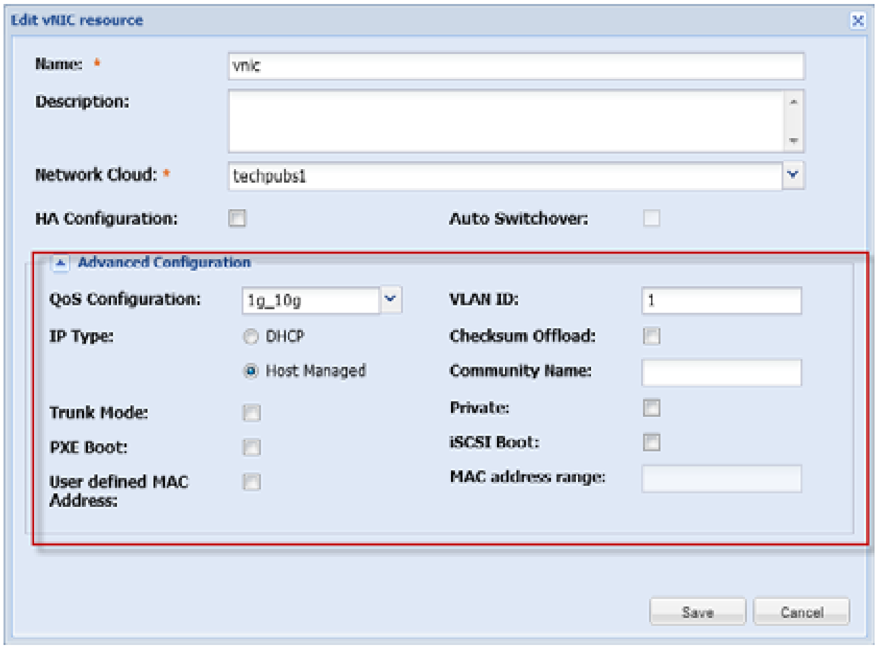
In this example, the *HA Configuration* checkbox is empty because the vNIC you are creating is not an HA vNIC. For information about configuring an I/O Template for an HA vNIC, see Creating an HA vNIC Template.

Step 40 If the vNIC will be one of an HA vNIC pair, click the *Auto Switchover* checkbox if you want the secondary vNIC to give traffic back to the primary vNICs when the primary comes back online.

At this point you have completed configuring the basic vNIC properties. However, you can configure additional properties if needed by using the procedure in the following section. If you do not want to configure advanced properties, proceed to Adding vHBAs to the I/O Template.

Configuring Advanced vNIC Properties

If you want to configure advanced features for the vNIC, display the Advanced Configuration options as shown in Figure 11.



Name: * vnic
Description:
Network Cloud: * techpubs1
HA Configuration: □
Auto Switchover: □
QoS Configuration: 1g_10g
VLAN ID: 1
IP Type: ○ DHCP ● Host Managed
Checksum Offload: □
Community Name:
Trunk Mode: □
Private: □
PXE Boot: □
iSCSI Boot: □
User defined MAC Address: □
MAC address range:

Figure 11 Edit vNIC Resource — Advanced Configuration Options for a vNIC

Step 41 As needed, from the *QoS Configuration* dropdown menu, select the Network QoS Profile required for the vNIC.

Step 42 If the vNIC will be required to participate in a VLAN, enter the VLAN number in the *VLAN ID* field.

Step 43 In the *IP Type* field, select whether the vNIC's IP address will be assigned by the host server, or by DHCP.

Step 44 If the vNIC will be supporting checksum offload, which allows the module to send checksumming tasks to the I/O module instead of the port terminating the vNIC, click the *Checksum Offload* checkbox.

Step 45 If the vNIC needs to be part of a specific SNMP community, in the *Community Names* field, enter the names of the SNMP communities.

Step 46 If the vNIC will be configured in a VLAN, click the *Trunk Mode* checkbox to determine whether the vNIC will be trunk or access. If the *Trunk Mode* checkbox contains a checkmark, the vNIC will operate in trunk mode. If the *Trunk Mode* checkbox is empty, the vNIC will operate in access mode.

Step 47 If the vNIC needs to be accessible only by private vNICs (non-public vNICs), click the *Private* checkbox.

Step 48 If the vNIC will be booting over an iSCSI vNIC attached to an iSCSI target that contains boot information for the server where the vNIC is hosted, click the *iSCSI Boot* checkbox.

Step 49 If the vNIC will be booting over a PXE boot vNIC attached to a PXE boot server that contains boot information for the server where the vNIC is hosted, click the *PXE Boot* checkbox.

Step 50 *User Defined MAC Address*, for releasing the port's MAC address from the Fabric Director's MAC address pool and allowing you to specify a particular MAC address for the port supporting the vNIC. This option combines with the MAC Address Range to determine the appropriate MAC address.

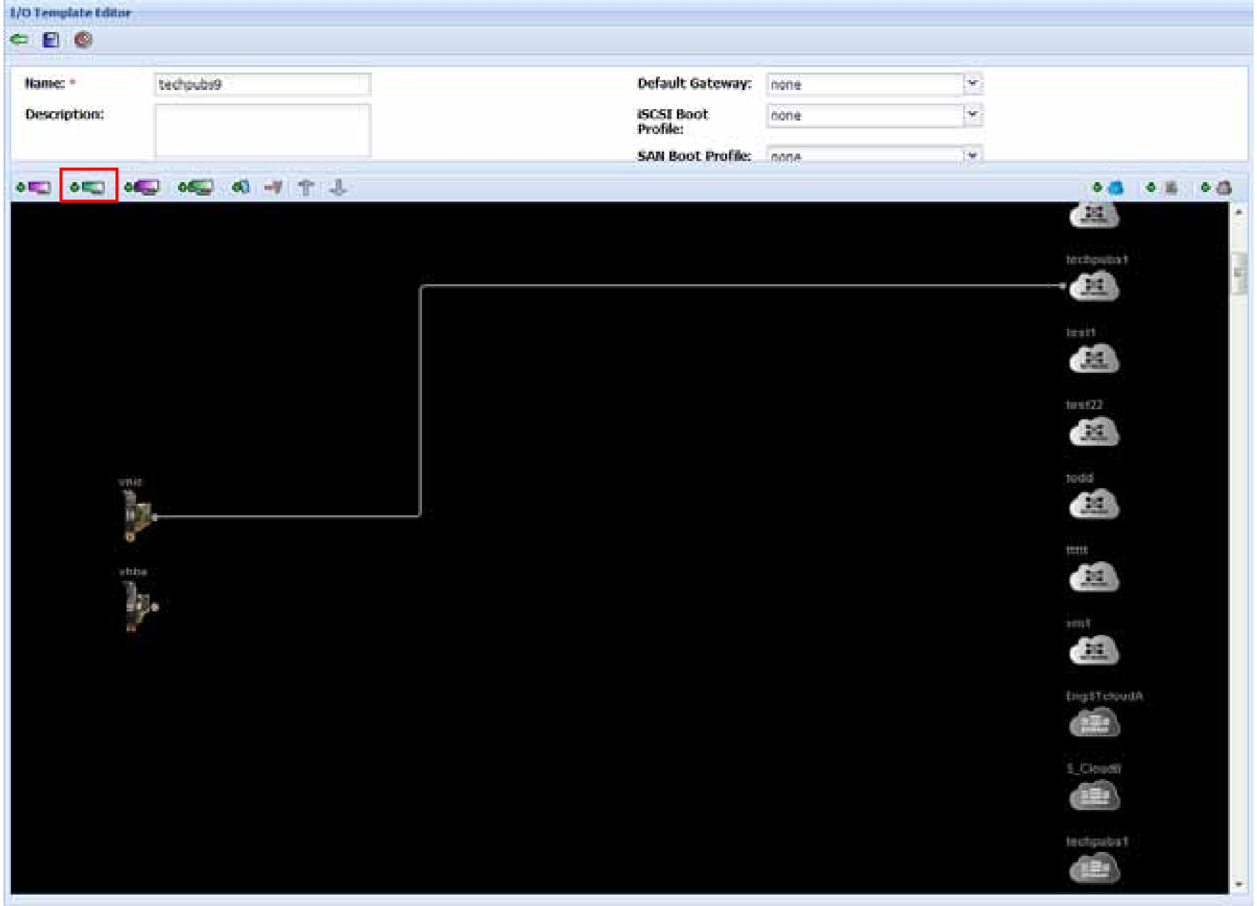
Step 51 *MAC Address Range*, to specify the MAC address range for the port supporting the vNIC.

Step 52 When the vNIC properties are specified, click ***Save***.

Adding vHBAs to the I/O Template

Continue the main workflow for creating an I/O Template by adding one or more vHBAs to the I/O Template:

Step 53 Click the ***Add vHBA*** button to add an instance of a vHBA to the I/O Template Editor. This procedure only adds one, but you can add as many vHBAs to the I/O Template as needed. Figure 12 shows adding a single vHBA to the pending I/O Template.



I/O Template Editor

Name: * techpubs9

Description:

Default Gateway: none

iSCSI Boot Profile: none

SAN Boot Profile: none

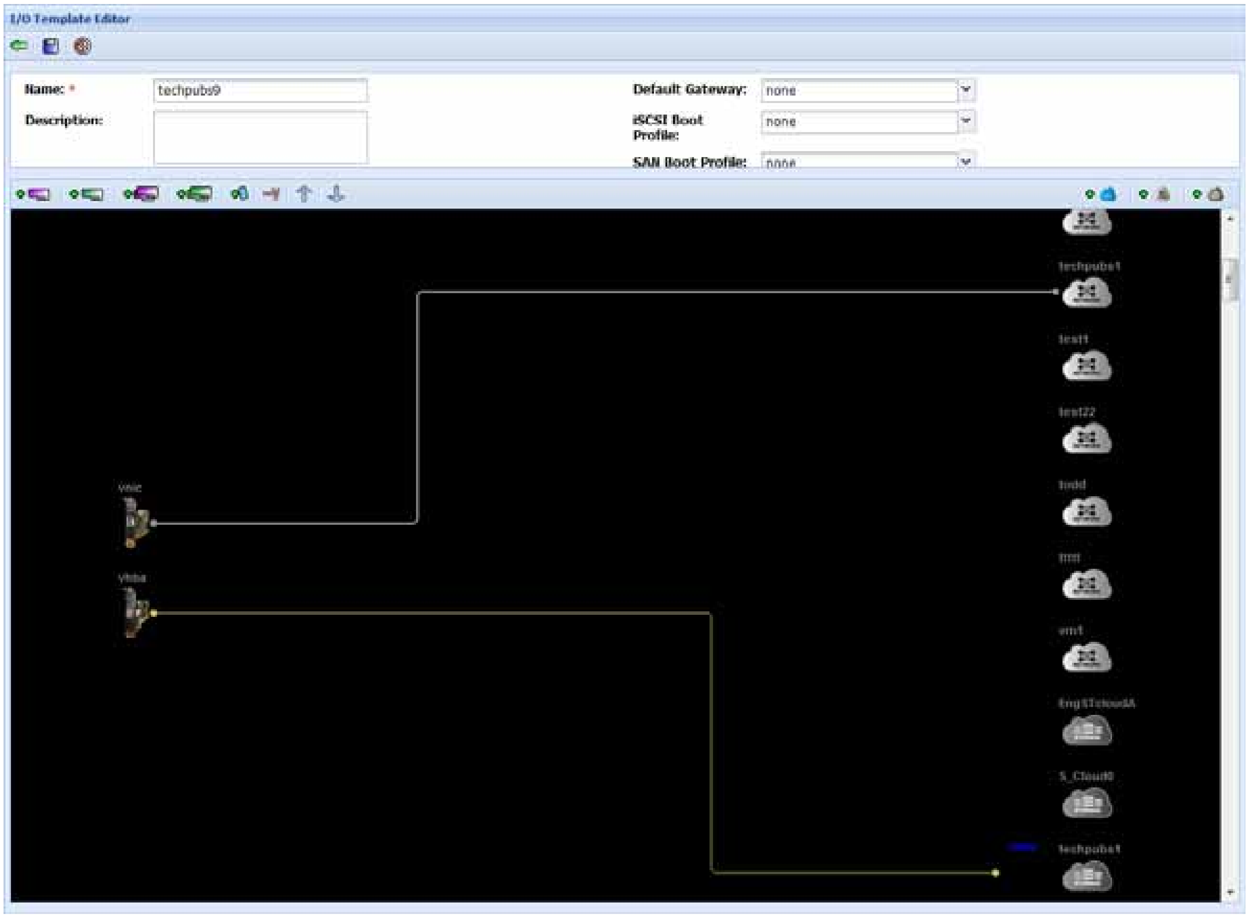
Figure 12 I/O Template Editor — Adding a vHBA to the Pending Template

Step 54 When the vHBA is added to the I/O Template Editor’s work space, click and drag a connection from the vHBA to the correct Storage Cloud, as shown in Figure 13.

This step creates a vHBA with default parameters and terminates it on a Storage Cloud. You will want to edit the vHBA parameters.

Note

This step does not provide the virtual I/O connection to the host server. It simply creates a vHBA and terminates it on a port in the Storage Cloud. The vHBA will not be pushed to the host server until the I/O Template is saved, and after that an I/O Profile is created from the I/O Template, and then that I/O Profile is connected to a server.



I/O Template Editor

Name: * techpubs9

Description:

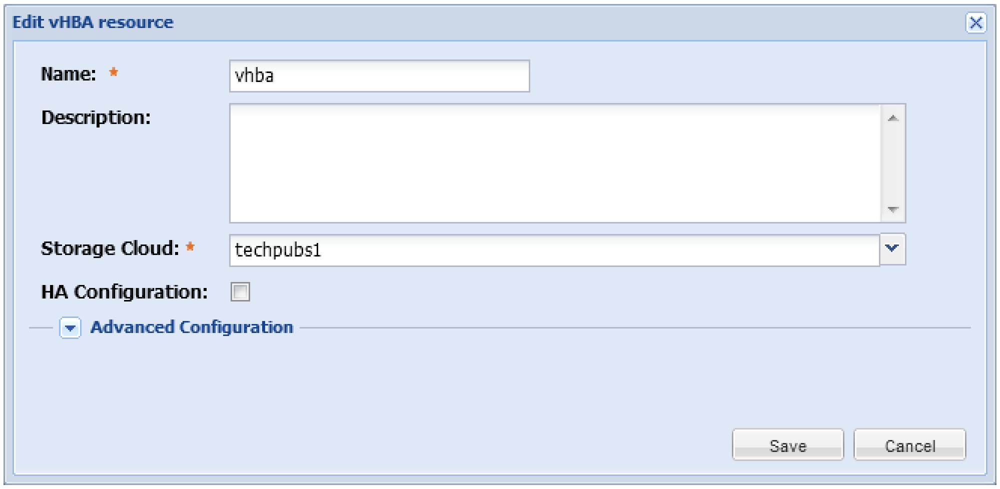
Default Gateway: none

iSCSI Boot Profile: none

SAN Boot Profile: none

Figure 13 I/O Template Editor — Connecting a vHBA to a Storage Cloud

Step 55 When the vHBA is connected to the Storage Cloud, double click the vHBA icon in the work space to display the Edit vHBA Properties dialog and set or change vHBA parameters as needed. Figure 14 shows the Edit vHBA Resource dialog.



Name: * vhba

Description:

Storage Cloud: * techpubs1

HA Configuration: □

Figure 14 Edit vHBA Resource

Step 56 In the *Name* field, set or change the vHBA name.

Step 57 As an option, in the *Description* field, enter an alphanumeric string that describes the vHBA.

Step 58 As needed, from the *Storage Cloud* dropdown menu, select the Storage Cloud to which the vHBA will belong.

Note

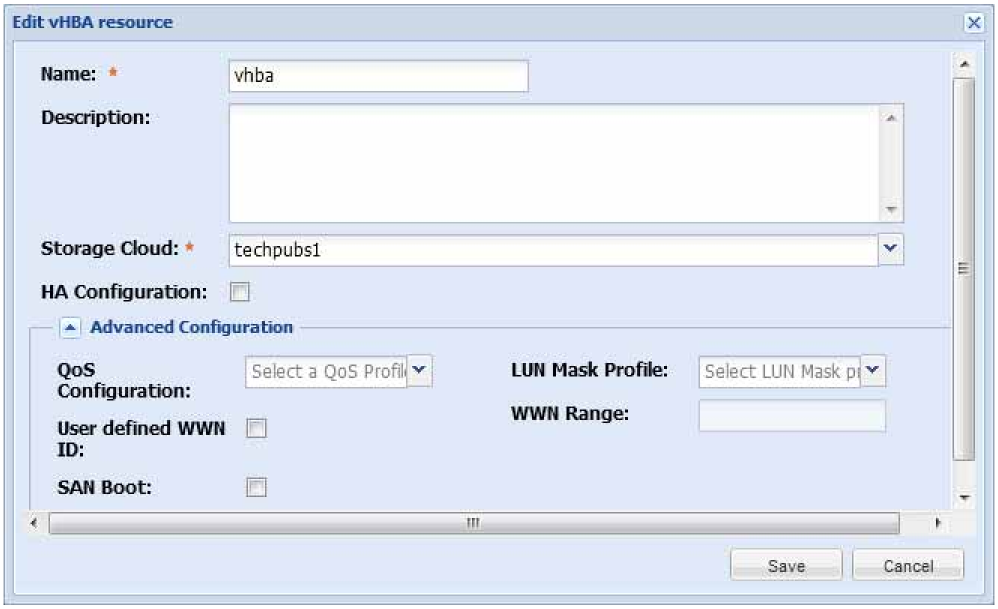
Because you have already connected the vHBA to the Storage Cloud by clicking and dragging a connection from the vHBA icon to the cloud icon, you should not need to do this step. However, you can use the Storage Cloud dropdown menu to change the vHBA's termination to a different cloud if needed.

Step 59 If the vHBA will be part of an HA vHBA, click the *HA Configuration* checkbox.

At this point you have completed configuring the basic vHBA properties. However, you can configure additional properties if needed by using the procedure in the following section. If you do not want to configure advanced properties, proceed to Adding vHBAs to the I/O Template.

Configuring Advanced vHBA Properties

If you want to configure advanced features for the vHBA, display the Advanced Configuration options as shown in Figure 15.



Name: * vhba

Description:

Storage Cloud: * techpubs1

HA Configuration: □

QoS Configuration: Select a QoS Profil

LUN Mask Profile: Select LUN Mask pr

User defined WWN ID: □

WWN Range:

SAN Boot: □

Figure 15 Edit vHBA Resource — Advanced Configuration Options for a vHBA

Step 60 As needed, from the *QoS Configuration* dropdown menu, select the SAN QoS Profile required for the vHBA. The SAN QoS Profile must already exist to be a selectable item in the dropdown menu.

Step 61 As needed, from the *LUN Mask Profile* dropdown menu, select the LUN Mask Profile required for the vHBA. The LUN Mask Profile must already exist to be a selectable item in the dropdown menu.

Step 62 If the vHBA's WWN ID must be assigned from a specific range of WWNs, click the *User Defined WWN ID* checkbox to have the Fabric Director bypass automatically assigning the vHBA's WWN from the Fabric Director's pool if WWN IDs. Use this option if you, or a SAN device, will be assigning WWNs.

Step 63 If the vHBA's WWN ID must be assigned from a specific range of WWNs, enter the WWN range in the *WWN Range* field. Enter the WWN range as a starting WWN ID, then either a dash (-) or colon (:), then the ending WWN ID.

Step 64 If the vHBA will need to support SAN Booting the host server on which the vHBA is deployed, click the *SAN Boot* checkbox.

Step 65 When the vHBA properties are specified, click ***Save***.

Saving the I/O Template

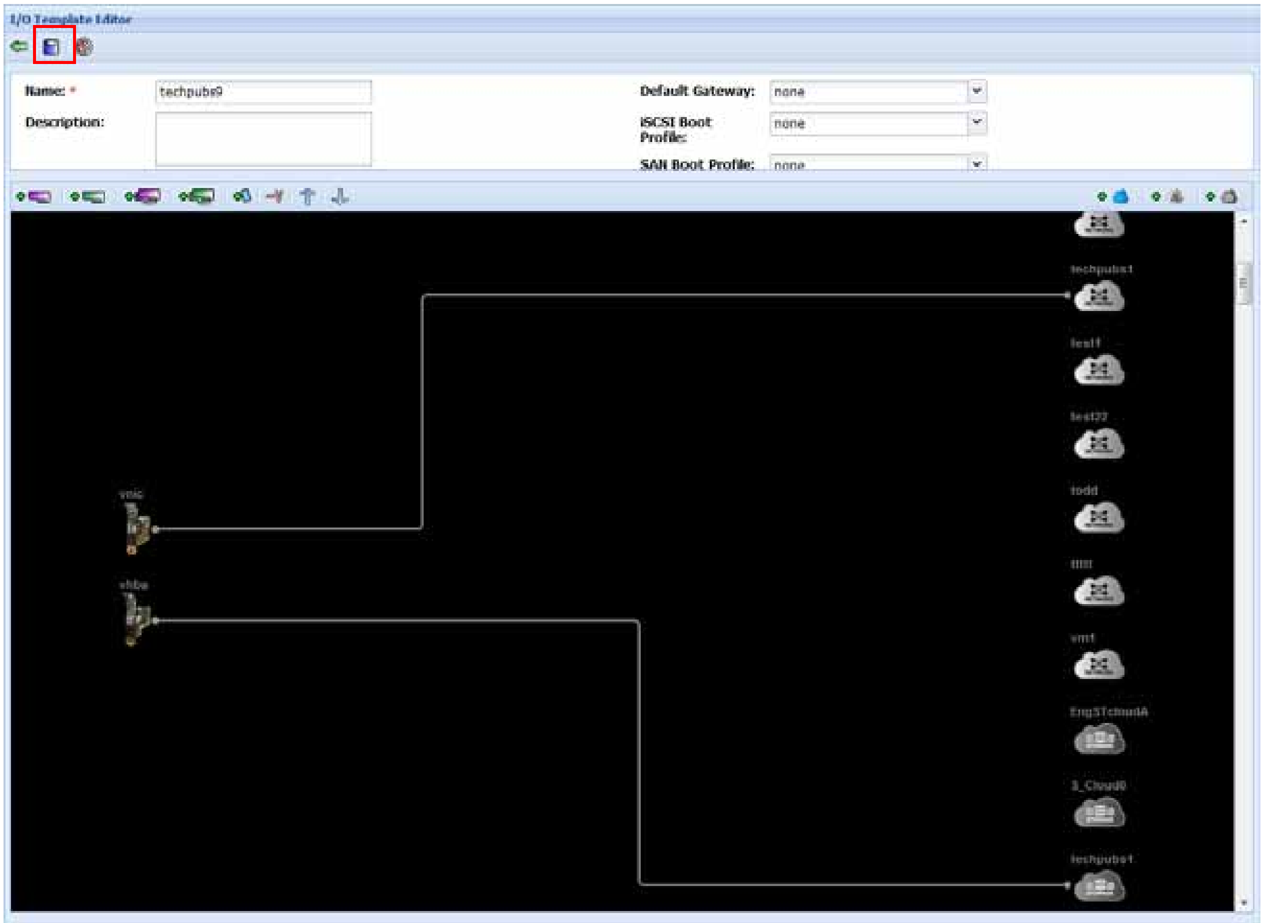
Complete the workflow of configuring an I/O Template by following these steps:

Step 66 Check the work area to make sure that all vNICs, vHBAs, Network Clouds, and Storage Clouds are in the I/O Template, and have been connected appropriately.

- If vNICs and vHBAs need to be deleted, you can click to select them, then click ***Delete*** to remove them from the I/O Template before saving the I/O Template.

- If vNICs and vHBAs are not connected, you can either double click the vNIC or vHBA and set the Network and Storage Cloud as needed, or you can click and drag to draw a line between the virtual resource and the I/O Clouds.

Step 67 When the I/O Template contains the proper virtual connections, click the ***Save*** icon to complete creating the I/O Template and display the I/O Template Summary as shown in Figure 16.



I/O Template Editor

Name: * techpubs9

Description:

Default Gateway: none

iSCSI Boot Profile: none

SAN Boot Profile: none

Figure 16 I/O Template Editor — Completed I/O Template

Note

At this point, the I/O Template is created, but not yet deployed. You will need to create an I/O Profile from the I/O Template, and connect that I/O Profile to a physical server in order to push the vNICs and vHBAs in the I/O Template to the server.

Creating an HA vNIC Template

HA vNICs allow for redundancy and fault tolerance for network-connected hosts. With each HA vNIC, a pair of vNICs is created and assigned to two ports in the cloud, or two separate Fabric Directors.

When you create an HA vNIC, the OS where the vNIC is deployed determines how the vNIC operates:

- For Linux and Windows, the HA vNIC is a pair of vNICs in which one is the primary (which is the online, active vNIC) and a secondary vNIC (which is the online standby). The primary vNIC in the HA pair carries traffic to and from the host server. The secondary vNIC does not carry traffic unless the primary encounters an error that downs the vNIC, and after a very brief failover period, the secondary takes over and the traffic resumes on the secondary vNIC. As an option, you can set the secondary to failback, which allows the secondary to return the traffic to the primary vNIC when the primary comes back online.
- For ESX, the HA vNIC is simply two separate vNICs. There is no Primary or Secondary vNIC. Instead the ESX OS settings on the host determine how the HA vNIC is used. Typically, on an ESX Server, VMware’s native NIC Teaming is used to provide the high availability mechanism, and the Xsigo vNICs are just two vNICs that provide the connectivity.

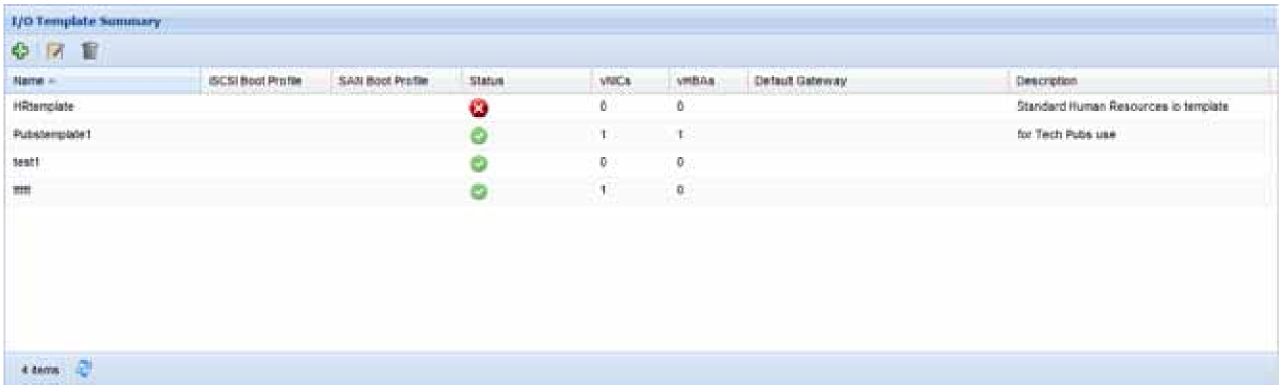
HA vNICs can be terminated on different physical hardware depending on the level of fault tolerance you require:

- to avoid a single point of failure at the module level, terminate the primary and secondary vNICs on different modules in the same chassis.
- to avoid a single point of failure at the chassis level, terminate the primary and secondary vNICs on different Fabric Directors (if you have a multi-chassis configuration).

When you are configuring an HA vNIC pair through Fabric Manager, two vNICs are added in the I/O Template to represent the primary and secondary vNICs in the HA pair. When the HA vNIC pair is assigned to a Network Cloud, the termination ports are assigned to the primary and secondary vNIC based on which ports were configured in the Network Cloud.

To create an HA vNIC Template, follow this procedure:

Step 1 Display the I/O Template Summary by selecting *Server Resource Manager->I/O Templates*. Figure 17 shows the I/O Template Summary.



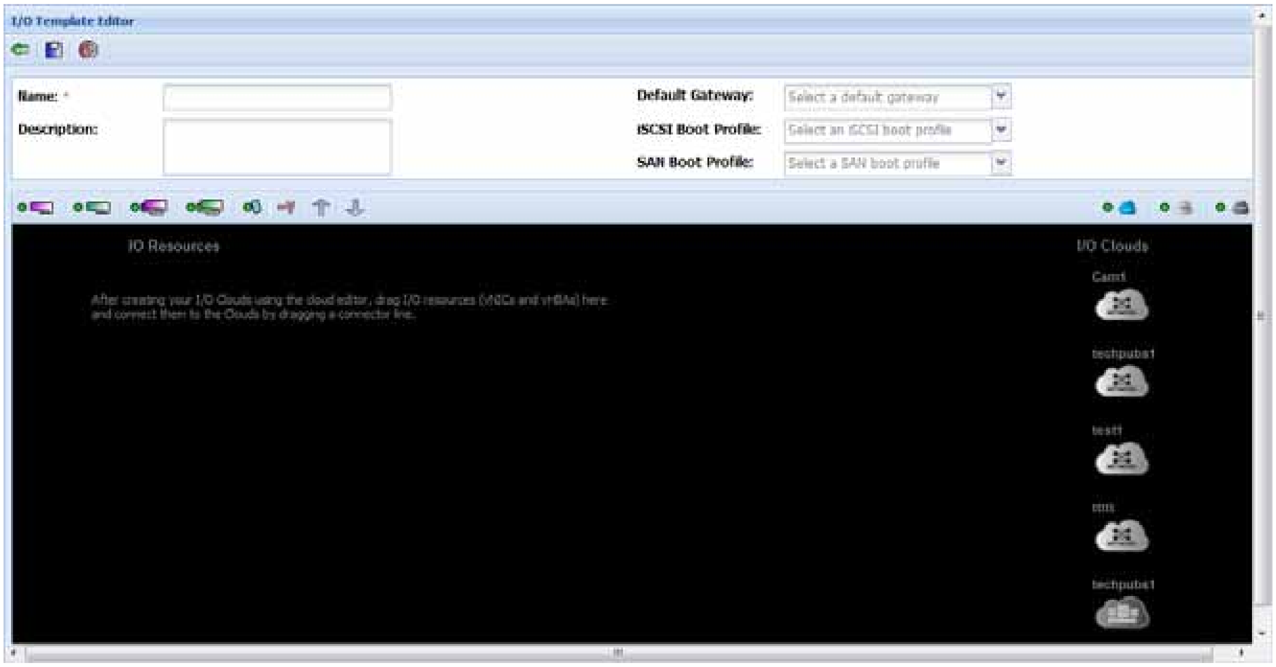
I/O Template Summary

Name	iSCSI Boot Profile	SAN Boot Profile	Status	vNICs	vHBAs	Default Gateway	Description
HRtemplate			☒	0	0		Standard Human Resources io template
Pubstemplate1			✓	1	1		for Tech Pubs use
test1			✓	0	0		
ttttt			✓	1	0		

4 items

Figure 17 I/O Template Summary

Step 2 Click the plus sign to display the I/O Template Editor. Figure 18 shows the I/O Template Editor.



I/O Template Editor

Name: *

Description:

Default Gateway: Select a default gateway

iSCSI Boot Profile: Select an iSCSI boot profile

SAN Boot Profile: Select a SAN boot profile

IO Resources

After creating your I/O Clouds using the cloud editor, drag I/O resources (vNICs and vHBAs) here and connect them to the Clouds by dragging a connector line.

Figure 18 I/O Template Editor

Step 3 In the *Name* field, enter the name for the I/O Template that you are creating.

Step 4 As an option, from the *Default Gateway* dropdown menu, select a default gateway to assign to the vNIC I/O Template.

Step 5 As an option, you can enter a description in the *Description* field.

Step 6 As an option, if the host for the I/O Template will be iSCSI Booting, from the *iSCSI Boot Profile* dropdown menu, select an iSCSI Boot Profile.

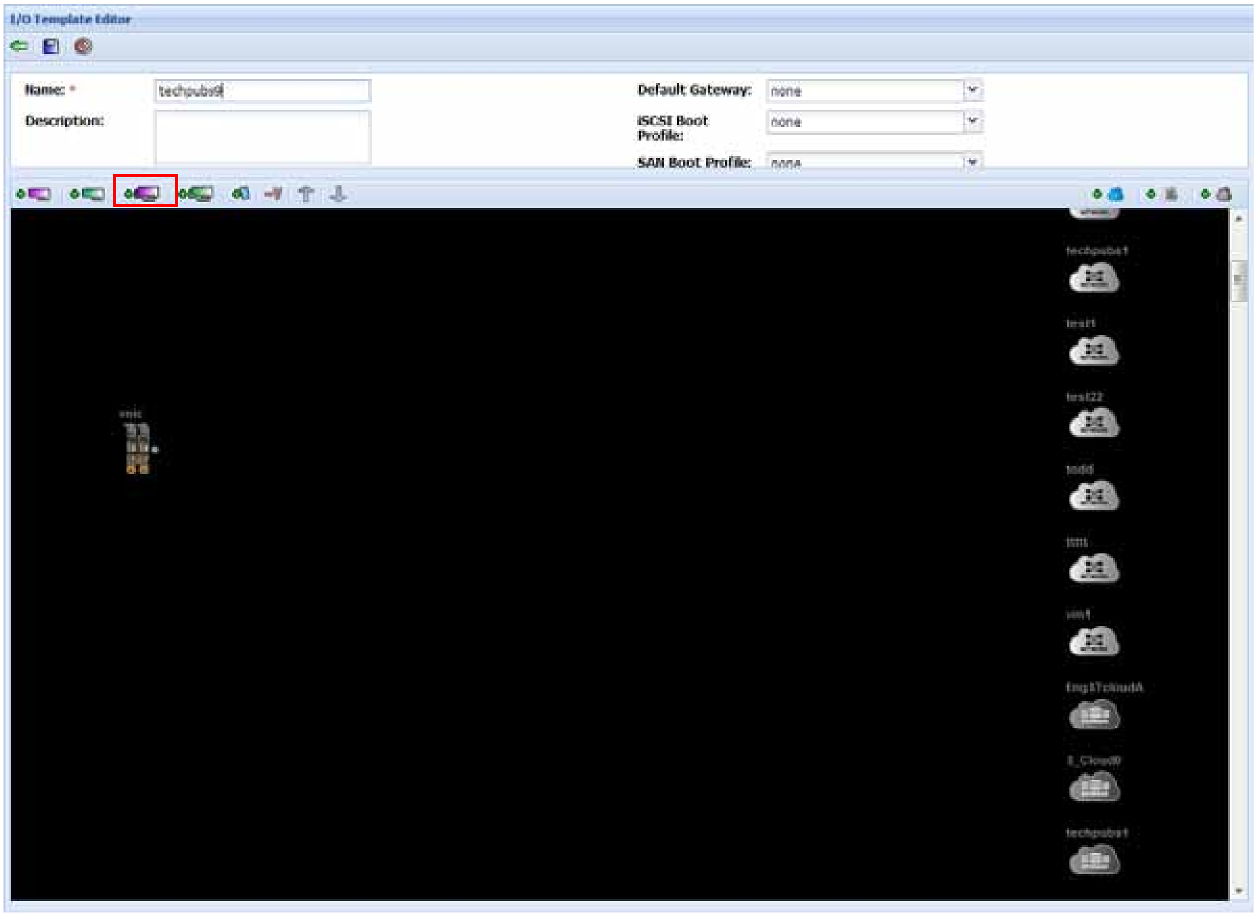
Step 7 As an option, if the host for the I/O Template will SAN Booting, from the *SAN Boot Profile* dropdown menu, select a SAN Boot Profile.

Step 8 If a Network Cloud is not already created, create one now by clicking the ***Add a Network Cloud*** button. For more information, see Step 8 through Step 21.

Note

For an HA vNIC, the Network Cloud you create must have at least 2 separate ports to terminate the HA vNIC that you will be creating.

Step 9 Click the ***Add an HA vNIC*** button to add an instance of an HA vNIC to the I/O Template. See Figure 19.



Name: * techpubs9

Description:

Default Gateway: none

iSCSI Boot Profile: none

SAN Boot Profile: none

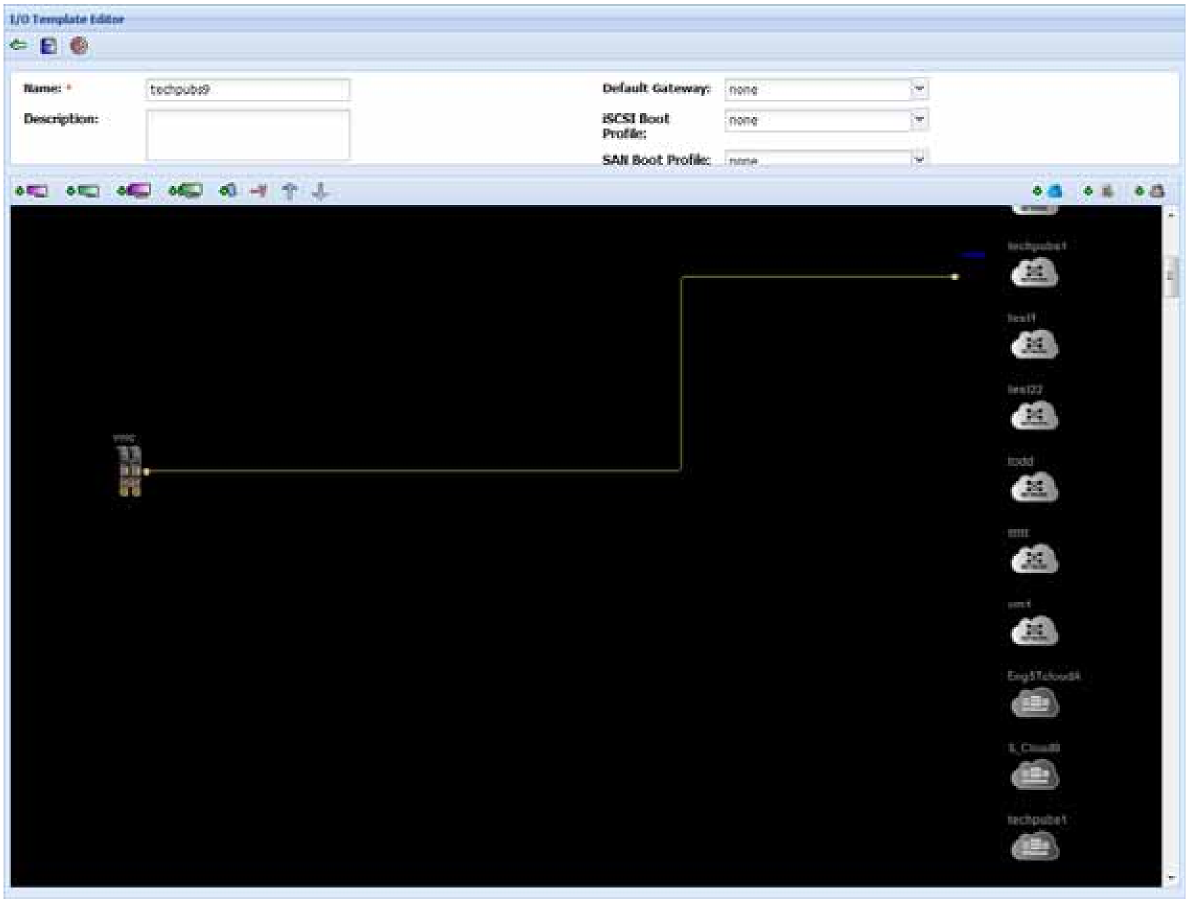
Figure 19 Adding an HA vNIC to the I/O Template Editor

Step 10 When the HA vNIC is added to the I/O Template Editor's work space, click and drag a connection from the HA vNIC to the correct Network Cloud, as shown in Figure 20. When the line is completely drawn, the HA vNIC has been terminated on Ethernet ports in the Network Cloud.

This step creates an HA vNIC with default parameters and terminates it on a Network Cloud. You will want to edit the HA vNIC parameters.

Note

This step does not provide the virtual I/O connection to the host server. It simply creates two vNICs and terminates them on a two Ethernet ports in the same Network Cloud. The HA vNIC will not be pushed to the host server until the I/O Template is saved, and after that an I/O Profile is created from the I/O Template, and then that I/O Profile is connected to a server.



I/O Template Editor

Name: * techpubs9

Description:

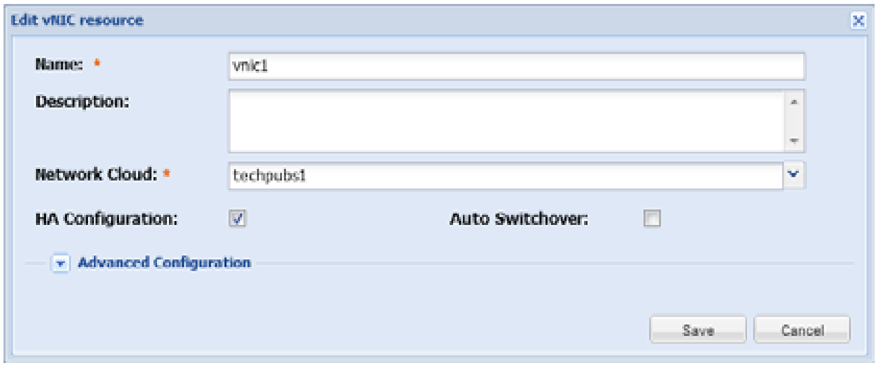
Default Gateway: none

iSCSI Boot Profile: none

SAN Boot Profile: none

Figure 20 I/O Template Editor — Connecting HA vNICs to I/O Clouds

Step 11 When the HA vNIC is connected to the Network Cloud, double click the HA vNIC to display the Edit vNIC Resource dialog for the HA vNIC that you are adding. Figure 21 shows this dialog.



Edit vNIC resource

Name: * vnic1

Description:

Network Cloud: * techpubs1

HA Configuration: ☑ Auto Switchover: □

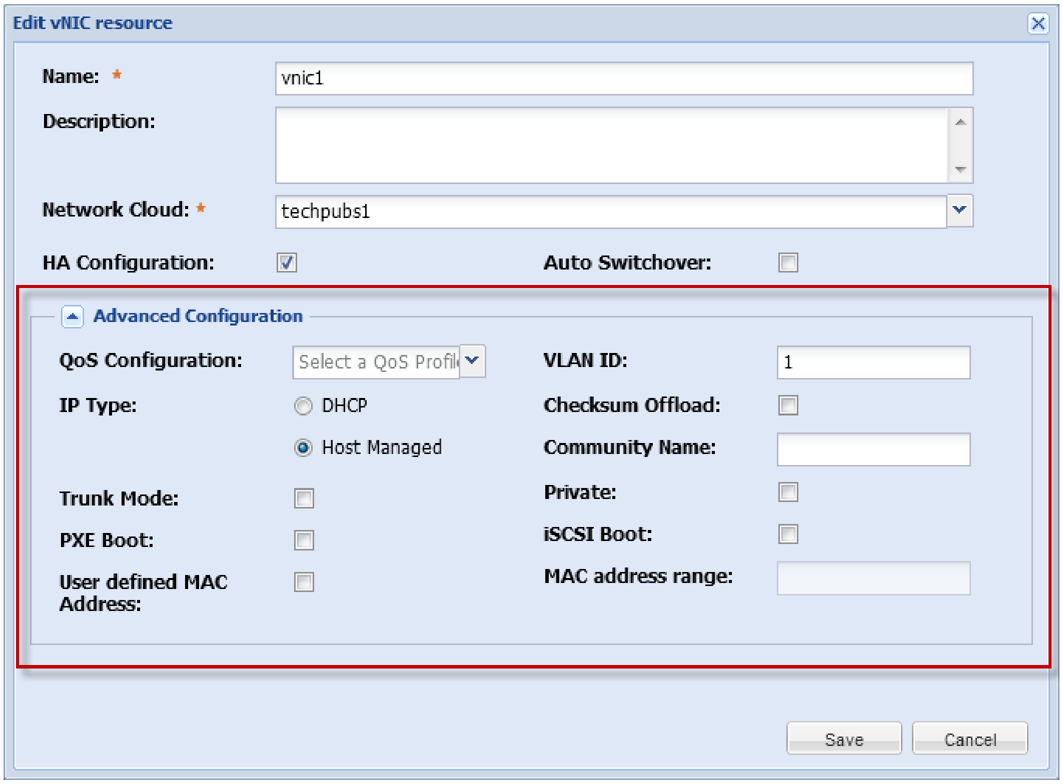
Figure 21 Edit vNIC Resource — HA vNIC

Note

Notice the *HA Configuration* checkbox is filled, which indicates that the vNIC you are configuring is an HA vNIC.

Step 12 Edit the HA vNIC parameters as needed. For information, see steps Step 36 through Step 39.

Step 13 As an option, you can configure additional options for the HA vNIC by clicking the *Advanced Configuration* checkbox. Figure 22 shows the advanced configuration options.



Edit vNIC resource

Name: * vnic1

Description:

Network Cloud: * techpubs1

HA Configuration: ☑

Auto Switchover: □

Advanced Configuration

QoS Configuration: Select a QoS Profil

VLAN ID: 1

IP Type: ○ DHCP ● Host Managed

Checksum Offload: □

Community Name:

Trunk Mode: □

Private: □

PXE Boot: □

iSCSI Boot: □

User defined MAC Address: □

MAC address range:

Figure 22 Edit vNIC Resource — Additional Configuration Options for HA vNIC

Step 14 As needed, from the *QoS Configuration* dropdown menu, select the Network QoS Profile required for the vNIC.

Step 15 If the vNIC will be required to participate in a VLAN, enter the VLAN number in the VLAN ID field.

Step 16 In the *IP Type* field, select whether the vNIC's IP address will be assigned by the host server, or by DHCP.

Step 17 If the vNIC will be supporting checksum offload, which allows the module to send checksumming tasks to the I/O module instead of the port terminating the vNIC, click the *Checksum Offload* checkbox.

Step 18 If the vNIC needs to be part of a specific SNMP community, in the *Community Names* field, enter the names of the SNMP communities.

Step 19 If the vNIC will be configured in a VLAN, click the *Trunk Mode* checkbox to determine whether the vNIC will be trunk or access. If the *Trunk Mode* checkbox contains a checkmark, the vNIC will operate in trunk mode. If the *Trunk Mode* checkbox is empty, the vNIC will operate in access mode.

Step 20 If the vNIC needs to be accessible only by private vNICs (non-public vNICs), click the *Private* checkbox.

Step 21 If the vNIC will be booting over an iSCSI vNIC attached to an iSCSI target that contains boot information for the server where the vNIC is hosted, click the *iSCSI Boot* checkbox.

Step 22 If the vNIC will be booting over a PXE boot vNIC attached to a PXE boot server that contains boot information for the server where the vNIC is hosted, click the *PXE Boot* checkbox.

Step 23 To allow you to specify a particular MAC address for the port supporting the vNIC (instead of allowing the Fabric Director to assign the MAC addresses for vNIC)s, click the *User Defined MAC Address* checkbox. This option combines with the MAC Address Range to determine the appropriate MAC address.

Step 24 If you are assigning MAC addresses for ports supporting the vNICs, in the *MAC Address Range*, specify the MAC address range for the port supporting the vNIC.

Step 25 When the appropriate parameters have been set for the HA vNIC, click ***Save***.

Step 26 On the I/O Template Editor toolbar, click ***Save*** to save the HA vNIC I/O Template.

⚠ Caution

All changes will be lost if you do not save the HA vNIC I/O Template.

Creating an HA vHBA Template

HA vHBAs provide some redundancy for hosts connected to a Fibre Channel SAN. With HA vHBAs, you create a pair of vHBAs on two separate ports from the same Storage Cloud, or two separate Fabric Directors.

- When configuring HA vHBAs, there is no implied primary or secondary vHBA. HA vHBAs do not have a failover mechanism like common applications of HA vNICs. Instead, the two vHBAs allow for a second logical path from the host to the storage target. How the data path is managed for reads and writes must still be configured through either the FC switch or the host (for example, through MPIO on a Linux host).
- HA vHBAs are not inherently multipathing. HA vHBAs simply create two instances of separate vHBAs on different Fibre Channel ports.

The vHBAs functionality differs depending on the OS of the server where the vHBA is deployed. However, HA vHBAs are typically used to provide two HBAs to the same host to support the connectivity for host-side multipathing.

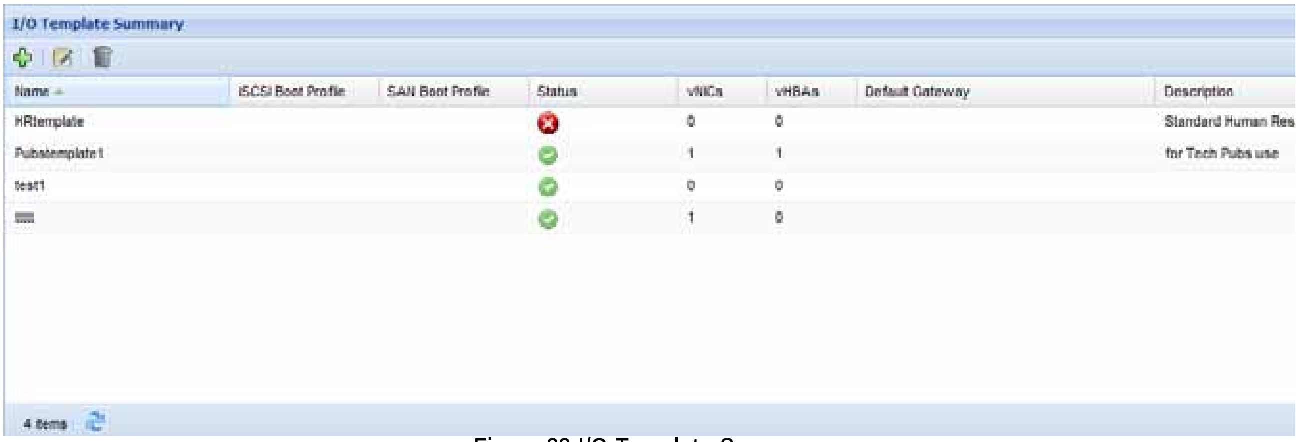
HA vHBAs can be terminated on different physical hardware depending on the level of fault tolerance you require:

- to avoid a single point of failure at the module level, terminate the primary and secondary vHBAs on different modules in the same chassis.
- to avoid a single point of failure at the chassis level, terminate the primary and secondary vHBAs on different Fabric Directors (if you have a multi-chassis configuration).

When you are configuring an HA vHBA pair through Fabric Manager, two vHBAs are added in the I/O Template to represent the HA pair. When the HA vHBA pair is associated to a Storage Cloud, the two termination ports are assigned randomly to support the HA vHBA pair.

To create an HA vHBA Template, follow this procedure:

Step 1 Display the I/O Template Summary by selecting *Server Resource Manager->I/O Templates*. Figure 23 shows the I/O Template Summary.



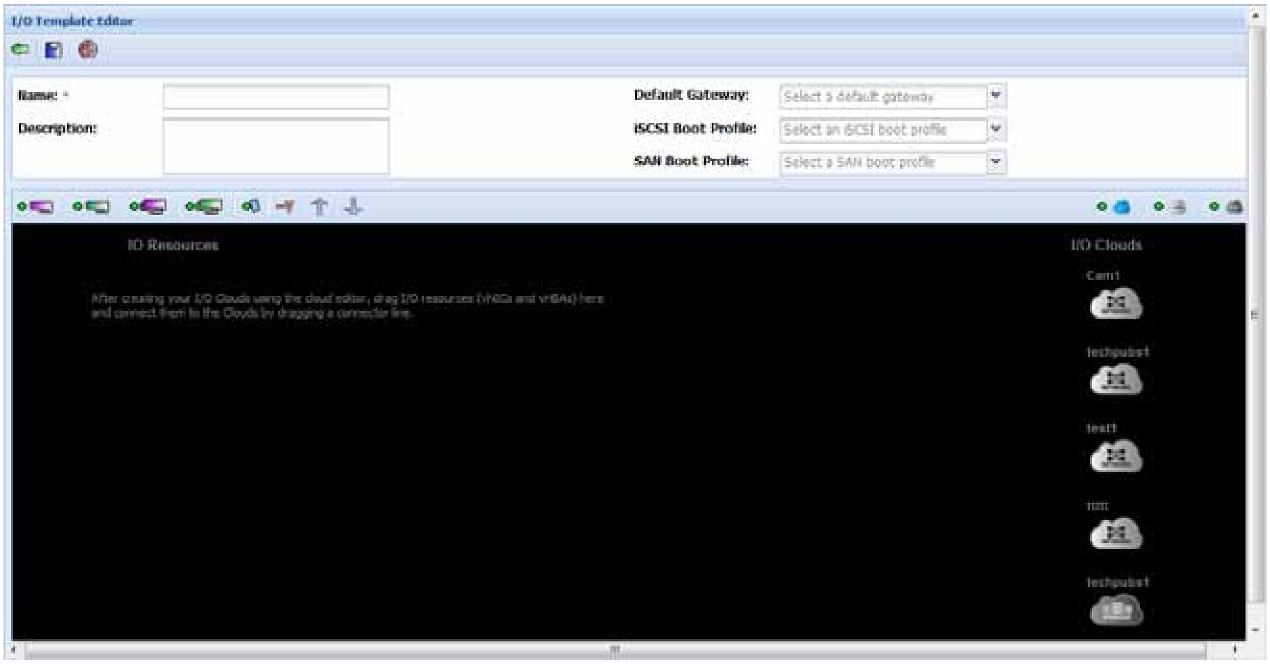
I/O Template Summary

Name	iSCSI Boot Profile	SAN Boot Profile	Status	vNICs	vHBAs	Default Gateway	Description
HRtemplate			✗	0	0		Standard Human Res
Pubstemplate1			✓	1	1		for Tech Pubs use
test1			✓	0	0		
[illegible]			✓	1	0		

4 items

Figure 23 I/O Template Summary

Step 2 Click the plus sign to display the I/O Template Editor. Figure 24 shows the I/O Template Editor.



I/O Template Editor

Name: *

Description:

Default Gateway: Select a default gateway

iSCSI Boot Profile: Select an iSCSI boot profile

SAN Boot Profile: Select a SAN boot profile

IO Resources

After creating your I/O Clouds using the cloud editor, drag I/O resources (vNICs and vHBAs) here and connect them to the Clouds by dragging a connector line.

Figure 24 I/O Template Editor — Creating an I/O Template

Step 3 In the *Name* field, enter the name for the I/O Template that you are creating.

Step 4 As an option, from the *Default Gateway* dropdown menu, select a default gateway to assign to the I/O Template.

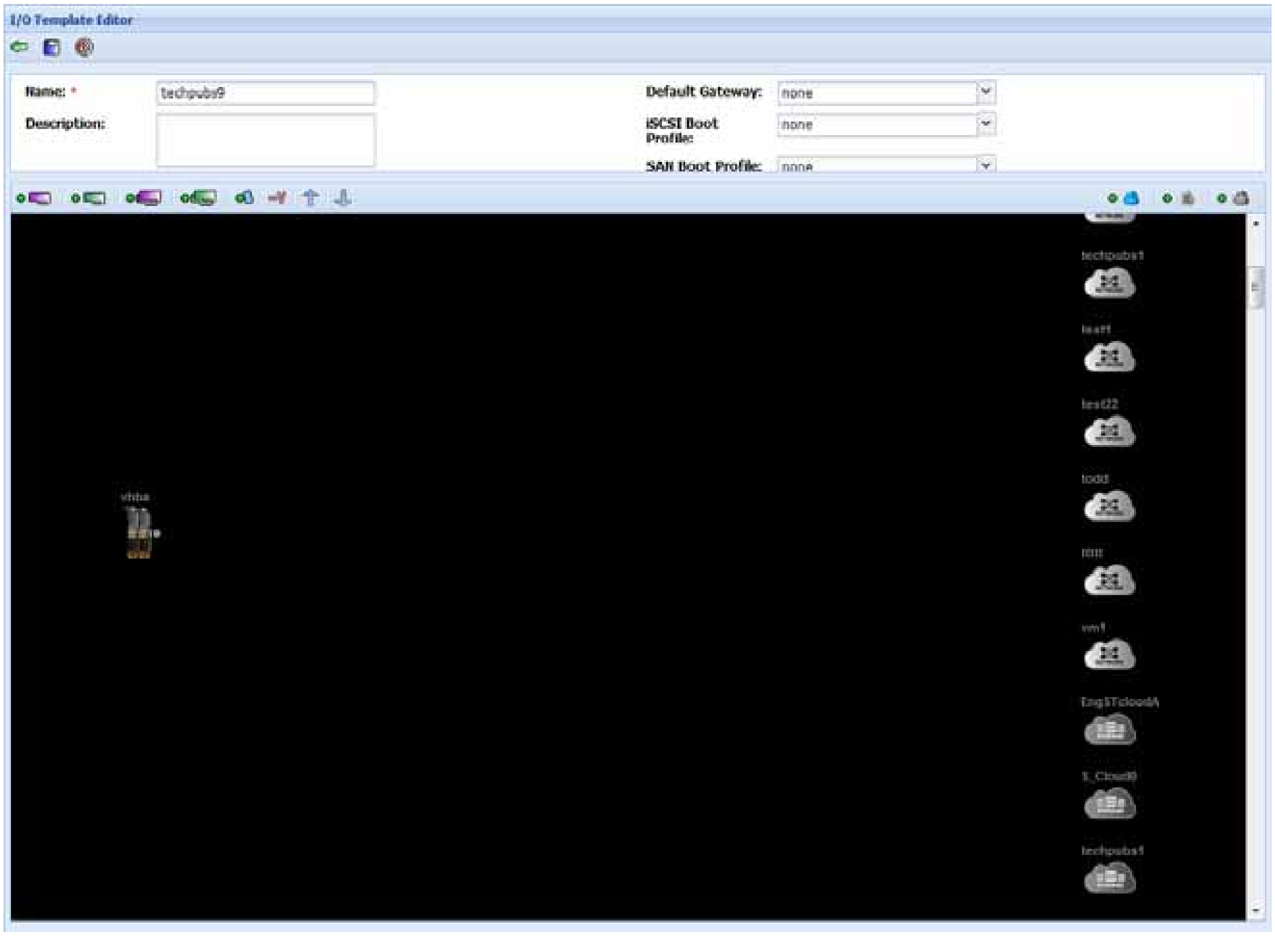
Step 5 As an option, if the host for the I/O Template will be iSCSI Booting, from the *iSCSI Boot Profile* dropdown menu, select an iSCSI Boot Profile.

Step 6 As an option, if the host for the I/O Template will SAN Booting, from the *SAN Boot Profile* dropdown menu, select a SAN Boot Profile.

Step 7 As an option, you can enter a description in the *Description* field.

Step 8 If a Storage Cloud is not already created, add one now by clicking the ***Add a Storage Cloud*** button on the toolbar. For more information, see Step 22 through Step 32.

Step 9 When the Storage Cloud is added to the I/O Template's work area, click the ***Add an HA vHBA*** button to add an instance of an HA vHBA to the I/O Template. See Figure 25.



Name: * techpubs9

Description:

Default Gateway: none

iSCSI Boot Profile: none

SAN Boot Profile: none

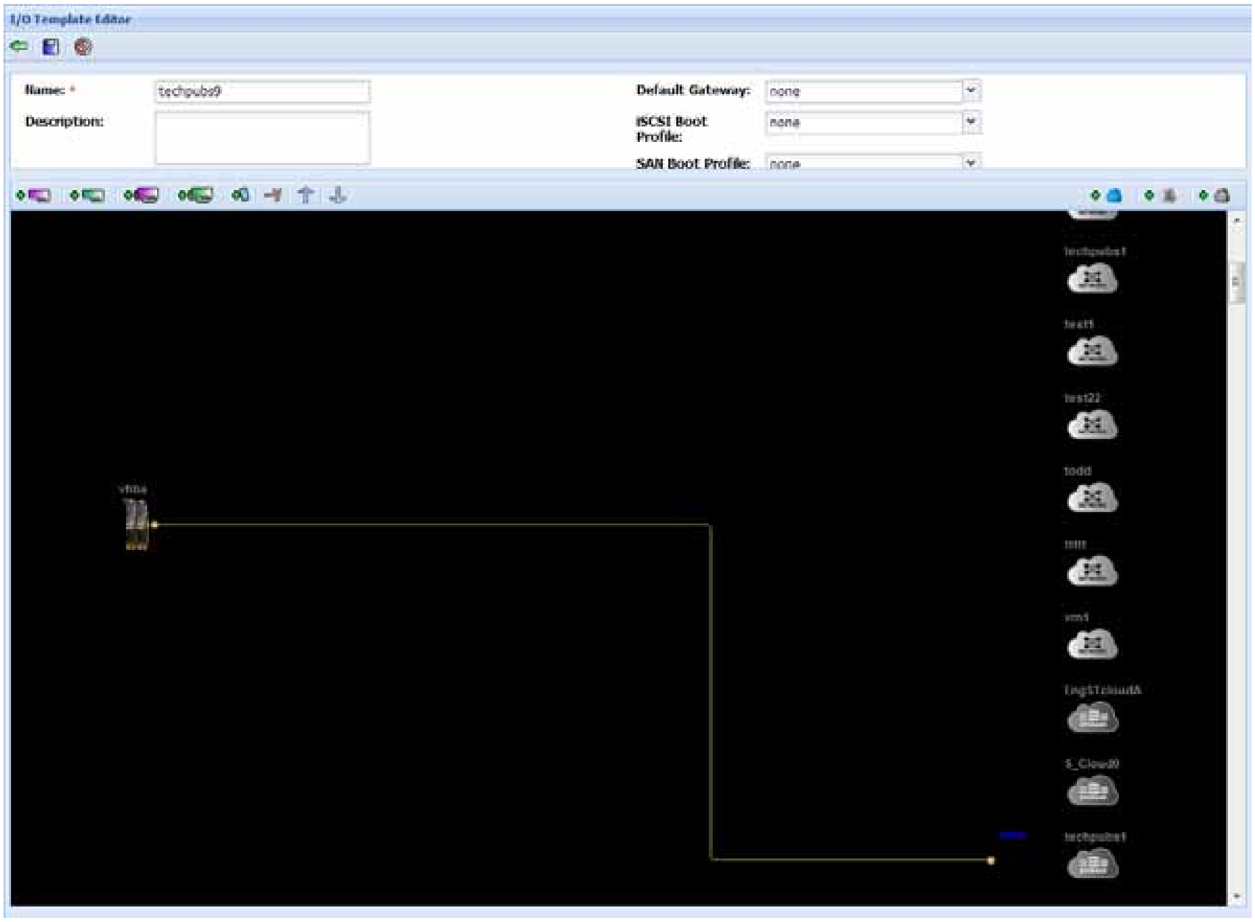
Figure 25 Adding an HA vHBA to the I/O Template Editor

Step 10 When the HA vHBA is added to the I/O Template Editor's work space, click and drag a connection from the HA vHBA icon to the correct Storage Cloud, as shown in Figure 26. When the line is completely drawn, HA vHBA has been terminated on Fibre Channel ports in the Storage Cloud.

This step creates an HA vHBA with default parameters and terminates it on a Storage Cloud. You will want to edit the HA vHBA parameters.

Note

This step does not provide the virtual I/O connection to the host server. It simply creates two vHBAs and terminates them on two ports in the same Storage Cloud. The HA vHBA will not be pushed to the host server until the I/O Template is saved, and after that, an I/O Profile is created from the I/O Template, and then that I/O Profile is connected to a server.



I/O Template Editor

Name: * techpubs9

Description:

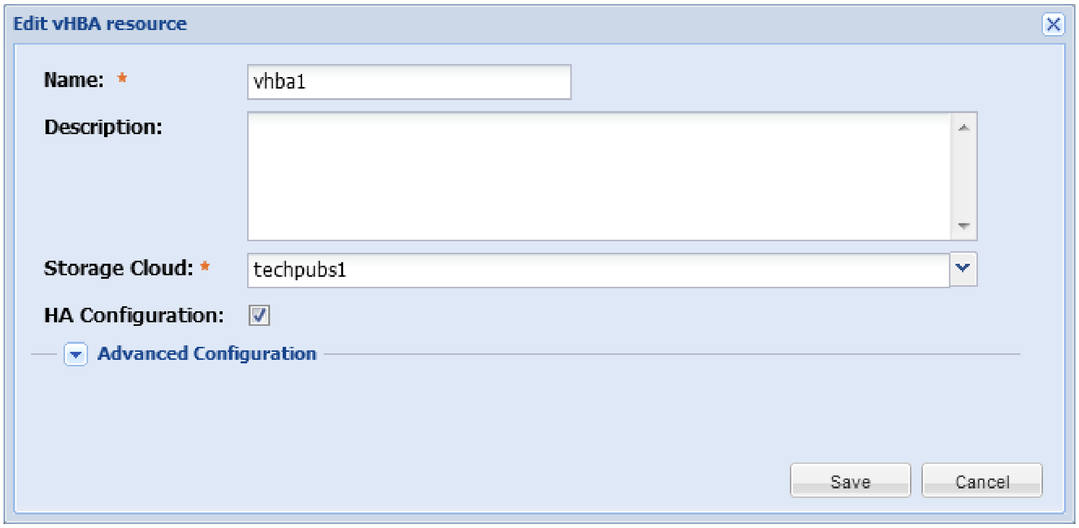
Default Gateway: none

iSCSI Boot Profile: none

SAN Boot Profile: none

Figure 26 I/O Template Editor — Connecting HA vHBAs to I/O Clouds

Step 11 When the HA vHBA is connected to the Storage Cloud, double click the HA vHBA icon in the work space to display the Edit vHBA Properties dialog and set or change HA vHBA parameters as needed. Figure 27 shows the Edit vHBA Resource dialog.



Edit vHBA resource

Name: * vhba1

Description:

Storage Cloud: * techpubs1

HA Configuration: ☑

Figure 27 Edit vHBA Resource

Step 12 In the *Name* field, set or change the HA vHBA name.

Step 13 As an option, in the *Description* field, enter an alphanumeric string that describes the HA vHBA.

Step 14 As needed, from the *Storage Cloud* dropdown menu, select the Storage Cloud to which the HA vHBA will belong.

Note

Because you have already connected the HA vHBA to the Storage Cloud by clicking and dragging a connection from the HA vHBA icon to the cloud icon, you should not need to do this step. However, you can use the Storage Cloud dropdown menu to change the HA vHBA's termination to a different cloud if needed.

Step 15 If the vHBA will be part of an HA vHBA, click the *HA Configuration* checkbox.

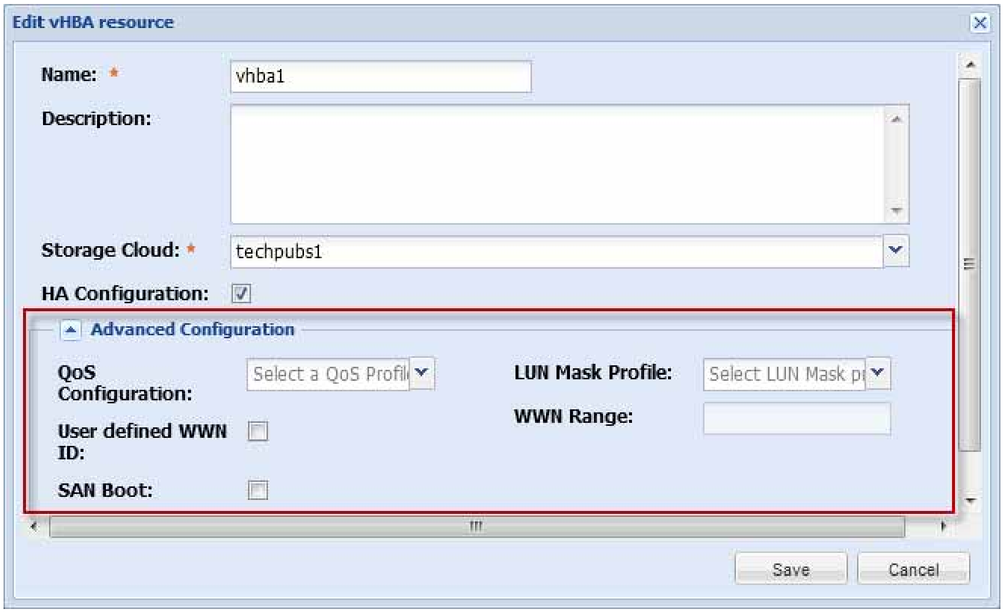
Note

Notice the *HA Configuration* checkbox is filled, which indicates that the vHBA you are configuring is an HA vHBA.

At this point you have completed configuring the basic vHBA properties. However, you can configure additional properties if needed by using the procedure in the following section.

Configuring Advanced vHBA Properties

If you want to configure advanced features for the HA vHBAs, display the Advanced Configuration options as shown in Figure 28.



Edit vHBA resource

Name: * vhba1

Description:

Storage Cloud: * techpubs1

HA Configuration: ☑

Figure 28 Edit vHBA Resource — Advanced Configuration Options for a vHBA

Step 16 As needed, from the *QoS Configuration* dropdown menu, select the SAN QoS Profile required for the HA vHBA.

Step 17 As needed, from the *LUN Mask Profile* dropdown menu, select the LUN Mask Profile required for the HA vHBA. The LUN Mask Profile must already exist to be a selectable item in the dropdown menu.

Step 18 If the HA vHBA's WWN ID must be assigned from a specific range of WWNs, click the *User Defined WWN ID* checkbox to have the Fabric Director bypass automatically assigning the HA vHBA's WWN from the Oracle Xsigo Fabric Director's pool if WWN IDs. Use this option if you, or a SAN device, will be assigning WWNs.

Step 19 If the HA vHBA's WWN ID must be assigned from a specific range of WWNs, enter the WWN range in the *WWN Range* field. Enter the WWN range as a starting WWN ID, then either a dash (-) or colon (:), then the ending WWN ID.

Step 20 If the HA vHBA will need to support SAN Booting the host server on which the vHBA is deployed, click the *SAN Boot* checkbox.

Step 21 When the HA vHBA properties are specified, click ***Save***.

Step 22 On the I/O Template Editor toolbar, click ***Save*** to save the HA vHBA configuration.

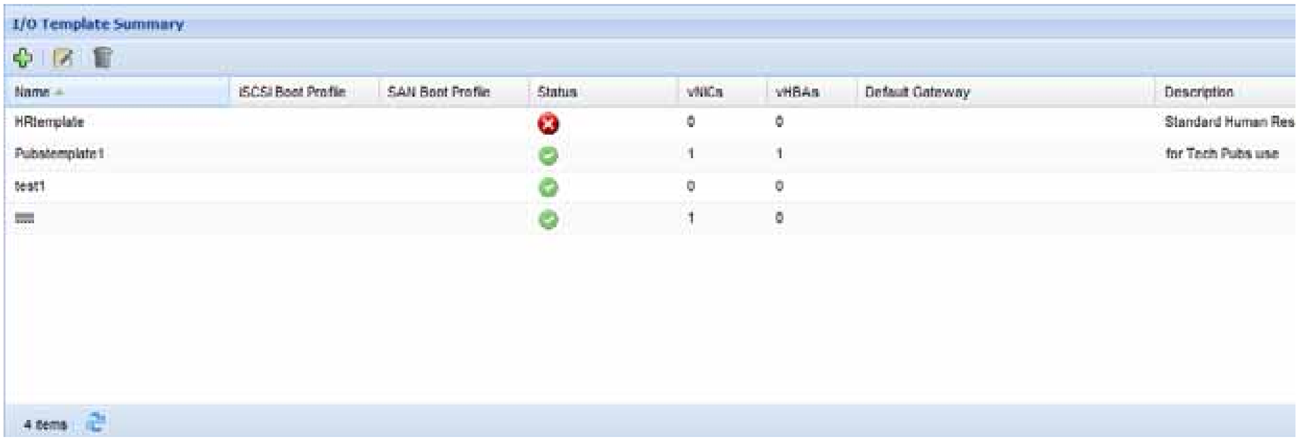
Caution

All changes will be lost if you do not save the HA vHBA I/O Template.

Displaying All I/O Templates

When I/O Templates are configured, they are listed in the I/O Template Summary, which is a listing of all I/O Templates regardless of whether they are deployed to a host server or not. Through the I/O Templates Summary you can create and delete I/O Templates, and edit existing I/O Templates to set or change properties.

Figure 29 shows the I/O Template Summary.



Name	iSCSI Boot Profile	SAN Boot Profile	Status	vNICs	vHBAs	Default Gateway	Description
HRtemplate			✗	0	0		Standard Human Res
Pubstemplate1			✓	1	1		for Tech Pubs use
test1			✓	0	0		
[redacted]			✓	1	0		

Figure 29 I/O Template Summary

Table 1 shows the fields in the I/O Template Summary and explains what each field means.

Table 1 Contents of the I/O Template Summary

Field	Indicates
Name	The name of each configured Storage Cloud.
iSCSI Boot Profile	The name of the iSCSI Boot Profile (if any) assigned to the I/O Template Profile.
SAN Boot Profile	The name of the SAN Boot Profile (if any) assigned to the I/O Template Profile.
Status	The operational status of the I/O Template displayed as an icon: • a green checkmark indicates that the I/O Template is up and available. • an empty field indicates that the I/O Template is not finished, or is in an indeterminate state. • a red “X” indicates that the I/O Template is not up or is not available for deployment.
vNICs	The total number of vNICs configured in each I/O Template.

Table 1 (continued) Contents of the I/O Template Summary

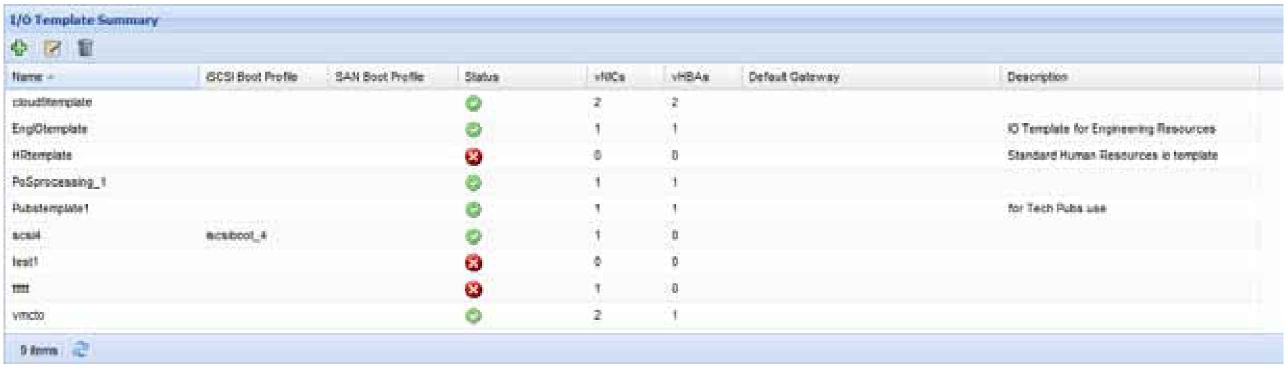
Field	Indicates
vHBAs	The total number of vHBAs configured in each I/O Template.
Default Gateway	The IP address of the default gateway configured in the I/O Template.
Description	The description string (if any) that was applied to the I/O Template. If this field is blank, either no description string was specified when the I/O Template was created, or the I/O Template was originally created with a description string, but the I/O Template was later edited and the description string was removed.

Renaming an I/O Template

Oracle’s Xsigo Fabric Manager supports renaming an I/O Template, which enables you to change the name without having to completely delete and recreate the entire virtual I/O configuration. When the I/O Template is renamed, all other properties for it are retained, including the vNIC and vHBA configuration. As an option, you can also set or change the description for the I/O Template.

You can rename an I/O Template through the I/O Template Details frame. To rename an I/O Template, follow this procedure:

Step 1 On the Navigation Frame, select *I/O Templates*. Figure 30 shows the I/O Template Summary.



I/O Template Summary

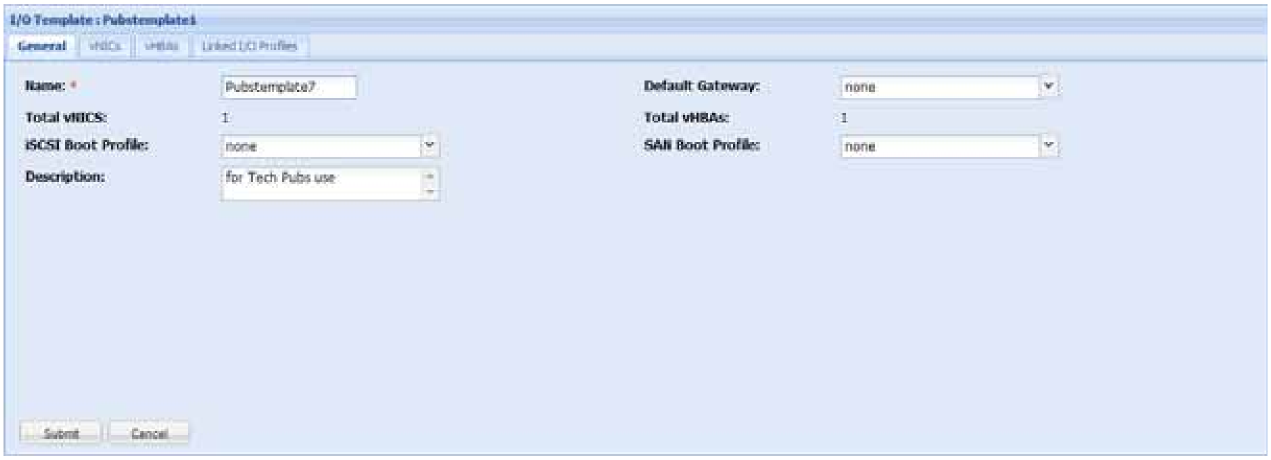
Name	iSCSI Boot Profile	SAN Boot Profile	Status	vNICs	vHBAs	Default Gateway	Description
cloudtemplate			✓	2	2		
EngIOtemplate			✓	1	1		IO Template for Engineering Resources
HRtemplate			✗	0	0		Standard Human Resources io template
PoSprocessing_1			✓	1	1		
Pubstemplate1			✓	1	1		for Tech Pubs use
iscsi4	iscsiboot_4		✓	1	0		
test1			✗	0	0		
ttttt			✗	1	0		
vmcto			✓	2	1		

9 items

Figure 30 I/O Template Summary

Step 2 Select an I/O Template to populate the details frame with its properties.

Step 3 Click the ***Edit*** button to edit the properties of the selected I/O Template, as shown in Figure 31.



I/O Template : Pubstemplate1

Name: *	Pubstemplate7	Default Gateway:	none
Total vNICS:	1	Total vHBAs:	1
iSCSI Boot Profile:	none	SAN Boot Profile:	none
Description:	for Tech Pubs use		

Figure 31 I/O Template Details — Editing to Rename I/O Template

Step 4 In the *Name* field, enter the new name for the I/O Template.

Step 5 As an option, you also can set or change the description for the selected I/O Template.

Step 6 When the new name has been specified for the I/O Template, click ***Submit***.

Editing an I/O Template

When an I/O Template exists, you can edit it to set or change features for the I/O Template and its building blocks. For example, if you find a host server is not getting enough bandwidth, you can edit the I/O Template to change the Network QoS properties in the Network Cloud in the I/O Template. You can also edit an I/O Template to add or delete vNICs or vHBAs, or set a specific boot policy for the host (for example, set up the I/O Template for SAN Booting).

Note

Although the procedures documented in this section are valid, an easier way to edit an I/O Template is to use the I/O Template Editor, which provides a more graphical approach to modifying vNICs, vHBAs, and I/O Templates.

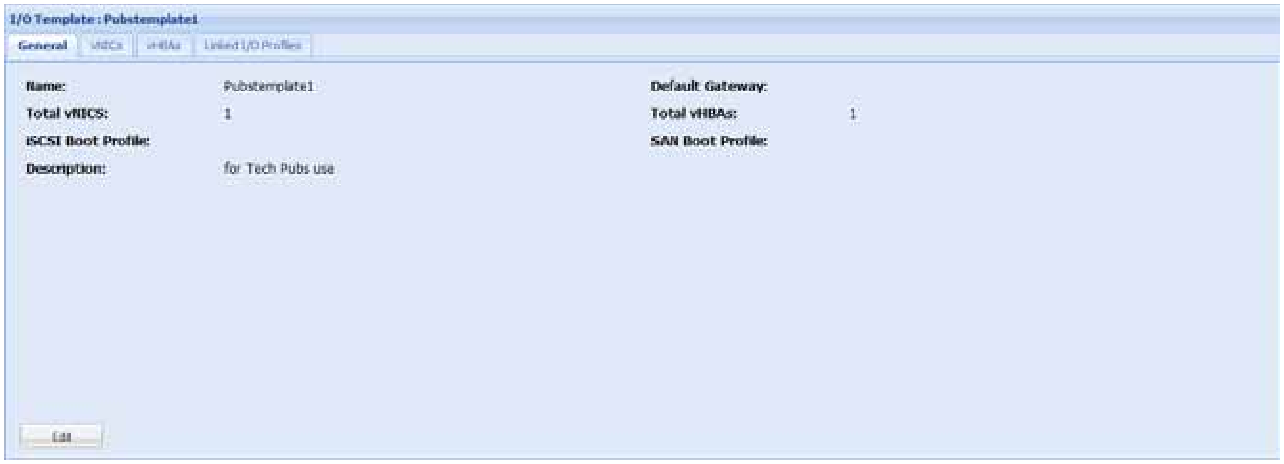
Editing an I/O Template occurs through the I/O Template Editor, which supports the following functionality:

- Changing I/O Template General Properties
- Adding or Deleting a Template’s vNICs
- Adding or Deleting a Template’s vHBA

Changing I/O Template General Properties

Through the I/O Template Details frame, you can display the general properties of an individual I/O Template. The general properties appear on the *General* tab.

Figure 32 shows the *General* tab of an I/O Template.

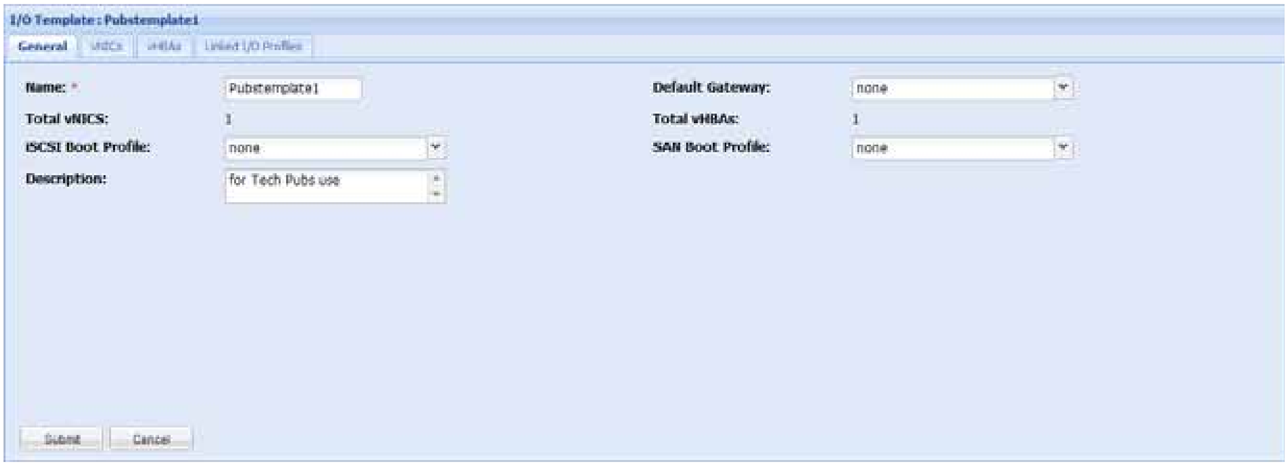


Name: Pubstemplate1
Total vNICS: 1
iSCSI Boot Profile:
Description: for Tech Pubs use
Default Gateway:
Total vHBAs: 1
SAN Boot Profile:

Figure 32 I/O Template Details Frame — General Tab

The *General* tab also contains an ***Edit*** button that allows you to set or change parameters as needed. For example, through the *General* tab you could add or change a server boot profile.

Figure 33 shows the *General* tab of an I/O Template.



I/O Template : Pubstemplate1

Name: *	Pubstemplate1	Default Gateway:	none
Total vNICS:	1	Total vHBAs:	1
iSCSI Boot Profile:	none	SAN Boot Profile:	none
Description:	for Tech Pubs use		

Figure 33 Editable General Tab

To edit the general properties for an I/O Template, follow this procedures:

Step 1 Display the I/O Templates Summary (*Server Resource Manager->I/O Templates*).

Step 2 On the I/O Template Summary, select an I/O Template to display it in the details frame.

Step 3 Click the *General* tab, then click the ***Edit*** button to unlock the editable fields on the *General* tab.

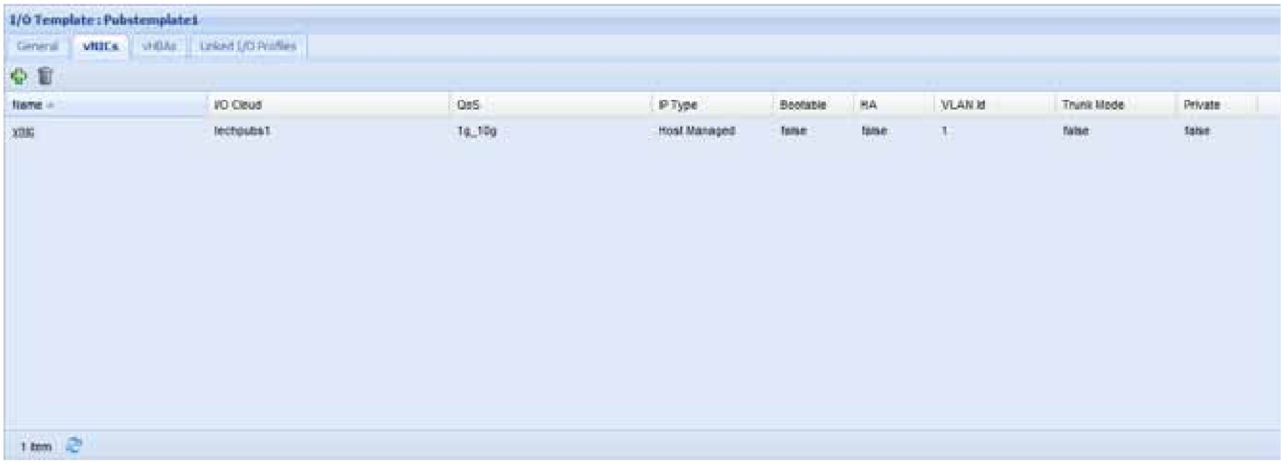
Step 4 Make the necessary modifications.

Step 5 When the properties are configured correctly, click ***Submit***.

Adding or Deleting a Template's vNICs

Through the I/O Template Details frame, you can display the *vNICs* tab, which is a list of the vNICs that are assigned to an I/O Template.

Figure 34 shows the *vNICs* tab of an I/O Template.

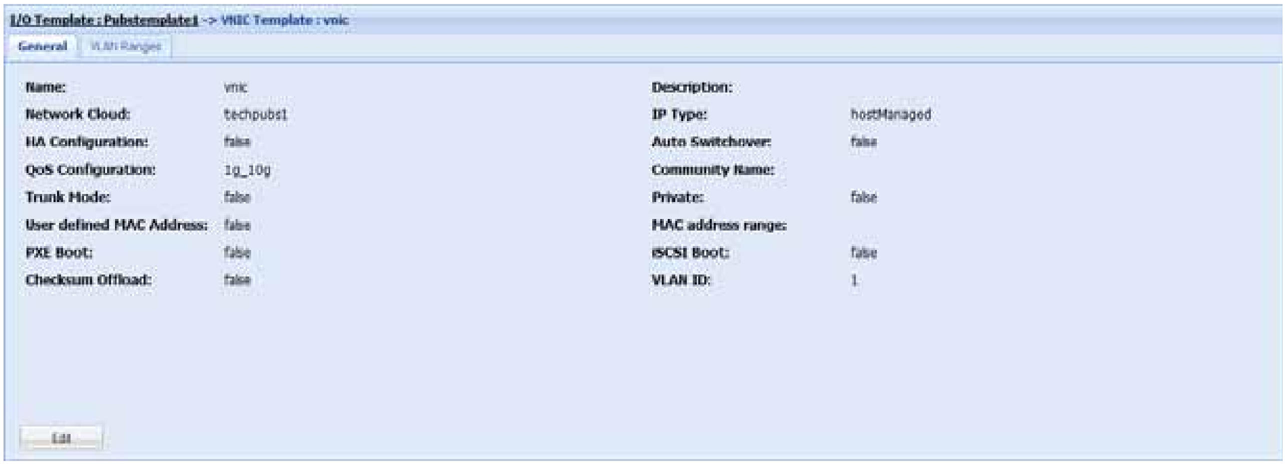


Name	I/O Cloud	QoS	IP Type	Bootable	HA	VLAN Id	Trunk Mode	Private
vnic	techpubs1	1g_10g	Host Managed	false	false	1	false	false

Figure 34 I/O Template Details Frame — vNICs Tab

The individual vNICs on this tab are also links to vNIC properties, which you can use to edit properties of the vNICs in the I/O Template. The general properties appear on the *General* tab. Clicking the vNIC name displays the vNIC properties for that specific vNIC.

Figure 35 shows the vNIC properties.



Name: vnic
Network Cloud: techpubs1
HA Configuration: false
QoS Configuration: 1g_10g
Trunk Mode: false
User defined MAC Address: false
PXE Boot: false
Checksum Offload: false

Description:
IP Type: hostManaged
Auto Switchover: false
Community Name:
Private: false
MAC address range:
iSCSI Boot: false
VLAN ID: 1

Figure 35 vNICs Details Frame

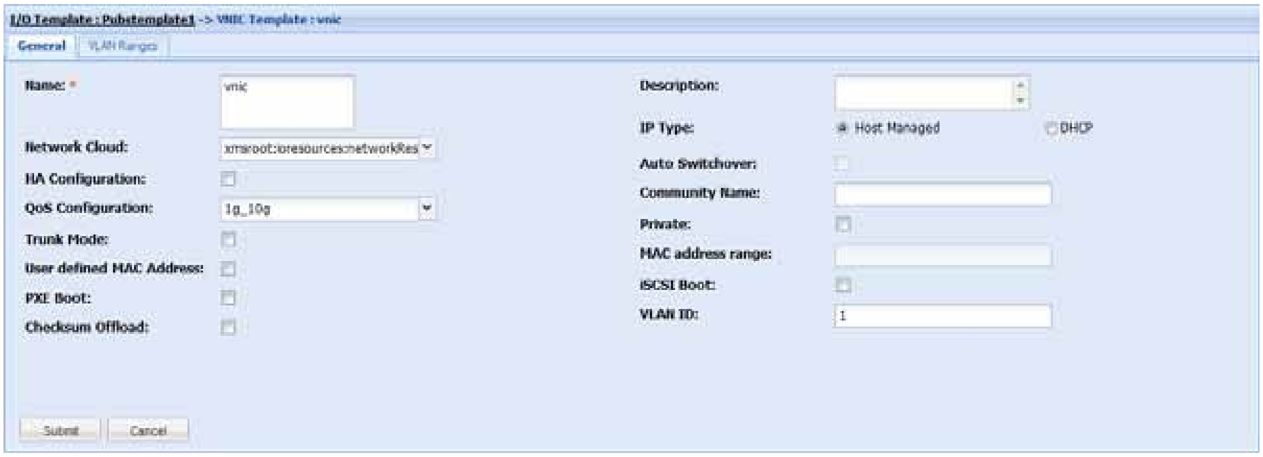
To edit the vNIC properties for an I/O Template’s vNIC, follow this procedure:

Step 1 Display the I/O Templates Summary (*Server Resource Manager->I/O Templates*).

Step 2 On the I/O Template Summary, select an I/O Template to display it in the details frame.

Step 3 Click the *vNICs* tab.

Step 4 On the *vNICs* tab, click a vNIC name to display the vNIC Details frame, then click the ***Edit*** button to unlock the editable fields as shown in Figure 36.



Name: *	vnic	Description:	
		IP Type:	● Host Managed ○ DHCP
Network Cloud:	xmsroot:ioresources:networkRes	Auto Switchover:	□
HA Configuration:	□	Community Name:	
QoS Configuration:	1g_10g	Private:	□
Trunk Mode:	□	MAC address range:	
User defined MAC Address:	□	iSCSI Boot:	□
PXE Boot:	□	VLAN ID:	1
Checksum Offload:	□		

Figure 36 Editable vNICs Details Frame

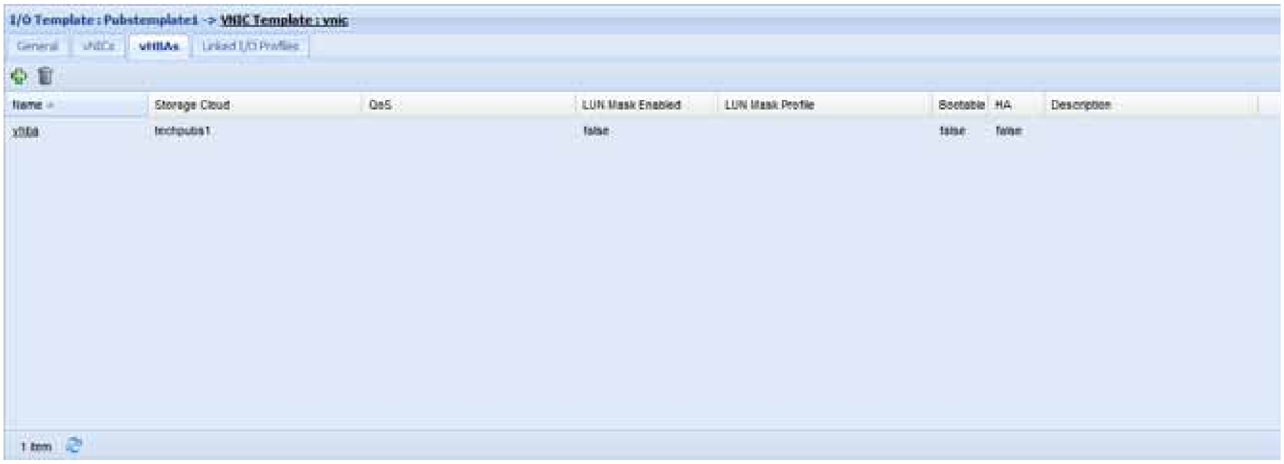
Step 5 Make the required modifications.

Step 6 When the properties are configured correctly, click ***Submit***.

Adding or Deleting a Template’s vHBA

Through the I/O Template Details frame, you can display the *vHBAs* tab, which is a list of the vHBAs that are assigned to an I/O Template.

Figure 37 shows the *vHBAs* tab of an I/O Template.

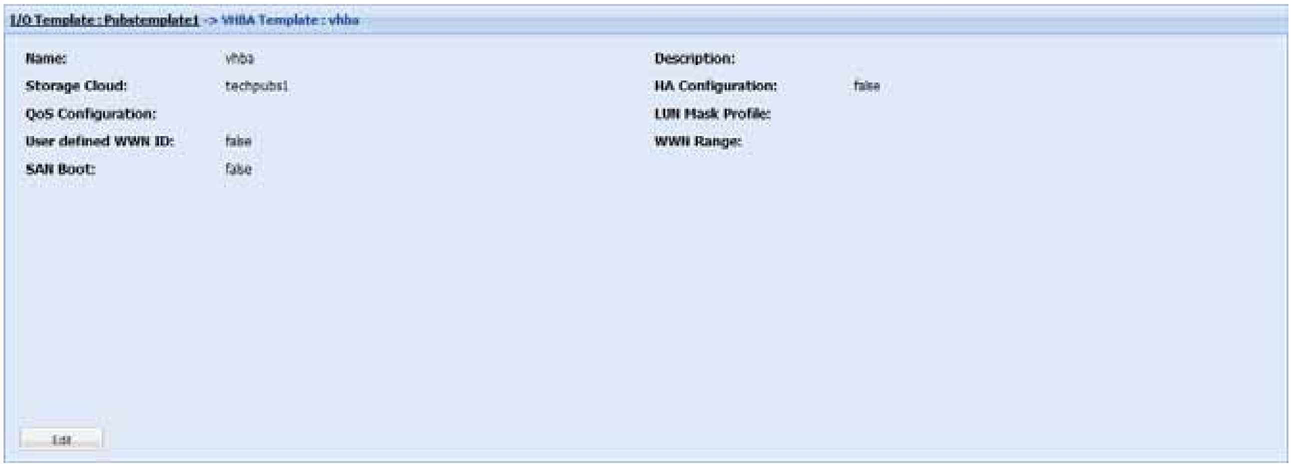

I/O Template : Pubstemplate1 -> VNIC Template : vnic

Name	Storage Cloud	QoS	LUN Mask Enabled	LUN Mask Profile	Bootable	HA	Description
vHBA	techpubs1		false		false	false	

Figure 37 I/O Template Details Frame — vHBAs Tab

The individual vHBAs on this tab are also links to vHBA properties, which you can use to edit to the general properties appear on the *General* tab. Clicking the vHBA name displays the vHBA properties for that specific vHBA.

Figure 38 shows the vHBA properties.


I/O Template : Pubstemplate1 -> VHBA Template : vhba

Name:	vhba	**Description:**	
Storage Cloud:	techpubs1	**HA Configuration:**	false
QoS Configuration:		**LUN Mask Profile:**	
User defined WWN ID:	false	**WWN Range:**	
SAN Boot:	false		

Figure 38 vHBA Details Frame

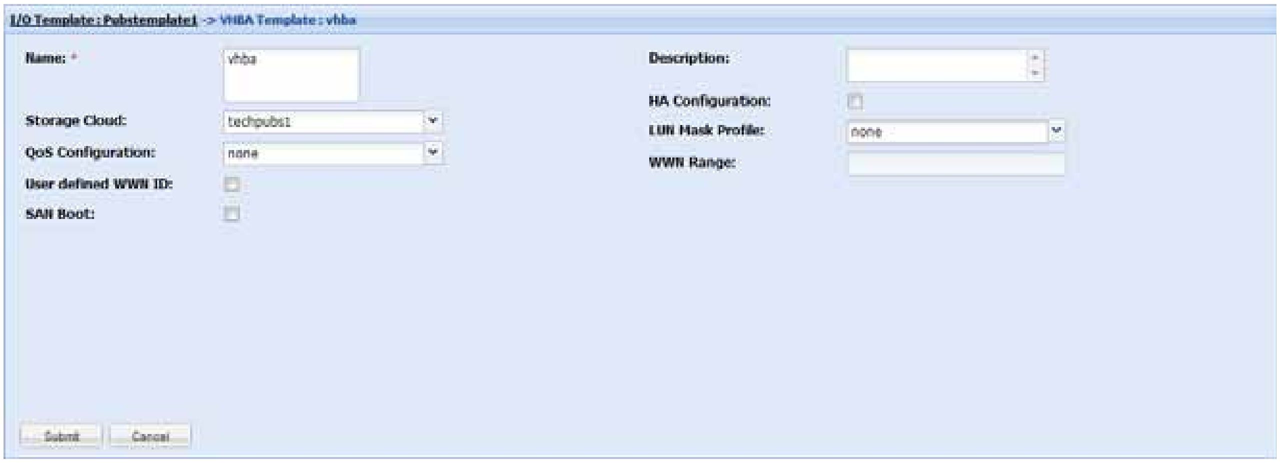
To edit the vHBA properties for an I/O Template’s vHBAs, follow this procedure:

Step 1 Display the I/O Templates Summary (*Server Resource Manager->I/O Templates*).

Step 2 On the I/O Template Summary, select an I/O Template to display it in the details frame.

Step 3 Click the *vHBAs* tab.

Step 4 On the *vHBAs* tab, click a vHBA name to display the vHBA Details frame, then click the ***Edit*** button to unlock the editable fields on the *vHBAs* tab as shown in Figure 39.



I/O Template : Pubstemplate1 -> VHBA Template : vhba

Name: * vhba

Storage Cloud: techpubs1

QoS Configuration: none

User defined WWN ID: □

SAN Boot: □

Description:

HA Configuration: □

LUN Mask Profile: none

WWN Range:

Figure 39 Editable vHBA Details Frame

Step 5 Make the required modifications.

Step 6 When the properties are configured correctly, click ***Submit***.

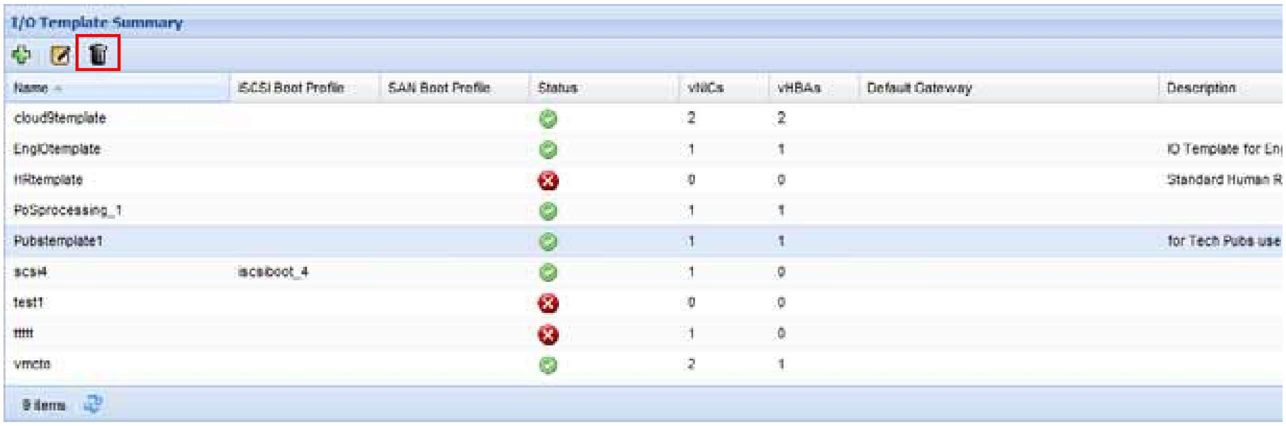
Deleting an I/O Template

Anytime an I/O Template is configured, it can be deleted from the I/O Template Summary. When you delete the I/O Template, it is no longer available to any servers that use it. Any servers that are running with vNICs and vHBAs provided through the I/O Template will continue to run with the vNICs and vHBAs. But the next time the I/O Template is used, the server will no longer be connected to the network and storage attached to the vNIC(s) and vHBA(s) that were in the deleted I/O Template.

To delete an I/O Template, follow this procedure:

Step 1 Display the I/O Template Summary.

Step 2 Select the I/O Template(s) that you want to delete, then click the garbage can icon as shown in Figure 40.



I/O Template Summary

Name	iSCSI Boot Profile	SAN Boot Profile	Status	vNICs	vHBAs	Default Gateway	Description
cloud9template			✓	2	2		
EngIOtemplate			✓	1	1		IO Template for En
HRtemplate			☒	0	0		Standard Human R
PoSprocessing_1			✓	1	1		
Pubstemplate1			✓	1	1		for Tech Pubs use
scsi4	iscsiboot_4		✓	1	0		
test1			☒	0	0		
ttttt			☒	1	0		
vmcto			✓	2	1		

9 items

Figure 40 I/O Template Summary

Step 3 When you click the garbage can icon, a dialog is displayed that confirms that you actually want to delete the selected I/O Template.

Step 4 On the confirmation dialog, click ***Yes*** to confirm the deletion. Or, you can click ***No*** to abort the deletion and leave the I/O Template configured.

Assigning Allowed VLANs to an I/O Template

With the Allowed VLANs feature, you can specify a list of VLANs that are allowed to pass over any trunk vNICs. (Access mode vNICs cannot receive the Allowed VLANs setting.) The Network Cloud has a set of ranges of VLAN IDs that are allowed, and only traffic that is in the specified VLAN range is allowed to pass over trunk vNICs connected to the Network Cloud. By default, this option is set to allow all VLANs (1-4095) on the Network Cloud. Allowed VLANs are configured per network, so the server will receive the associated VLAN traffic when one or more vNICs terminated in a Network Cloud are deployed to any number of servers.

Note

This feature is also configurable at the Network Cloud level so that all vNICs that connect to the Network Cloud receive the same range of allowed VLANs. For information, see Working with Network Clouds.

As an alternative, you can also assign Allowed VLANs to individual vNICs deployed to a Physical Server. To do so, click the *vNICs* tab on the Physical Server Details frame, then click the vNIC name, then click the plus sign (+) on the *VLAN Ranges* tab.

Configuring Allowed VLANs in an I/O Template

By specifying the Allowed VLANs at the I/O Template level, you gain some flexibility in which vNICs have Allowed VLANs. When the I/O Template is deployed to a server, only the vNICs that are pushed to that server get the configured Allowed VLANs. By contrast, if you assign the Allowed VLANs feature at the Network Cloud level, all vNICs connected to the cloud have the same Allowed VLANs.

By using an I/O Template, you can set the allowed VLANs feature on specific vNICs in an I/O Template, regardless of which Network Cloud the I/O Template is using.

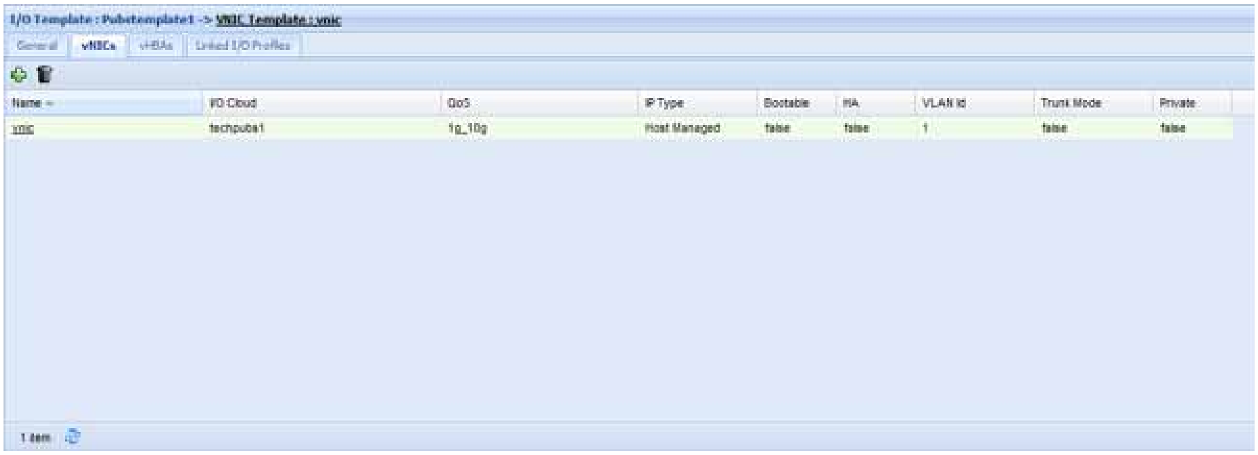
To configure allowed VLANs for an I/O Template, you first create the I/O Template, then edit it to apply the VLAN ranges. Follow this procedure:

Step 1 Create the I/O Template as documented in Creating an I/O Template.

Step 2 When the I/O Template is created, select *Server Resource Manger->I/O Templates* to display the I/O Template Summary.

Step 3 On the I/O Template Summary, click the name of the I/O Template where you want to set the allowed VLANs. This step populates the I/O Template details frame.

Step 4 In the I/O Template Details frame, click the *vNICs* tab to display the vNICs associated with the I/O Template, as shown in Figure 41.



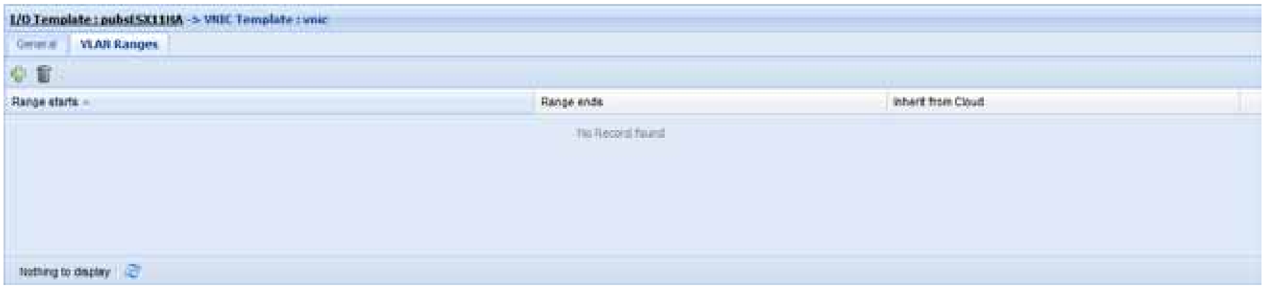
I/O Template : Pubstemplate1 -> VNIC Template : vnic

Name	I/O Cloud	QoS	IP Type	Bootable	HA	VLAN Id	Trunk Mode	Private
vnic	techpubs1	1g_10g	Host Managed	false	false	1	false	false

1 item

Figure 41 I/O Template Details — vNICs Tab

Step 5 Click the name of the vNIC for which you want to configure the Allowed VLANs. This step displays the *VLAN Ranges* tab for the selected vNIC. Figure 42 shows the *VLAN Ranges* tab.



I/O Template : pubsESX11HA -> VNIC Template : vnic

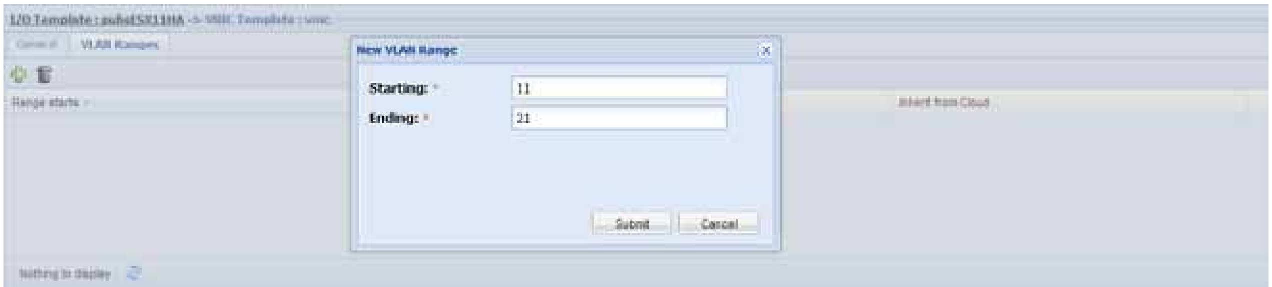
Range starts	Range ends	Inherit from Cloud

No Record found

Nothing to display

Figure 42 I/O Template Details — vNIC VLAN Ranges

Step 6 On the *VLAN Ranges* tab, click the plus sign (+) to display the New VLAN Range dialog as shown in Figure 43.



Starting: * 11

Ending: * 21

Figure 43 Allowed VLANs — Specify VLAN Range

Step 7 In the *Starting* field, enter the first VLAN ID that you want carried on the trunk VLAN.

- If you want only one VLAN on the trunk vNIC, set the same VLAN ID for the starting and ending fields. For example, to have only VLAN ID 256 carried on the vNIC, set 256 as the starting value and ending value.
- If you want multiple individual VLANs on the trunk vNIC, set the single VLAN ID (as documented in the previous bullet), and do this one time for each of the VLAN IDs. For example, if you want VLANs 256, 512, and 1024 carried on the trunk vNIC, you would need to create one range for each VLAN.
- If you want multiple VLAN ranges on the trunk vNIC, set the appropriate VLAN ranges on the same vNIC. You will need to complete this procedure multiple times.

Step 8 In the *Ending* field, enter the last VLAN ID that you want carried on the trunk VLAN.

Step 9 When the VLAN Range has been specified, click ***Submit*** to complete the configuration of the Allowed VLAN Range.

Working with I/O Profiles

This chapter contains the following topics:

Understanding I/O Profiles

I/O Profiles provide a more simplified connection policy that specifies the number of vNICs, vHBAs, or both that are required for a specific server.

I/O Profiles are a software construction that act as a container for virtual I/O resources. I/O Profiles hold all the virtual I/O information for a particular server under management by Oracle’s Xsigo Fabric Manager. The virtual I/O information in the I/O Profile is related to vNICs and HA vNICs, vHBAs and HA vHBAs, all server profiles for a server, and all Oracle Xsigo Fabric Director objects on the Fabric Directors that connect to the server.

An I/O Profile is derived from an I/O Template. The I/O Template provides the basic scope and type of connections that the server has, and the I/O Template is used to create one or more I/O Profiles for a server. However, it is the I/O Profile—not the I/O Template—that is the object that actually gets connected to a server. When the I/O Profile is connected to the server, the vNICs and vHBAs in the I/O Template are pushed to the server.

Because I/O Profiles are created from I/O Templates, the workflow for deploying vNICs and vHBAs on a server has changed if you are deploying connectivity through I/O Templates. The new workflow is:

1. Create an I/O Template
2. Create one or more I/O Profiles from the I/O Template
3. Connect an I/O Profile to a server to deploy the vNICs or vHBAs to the server

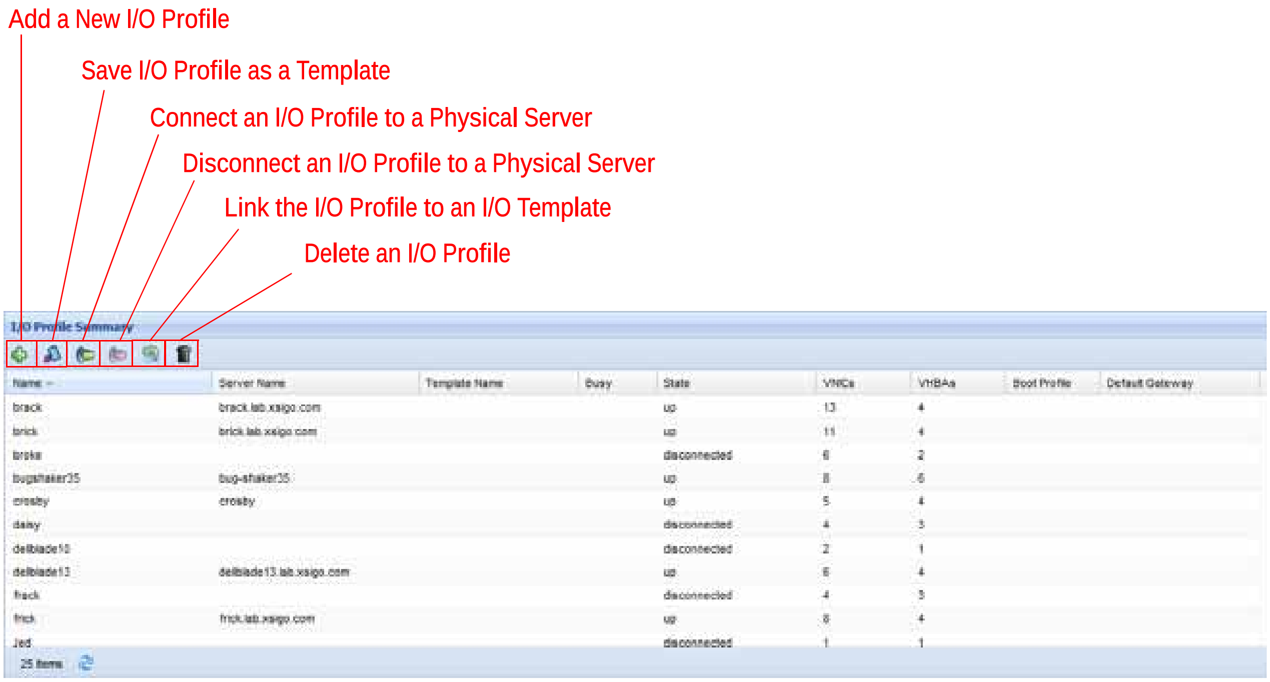
I/O Profiles are also used when you create vNICs and vHBAs directly on a physical server (without an I/O Template) through Physical Server details page. In this case, an I/O Profile is created automatically and assigned the name of the server so that the server, I/O Profile, and all Server Profiles for the server are intuitively and consistently named.

For ease-of use, you can create an I/O Profile without actually connecting it, which enables you to pre-provision an I/O Profile then deploy it when it is needed. For example, if you will be deploying a new server in your datacenter, you can create the I/O Profile before the server is actually built up if you know its connection needs.

Displaying I/O Profiles

I/O Profiles are displayed in the I/O Profiles Summary, which shows a list of all the I/O Profiles created in Fabric Manager. I/O Profiles are listed in the I/O Profile Summary regardless of whether or not they are connected to servers. Through the I/O Profile you can see which I/O Profile is connected to which server, as well as other information about connectivity and boot options supported through the I/O Profile.

Figure 1 shows the I/O Profile Summary.



Add a New I/O Profile

Save I/O Profile as a Template

Connect an I/O Profile to a Physical Server

Disconnect an I/O Profile to a Physical Server

Link the I/O Profile to an I/O Template

Delete an I/O Profile

I/O Profile Summary

Name	Server Name	Template Name	Busy	State	VNICs	VHBAs	Boot Profile	Default Gateway
brack	brack.lab.xsigo.com			up	13	4		
brick	brick.lab.xsigo.com			up	11	4		
broke				disconnected	6	2		
bugshaker35	bug-shaker35			up	8	6		
crosby	crosby			up	5	4		
daisy				disconnected	4	3		
dellblade10				disconnected	2	1		
dellblade13	dellblade13.lab.xsigo.com			up	6	4		
frack				disconnected	4	3		
frick	frick.lab.xsigo.com			up	8	4		
Jed				disconnected	1	1		

25 items

Figure 1 I/O Profiles Summary

Table 1 shows the contents of the I/O Profile Summary and explains what each field means.

Table 1 Contents of the I/O Profile Summary

Field	Means
Name	The name of each configured I/O Profile.
Server Name	The name of the server on which the I/O Profile is deployed. If no server name is displayed, the I/O Profile is not connected to any server.
Template Name	The name of the I/O Template (if any) that is linked to the I/O Profile. It is possible to create an I/O Profile and connect it to a server without creating an I/O Template. If no I/O Template name is present, then the I/O Profile is not linked to an I/O Template.
Busy	Indicates the state of the I/O Profile as either in the process of binding to the server or disconnecting from the server.

Table 1 (continued) Contents of the I/O Profile Summary

Field	Means
State	Indicates the current state of the listed I/O Profiles. Valid states are: • Up, when the I/O Profile is successfully connected to a server. • Connected, when the I/O Profile is connected to a server. • Disconnected, when the I/O Profile is not connected to a server. This state is the default state of an I/O Profile after it has been created. • Partial, when the I/O Profile is not completely connected to a server. This state requires your attention because it usually means that an error has occurred.
vNICs	The number of vNICs that are controlled by the I/O Profile.
vHBAs	The number of vHBAs that are controlled by the I/O Profile.
Boot Profile	The name of the Boot Profile(s) that are controlled by the I/O Profile.
Default Gateway	The default gateway that is controlled by the I/O Profile.

Creating an I/O Profile

When you create an I/O Profile, you are specifying the individual vNIC and vHBA connections for each servers. The I/O Profile is the policy that contains the vNICs and vHBAs, and it is the object that can be connected to, or disconnected from, a server to deploy or remove the network and storage connectivity for the server.

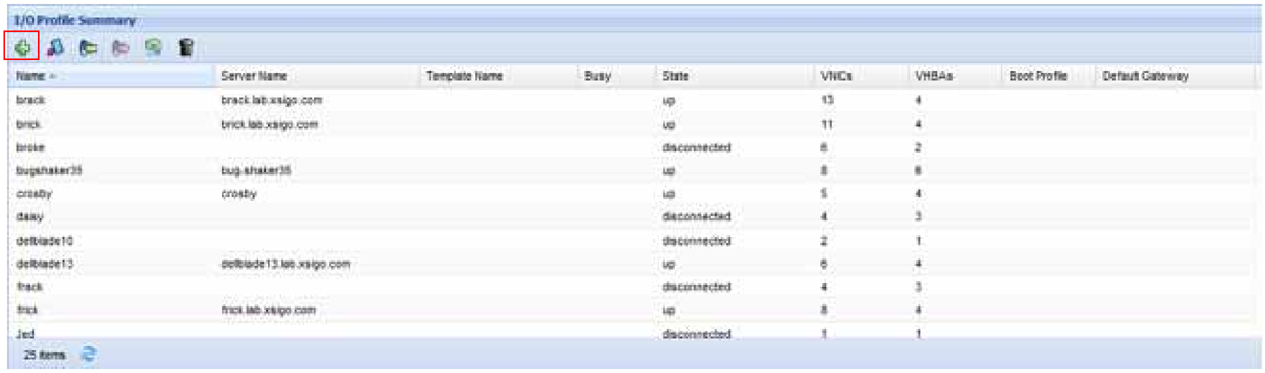
I/O Profiles are created from I/O Templates, in any number from 1 to 20. For example, after you have created an I/O Template, if 6 servers need the same connectivity, you can use the I/O Template to create 6 different I/O Profiles. Each I/O Profile can then be connected to a server as needed. This method allows you granular control over which servers get connectivity without requiring you to take the time to create 6 different sets of vNICs and vHBAs. Instead, creation occurs once through the I/O Template, and control over which servers receive connectivity is accomplished on a server-by-server basis.

When I/O Profiles are created from an I/O Template, they are displayed in the I/O Profile Summary. If multiple I/O Profiles are created from the same I/O Template, you give them a name and Fabric Manager adds an enumerated suffix in the form of _X where X is a number. For example, if you created 6 I/O Profiles for your security auditing servers with the name “AuditServers”, then the I/O Profiles would be named “AuditServer_1” through “AuditServer_6”. Because of the suffix, each of the I/O Profiles is a unique object in Fabric Manager, and as a result, can be used and managed separate of the other 5 I/O Profiles.

Creating an I/O Profile starts from the I/O Profile Summary, and requires that an I/O Template has already been created and saved. If you do not have an appropriate I/O Template created, create one now. See Working with I/O Templates.

To create an I/O Profile, follow this procedure:

Step 1 Select Display the I/O Profile Summary See Figure 2.



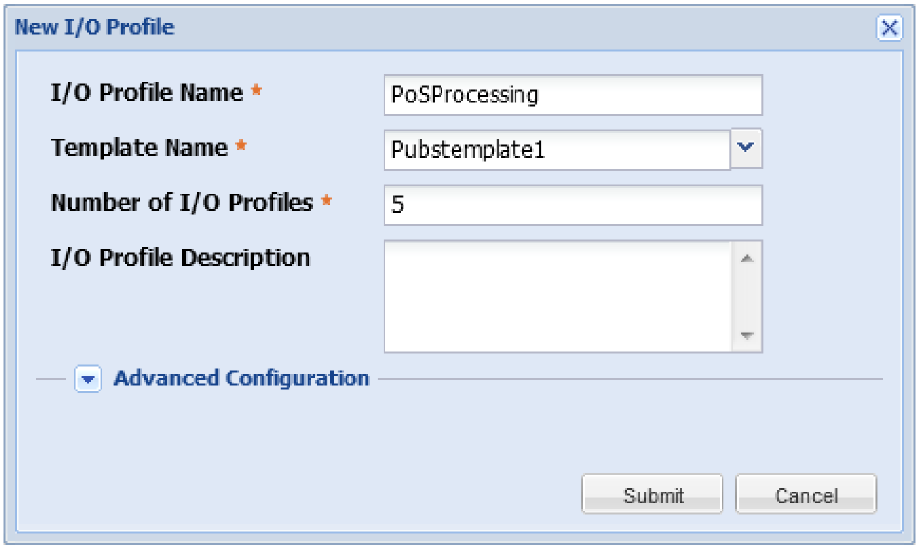
I/O Profile Summary

Name	Server Name	Template Name	Busy	State	VNICs	VHBAs	Boot Profile	Default Gateway
brack	brack.lab.xsigo.com			up	13	4		
brick	brick.lab.xsigo.com			up	11	4		
broke				disconnected	6	2		
bugshaker35	bug-shaker35			up	8	6		
crosby	crosby			up	5	4		
daisy				disconnected	4	3		
dellblade10				disconnected	2	1		
dellblade13	dellblade13.lab.xsigo.com			up	6	4		
frack				disconnected	4	3		
frick	frick.lab.xsigo.com			up	8	4		
Jed				disconnected	1	1		

25 items

Figure 2 I/O Profile Summary

Step 2 Click the plus sign (+) to display the New I/O Profile dialog as shown in Figure 3.



New I/O Profile

I/O Profile Name * PoSProcessing

Template Name * Pubstemplate1

Number of I/O Profiles * 5

I/O Profile Description

Figure 3 New I/O Profile Dialog

Step 3 From the *Template Name* dropdown menu, select the I/O Template that you want to use to create I/O Profiles. If the I/O Template you want to use is not listed, it has not been successfully created. You will need to cancel out of this procedure and create an I/O Template before returning to this procedure.

Step 4 In the *Number of I/O Profiles* field, enter a number from 1 to 20 that specifies the number of I/O Profiles that will be created from the selected I/O Template. When more than one I/O Profile is created, each I/O Profile is created with a numerical suffix appended to the I/O Profile name.

Step 5 In the *I/O Profile Name* field, enter a name for the I/O Profile that you want to created. If more than one I/O Profile will be created, the name you specify is a baseline to which a number is appended (for example, `PoSProcessing_1`).

Step 6 As an option, in the I/O Profile Description field, you can enter an alphanumeric character string that describes the I/O Profile(s) that you are creating.

Note

At this point, you have completed the basic configuration of an I/O Profile. However, you can specify which Fabric Directors are connecting the I/O Profiles by using options in the Advanced Configuration section. See Connecting Specific I/O Profiles to Specific Fabric Directors.

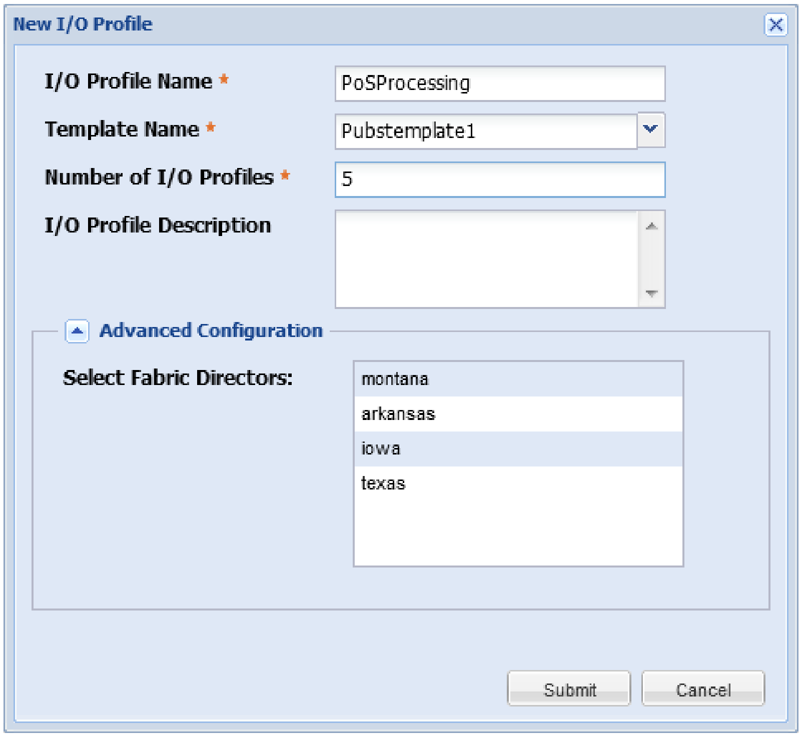
Step 7 Click ***Submit*** to create the I/O Profile(s) from the selected I/O Template.

Connecting Specific I/O Profiles to Specific Fabric Directors

As part of configuring an I/O Profile, you can select the individual Fabric Directors that are connecting the I/O Profile to a server. For example, assume you have a dual-Fabric Director environment, but you want only one of the Fabric Directors to connect the I/O Profile to the server. Through the New I/O Profile dialog, you can specify which Fabric Directors can support one or more I/O Profiles. By default, any Fabric Director that Fabric Manager is managing can support the connection, but using the Advanced Configuration section, you can control where the I/O Profile is supported.

To connect I/O Profiles to specific Fabric Directors, follow this procedure:

Step 1 On the New I/O Profile dialog, click the ***Advanced Configuration*** button to display the advanced properties for an I/O Profile, as shown in Figure 4.



I/O Profile Name * PoSProcessing

Template Name * Pubstemplate1

Number of I/O Profiles * 5

I/O Profile Description

Select Fabric Directors:
montana
arkansas
iowa
texas

Figure 4 New I/O Profile — Advanced Configuration Properties

As shown in Figure 4, all Fabric Directors that Fabric Manager is managing are listed. If you have specific connection needs for the I/O Profile, you can make sure that the correct Fabric Director(s) connect the I/O Profile to the server by selecting the Fabric Director(s) from the pick list.

Step 2 Select the Oracle Xsigo Fabric Directors that need to support the I/O Profile.

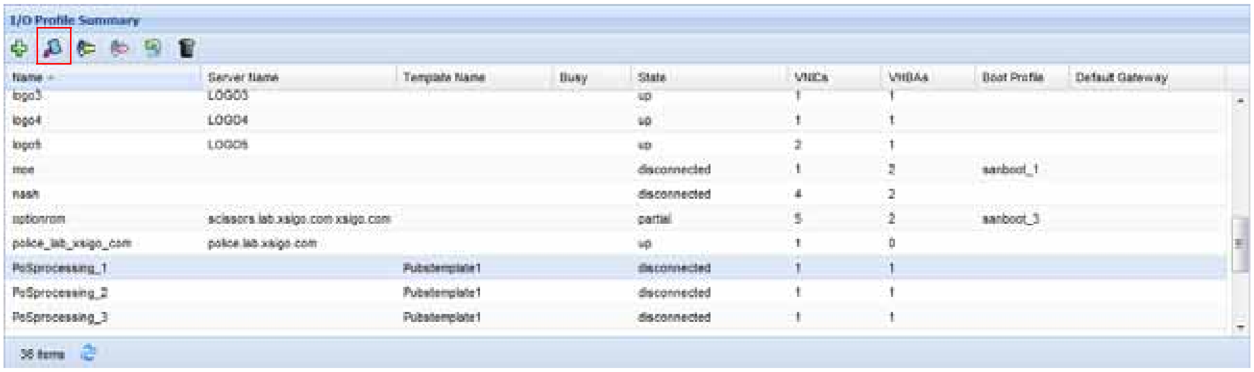
Step 3 Click ***Submit***.

Saving an I/O Profile as an I/O Template

When an I/O Profile is created, you can save it as an I/O Template. If you do, the current I/O Profile is created as a brand new I/O Template and is added to the I/O Template Summary. This functionality allows you to create a new I/O Template after customizing an I/O Profile. For example, you could create a simple I/O Template with a single vNIC and vHBA that you use to create an I/O Profile. After using the I/O Profile, you might promote a server to a more important role which requires HA vNICs and multipath vHBAs. You could then modify the I/O Profile, and save it as an I/O Template which could then be used as the source for creating additional I/O Profiles featuring HA.

To save an I/O profile, follow this procedure:

Step 1 Display the I/O Profile Summary as shown in Figure 5.



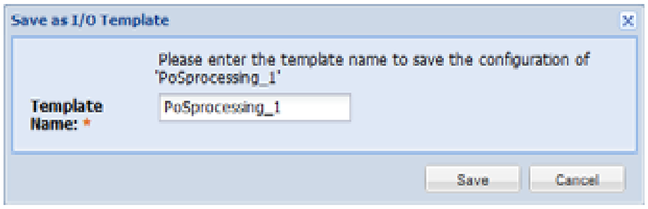
I/O Profile Summary

Name	Server Name	Template Name	Busy	State	VNICs	VHBAs	Boot Profile	Default Gateway
logo3	LOGO3			up	1	1		
logo4	LOGO4			up	1	1		
logo5	LOGO5			up	2	1		
moe				disconnected	1	2	sanboot_1	
nash				disconnected	4	2		
optionrom	scissors.lab.xsigo.com.xsigo.com			partial	5	2	sanboot_3	
police_lab_xsigo_com	police.lab.xsigo.com			up	1	0		
PoSprocessing_1		Pubstemplate1		disconnected	1	1		
PoSprocessing_2		Pubstemplate1		disconnected	1	1		
PoSprocessing_3		Pubstemplate1		disconnected	1	1		

36 items

Figure 5 I/O Profile Summary

Step 2 Click the ***Save as I/O Template*** button to display the Save as I/O Template dialog. See Figure 6.



Save as I/O Template

Please enter the template name to save the configuration of 'PoSprocessing_1'

Template Name: * PoSprocessing_1

Figure 6 Save as I/O Template

Step 3 In the *Template Name* field, enter an alphanumeric character string that names the I/O Template you are creating, or accept the I/O Profile name which is supplied by default.

Step 4 Click ***Save***.

Connecting an I/O Profile to a Server

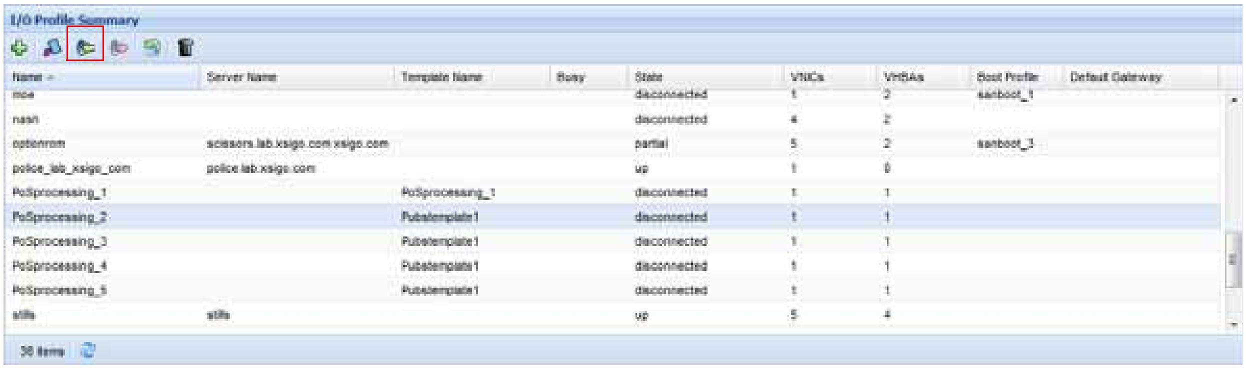
An I/O Profile is the container for vNICs and vHBAs, but it doesn't actually provide any connectivity until you connect that I/O Profile to a server. The I/O Profile is the object that you connect to a server, and when you do so, the vNICs and vHBAs contained in the I/O Profile are pushed to the host.

An I/O Profile in the "disconnected" state can be applied to a server. If you want to connect an I/O Profile that is already connected to a server, you must explicitly disconnect that I/O Profile first. Also, an I/O Profile can be connected to a server that is in any state, but only when the server is fully up and online will the I/O Profile support traffic.

But remember that an I/O Profile is not automatically connected to a server when it is created. You must manually connect the I/O Profile to a server to deploy the vNICs or vHBAs to the server.

To connect an I/O Profile follow this procedure:

Step 1 Display the I/O Profile Summary as shown in Figure 7.



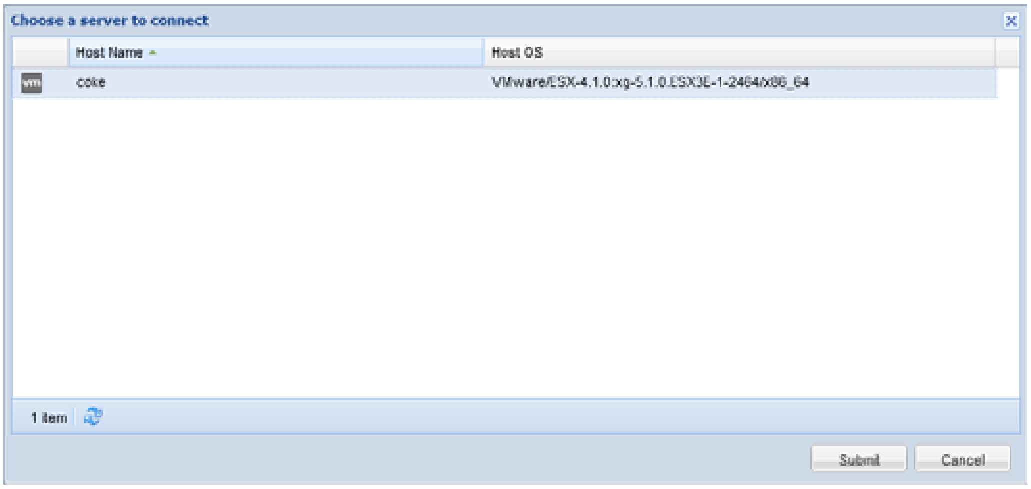
I/O Profile Summary

Name	Server Name	Template Name	Busy	State	VNICs	VHBAs	Boot Profile	Default Gateway
moe				disconnected	1	2	sanboot_1	
nash				disconnected	4	2		
optionrom	scissors.lab.xsigo.com.xsigo.com			partial	5	2	sanboot_3	
police_lab_xsigo_com	police.lab.xsigo.com			up	1	0		
PoSprocessing_1		PoSprocessing_1		disconnected	1	1		
PoSprocessing_2		Pubstemplate1		disconnected	1	1		
PoSprocessing_3		Pubstemplate1		disconnected	1	1		
PoSprocessing_4		Pubstemplate1		disconnected	1	1		
PoSprocessing_5		Pubstemplate1		disconnected	1	1		
stills	stills			up	5	4		

Figure 7 I/O Profile Summary

Step 2 Click an I/O Profile to select it. This step activates the ***Connect I/O Profile to a Server*** button.

Step 3 Click the ***Connect to a Server*** button to display the Choose a Server to Connect dialog, as shown in Figure 8.



Choose a server to connect

	Host Name	Host OS
vm	coke	VMware/ESX-4.1.0:xg-5.1.0.ESX3E-1-2464/x86_64

1 item

Figure 8 Choose a Server to Connect Dialog

Step 4 Select the server(s) to which you want to connect the I/O Profile. This step activates the ***Submit*** button.

Step 5 Click ***Submit*** to connect the I/O Profile to the selected server.

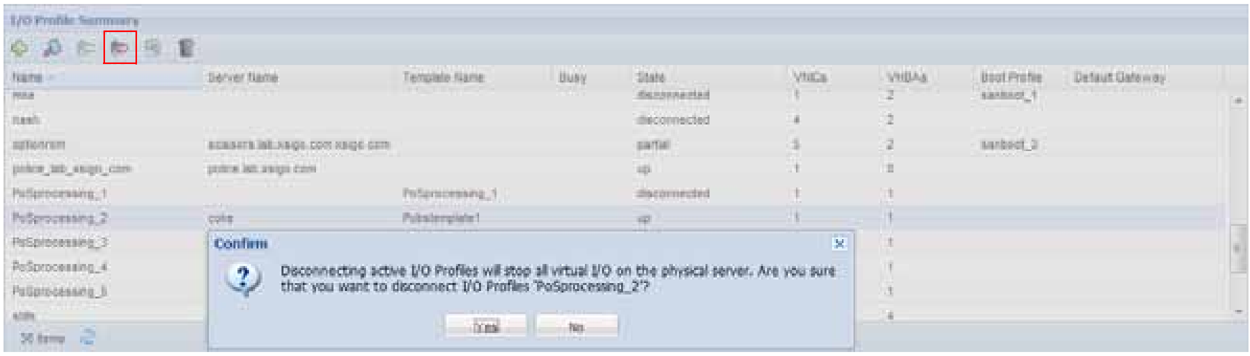
Disconnecting an I/O Profile from a Server

An I/O Profile in the “connected” state can be removed from a server. If you want to remove the vNICs and vHBAs from a server without deleting the I/O Profile, you can simply disconnect the I/O Profile. All the connectivity in the I/O Profile remains intact and can be used again on the same server or another. By disconnecting the I/O Profile, you will remove the network and storage connections for a server, which will cause a service interruption, but does not affect the admin or operational state of the server itself.

If you want to completely delete an I/O Profile, you must first disconnect the I/O Profile.

To disconnect an I/O Profile, follow this procedure:

Step 1 Display the I/O Profile Summary as shown in Figure 9.



I/O Profile Summary

Name	Server Name	Template Name	Busy	State	VNICs	VHBAs	Boot Profile	Default Gateway
moe				disconnected	1	2	sanboot_1	
nash				disconnected	4	2		
optionrom	scissors.lab.xsigo.com.xsigo.com			partial	5	2	sanboot_3	
police_lab_xsigo_com	police.lab.xsigo.com			up	1	0		
PoSprocessing_1		PoSprocessing_1		disconnected	1	1		
PoSprocessing_2	coke	Pubstemplate1		up	1	1		
PoSprocessing_3						1		
PoSprocessing_4						1		
PoSprocessing_5						1		
stills						4		

36 items

Confirm

Disconnecting active I/O Profiles will stop all virtual I/O on the physical server. Are you sure that you want to disconnect I/O Profiles 'PoSprocessing_2'?

Figure 9 Disconnect an I/O Template

Step 2 Select the I/O Profile that you want to disconnect. This step activates the ***Disconnect I/O Profile from Server*** button.

Step 3 Click the ***Disconnect I/O Profile from Server*** button, which causes a confirmation dialog to be displayed.

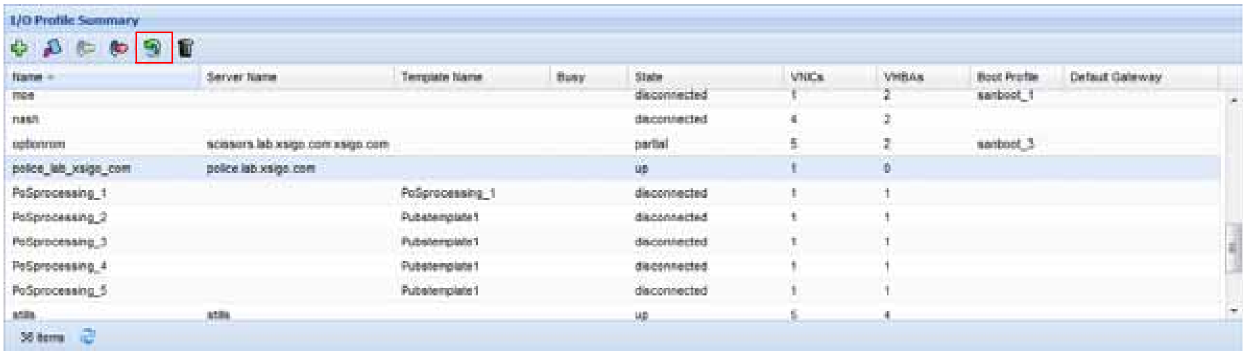
Step 4 On the confirmation dialog, click ***Yes*** to disconnect the selected I/O Profile. As an alterative, you can click ***No*** to abort the disconnect.

Linking an I/O Profile to an I/O Template

When an I/O Profile is not associated with an I/O Template, you can link it to an I/O Template. If you do, the vNICs and vHBAs in the I/O Profile are added to an existing I/O Template. With this feature, you can start with an I/O Template and add virtual connectivity to it over time to create a more robust I/O Template.

To link an I/O Profile to an I/O Template, follow this procedure:

Step 1 Display the I/O Profile Summary as shown in Figure 10.



I/O Profile Summary

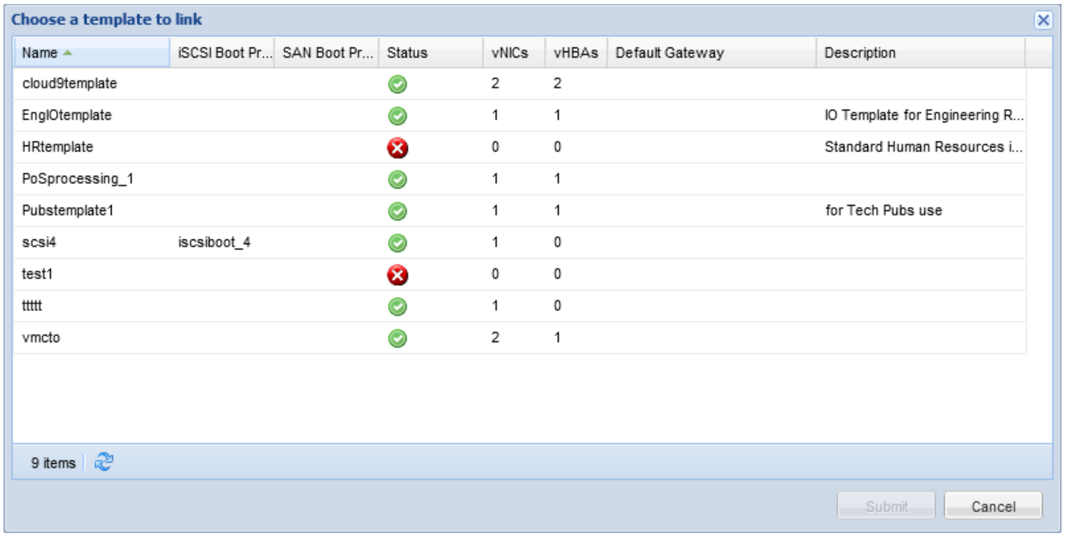
Name	Server Name	Template Name	Busy	State	VNICs	VHBAs	Boot Profile	Default Gateway
moe				disconnected	1	2	sanboot_1	
nash				disconnected	4	2		
optionrom	scissors.lab.xsigo.com.xsigo.com			partial	5	2	sanboot_3	
police_lab_xsigo_com	police.lab.xsigo.com			up	1	0		
PoSprocessing_1		PoSprocessing_1		disconnected	1	1		
PoSprocessing_2		Pubstemplate1		disconnected	1	1		
PoSprocessing_3		Pubstemplate1		disconnected	1	1		
PoSprocessing_4		Pubstemplate1		disconnected	1	1		
PoSprocessing_5		Pubstemplate1		disconnected	1	1		
stills	stills			up	5	4		

36 items

Figure 10 I/O Profile Summary

Step 2 Select the I/O Profile that you want to link to an I/O Template. This step activates the ***Link I/O Profile to I/O Template*** button.

Step 3 Click the ***Link I/O Profile to I/O Template*** button to display the Choose a Template to Link dialog as shown in Figure 11.



Choose a template to link

Name	iSCSI Boot Pr...	SAN Boot Pr...	Status	vNICs	vHBAs	Default Gateway	Description
cloud9template			✓	2	2		
EnglOtemplate			✓	1	1		IO Template for Engineering R...
HRtemplate			✗	0	0		Standard Human Resources i...
PoSprocessing_1			✓	1	1		
Pubstemplate1			✓	1	1		for Tech Pubs use
scsi4	iscsiboot_4		✓	1	0		
test1			✗	0	0		
ttttt			✓	1	0		
vmcto			✓	2	1		

9 items

Figure 11 Choose Template to Link Dialog

Step 4 Select an I/O Template from the dialog. Only Templates with a green checkmark in the Status column can be linked to an I/O Profile.

Step 5 When a valid I/O Template is selected, click ***Submit***.

Deleting an I/O Profile

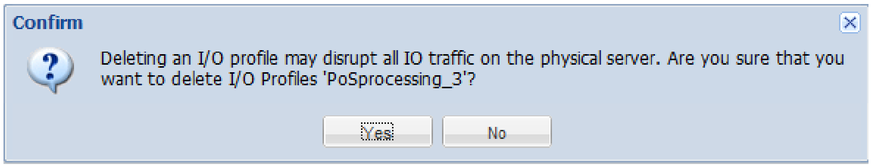
An I/O Profile can be deleted at any time, even if the I/O Profile is connected to a server. When you delete an I/O Profile, you are removing the I/O Profile and its vNICs and vHBAs from Oracle’s Xsigo Fabric Manager. A deleted I/O Profile is not kept, so if you need to use it later, you will need to recreate it. Deleting an I/O Profile removes all the vNICs and vHBAs bound to that server, so if you delete an I/O Profile, you will disconnect is network and storage connections, and service will be interrupted.

To delete an I/O Profile, follow this procedure:

Step 1 Display the I/O Profile Summary.

Step 2 On the I/O Profile Summary, select the I/O Profile that you want to delete. This step activates the ***Delete I/O Profile*** button.

Step 3 When the I/O Profile is selected, click ***Delete I/O Profile*** (the garbage can icon) to display a confirmation dialog as shown in Figure 12.



Deleting an I/O profile may disrupt all IO traffic on the physical server. Are you sure that you want to delete I/O Profiles 'PoSprocessing_3'?

Figure 12 Confirmation Dialog

Step 4 Click ***Yes*** to delete the selected I/O Profile. As an alternative, you can click ***No*** to abort the deletion.

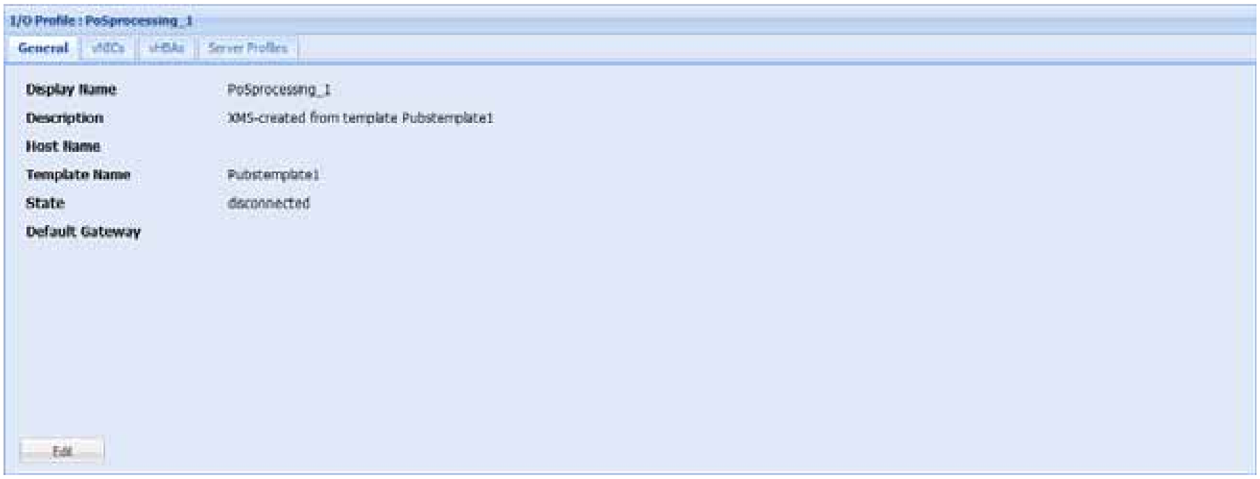
Displaying I/O Profile Details

Through the I/O Profile Summary, you can display additional details about individual I/O Profiles. By clicking an I/O Profile, the details frame is populated with additional details about the profile. The I/O Profile Details frame contains the following tabs:

- General Properties
- vNICs in the I/O Profile
- vHBAs in the I/O Profile
- Server Profiles in an I/O Profile
- Boot Info, which is conditional. The presence of this tab depends on whether a Boot Profile for iSCSI, SAN Boot, or PXE Boot is configured in the I/O Template that was used to create the I/O Profile. An example of the Boot Info tab is displayed for SAN Boot in Displaying Boot Information for an I/O Profile.

Displaying General Properties

General properties are available for the I/O Profile through the *General* tab. General properties include the I/O Profile's name, information about the server where the I/O Profile is connected, and the I/O Template that was used to derive the I/O Profile. Figure 13 shows the *General* properties tab.



Display Name	PoSprocessing_1
Description	XMS-created from template Pubstemplate1
Host Name	
Template Name	Pubstemplate1
State	disconnected
Default Gateway	

Figure 13 I/O Profile Details — General Properties Tab

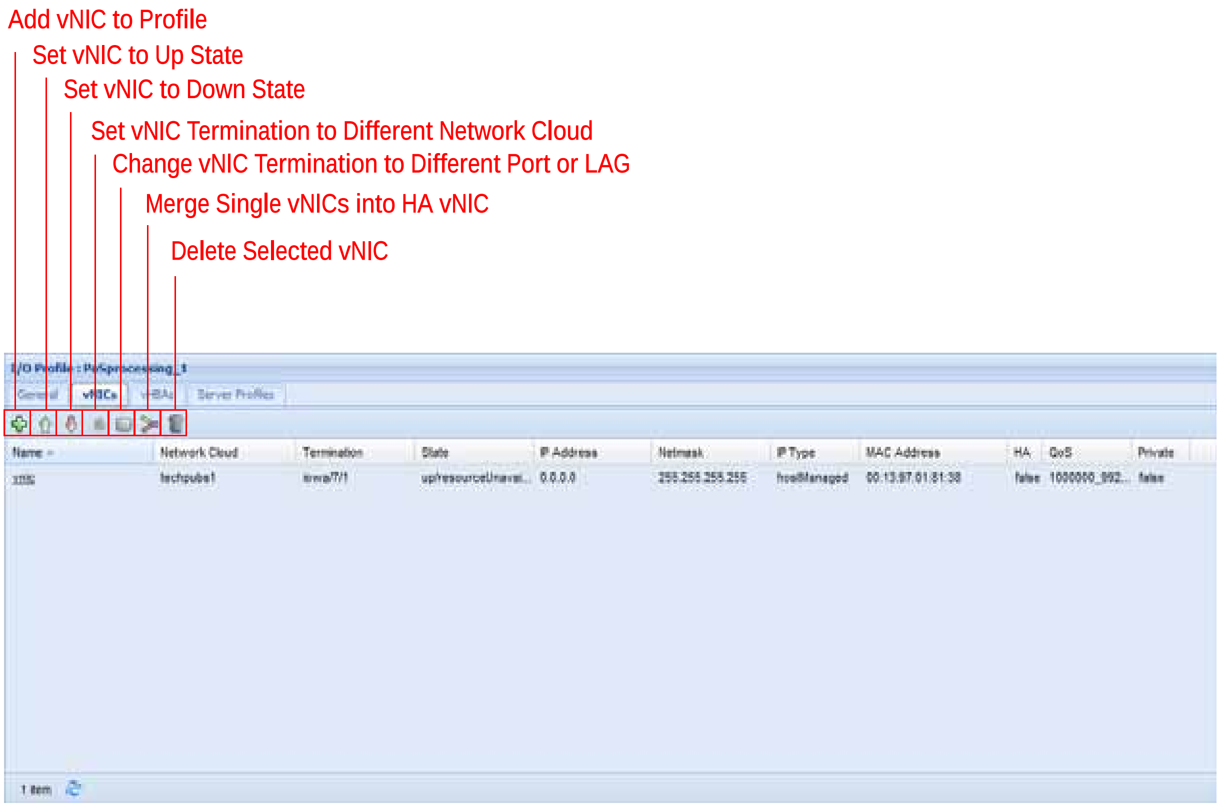
Table 2 shows the contents of the *General* tab, and explains what each field means.

Table 2 Contents of the General Properties Tab

Field...	Means...
Display Name	The name of the I/O Profile
Description	Is an optional alphanumeric character string that describes the I/O Profile.
Host Name	Is the name of the server to which the I/O Profile is connected.
Template Name	Is the name of the I/O Template that was used to derive the I/O Profile.
State	Is the state of the I/O Profile. Valid states are: • Connected • Partial • Disconnected • Down
Default Gateway	The name of the default gateway for the server where the I/O Profile is connected.

Displaying vNICs in an I/O Profile

An I/O Profile controls one or more vNICs that are originally assigned through the I/O Template that was used to create the I/O Profile. However, after the I/O Profile is created, you can customize the I/O Profile by using the toolbar buttons on the *vNICs* tab. Figure 14 shows the *vNICs* tab and the buttons available on it.



Add vNIC to Profile

Set vNIC to Up State

Set vNIC to Down State

Set vNIC Termination to Different Network Cloud

Change vNIC Termination to Different Port or LAG

Merge Single vNICs into HA vNIC

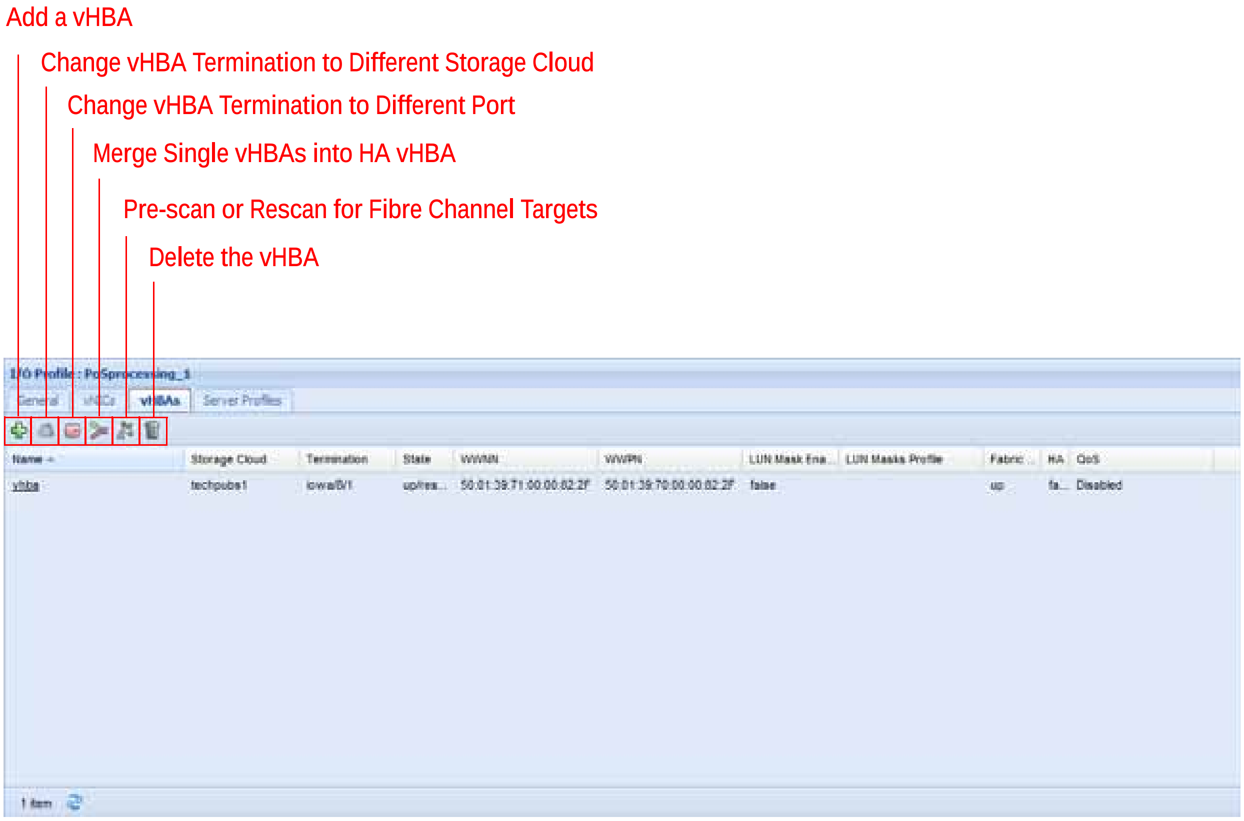
Delete Selected vNIC

Name	Network Cloud	Termination	State	IP Address	Netmask	IP Type	MAC Address	HA	QoS	Private
xis	techpubs1	iowa/7/1	up/resourceUnavai...	0.0.0.0	255.255.255.255	hostManaged	00:13:97:01:81:38	false	1000000_992...	false

Figure 14 I/O Profile Details — vNICs Tab

Displaying vHBAs in an I/O Profile

An I/O Profile controls one or more vHBAs that are originally assigned through the I/O Template that was used to create the I/O Profile. However, after the I/O Profile is created, you can customize the I/O Profile by using the toolbar buttons on the *vHBAs* tab. Figure 15 shows the *vHBAs* tab and the buttons available on it.



Add a vHBA

Change vHBA Termination to Different Storage Cloud

Change vHBA Termination to Different Port

Merge Single vHBAs into HA vHBA

Pre-scan or Rescan for Fibre Channel Targets

Delete the vHBA

I/O Profile : PoSprocessing_1

Name	Storage Cloud	Termination	State	WWNN	WWPN	LUN Mask Ena...	LUN Masks Profile	Fabric ...	HA	QoS
vhba	techpubs1	iowa/8/1	up/res...	50:01:39:71:00:00:82:2F	50:01:39:70:00:00:82:2F	false		up	fa...	Disabled

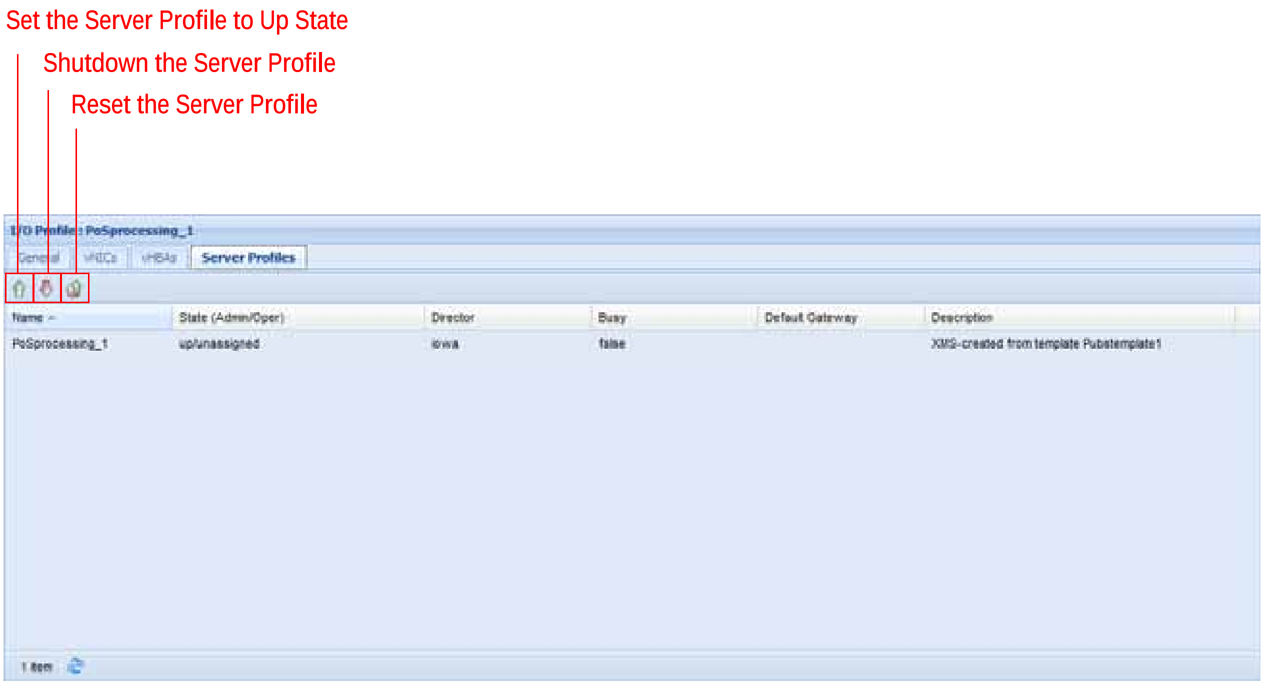
Figure 15 I/O Profile Details — vHBAs Tab

Displaying Server Profiles in an I/O Profile

I/O Profiles contain all the objects on a server, including I/O Templates and Server Profiles. You can display the server profile(s) that are controlled through an I/O Profile by selecting the *Server Profiles* tab on the I/O Profile details frame.

In addition to displaying detailed information about the server profiles associated with an I/O Profile, you can also perform basic management functions for the server profile, such as turn up, shut down, and reset of the server profile.

Figure 16 shows the *Server Profiles* tab.



Set the Server Profile to Up State

Shutdown the Server Profile

Reset the Server Profile

I/O Profile : PoSprocessing_1

Name	State (Admin/Oper)	Director	Busy	Default Gateway	Description
PoSprocessing_1	up/unassigned	iowa	false		XMS-created from template Pubstemplate1

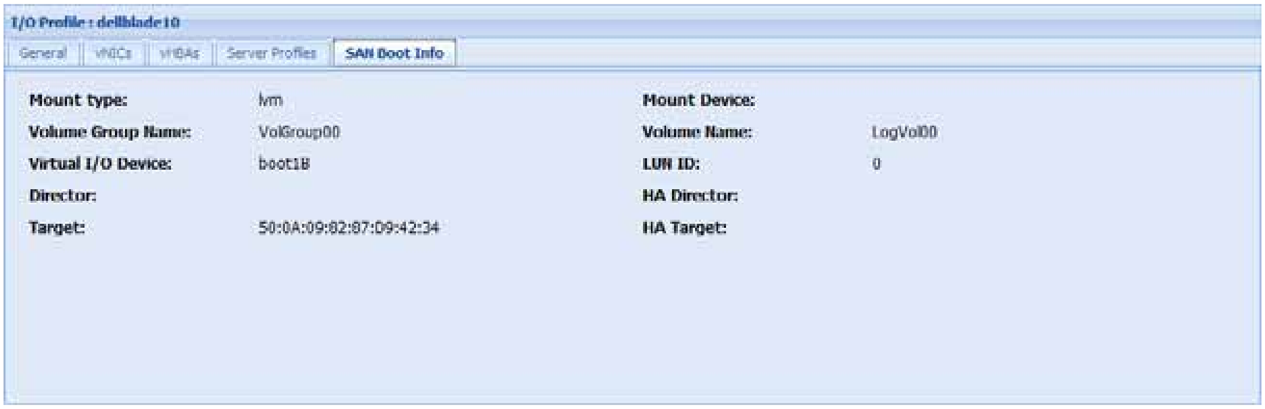
1 item

Figure 16 I/O Profile Details — Server Profiles Tab

Displaying Boot Information for an I/O Profile

For I/O Profiles that are configured with SAN Boot vHBAs, PXE Boot vNICs, or iSCSI Boot vNICs, the I/O Profile details frame contains a conditional tab called *Boot Info*. This tab is conditional because it is not displayed in the I/O Profile details frame unless you have a SAN Boot vHBA, or a PXE Boot or iSCSI Boot vNIC configured in the I/O Template from which the I/O Profile was derived. Also, this tab's name is conditional. For SAN Boot I/O Profiles, the tab is named *SAN Boot Info*; for iSCSI Boot Profiles the tab is named *iSCSI Boot Info*; for PXE Boot I/O Profile this tab is named *PXE Boot Info*.

Through the *Boot Info* tab, you can display a list of the remote boot properties for the I/O Profile, such as the bootable vNIC or vHBA as well as other properties. Figure 17 shows an example of the *Boot Info* tab for a SAN Boot I/O Profile.



Mount type:	lvm	**Mount Device:**	
Volume Group Name:	VolGroup00	**Volume Name:**	LogVol00
Virtual I/O Device:	boot1B	**LUN ID:**	0
Director:		**HA Director:**	
Target:	50:0A:09:82:87:09:42:34	**HA Target:**	

Figure 17 I/O Profile Details — SAN Boot Info Tab

In this example, the *SAN Boot Info* tab shows properties for an I/O Profile configured for SAN Booting through the logical volume manager method.

Working with Link Aggregation

This chapter contains the following topics:

Configuring Link Aggregation Groups

A Link Aggregation Group (LAG) enables you to combine multiple individual physical Ethernet ports into one logical port group. As a result, the ports combined into a LAG can operate in parallel with the benefit of increased link speed and high availability.

Oracle's Xsigo Fabric Manager supports LAG at the I/O module level. When you configure LAG, you specify a group name for the LAG, then assign ports from the same Ethernet I/O module to the group. LAGs are supported on the 4-Port 10 GE module and the 10-Port GE module only (not the 10 GE module).

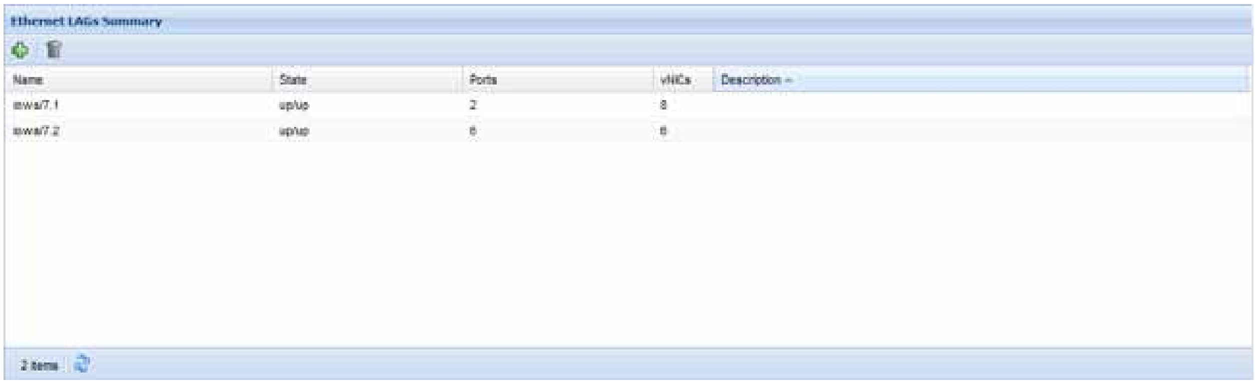
LAGs are associated with a Network Cloud and, just like Ethernet ports, can be the termination point for vNICs. If you will be provisioning LAGs in your network, you will need to create them before associating a Network Cloud with them. By doing so, you make the LAG available as a selectable object in the dialog that supports Network Cloud creation.

Each LAG can be supported as a static LAG or passive-mode LAG:

- after initially specifying the ports that are members of the LAG, static LAGs require user intervention to add ports to and delete ports from a LAG.
- after initially specifying the ports that are members of the LAG, passive-mode LAGs use Link Aggregation Control Protocol (LACP) in combination with a neighboring Gigabit Ethernet switch to dynamically control port additions and deletions within a LAG.

To configure Link Aggregation Groups, follow this procedure:

Step 1 Display the Ethernet LAG Summary by selecting *Network Cloud Manager->Link Aggregation Groups*. Figure 1 shows the Ethernet LAG Summary.



Ethernet LAGs Summary

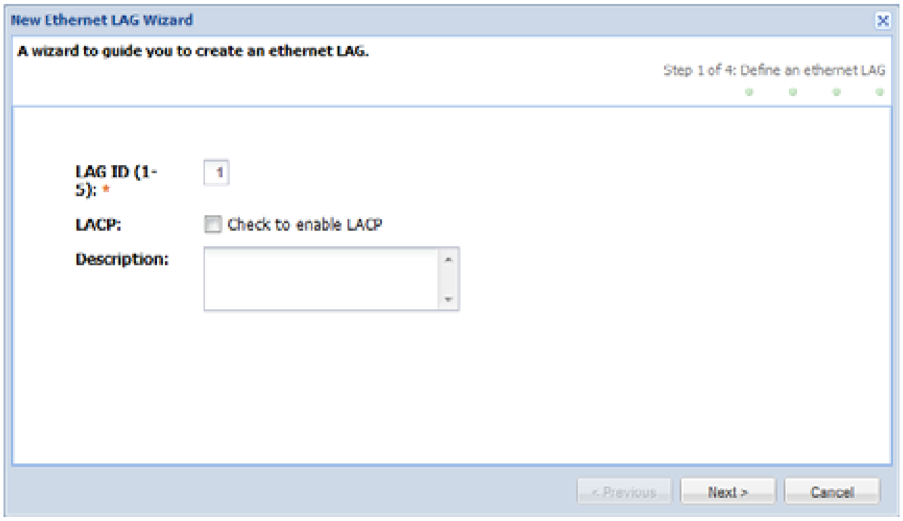
Name	State	Ports	vNICs	Description
iswa/7.1	up/up	2	8	
iswa/7.2	up/up	6	6	

2 items

Figure 1 Ethernet LAG Summary Page

LAGs can be added by clicking the plus sign (+), and LAGs can be deleted by clicking the garbage can icon.

Step 2 Click the plus sign (+) to start the Create Link Aggregation wizard and add a LAG to Fabric Manager. Figure 2 shows this wizard.



A wizard to guide you to create an ethernet LAG.

Step 1 of 4: Define an ethernet LAG

LAG ID (1-5): * 1

LACP: □ Check to enable LACP

Description:

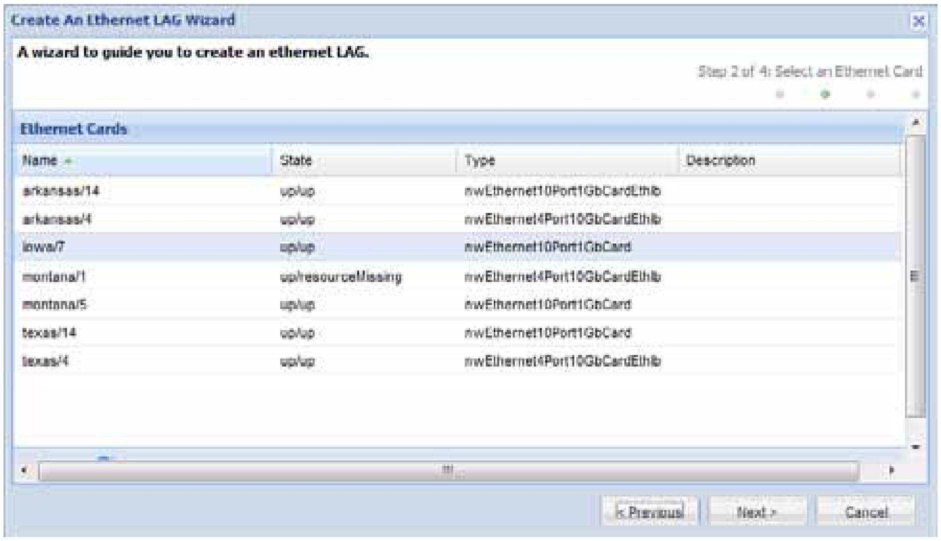
Figure 2 Create the LAG Profile

Step 3 In the *LAG ID* field, enter a number from 1 to 5 to create the LAG Profile into which you will put individual LAG ports.

Step 4 As an option, check the *LACP* checkbox to enable LACP. By default, LAG ports are not managed by LACP. Enable LACP if the peer network switch for the LAG ports is using LACP.

Step 5 As an option, in the *Description* field, enter a description string for the link aggregation group.

Step 6 Click ***Next*** to display the Select Ethernet Card dialog. Figure 3 shows this dialog.



A wizard to guide you to create an ethernet LAG.

Step 2 of 4: Select an Ethernet Card

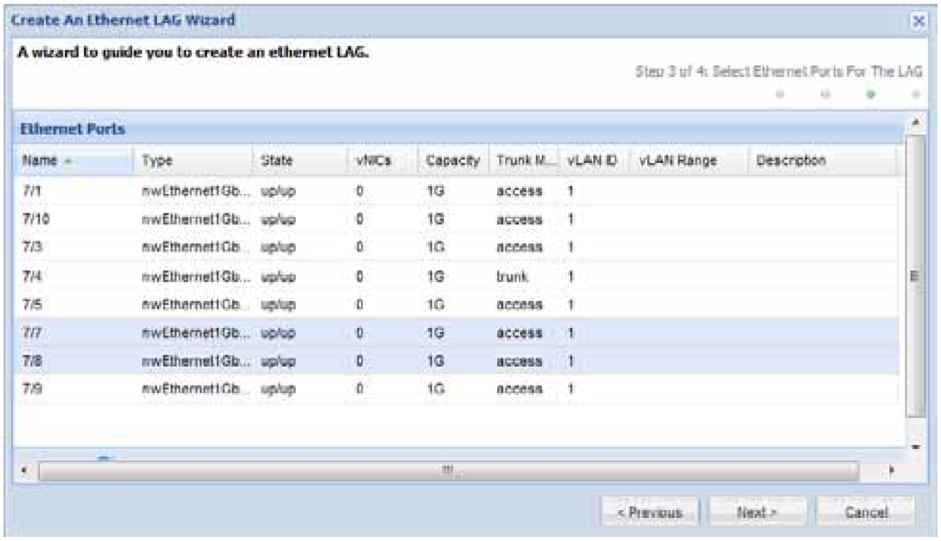
Ethernet Cards

Name	State	Type	Description
arkansas/14	up/up	nwEthernet10Port1GbCardEthIb	
arkansas/4	up/up	nwEthernet4Port10GbCardEthIb	
iowa/7	up/up	nwEthernet10Port1GbCard	
montana/1	up/resourceMissing	nwEthernet4Port10GbCardEthIb	
montana/5	up/up	nwEthernet10Port1GbCard	
texas/14	up/up	nwEthernet10Port1GbCard	
texas/4	up/up	nwEthernet4Port10GbCardEthIb	

Figure 3 Create a LAG — Select Ethernet Card for the LAG

Step 7 Select the Ethernet module on which you will be creating the LAG.

Step 8 Click ***Next*** to display the Select LAG Port dialog. Figure 4 shows this dialog.


Create An Ethernet LAG Wizard
A wizard to guide you to create an ethernet LAG.
Step 3 of 4: Select Ethernet Ports For The LAG
Ethernet Ports
< Previous
Next >
Cancel

Name	Type	State	vNICs	Capacity	Trunk M...	vLAN ID	vLAN Range	Description
7/1	nwEthernet1Gb...	up/up	0	1G	access	1		
7/10	nwEthernet1Gb...	up/up	0	1G	access	1		
7/3	nwEthernet1Gb...	up/up	0	1G	access	1		
7/4	nwEthernet1Gb...	up/up	0	1G	trunk	1		
7/5	nwEthernet1Gb...	up/up	0	1G	access	1		
7/7	nwEthernet1Gb...	up/up	0	1G	access	1		
7/8	nwEthernet1Gb...	up/up	0	1G	access	1		
7/9	nwEthernet1Gb...	up/up	0	1G	access	1		

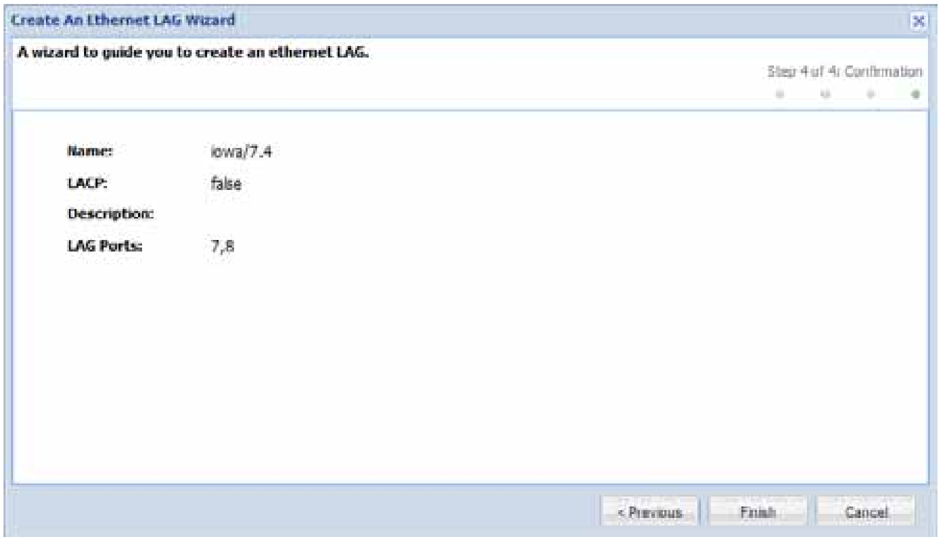
Figure 4 Create a LAG — Select Ethernet Ports for the LAG

Step 9 Select one or more Ethernet ports that will be used to create the LAG.

Note

Standard keyboard shortcuts can be used to select multiple ports in the table. For example, ***Shift*** + click and ***Ctrl*** + click allow you to select all ports or individual ports in the table.

Step 10 When the ports you want to add to the LAG are selected, click ***Next*** to display the Summary for the LAG you are creating. Figure 5 shows this page.


Create An Ethernet LAG Wizard

A wizard to guide you to create an ethernet LAG.

Step 4 of 4: Confirmation

Name: iowa/7.4
LACP: false
Description:
LAG Ports: 7,8

Figure 5 Create a LAG — Summary

Step 11 Review the information on the Summary. If any of the information is incorrect, click ***Previous*** to page backward through the wizard until you find the page where you can make the appropriate corrections.

Step 12 When the Summary contains the correct information, click ***Finish*** to create the LAG in Fabric Manager.

Step 13 Check the LAG Summary table to verify that the LAG was created. At this point, the LAG is available for use in other wizards and can be assigned to other Fabric Manager entities—for example, Network Clouds.

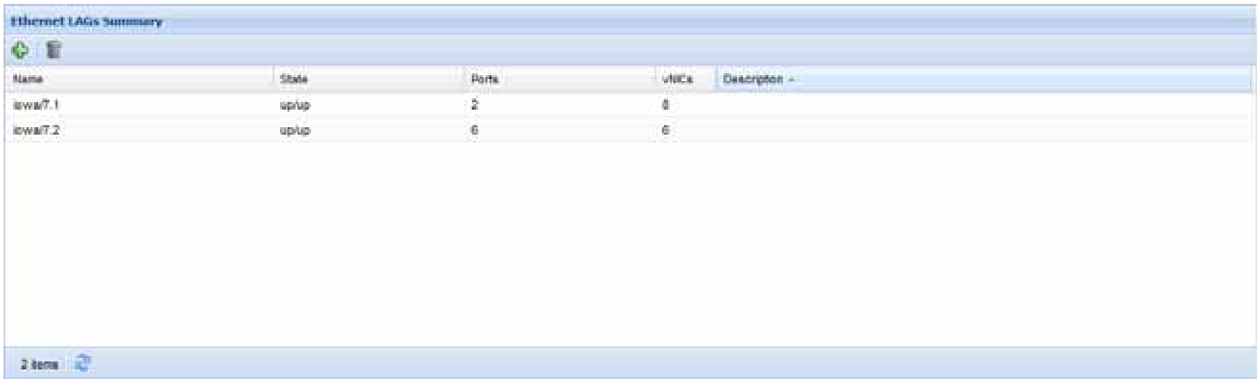
Displaying LAG Properties

Detailed information about each LAG is displayed in the LAG Details frame. When you click to select a single LAG in the LAG Summary table, details about that LAG are displayed in the frame below.

Displaying the LAG Summary

In the LAG Summary, you will notice that the naming convention uses a dot instead of a slash to separate the slot and port notation. For example, the LAG name “arkansas/14.4” indicates that LAG 4 exists on slot 14 of the Oracle Xsigo Fabric Director “arkansas”. This notation is standard for Xsigo LAGs and is also used in Oracle’s XgOS CLI.

Figure 6 shows the LAG Summary.



Ethernet LAGs Summary

Name	State	Ports	vNICs	Description
iowa/7.1	up/up	2	8	
iowa/7.2	up/up	6	6	

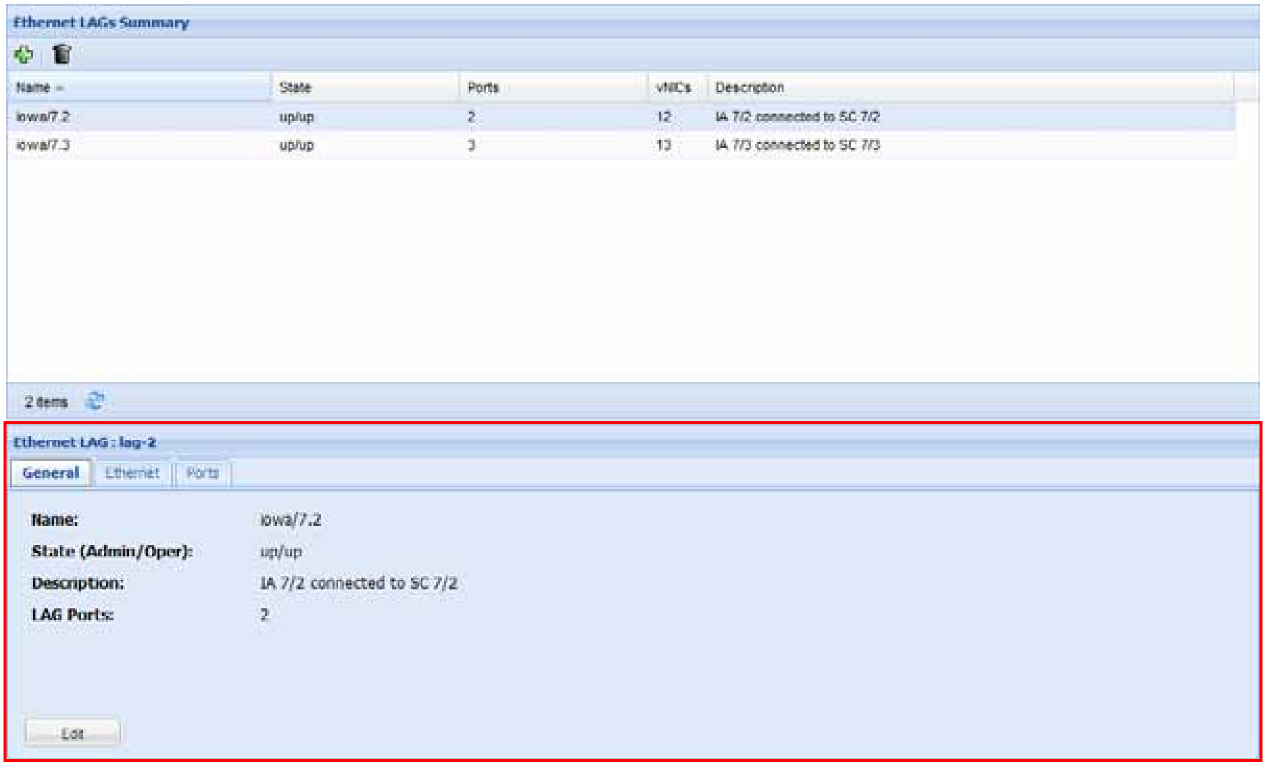
2 items

Figure 6 Link Aggregation Groups Summary

Displaying LAG Details

Details for a specific LAG are displayed in the LAG Details frame, which exists below the LAG Summary. Through the LAG Details frame, you can see additional information for a specific LAG, and also edit some LAG parameters.

Figure 7 shows the LAG Details frame.



Ethernet LAGs Summary

Name	State	Ports	vNICs	Description
iowa/7.2	up/up	2	12	IA 7/2 connected to SC 7/2
iowa/7.3	up/up	3	13	IA 7/3 connected to SC 7/3

2 items

Ethernet LAG : lag-2

Name: iowa/7.2
State (Admin/Oper): up/up
Description: IA 7/2 connected to SC 7/2
LAG Ports: 2

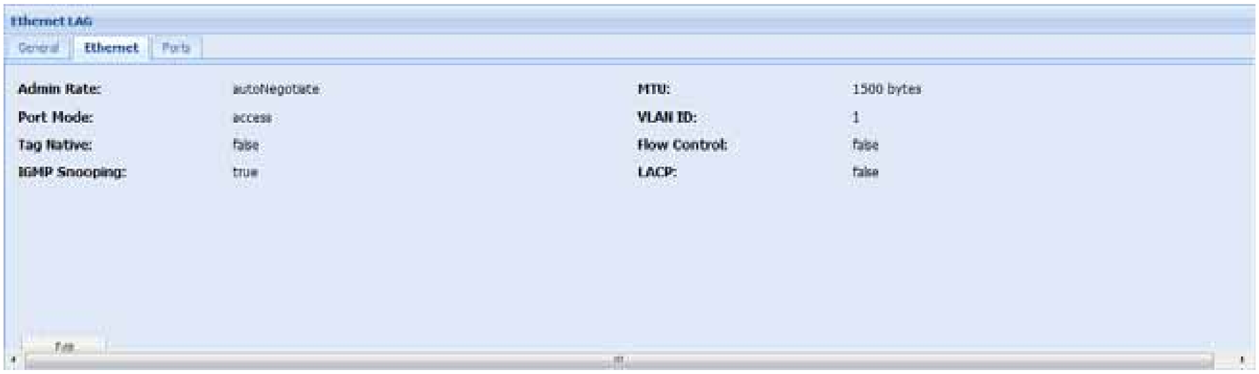
Figure 7 Ethernet LAGs Details Frame

The LAG Details frame contains the following tabs, which allow basic management and editing for a configured LAG:

- General
- Ethernet
- Ports

Displaying LAG Ethernet Properties

Fabric Manager supports Ethernet properties for the traffic that is carried on the LAG. Properties such as MTU size, VLAN ID, and others can be displayed or edited through the *Ethernet* tab on the LAG Details frame, as shown in Figure 8.



Admin Rate:	autoNegotiate	MTU:	1500 bytes
Port Mode:	access	VLAN ID:	1
Tag Native:	false	Flow Control:	false
IGMP Snooping:	true	LACP:	false

Figure 8 LAG Details — Ethernet Properties Tab

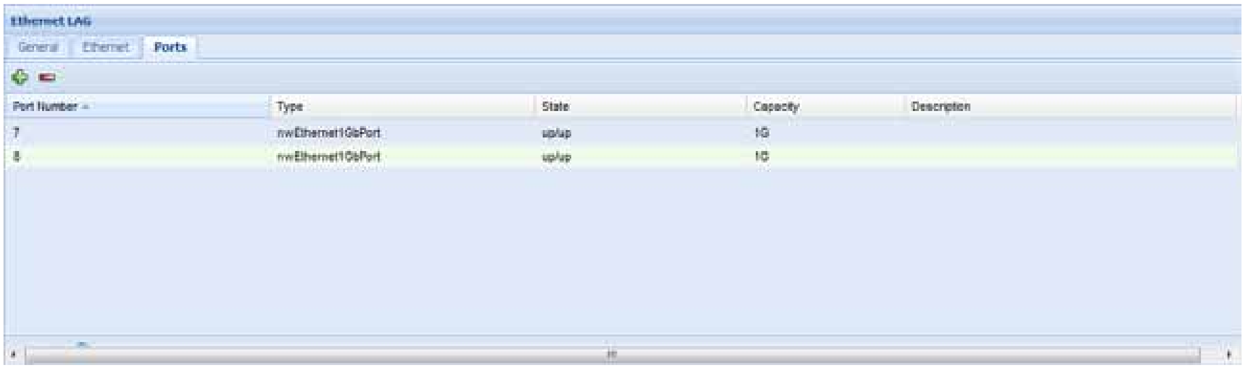
Table 1 shows the Ethernet Properties for a LAG and explains what each property means. All fields in on this tab are editable by clicking the ***Edit*** button.

Table 1 LAG Ethernet Properties

Property...	Means...
Admin Rate	The admin rate at which the network traffic is supported. This is typically 10 Gbps or lower, or auto negotiated to the highest value supported on the LAG.
MTU	The maximum transmission unit, which is the largest size data packet supported without fragmentation.
Port Mode	The VLAN mode for the port — either trunk or access.
VLAN ID	The VLAN ID supported on the port in the LAG.
Tag Native	Whether or not traffic on the port is retagged or retains its VLAN ID when the traffic is from the native VLAN.
Flow Control	Whether flow control is enabled or not on the port.
IGMP Snooping	Whether IGMP Snooping is enabled or not on the port.
LACP	Whether LACP is enabled or not on the port.

Displaying Port Properties in the LAG

Fabric Manager supports Ethernet properties for the traffic that is carried on the LAG. Properties such as MTU size, VLAN ID, and others can be displayed or edited through the *Ethernet* tab on the LAG Details frame, as shown in Figure 9.



Port Number	Type	State	Capacity	Description
7	nwEthernet1GbPort	up/up	1G	
8	nwEthernet1GbPort	up/up	1G	

Figure 9 LAG Details — Ports Tab

Table 2 shows the contents of the *Ports* tab and explains what each field on the tab means. No fields on this tab are editable.

Table 2 LAG Port Properties

Property...	Means...
Port Number	The number of individual ports in the LAG
Type	The type of port in the LAG. Typically, ports in the LAG are 1 Gbps Ethernet ports as indicated by the type string `nwEthernet1GbPort`.
State	The admin and operational state of the port in the LAG. When the port is `up/up` it is online and able to pass traffic in the LAG.
Capacity	The maximum rate of traffic that each port in the LAG can support.
Description	An optional field that contains a description for each port in the LAG.

Adding More Ports to an Existing LAG

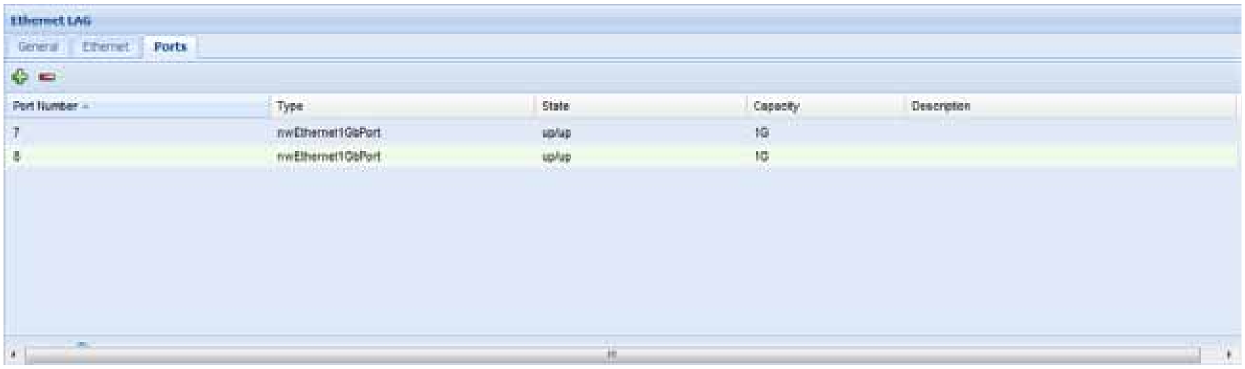
When a LAG is configured, you can add more ports to it as long as other ports are available that are not already part of another LAG. If ports are assigned to another LAG, they cannot be directly assigned into a different LAG. If you need to take a port from another LAG, you must delete it from its LAG before assigning it to another LAG.

To add more ports to an existing LAG, follow this procedure:

Step 1 On the navigation panel, select *Network Cloud Manager->Link Aggregation Groups* to display the Ethernet LAG Summary.

Step 2 On the Ethernet LAG Summary, select the LAG to which you want to add one or more ports. This step populates the Ethernet LAG Details frame.

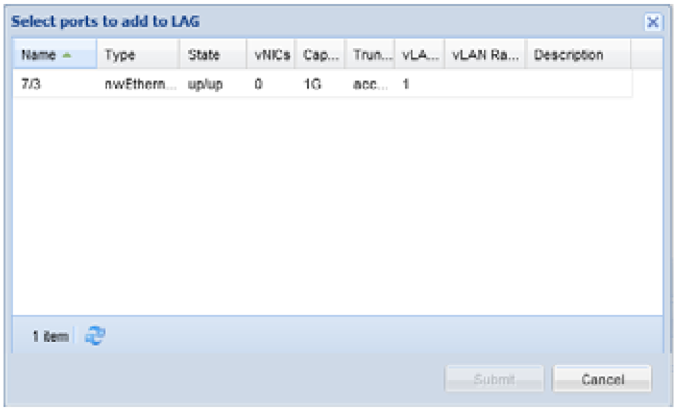
Step 3 Click the *Ports* tab to display the current port contents of the LAG, as shown in Figure 10.



Port Number	Type	State	Capacity	Description
7	nwEthernet1GbPort	up/up	1G	
8	nwEthernet1GbPort	up/up	1G	

Figure 10 LAG Details — Ports Tab

Step 4 Click the plus sign (+) to display the Select Ports to Add to LAG dialog, as shown in Figure 11.



Name	Type	State	vNICs	Cap...	Trun...	vLA...	vLAN Ra...	Description
7/3	nwEthern...	up/up	0	1G	acc...	1		

Figure 11 Select Ports to Add to LAGs

Step 5 Select the port(s) you want to add to the LAG. When at least one port is selected, the ***Submit*** button becomes active.

Step 6 Click ***Submit*** to add the port to the selected LAG.

Deleting Ports from an Existing LAG

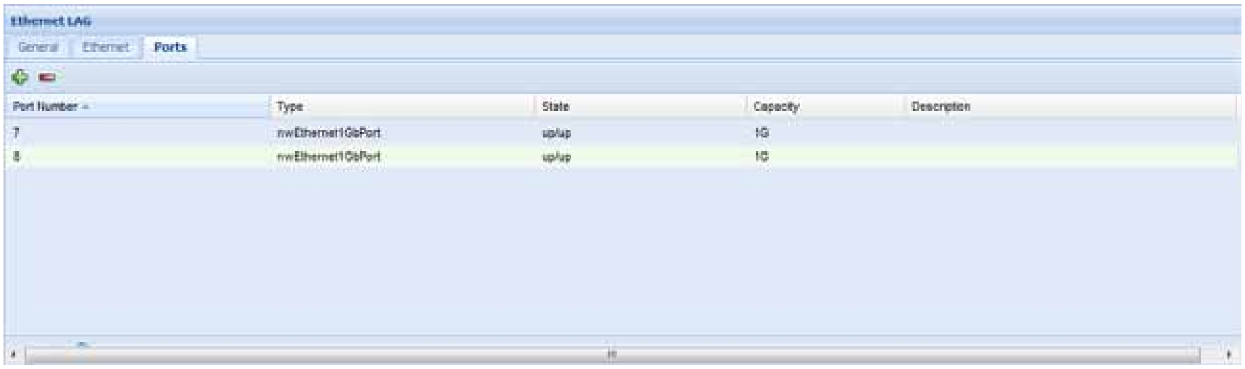
When ports are in a LAG, they can be removed to become individual ports. When you delete one or more ports from a LAG, they are then configurable as an individual network port, or they can be assigned to another LAG. It is possible to remove all ports from a LAG without deleting the LAG. In this case, the LAG exists in Oracle's Xsigo Fabric Manager as an empty LAG, which can then be assigned more ports (See Adding More Ports to an Existing LAG.)

To delete one or more ports from an existing LAG, follow this procedure:

Step 1 On the navigation panel, select *Network Cloud Manager->Link Aggregation Groups* to display the Ethernet LAG Summary.

Step 2 On the Ethernet LAG Summary, select the LAG to which you want to add one or more ports. This step populates the Ethernet LAG Details frame.

Step 3 Click the *Ports* tab to display the current port contents of the LAG, as shown in Figure 12.



Port Number	Type	State	Capacity	Description
7	nwEthernet1GbPort	up/up	1G	
8	nwEthernet1GbPort	up/up	1G	

Figure 12 LAG Details — Ports Tab

Step 4 On the *Ports* tab, select the port(s) that you want to delete from the LAG. This step activates the ***Delete a Port*** button (the red dash).

Step 5 Click the ***Delete a Port*** button to remove the selected port(s) from the LAG.

Working with Network QoS

This chapter contains the following topics:

Understanding Network QoS Profiles

A Network QoS Profile allows you to place bandwidth usage parameters on a Network Cloud or a vNIC so that specific amounts of traffic are allowed, or specific amounts of throughput are available.

Through Oracle's Xsigo Fabric Manager, network Quality of Service (QoS) ensures that bandwidth is available by using parameters to control how much traffic is allowed on Network Cloud at any given time. QoS parameters are configured within a Network QoS Profile, which is then bound to a Network Cloud or vNIC. For more information, see QoS Assignment at Cloud Level and vNIC Level.

Fabric Manager supports Network QoS through policers on Network Clouds and their underlying Ethernet links. Policers guarantee bandwidth by controlling traffic through dropping packets that exceed the peak information rate (PIR).

The Network QoS Profile uses the following parameters to guarantee bandwidth:

- Committed Information Rate (CIR), which you specify
- Peak Information Rate (PIR), which is you specify

Xsigo provides a number of pre-defined Network QoS Profiles, complete with commonly used CIR and PIR parameters for typical network usage scenarios.

Understanding Pre-Defined Network QoS Profiles

Fabric Manager contains pre-defined Network QoS Profiles. Within the pre-defined QoS Profile, one or more entries exist. Each entry is pre-configured for efficient bandwidth availability and resource usage. You can associate a pre-defined QoS Profile directly with a Network Cloud.

Multiple pre-defined QoS Profiles exist, and they have been created for different bandwidth configurations–for example a 1 Gbps bandwidth pre-defined QoS Profile, a 2 Gbps pre-defined QoS Profile, and so on.

When you are binding a QoS Profile to a Network Cloud, you can select a pre-defined QoS Profile from the list of all available QoS Profiles for that particular module.

Pre-defined QoS Profiles are supported for Network QoS. Table 1 shows each of the pre-defined Policer Profiles and the QoS parameters that the Policer Profiles contain.

Table 1 Default QoS Profiles and Network QoS Parameters Enforced

Default QoS Profile	CIR	PIR
100m_1g	100 mbps	1 gbps
100m_250m	100 mbps	250 mbps
10m_100m	10 mbps	100 mbps
10m_1g	10 mbps	1 gbps
10m_50m	10 mbps	50 mbps
1g_10g	1 gbps	9.9297 gbps
1m_10m	1 mbps	10 mbps
250m_500m	250 mbps	500 mbps

Table 1   (continued) Default QoS Profiles and Network QoS Parameters Enforced

Default QoS Profile	CIR	PIR
2g_10g	2 gbps	9.9297 gbps
3g_10g	3.00293 gbps	9.9297 gbps
4g_10g	4 gbps	9.9297 gbps
500m_750m	500 mbps	750 mbps
50m_100m	50 mbps	100 mbps
5g_10g	5.00122 gbps	9.9297 gbps
64k_1m	66 kbps	1 mbps
6g_10g	6.00587 gbps	9.9297 gbps
750m_1g	750 mbps	1 gbps
7g_10g	7.00171 gbps	9.9297 gbps
8g_10g	8 gbps	10 gbps
9g_10g	9.00212 gbps	9.9297 gbps

Displaying Network QoS Information

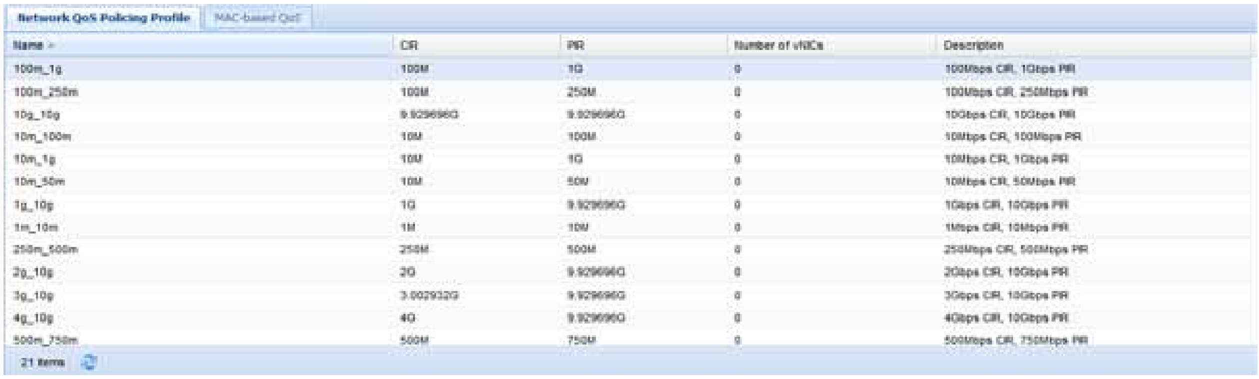
When Network QoS Profiles are configured, you can display them through the Network QoS Summary, which is a table of all Network QoS Profiles configured in Fabric Manager. Additional, detailed information about individual Network QoS Profiles is available in the Network QoS Profile Details frame below the Network QoS Profile Summary.

Displaying the Network QoS Summary

The Network QoS Summary contains all configured Network QoS Profiles in Fabric Manager regardless of whether they are assigned to a Network Cloud.

To display the Network QoS Summary, follow this procedure:

Step 1   Display the Network QoS Summary by selecting *Network Cloud Manager->Network QoS*. Figure 1 shows the Network QoS Summary.



Network QoS Policing Profile | MAC-based QoS

Name	CIR	PIR	Number of vNICs	Description
100m_1g	100M	1G	0	100Mbps CIR, 1Gbps PIR
100m_250m	100M	250M	0	100Mbps CIR, 250Mbps PIR
10g_10g	9.929696G	9.929696G	0	10Gbps CIR, 10Gbps PIR
10m_100m	10M	100M	0	10Mbps CIR, 100Mbps PIR
10m_1g	10M	1G	0	10Mbps CIR, 1Gbps PIR
10m_50m	10M	50M	0	10Mbps CIR, 50Mbps PIR
1g_10g	1G	9.929696G	0	1Gbps CIR, 10Gbps PIR
1m_10m	1M	10M	0	1Mbps CIR, 10Mbps PIR
250m_500m	250M	500M	0	250Mbps CIR, 500Mbps PIR
2g_10g	2G	9.929696G	0	2Gbps CIR, 10Gbps PIR
3g_10g	3.002932G	9.929696G	0	3Gbps CIR, 10Gbps PIR
4g_10g	4G	9.929696G	0	4Gbps CIR, 10Gbps PIR
500m_750m	500M	750M	0	500Mbps CIR, 750Mbps PIR

21 items

Figure 1 Network QoS Profiles Summary

Table 2 shows the contents of the Network QoS Summary and explains what each field means.

Table 2 Contents of the Network QoS Summary

Field	Indicates
Name	The name of each configured Network QoS Profile. The name is in the format CIR_PIR, so the “100m_ 1g” profile sets 100 Mbps of CIR and 1 Gbps of PIR.
CIR	The committed information rate, which is the amount of guaranteed bandwidth for constant traffic.
PIR	The peak information rate, which the amount of peak bandwidth for constant traffic.
Number of vNICs	The total number of vNICs that are associated with each Network QoS Profile.
Description	The description string (if any) that was applied to the Network QoS Profile. If this field is blank, either no description string was specified when the Network QoS Profile was created, or the Network QoS Profile was originally created with a description string, but the Network QoS Profile was later edited and the description string was removed.

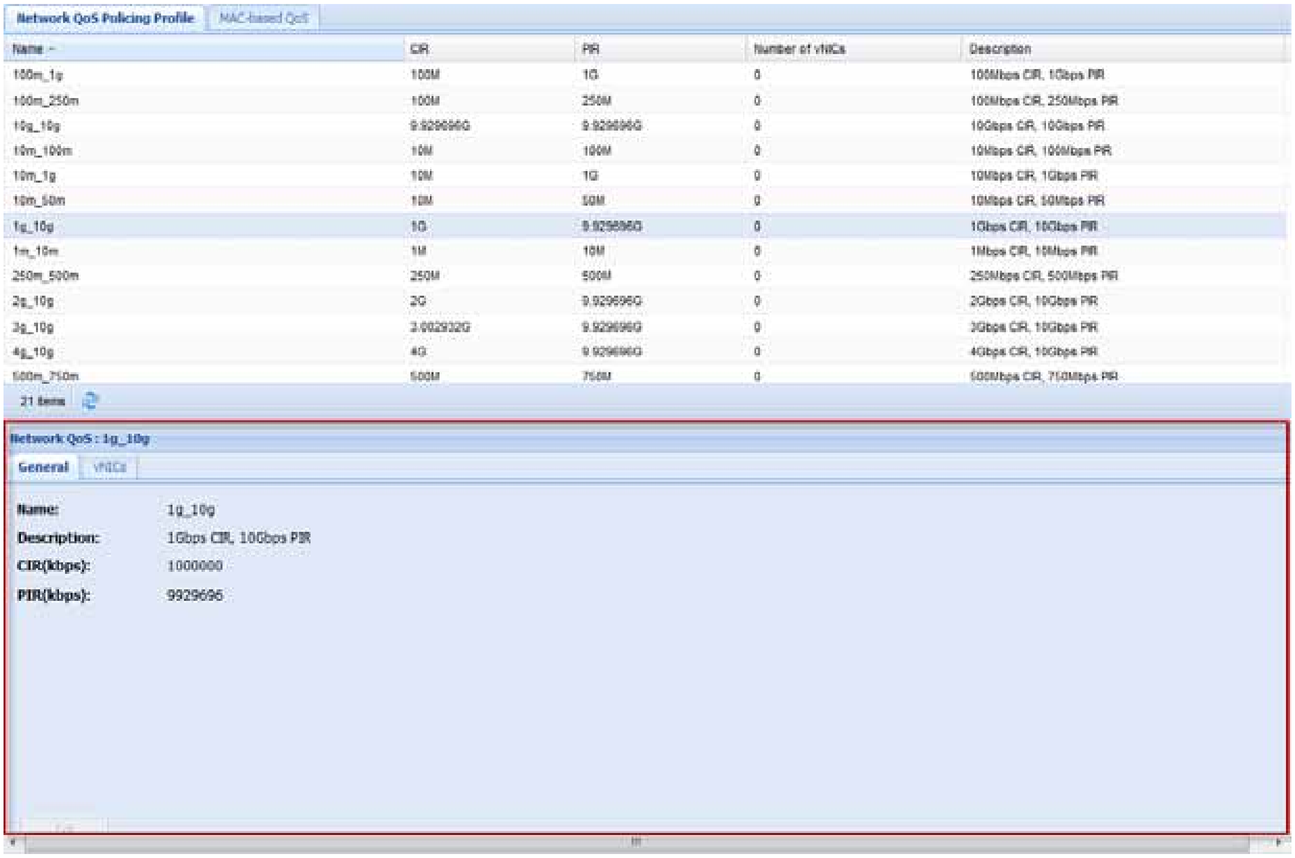
Displaying the Network QoS Details

The Network QoS Profile Details frame is a section of the work panel that is located below the Network QoS Profile Summary. This frame is a list of fields for a selected Network QoS Profile that shows the CIR and PIR policing parameters that control bandwidth usage.

The Network QoS Profile Details frame enables you to display additional, detailed information for a single Network QoS Profile and contains an ***Edit*** button, which unlocks editable parts of the details frame so that you can set or change information elements of the details frame.

To use the Network QoS Profile Details frame, you must first select a configured Network QoS Profile from the Network QoS Profile Summary. By selecting a Network QoS Profile from the summary, you provide an element that will be the focus of the Network QoS Profile Details frame. When the Network QoS Profile is selected in the summary, you will see its details displayed in the Details frame.

Figure 2 shows the Network QoS Profile Details frame. Notice that the details frame is contextual, so that it displays detailed information for the item selected in the Network Cloud Summary.



Name	CIR	PIR	Number of vNICs	Description
100m_1g	100M	1G	0	100Mbps CIR, 1Gbps PIR
100m_250m	100M	250M	0	100Mbps CIR, 250Mbps PIR
10g_10g	9.929696G	9.929696G	0	10Gbps CIR, 10Gbps PIR
10m_100m	10M	100M	0	10Mbps CIR, 100Mbps PIR
10m_1g	10M	1G	0	10Mbps CIR, 1Gbps PIR
10m_50m	10M	50M	0	10Mbps CIR, 50Mbps PIR
1g_10g	1G	9.929696G	0	1Gbps CIR, 10Gbps PIR
1m_10m	1M	10M	0	1Mbps CIR, 10Mbps PIR
250m_500m	250M	500M	0	250Mbps CIR, 500Mbps PIR
2g_10g	2G	9.929696G	0	2Gbps CIR, 10Gbps PIR
3g_10g	3.002932G	9.929696G	0	3Gbps CIR, 10Gbps PIR
4g_10g	4G	9.929696G	0	4Gbps CIR, 10Gbps PIR
500m_750m	500M	750M	0	500Mbps CIR, 750Mbps PIR

21 items

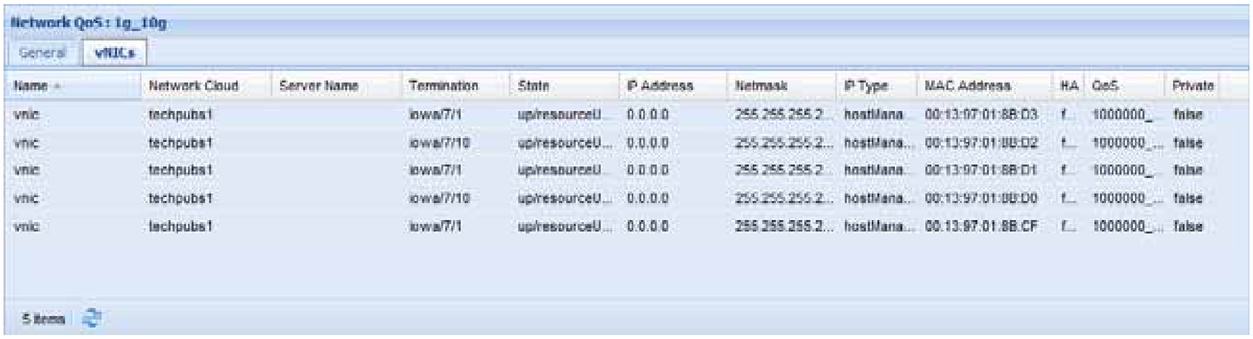
Network QoS : 1g_10g

Name: 1g_10g
Description: 1Gbps CIR, 10Gbps PIR
CIR(kbps): 1000000
PIR(kbps): 9929696

Figure 2 Network QoS Profile Details

Displaying the vNICs Using a Network QoS Profile

Through the *vNICs* tab, you can display a table of the vNICs that are currently using a specific Network QoS Profile. To display the vNICs that are using a Network QoS Profile, select a Network QoS Profile in the Network QoS Profile Summary. Then, click the *vNICs* tab to display the vNICs that are using that profile. See Figure 3.



Name	Network Cloud	Server Name	Termination	State	IP Address	Netmask	IP Type	MAC Address	HA	QoS	Private
vnic	techpubs1		iowa/7/1	up/resourceU...	0.0.0.0	255.255.255.2...	hostMana...	00:13:97:01:8B:D3	f...	1000000_...	false
vnic	techpubs1		iowa/7/10	up/resourceU...	0.0.0.0	255.255.255.2...	hostMana...	00:13:97:01:8B:D2	f...	1000000_...	false
vnic	techpubs1		iowa/7/1	up/resourceU...	0.0.0.0	255.255.255.2...	hostMana...	00:13:97:01:8B:D1	f...	1000000_...	false
vnic	techpubs1		iowa/7/10	up/resourceU...	0.0.0.0	255.255.255.2...	hostMana...	00:13:97:01:8B:D0	f...	1000000_...	false
vnic	techpubs1		iowa/7/1	up/resourceU...	0.0.0.0	255.255.255.2...	hostMana...	00:13:97:01:8B:CF	f...	1000000_...	false

5 items

Figure 3 Network QoS Details — vNICs Tab

Table 3 shows the fields in the *vNICs* tab and explains what each field means.

Table 3 Contents of the vNICs Tab

Field	Indicates
Name	The name of each configured vNIC that is using the Network QoS profile.
Network Cloud	The name of the Network Cloud to which the vNICs are connected.
Server Name	The name of all servers connected to the vNIC.
Termination	The termination point for the vNICs. The termination point is either a port which is displayed in slot/port notation, or a LAG which is displayed in `slot.port` notation.
State	The administrative and operational state of the vNICs that are using the selected Network QoS profile.
IP Address	The IP address of each vNIC that is using the Network QoS Profile.
Netmask	The network mask for each vNIC that is using the Network QoS Profile.
IP Type	The method by which the IP address for the vNIC was assigned. Valid values are: • Static, for a statically assigned IP address. • DHCP, for an address that was assigned through DHCP. • Host managed, for an address that was assigned by the host instead of through the Oracle Xsigo Fabric Director.

Table 3 (continued) Contents of the vNICs Tab

Field	Indicates
MAC Address	The MAC address of each vNIC that is using the Network QoS Profile. MAC addresses can either be statically assigned by you, or automatically assigned from the Oracle Xsigo Fabric Director's MAC address pool.
HA	The state of high availability for each vNIC that is using the Network QoS Profile: • If this field displays false, then the vNIC is not part of an HA pair. • If this field displays true, then the vNIC is either the primary or secondary vNIC in an HA vNIC pair.
QoS	The bandwidth usage parameters for each vNIC. The name is in the format CIR_PIR in megabits per second.
Private	Whether the individual vNICs shown are Private vNICs: • If the field displays true, the vNIC is a Private vNIC. Private vNICs are used in vNIC-to-vNIC switching to ensure enhanced security and isolation from standard "public" vNICs. • If the field displays false, the vNIC is not a Private vNICs. Instead, it is a standard public vNIC.

Understanding MAC-Based QoS

In addition to network QoS which governs the amount of bandwidth used on vNICs, Fabric Manager also supports MAC-Based QoS. MAC-Based QoS is a method of controlling which devices on a vNIC can use specific amounts of bandwidth. Through MAC-Based QoS, Fabric Manager supports assigning a usage condition to traffic sent or received by a specific network device, which is identified by its MAC address. The usage condition are enforced by QoS application flows.

When you configure MAC-Based QoS, you set conditions for a specific device address on a vNIC. When MAC-Based QoS is configured on a vNIC, the actual match against traffic on the vNIC occurs at the I/O Card level, so traffic will be controlled at the chip that controls the vNIC's termination port.

A MAC-Based QoS Profile is composed of the following information elements:

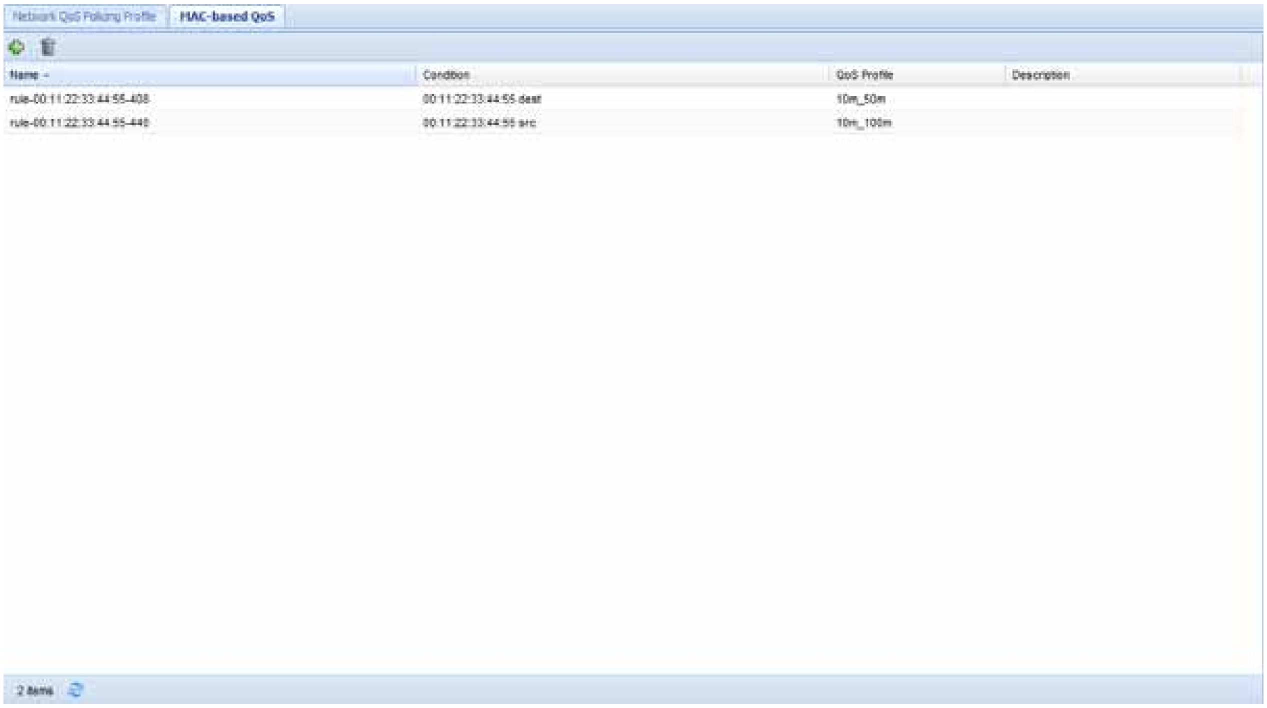
- a MAC Address, which is the MAC address of a shared vNIC—for example, a vNIC deployed on a VM. If a vNIC is deployed on a physical server, there is no need to configure a MAC-Based QoS Profile because the vNIC has only one MAC address. As a result, MAC-Based QoS Profiles are not configurable in a non-VM environment.
- Network QoS Profile, which controls the amount of bandwidth and traffic that can be used on the shared vNIC.
- Direction, which determines a traffic flow for the Network QoS Profile.
- an optional description.

MAC-Based QoS Profiles are useful on a shared vNIC, which occurs when multiple devices are supported on the same vNIC, and each device requires a different QoS flow to or from the device (ingress or egress) or both.

Displaying MAC-Based QoS

Fabric Manager supports MAC-Based QoS as an option to the Network QoS feature. MAC-Based QoS is available as a tab through the Network QoS Summary. This option displays the MAC-Based QoS Summary, which is a table of all the configured MAC-Based QoS profiles.

Figure 4 shows the MAC-Based QoS Summary.



Name -	Condition	QoS Profile	Description
rule-00:11:22:33:44:55-408	00:11:22:33:44:55 dest	10m_50m	
rule-00:11:22:33:44:55-440	00:11:22:33:44:55 src	10m_100m	

Figure 4 MAC-Based QoS Profile Summary

Table 4 shows the contents of the MAC-Based QoS Profile Summary and explains what each field means.

Table 4 Contents of the MAC-Based QoS Profile Summary

Field	Indicates
Name	The name of the MAC-Based QoS Profile, which is generated from the specified MAC Address.

Table 4 (continued) Contents of the MAC-Based QoS Profile Summary

Field	Indicates
Condition	The specific MAC-Based QoS Profile conditions created. These conditions consist of the MAC Address specified plus either source (src) or destination (dest) which refers to the direction on which the QoS flow will be applied to traffic.
QoS Profile	The name of each configured Network QoS Profile associated with each MAC-Based QoS Profile. The name is in the format CIR_PIR, so the “100m_ 1g” profile sets 100 Mbps of CIR and 1 Gbps of PIR.
Description	The description string (if any) that was applied to the MAC-Based QoS Profile. If this field is blank, either no description string was specified when the MAC-Based QoS Profile was created, or the MAC-Based QoS Profile was originally created with a description string which was later edited and the description string was removed.

Configuring a MAC-Based QoS Profile

Fabric Manager supports MAC-Based QoS through the Network QoS Profile icon in the Navigation Panel. The Network QoS Profile object leads to the Network QoS Profile Summary which has a separate tab for MAC-Based QoS. The *MAC-Based QoS* tab displays the summary list of all configured MAC-Based QoS profiles. Through the *MAC-Based QoS* tab, you can add, configure, and delete specific MAC-Based QoS Profiles.

As part of configuring a MAC-Based QoS Profile, you will associate the shared vNIC’s MAC address with a Network QoS Policing Profile. Before beginning the MAC-Based QoS Profile configuration procedure, make sure that the Network QoS Profile exists so that it is a selectable option.

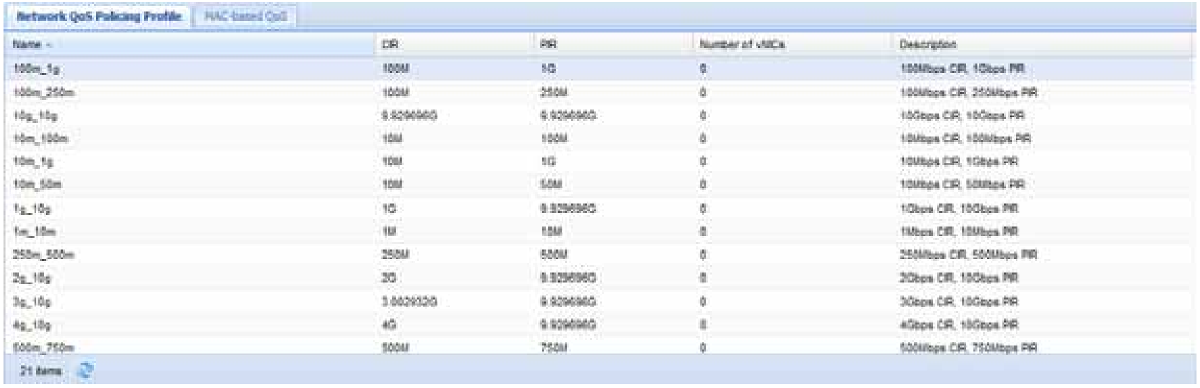
Creating a MAC-Based QoS Profile

When you create a MAC-Based QoS Profile, you are creating a profile that applies a pre-defined Network QoS Profile to a specific MAC address. You are also determining the direction on which the Network QoS flow is applied, either ingress, egress, or both. Traffic on a shared vNIC that originates from, or is destined to, the MAC address will be controlled based on the Network QoS profile.

You can create an MAC-Based QoS Profile through the plus sign (+) on the MAC-Based QoS Profile Summary.

To create a MAC-Based QoS Profile, follow this procedure:

Step 1 On the navigation panel, click *Network Cloud Manager->Network QoS* to display the Network QoS Profile Summary page. Figure 5 shows this page.

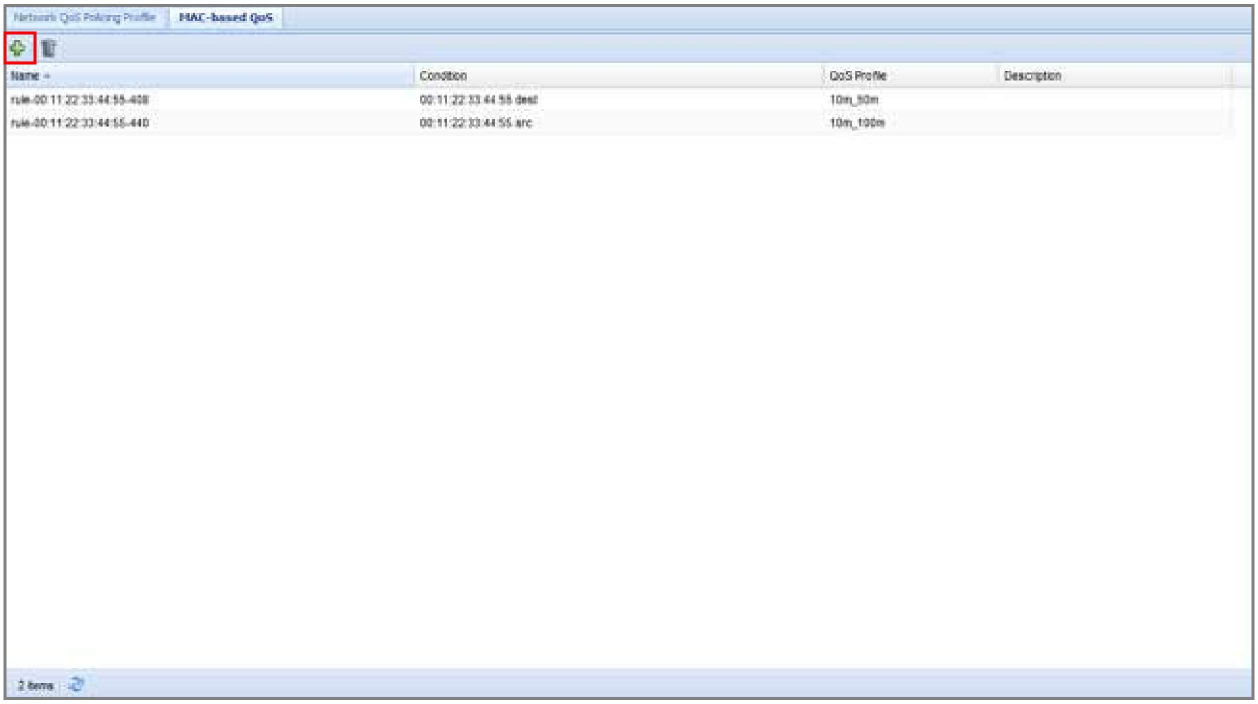


Name ⌄	CIR	PIR	Number of vNICs	Description
100m_1g	100M	1G	0	100Mbps CIR, 1Gbps PIR
100m_250m	100M	250M	0	100Mbps CIR, 250Mbps PIR
10g_10g	9.929696G	9.929696G	0	10Gbps CIR, 10Gbps PIR
10m_100m	10M	100M	0	10Mbps CIR, 100Mbps PIR
10m_1g	10M	1G	0	10Mbps CIR, 1Gbps PIR
10m_50m	10M	50M	0	10Mbps CIR, 50Mbps PIR
1g_10g	1G	9.929696G	0	1Gbps CIR, 10Gbps PIR
1m_10m	1M	10M	0	1Mbps CIR, 10Mbps PIR
250m_500m	250M	500M	0	250Mbps CIR, 500Mbps PIR
2g_10g	2G	9.929696G	0	2Gbps CIR, 10Gbps PIR
3g_10g	3.002932G	9.929696G	0	3Gbps CIR, 10Gbps PIR
4g_10g	4G	9.929696G	0	4Gbps CIR, 10Gbps PIR
500m_750m	500M	750M	0	500Mbps CIR, 750Mbps PIR

21 items

Figure 5 Network QoS Profile Summary

Step 2 On the Network QoS Summary, click the *MAC-Based QoS* tab to display the MAC-Based QoS Summary. Figure 6 shows this dialog.



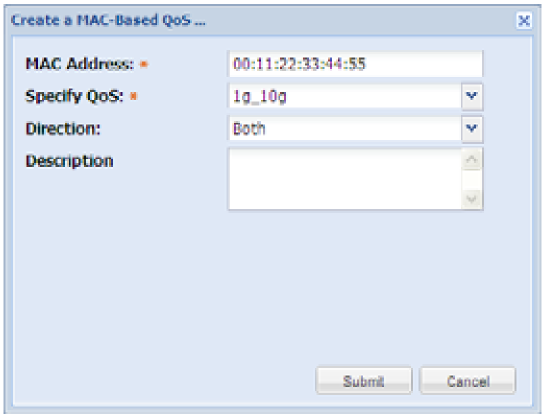
Name ⌄	Condition	QoS Profile	Description
rule-00:11:22:33:44:55-408	00:11:22:33:44:55 dest	10m_50m	
rule-00:11:22:33:44:55-440	00:11:22:33:44:55 src	10m_100m	

2 items

Figure 6 MAC-Based QoS Summary

Notice that you can create or delete MAC-Based QoS Profiles by clicking the plus sign (+) or garbage can, respectively. Also, notice that the MAC-Based QoS feature has a Summary, but no details frame for individual MAC-Based QoS Profiles.

Step 3 Click the plus sign (+) to display the Create a MAC-Based QoS dialog. Figure 7 shows this dialog.



Create a MAC-Based QoS ...

MAC Address: * 00:11:22:33:44:55
Specify QoS: * 1g_10g
Direction: Both
Description

Figure 7 Create MAC-Based QoS Profile

Step 4 In the *MAC Address* field enter the MAC Address for the shared vNIC.

Step 5 From the *Specify QoS* dropdown menu, select the QoS Profile that you want to assign to the vNIC for the specific application.

Step 6 From the *Direction* dropdown menu, select a direction (or both) to which the MAC-Based QoS Profile will be applied.

Step 7 As an option, in the *Description* field, enter a description for the MAC-Based QoS Profile that you are creating.

Step 8 Click ***Submit*** to create the MAC-Based QoS Profile.

Step 9 As needed, repeat this procedure as needed to create any additional MAC-Based QoS Profiles for individual MAC addresses on the shared vNIC.

Deleting MAC-Based QoS Profiles

When a MAC-Based QoS Profile is configured, it is displayed in the MAC-Based QoS Summary page. Any configured MAC-Based QoS Profile can be deleted through the garbage can icon on the MAC-Based QoS Profile Summary.

If multiple MAC-Based QoS Profiles exist, you can delete multiple profiles by selecting multiple entries then deleting them. Selecting multiple instances in the MAC-Based QoS Profile Summary is supported though standard keyboard conventions—for example, ***CTRL*** + click or ***ALT*** + click.

When you attempt to delete a MAC-Based QoS Profile, Oracle's Xsigo Fabric Manager prompts you with a pop-up dialog to requires you to confirm the deletion. As a result, if you have selected the wrong MAC-Based QoS Profile, you have a chance to correct the error before committing the deletion.

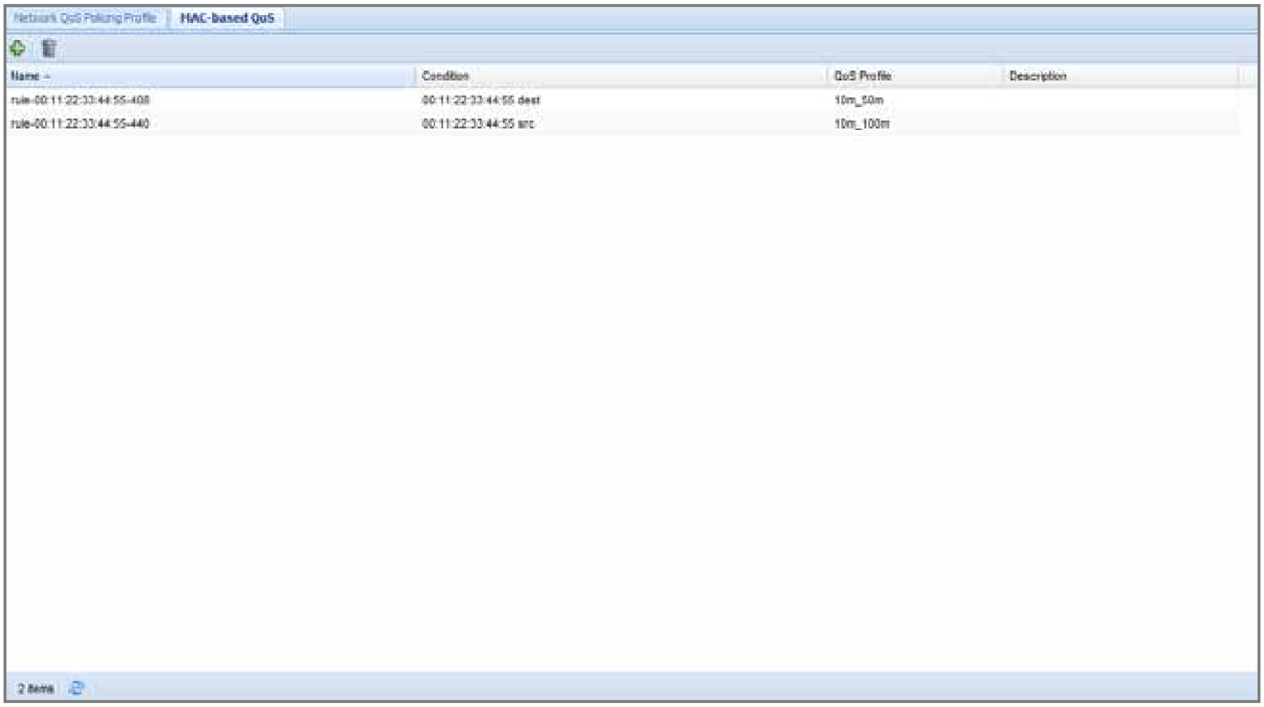
Deleting a MAC-Based QoS Profile

When you delete a MAC-Based QoS Profile, the deletion is immediate after the confirmation dialog is answered. When deleted, the MAC-Based QoS Profile that matches against a specific traffic flow is no longer applied, so the traffic flow is not affected.

To delete an MAC-Based QoS Profile, follow this procedure:

Step 1 From the navigation panel, select *Network Cloud Manager->Network QoS* to display the Network QoS Profile Summary.

Step 2 Click the *MAC-Based QoS* tab to display the MAC-Based QoS Summary. Figure 8 shows this page.

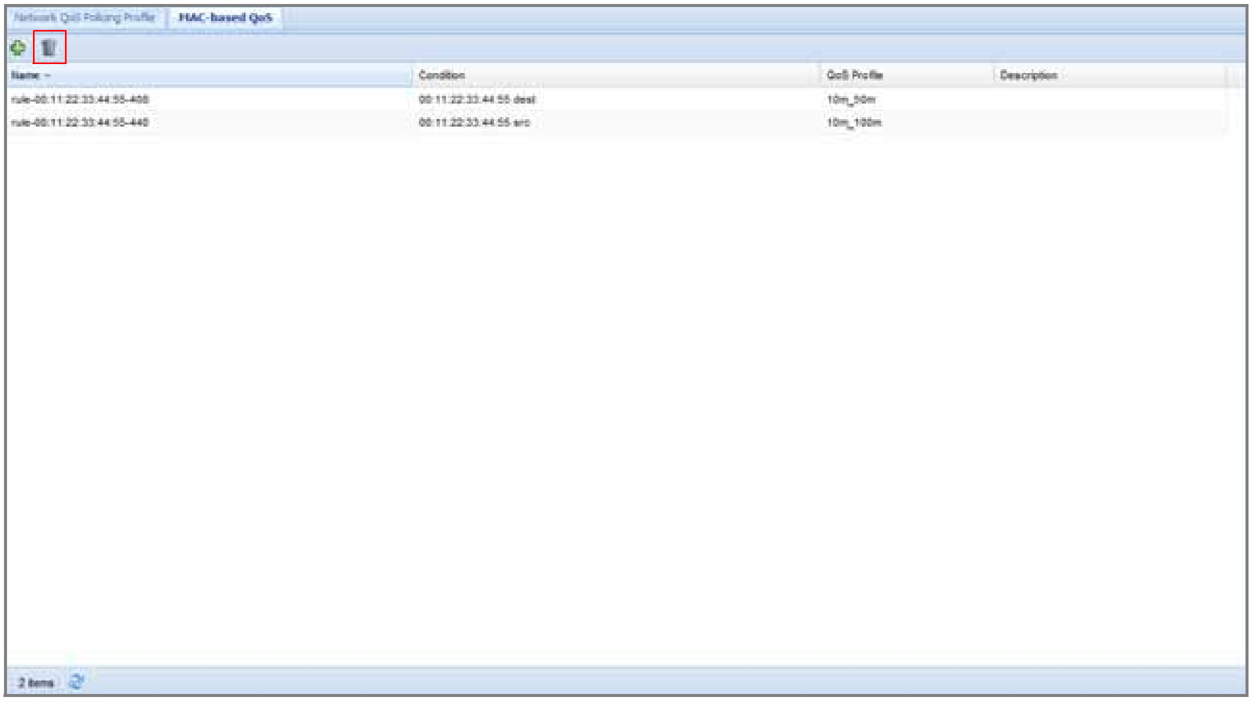


Name ▲	Condition	QoS Profile	Description
rule-00:11:22:33:44:55-408	00:11:22:33:44:55 dest	10m_50m	
rule-00:11:22:33:44:55-440	00:11:22:33:44:55 src	10m_100m	

Figure 8 MAC-Based QoS Summary

Step 3 Click the MAC-Based QoS Profile that you want to delete. The entry is selected when it is highlighted.

Step 4 Click the garbage can icon to delete the selected MAC-Based QoS Profile as shown Figure 9.



Name	Condition	QoS Profile	Description
rule-00:11:22:33:44:55-400	00:11:22:33:44:55 dest	10m_50m	
rule-00:11:22:33:44:55-440	00:11:22:33:44:55 src	10m_100m	

Figure 9 MAC-Based QoS Summary — Deleting a MAC-Based QoS Profile

When you click the garbage can icon, a confirmation dialog is displayed to verify that you want to delete the selected MAC-Based QoS Profile.

Step 5 When the confirmation dialog is displayed, click ***OK*** to complete the deletion.

Working with Physical Servers

This chapter documents the following topics:

- Displaying All Physical Servers
- Displaying Physical Server Details
- Scanning for New Servers or Removing Stale Servers
- Saving a Server Configuration as a Template
- Connecting an I/O Profile to a Server
- Disconnecting an I/O Profile from a Server
- Creating a Server Group from Selected Servers

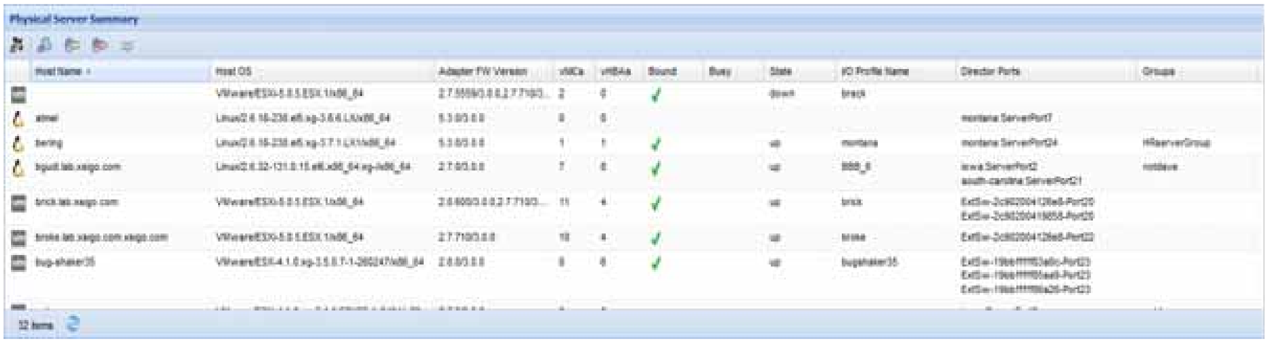
Displaying All Physical Servers

Physical servers are the host devices on which your applications run. They connect to the Oracle Xsigo Fabric Director through high-speed interconnect HCAs that are installed in each server. The Fabric Director and Oracle's Xsigo Fabric Manager support the commonly used server types including Linux, Windows, Citrix, and VMware. For information about specific OSes and hypervisors supported, see the Compatibility Matrix.

Fabric Manager discovers servers that are connected through the Fabric Director and have Xsigo host drivers installed. When Fabric Manager discovers physical servers, they are displayed in the Physical Servers Summary. Fabric Manager supports displaying summary and detailed information for physical servers.

To display the Physical Server Summary, follow this procedure:

Step 1 Select *Server Resource Manager->Physical Servers*. Figure 1 shows the Physical Server Summary.



Physical Server Summary

Host Name	Host OS	Adapter FW Version	vNICs	vHBAs	Bound	Busy	State	IO Profile Name	Director Ports	Groups
	VMware/ESXi-5.0.0.ESX.1/x86_64	2.7.5559/3.0.0,2.7.710/3...	2	0	✓		down	brack		
atmel	Linux/2.6.18-238.el5.xg-3.6.4.LX/x86_64	5.3.0/3.0.0	0	0					montana.ServerPort7	
bering	Linux/2.6.18-238.el5.xg-3.7.1.LX1/x86_64	5.3.0/3.0.0	1	1	✓		up	montana	montana.ServerPort24	HRserverGroup
bigsub.lab.xsigo.com	Linux/2.6.32-131.0.15.el6.x86_64.xg-/x86_64	2.7.0/3.0.0	7	6	✓		up	BBB_6	iowa.ServerPort2 south-carolina.ServerPort21	notdave
brick.lab.xsigo.com	VMware/ESXi-5.0.0.ESX.1/x86_64	2.6.600/3.0.0,2.7.710/3...	11	4	✓		up	brick	ExtSw-2c902004126e8-Port20 ExtSw-2c902004119858-Port20	
broke.lab.xsigo.com.xsigo.com	VMware/ESXi-5.0.0.ESX.1/x86_64	2.7.710/3.0.0	10	4	✓		up	broke	ExtSw-2c902004126e8-Port22	
bug-shaker35	VMware/ESX-4.1.0.xg-3.5.0.7-1-260247/x86_64	2.6.0/3.0.0	8	6	✓		up	bugshaker35	ExtSw-19bbffff53a0c-Port23 ExtSw-19bbffff50ae8-Port23 ExtSw-19bbffff58a26-Port23	

12 items

Figure 1 Physical Server Summary

Table 1 shows the contents of the Physical Server summary and explains what each field means.

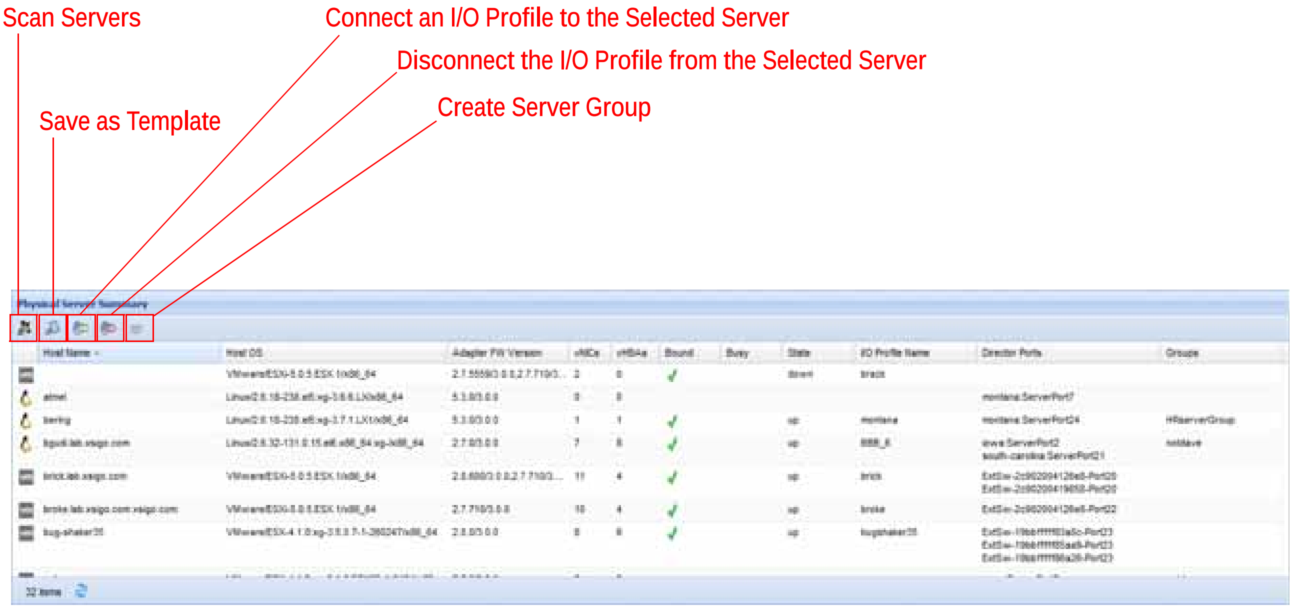
Table 1 Contents of the Physical Servers Table

Field	Indicates
Host Name	The name of each physical server that Fabric Manager has discovered. If a name has been assigned to the server, that name appears in this field. Otherwise, the GUID of the HCA that connects the server and Fabric Director is displayed. The name listed is a link to the Server Details frame. You can click this link to display additional information about a selected physical server.
Host OS	The Operating System currently in use on the host server.
Adapter FW Version	The version of Xsigo host driver or HCA firmware currently in use on the host or HCA.
vNICs	The total number of vNICs that are configured on the physical server.
vHBAs	The total number of vHBAs that are configured on the physical server.

Table 1 (continued) Contents of the Physical Servers Table

Field	Indicates
Bound	The state of whether or not the server is bound to an I/O Profile. A checkmark indicates that the server is bound. If this field shows no checkmark, the server is available for binding to an I/O Profile, but is not currently bound.
Busy	Whether Fabric Manager is busy with an operation related to the server, such as binding or unbinding an I/O Profile.
State	The current administrative state of the physical server. Valid values are: • Up • Down • Unbound • Initializing • Partial
I/O Profile Name	The name of the I/O Profile bound (if any) to each server.
Director Ports	The port string for the InfiniBand port on which the physical server is connected to the Fabric Director. The port string consists of the Fabric Director name, and the Server Port number separated by a colon (:). For example, iowa:ServerPort18 indicates that the host server is connected to the Fabric Director named “iowa” through port 18 on iowa’s InfiniBand fabric board. If the host server is connected to multiple Fabric Directors, a port string is displayed for each connection, and the individual port strings are arranged in a vertical list (as shown in Figure 1). As an example, see the entry iowa:ServerPort2 south-carolina:ServerPort21 This entry indicates two individual connections—one connection to the Fabric Director name “iowa” and the other connection to the Fabric Director named “south-carolina.” If the host server is connected through an intervening InfiniBand switch, the switch’s GUID is listed in this field. For example, the value `ExtSw-2c902004126e8-Port20` indicates a connection to an intervening IB switch between the host server and the Fabric Director.
Groups	The name of the Server Group(s) (if any) to which the selected server belongs.

The Physical Server Summary also contains various controls for creating and managing listed servers. Figure 2 shows the different controls.



Scan Servers
Connect an I/O Profile to the Selected Server
Disconnect the I/O Profile from the Selected Server
Save as Template
Create Server Group
Physical Server Summary

	Host Name	Host OS	Adapter FW Version	vNICs	vHBAs	Bound	Busy	State	I/O Profile Name	Director Ports	Groups
		VMware/ESXi-5.0.5.ESX.1/x86_64	2.7.5556/3.0.0,2.7.710/3....	2	0	✓		down	brack		
	atmel	Linux/2.6.18-238.el5.xg-3.6.6.LX/x86_64	5.3.0/3.0.0	0	0					montana.ServerPort7	
	bering	Linux/2.6.18-238.el5.xg-3.7.1.LX/x86_64	5.3.0/3.0.0	1	1	✓		up	montana	montana.ServerPort24	HRserverGroup
	bigudi.lab.xsigo.com	Linux/2.6.32-131.0.15.el6.x86_64.xg-/x86_64	2.7.0/3.0.0	7	8	✓		up	888_6	iowa.ServerPort2 south-carolina.ServerPort21	notdave
	brick.lab.xsigo.com	VMware/ESXi-5.0.5.ESX.1/x86_64	2.8.600/3.0.0,2.7.710/3....	11	4	✓		up	brick	ExtSw-2c902004126e8-Port20 ExtSw-2c902004190S8-Port20	
	broke.lab.xsigo.com.xsigo.com	VMware/ESXi-5.0.5.ESX.1/x86_64	2.7.710/3.0.0	10	4	✓		up	broke	ExtSw-2c902004126e8-Port22	
	bug-shaker35	VMware/ESX-4.1.0.xg-3.5.3.7-1-260247/x86_64	2.8.0/3.0.0	8	8	✓		up	bugshaker35	ExtSw-1f8bbffff83a5c-Port23 ExtSw-1f8bbffff85ae8-Port23 ExtSw-1f8bbffff86a28-Port23	

32 items

Figure 2 Physical Server Summary — Server Controls

Through the Physical Sever Summary, you can perform the following tasks:

- Saving a Server Configuration as a Template
- Connecting an I/O Profile to a Server
- Disconnecting an I/O Profile from a Server
- Creating a Server Group from Selected Servers

Displaying Physical Server Details

For each physical server in the Physical Servers table, you can display detailed information. Detailed server information is available through the Physical Server Details frame. Server details are available for individual servers by selecting a server in the Physical Server Summary, which provides the focus for the details frame.

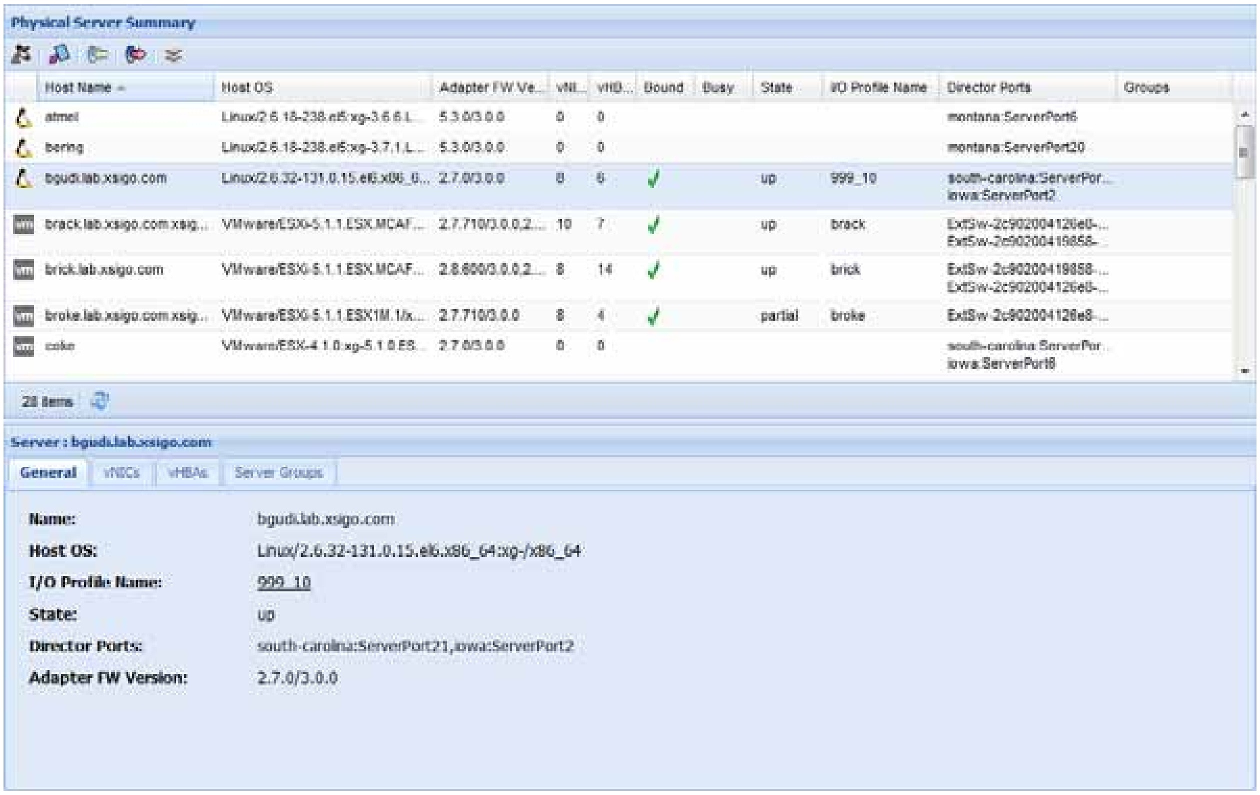
The Physical Server Details frame contains tabs that organize information about the server into logical groups. The following tabs are supported:

- General
- vNICs
- vHBAs
- Server Groups

To display the Physical Server Details frame, follow this procedure:

Step 1 Select *Server Resource Manager->Physical Servers*. Figure 1 shows the Physical Server Summary.

Step 2 Select a server in the Physical Server Summary to display the server in the details frame, as shown in Figure 3.



Physical Server Summary

	Host Name	Host OS	Adapter FW Ve...	vNI...	vHB...	Bound	Busy	State	I/O Profile Name	Director Ports	Groups
	atmel	Linux/2.6.18-238.el5:xg-3.6.6.L...	5.3.0/3.0.0	0	0					montana:ServerPort6	
	bering	Linux/2.6.18-238.el5:xg-3.7.1.L...	5.3.0/3.0.0	0	0					montana:ServerPort20	
	bgudi.lab.xsigo.com	Linux/2.6.32-131.0.15.el6.x86_6...	2.7.0/3.0.0	8	6	✓		up	999_10	south-carolina:ServerPor... iowa:ServerPort2	
vm	brack.lab.xsigo.com.xsig...	VMware/ESXi-5.1.1.ESX.MCAF...	2.7.710/3.0.0.2...	10	7	✓		up	brack	ExtSw-2c902004126e0-... ExtSw-2c90200419858-...	
vm	brick.lab.xsigo.com	VMware/ESXi-5.1.1.ESX.MCAF...	2.8.600/3.0.0.2...	8	14	✓		up	brick	ExtSw-2c90200419858-... ExtSw-2c902004126e0-...	
vm	broke.lab.xsigo.com.xsig...	VMware/ESXi-5.1.1.ESX1M.1/x...	2.7.710/3.0.0	8	4	✓		partial	broke	ExtSw-2c902004126e8-...	
vm	coke	VMware/ESX-4.1.0:xg-5.1.0.ES...	2.7.0/3.0.0	0	0					south-carolina:ServerPor... iowa:ServerPort8	

28 items

Server : bgudi.lab.xsigo.com

Name:	bgudi.lab.xsigo.com
Host OS:	Linux/2.6.32-131.0.15.el6.x86_64:xg-/x86_64
I/O Profile Name:	999_10
State:	up
Director Ports:	south-carolina:ServerPort21,iowa:ServerPort2
Adapter FW Version:	2.7.0/3.0.0

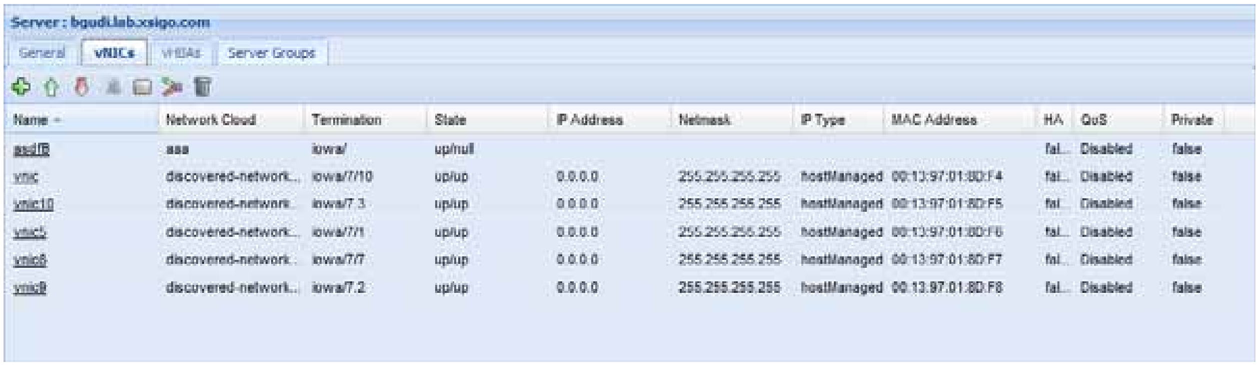
Figure 3 Physical Server Details Frame — General

Managing vNICs on a Physical Server

When a physical server is bound to an I/O Profile, it has virtual connectivity through vNICs, vHBAs, or both. When a server has vNICs deployed on it, they are listed on the *vNICs* tab for the selected server. The *vNICs* tab provides the following functionality:

- it displays information about each vNIC deployed on the sever.
- it provides ways to manage the vNICs.
- it lists vNICs by name, and the name is a link to additional details about each vNIC's individual properties.

Figure 4 shows the *vNICs* tab of the Physical Server Details frame.

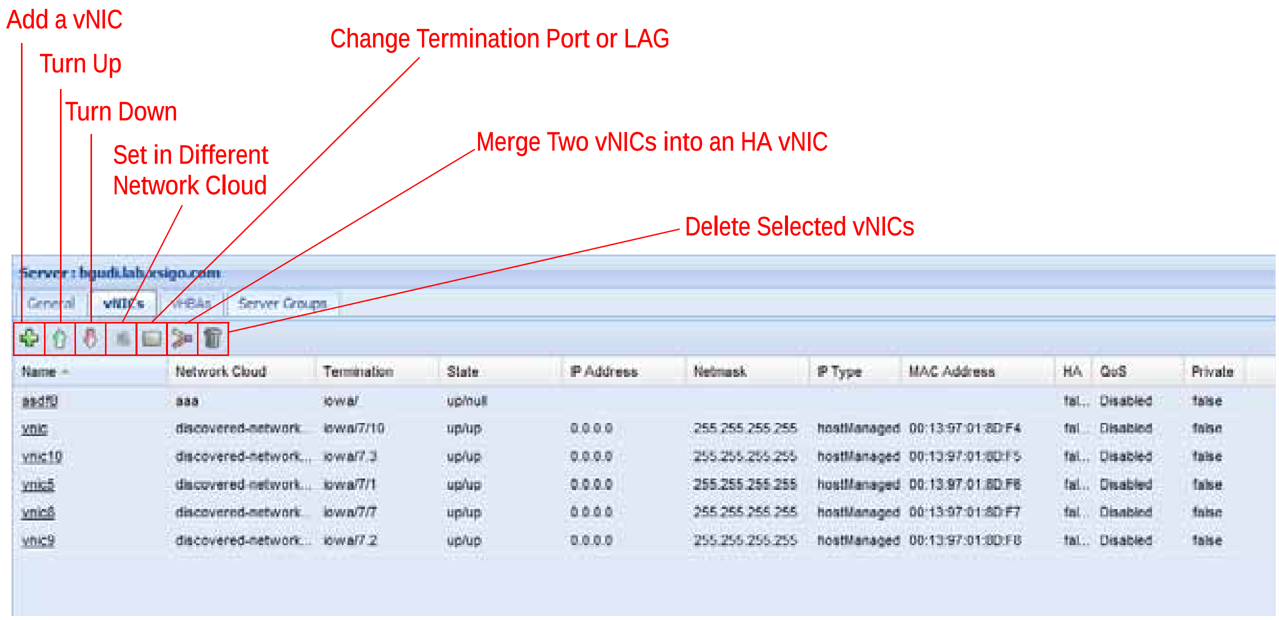


Server : bgudi.lab.xsigo.com

Name	Network Cloud	Termination	State	IP Address	Netmask	IP Type	MAC Address	HA	QoS	Private
asdfB	aaa	iowa/	up/null					fal...	Disabled	false
vnic	discovered-network...	iowa/7/10	up/up	0.0.0.0	255.255.255.255	hostManaged	00:13:97:01:8D:F4	fal...	Disabled	false
vnic10	discovered-network...	iowa/7.3	up/up	0.0.0.0	255.255.255.255	hostManaged	00:13:97:01:8D:F5	fal...	Disabled	false
vnic5	discovered-network...	iowa/7/1	up/up	0.0.0.0	255.255.255.255	hostManaged	00:13:97:01:8D:F6	fal...	Disabled	false
vnic6	discovered-network...	iowa/7/7	up/up	0.0.0.0	255.255.255.255	hostManaged	00:13:97:01:8D:F7	fal...	Disabled	false
vnic8	discovered-network...	iowa/7.2	up/up	0.0.0.0	255.255.255.255	hostManaged	00:13:97:01:8D:F8	fal...	Disabled	false

Figure 4 Physical Server Details Frame — vNICs

The *vNICS* tab offers various controls that allow you to affect the state of vNICs on the selected server. Figure 5 shows these controls.


Add a vNIC
Turn Up
Turn Down
Set in Different Network Cloud
Change Termination Port or LAG
Merge Two vNICs into an HA vNIC
Delete Selected vNICs
Server : hgudi.lab.xsigo.com
General
vNICs
vHBAs
Server Groups

Name	Network Cloud	Termination	State	IP Address	Netmask	IP Type	MAC Address	HA	QoS	Private
asdf0	aaa	iowa/	up/null					fal...	Disabled	false
vnic	discovered-network...	iowa/7/10	up/up	0.0.0.0	255.255.255.255	hostManaged	00:13:97:01:8D:F4	fal...	Disabled	false
vnic10	discovered-network...	iowa/7.3	up/up	0.0.0.0	255.255.255.255	hostManaged	00:13:97:01:8D:F5	fal...	Disabled	false
vnic5	discovered-network...	iowa/7/1	up/up	0.0.0.0	255.255.255.255	hostManaged	00:13:97:01:8D:F6	fal...	Disabled	false
vnic8	discovered-network...	iowa/7/7	up/up	0.0.0.0	255.255.255.255	hostManaged	00:13:97:01:8D:F7	fal...	Disabled	false
vnic9	discovered-network...	iowa/7.2	up/up	0.0.0.0	255.255.255.255	hostManaged	00:13:97:01:8D:F8	fal...	Disabled	false

Figure 5 Physical Server Details Frame — vNIC Controls

The Physical Server Details frame has a toolbar that allows you to control the following for one or more vNICs on the selected server:

- Add a vNIC
- Turn Up the vNIC to set it to up/up state
- Turn Down the vNIC to set its state to up/down
- Set in Different Network Cloud, to associate a vNIC on the server with a different Network Cloud.
- Change Termination Port or LAG to assign the vNIC to a different Gigabit or 10 Gigabit Ethernet port, or different link aggregation group.
- Merge Two vNICs into an HA vNIC, which takes two selected vNICs and creates one HA pair out of them. To merge the vNICs, they must be part of the same Network Cloud.
- Delete selected vNICs, which removes any number of selected vNICs from the server and deletes them from their respective Network Clouds.

Displaying Details About a vNIC

When you click a vNIC name, a separate details frame is displayed containing tabs for the vNIC. It is important to remember that this vNIC is in the context of the physical server you selected. The vNIC information is for only the selected vNIC on the selected server. Other vNICs on the server (or on other servers in the network) might or might not have the same vNIC properties.

General information about the vNIC properties is available through the *General* tab of the vNIC Details for the selected server.

To display a vNIC’s general properties, follow this procedure:

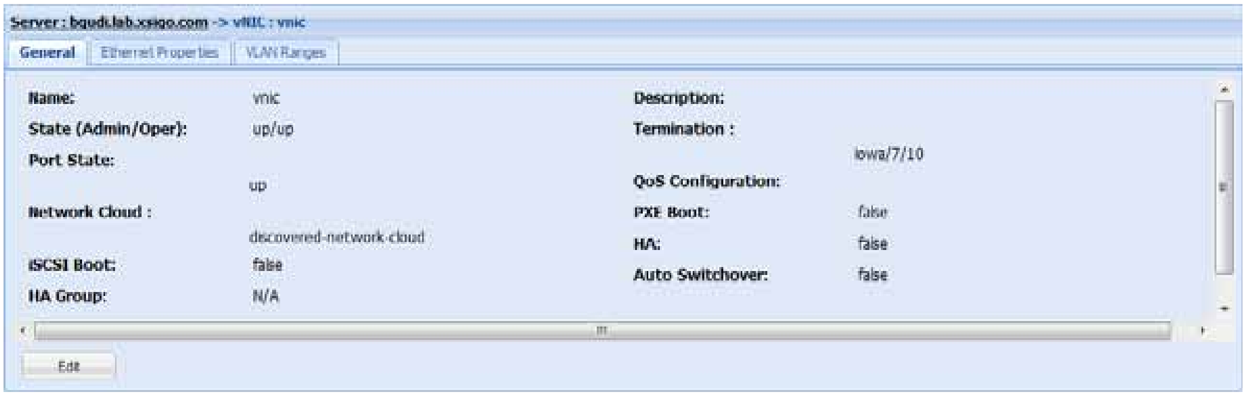
Step 1 Select *Server Resource Manager->Physical Servers* to display the Physical Server Summary.

Step 2 Select a server in the Physical Server Summary to display the server in the details frame.

Step 3 On the Physical Server details frame, click the *vNICs* tab.

Step 4 On the *vNICs* tab, click a vNIC name to display the vNIC Details frame for that vNIC.

Step 5 On the vNIC details frame, click the *General* tab. Figure 6 shows the *General* tab for one of a server's vNICs.



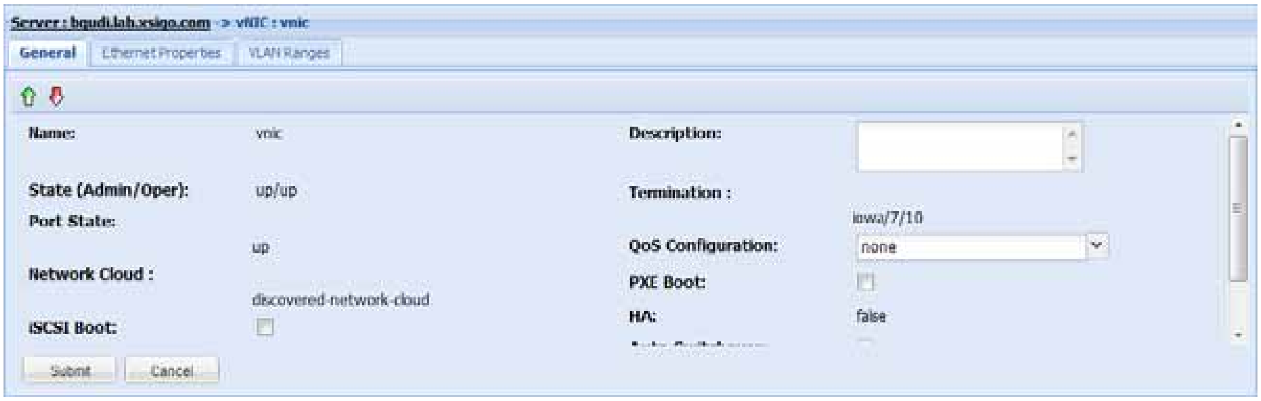
Name: vnic
State (Admin/Oper): up/up
Port State: up
Network Cloud : discovered-network-cloud
iSCSI Boot: false
HA Group: N/A
Description:
Termination : iowa/7/10
QoS Configuration:
PXE Boot: false
HA: false
Auto Switchover: false

Figure 6 vNIC Details Frame — General Properties Tab

The *General* tab contains an ***Edit*** button that allows you to unlock editable fields to set or change existing vNIC properties.

To edit the vNIC's General properties, follow this procedure:

Step 6 Click the ***Edit*** button.



Name: vnic
State (Admin/Oper): up/up
Port State: up
Network Cloud : discovered-network-cloud
iSCSI Boot: □
Description:
Termination : iowa/7/10
QoS Configuration: none
PXE Boot: □
HA: false

Figure 7 Editable vNIC General Properties Tab

Step 7 Edit the fields as needed, then click ***Submit*** to activate the changes.

Step 8 Check the *General* tab to verify that the correct properties are configured.

Note

While you are editing the vNIC’s general properties, you can also set the vNIC up or down by clicking the up or down arrow, respectively.

Displaying a vNIC’s Ethernet Properties

A vNIC is a software construction that virtualizes a physical NIC, and provides the same functionality as a physical NIC. As a result, a vNIC has the same Ethernet properties as a standard NIC.

The vNIC’s Ethernet properties are displayed in the *Ethernet Properties* tab on the vNIC Details frame.

To display a vNIC’s Ethernet properties, follow this procedure:

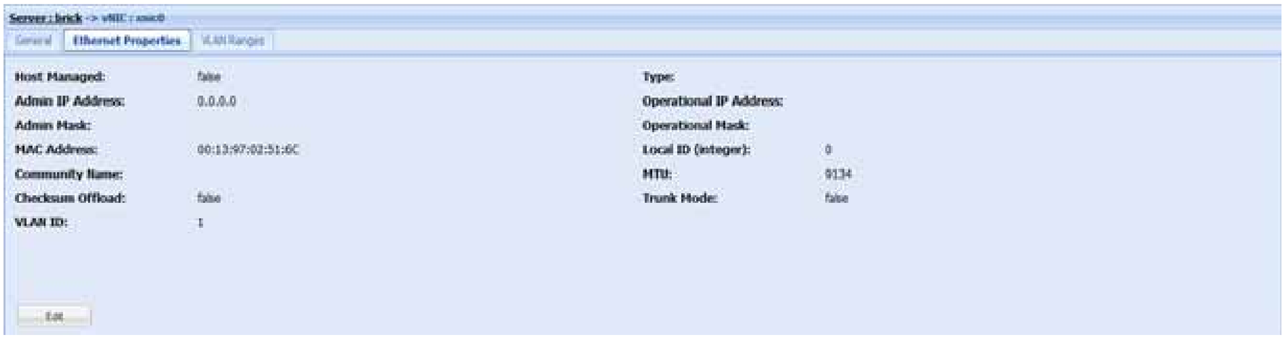
Step 1 Select *Server Resource Manager->Physical Servers* to display the Physical Server Summary.

Step 2 Select a server in the Physical Server Summary to display the server in the details frame.

Step 3 On the Physical Server details frame, click the *vNICs* tab.

Step 4 On the *vNICs* tab, click a vNIC name to display the vNIC Details frame for that vNIC.

Step 5 On the Physical Server details frame, click the *Ethernet Properties* tab. Figure 8 shows the *Ethernet Properties* tab for one of a server’s vNICs.



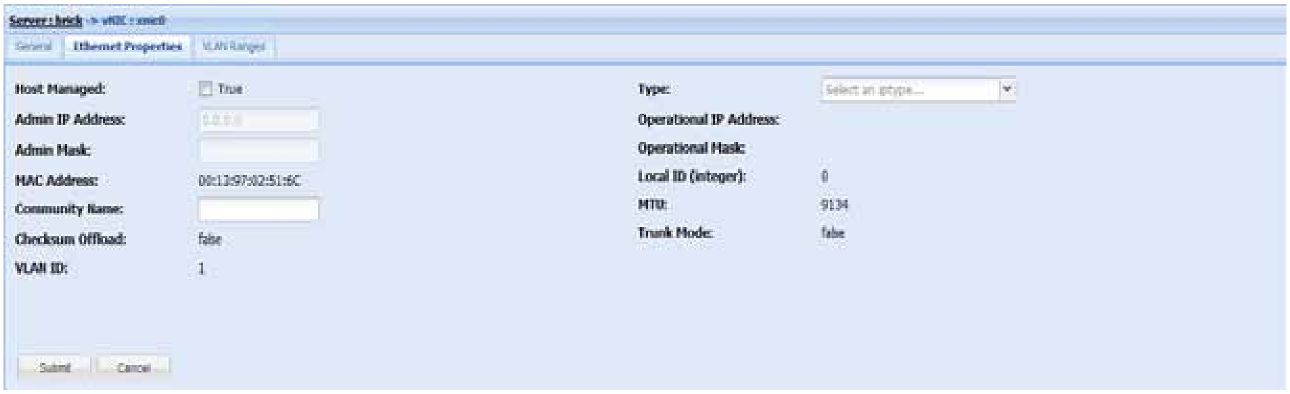
Host Managed:	false	Type:	
Admin IP Address:	0.0.0.0	Operational IP Address:	
Admin Mask:		Operational Mask:	
MAC Address:	00:13:97:02:51:6C	Local ID (integer):	0
Community Name:		MTU:	9134
Checksum Offload:	false	Trunk Mode:	false
VLAN ID:	1		

Figure 8 vNIC Details Frame — Ethernet Properties Tab

The *Ethernet Properties* tab also contains an ***Edit*** button that allows you to unlock editable field on the tab to set or change the existing Ethernet properties for the vNIC.

To edit the vNIC’s Ethernet Properties, follow this procedure:

Step 6 On the *Ethernet Properties* tab, click the ***Edit*** button to unlock the editable fields, as shown in Figure 9.



Host Managed: □ True

Admin IP Address: 0.0.0.0

Admin Mask:

MAC Address: 00:13:97:02:51:6C

Community Name:

Checksum Offload: false

VLAN ID: 1

Type: Select an iptype...

Operational IP Address:

Operational Mask:

Local ID (integer): 0

MTU: 9134

Trunk Mode: false

Figure 9 Editable vNIC Ethernet Properties Tab

Step 7 Edit the fields as needed, then click ***Submit*** to make the changes.

Step 8 Check the *Ethernet Properties* tab to verify that the correct properties are configured.

Configuring VLAN Ranges for vNICs on a Server

By default, the allowable VLAN range is from 1 to 4095. However, you can set a custom range of VLANs for a vNIC so that only the VLAN-tagged packets within the specified range are allowed on a vNIC. Traffic that has a VLAN tag not in the specified range is blocked from ever being transmitted or received on one or more specified vNICs.

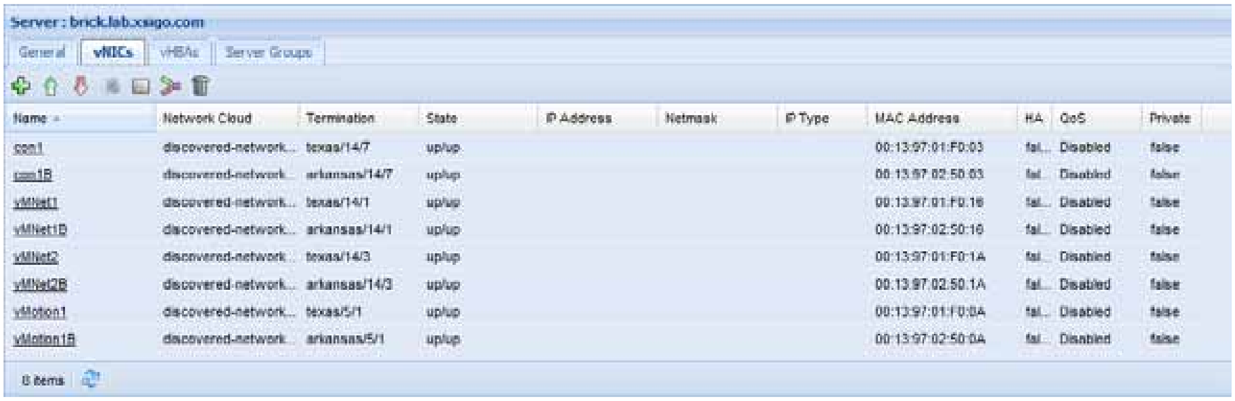
You can set or change the allowed VLAN range for a vNIC through the *Allowed VLANs* tab at the port level of the Ethernet Card Details Frame.

To set the allowed VLAN range for a specific Fabric Director, follow this procedure:

Step 1 Select *Server Resource Manager->Physical Servers* to display the Physical Server Summary page.

Step 2 Select the server for which you want to set the Allowed VLAN range by clicking the server in the summary. This step populates the details frame with information for that server.

Step 3 On the details frame, click the *vNICs* tab to display each vNIC configured on the selected server. Figure 10 shows an example of the *vNICs* tab.



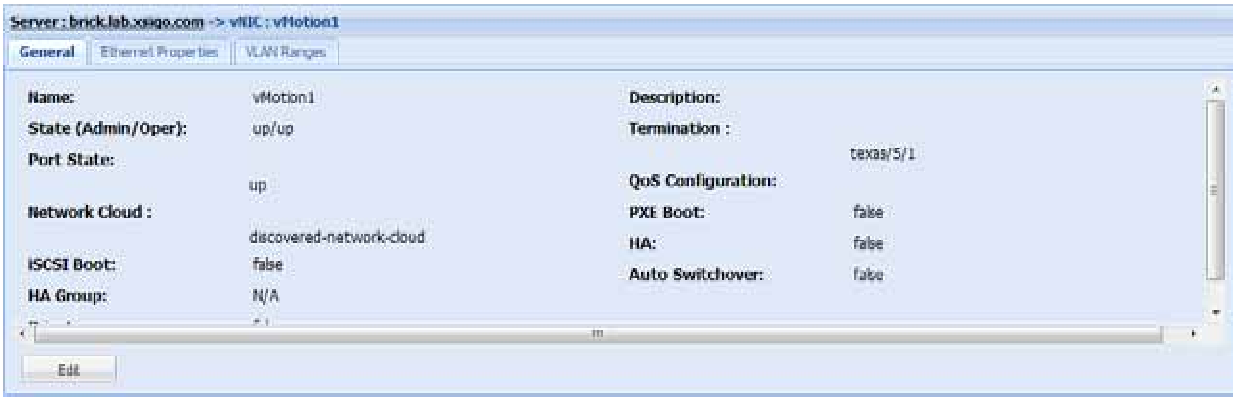
Server : brick.lab.xsigo.com

Name	Network Cloud	Termination	State	IP Address	Netmask	IP Type	MAC Address	HA	QoS	Private
con1	discovered-network...	texas/14/7	up/up				00:13:97:01:F0:03	fal...	Disabled	false
con1B	discovered-network...	arkansas/14/7	up/up				00:13:97:02:50:03	fal...	Disabled	false
vMNet1	discovered-network...	texas/14/1	up/up				00:13:97:01:F0:16	fal...	Disabled	false
vMNet1B	discovered-network...	arkansas/14/1	up/up				00:13:97:02:50:16	fal...	Disabled	false
vMNet2	discovered-network...	texas/14/3	up/up				00:13:97:01:F0:1A	fal...	Disabled	false
vMNet2B	discovered-network...	arkansas/14/3	up/up				00:13:97:02:50:1A	fal...	Disabled	false
vMotion1	discovered-network...	texas/5/1	up/up				00:13:97:01:F0:0A	fal...	Disabled	false
vMotion1B	discovered-network...	arkansas/5/1	up/up				00:13:97:02:50:0A	fal...	Disabled	false

8 items

Figure 10 Physical Server Details — vNICs Tab

Step 4 Double click the vNIC on which you want to set the Allowed VLAN range. This step displays the vNIC details for that vNIC, as shown in Figure 11.



Server : brick.lab.xsigo.com -> vNIC : vMotion1

Name: vMotion1

State (Admin/Oper): up/up

Port State: up

Network Cloud : discovered-network-cloud

iSCSI Boot: false

HA Group: N/A

Description:

Termination : texas/5/1

QoS Configuration:

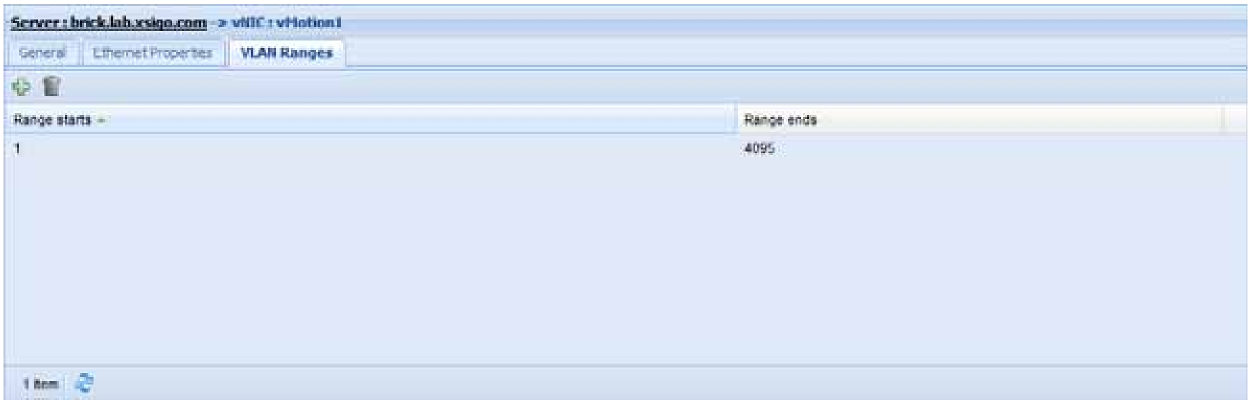
PXE Boot: false

HA: false

Auto Switchover: false

Figure 11 vNIC Details — General Tab

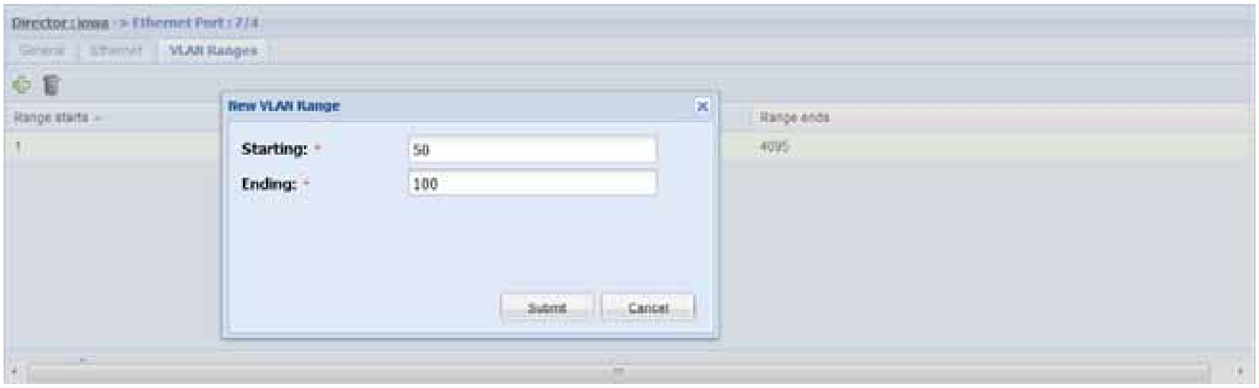
Step 5 Click the *VLAN Ranges* tab, as shown in Figure 12.



Range starts	Range ends
1	4095

Figure 12 Physical Server Details — VLAN Ranges Tab

Step 6 Click the plus sign (+) to display the New VLAN Range dialog as shown in Figure 13.



Starting: * 50

Ending: * 100

Figure 13 Physical Server Details — New VLAN Range Dialog

Step 7 In the *Starting* field, enter the first VLAN ID that you want to be available.

Step 8 In the *Ending* field, enter the last VLAN ID you want to be available.

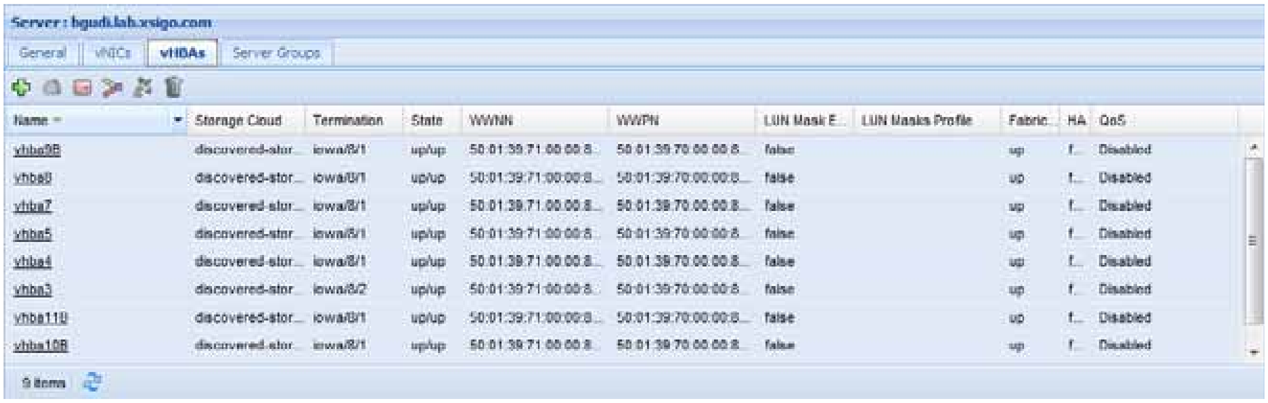
Step 9 When the Allowed VLAN Range is configured, click ***Submit***.

Managing vHBAs on a Physical Server

When a physical server is bound to an I/O Profile, it has virtual connectivity through vNICs, vHBAs, or both. When a server has vHBAs deployed on it, they are listed on the *vHBAs* tab for the selected server. The *vHBAs* tab provides the following functionality:

- it displays information about each vHBA deployed on the sever.
- it provides ways to manage the vHBAs.
- it lists vHBAs by name, and the name is a link to additional details about each vHBA's individual properties.

Figure 14 shows the *vHBAs* tab of the Physical Servers Details frame.



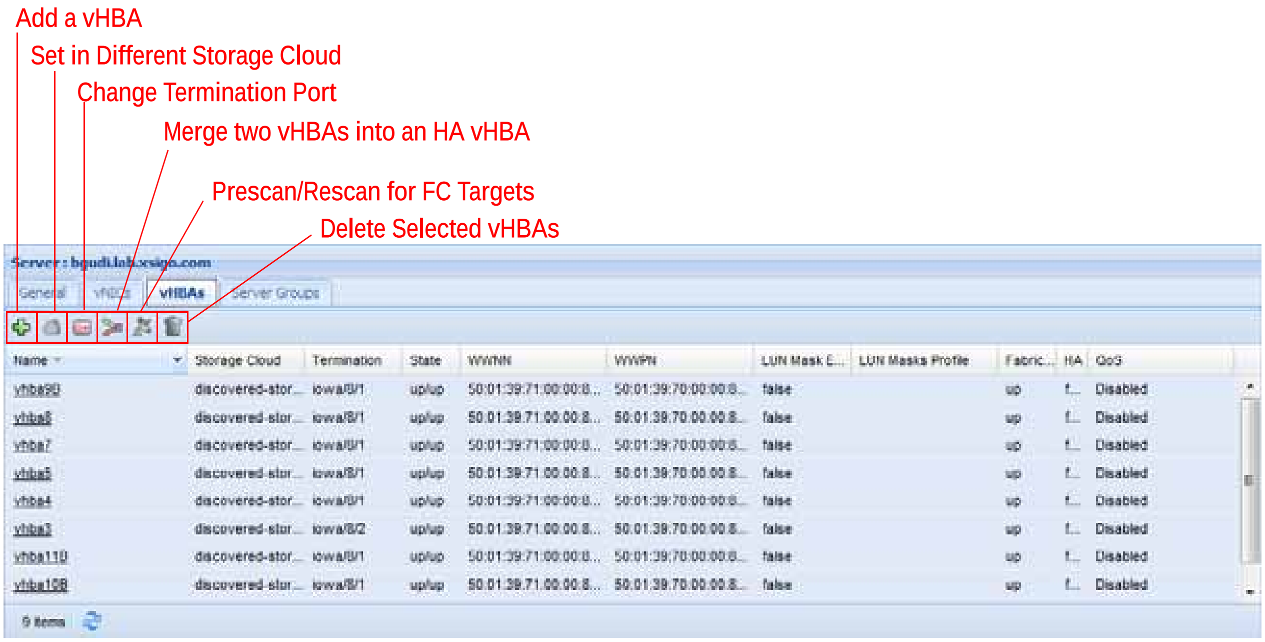
Server : hgudi.lab.xsigo.com

Name	Storage Cloud	Termination	State	WWNN	WWPN	LUN Mask E...	LUN Masks Profile	Fabric...	HA	QoS
vhba9B	discovered-stor...	iowa/8/1	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled
vhba8	discovered-stor...	iowa/8/1	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled
vhba7	discovered-stor...	iowa/8/1	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled
vhba5	discovered-stor...	iowa/8/1	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled
vhba4	discovered-stor...	iowa/8/1	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled
vhba3	discovered-stor...	iowa/8/2	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled
vhba11B	discovered-stor...	iowa/8/1	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled
vhba10B	discovered-stor...	iowa/8/1	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled

9 items

Figure 14 Physical Server Details Frame — vHBAs Tab

The *vHBAs* tab also contains various controls that allow you to affect the state of vHBAs on the selected server. Figure 15 shows these controls.


Add a vHBA
Set in Different Storage Cloud
Change Termination Port
Merge two vHBAs into an HA vHBA
Prescan/Rescan for FC Targets
Delete Selected vHBAs
Server : bgudi.lab.xsigo.com
General
vNICs
vHBAs
Server Groups
9 items

Name	Storage Cloud	Termination	State	WWNN	WWPN	LUN Mask E...	LUN Masks Profile	Fabric...	HA	QoS
vhba90	discovered-stor...	iowa/8/1	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled
vhba8	discovered-stor...	iowa/8/1	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled
vhba7	discovered-stor...	iowa/8/1	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled
vhba5	discovered-stor...	iowa/8/1	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled
vhba4	discovered-stor...	iowa/8/1	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled
vhba3	discovered-stor...	iowa/8/2	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled
vhba110	discovered-stor...	iowa/8/1	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled
vhba108	discovered-stor...	iowa/8/1	up/up	50:01:39:71:00:00:8...	50:01:39:70:00:00:8...	false		up	f...	Disabled

Figure 15 Physical Server Details Frame — vHBA Controls

The Physical Server Details frame has a toolbar that allows you to control the following for one or more vHBAs on the selected server:

- Add a vHBA
- Set in Different Storage Cloud, to associate a vHBA on the server with a different Storage Cloud.
- Change Termination Port, to assign the vHBA to a different Fibre Channel port.
- Merge Two vHBAs into an HA vHBA, which takes two selected vHBAs and creates one HA pair out of them. To merge the vHBAs, they must be part of the same Storage Cloud.
- Prescan/Rescan for Fibre Channel targets on the vHBA.
- Delete selected vHBAs, which removes any number of selected vHBAs from the server and deletes them from their respective Storage Clouds.

Displaying Details About a vHBA

When you click a vHBA name, a separate details frame is displayed containing tabs for the vHBA. It is important to remember that this vHBA is in the context of the physical server you selected. The vHBA information is for only the selected vHBA on the selected server. Other vHBAs on the server (or on other servers in the network) might or might not have the same vHBA properties.

General information about the vHBA properties is available through the *General* tab of the vHBA Details for the selected server.

To display a vHBA's general properties, follow this procedure:

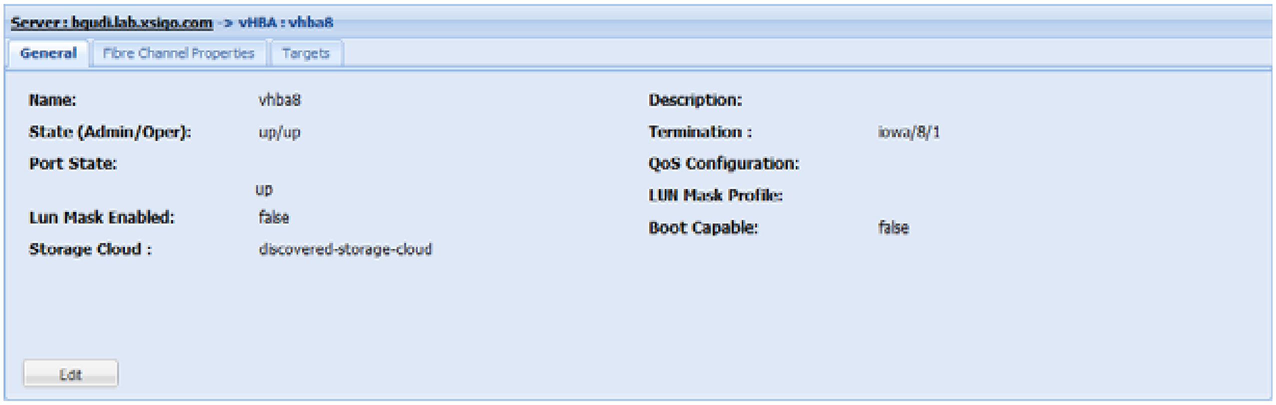
Step 1 Select *Server Resource Manager->Physical Servers* to display the Physical Server Summary.

Step 2 Select a server in the Physical Server Summary to display the server in the details frame.

Step 3 On the Physical Server details frame, click the *vHBAs* tab.

Step 4 On the *vHBAs* tab, click a vHBA name to display the vHBA Details frame for that vHBA.

Step 5 On the vHBA details frame, click the *General* tab. Figure 16 shows the *General* tab for one of a server's vHBAs.



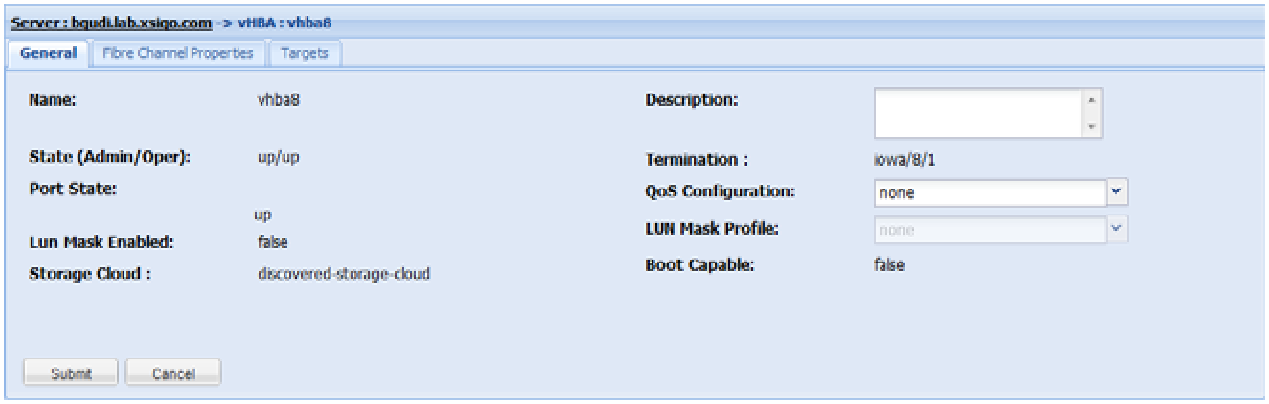
Name: vhba8
State (Admin/Oper): up/up
Port State: up
Lun Mask Enabled: false
Storage Cloud : discovered-storage-cloud
Description:
Termination : iowa/8/1
QoS Configuration:
LUN Mask Profile:
Boot Capable: false

Figure 16 Physical Servers Details Frame — vHBA General Properties Tab

The *General* tab also has an ***Edit*** button that allows you to unlock the editable fields on the tab.

To edit the vHBA's general properties, follow this procedure:

Step 6 On the *General* tab, click the ***Edit*** button to unlock the editable fields, as shown in Figure 17.



Name: vhba8
State (Admin/Oper): up/up
Port State: up
Lun Mask Enabled: false
Storage Cloud : discovered-storage-cloud
Description:
Termination : iowa/8/1
QoS Configuration: none
LUN Mask Profile: none
Boot Capable: false

Figure 17 Editable vHBA General Properties Tab

Step 7 Edit the fields as needed, then click ***Submit*** to make the changes.

Step 8 Check the *General* tab to verify that the correct properties are configured.

Displaying a vHBA's Fibre Channel Properties

A vHBA is a software construction that virtualizes a physical HBA, and provides the same functionality as a physical HBA. As a result, a vHBA has the same Fibre Channel properties as a standard HBA.

The vHBA Fibre Channel properties are displayed in the *Fibre Channel Properties* tab on the vHBA Details frame.

To display a vHBA's Fibre Channel properties, follow this procedure:

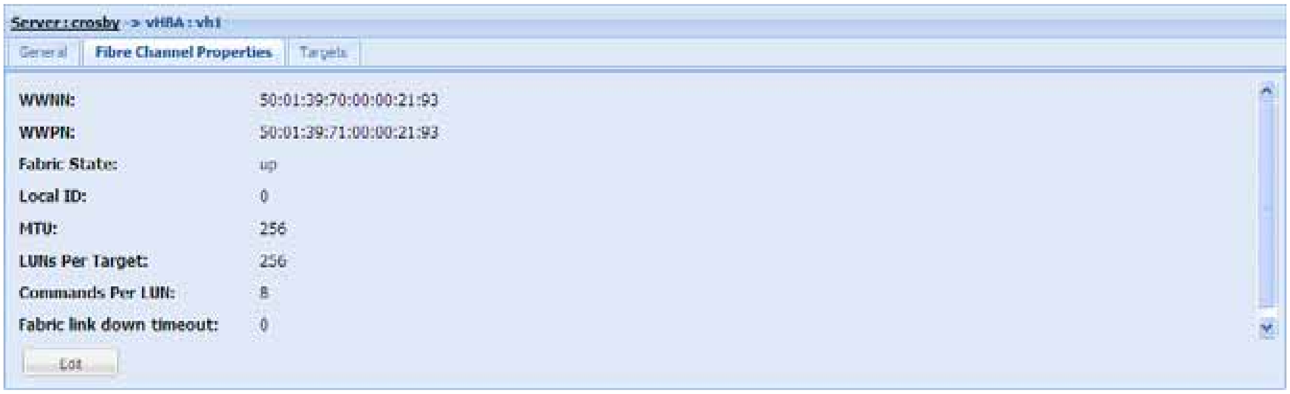
Step 1 Select *Server Resource Manager->Physical Servers* to display the Physical Server Summary.

Step 2 Select a server in the Physical Server Summary to display the server in the details frame.

Step 3 On the Physical Server details frame, click the *vHBAs* tab.

Step 4 On the *vHBAs* tab, click a vHBA name to display the vHBA Details frame for that vHBA.

Step 5 On the vHBA details frame, click the *Fibre Channel Properties* tab. Figure 18 shows the *Fibre Channel Properties* tab for one of a server's vHBAs.



WWNN: 50:01:39:70:00:00:21:93

WWPN: 50:01:39:71:00:00:21:93

Fabric State: up

Local ID: 0

MTU: 256

LUNs Per Target: 256

Commands Per LUN: 8

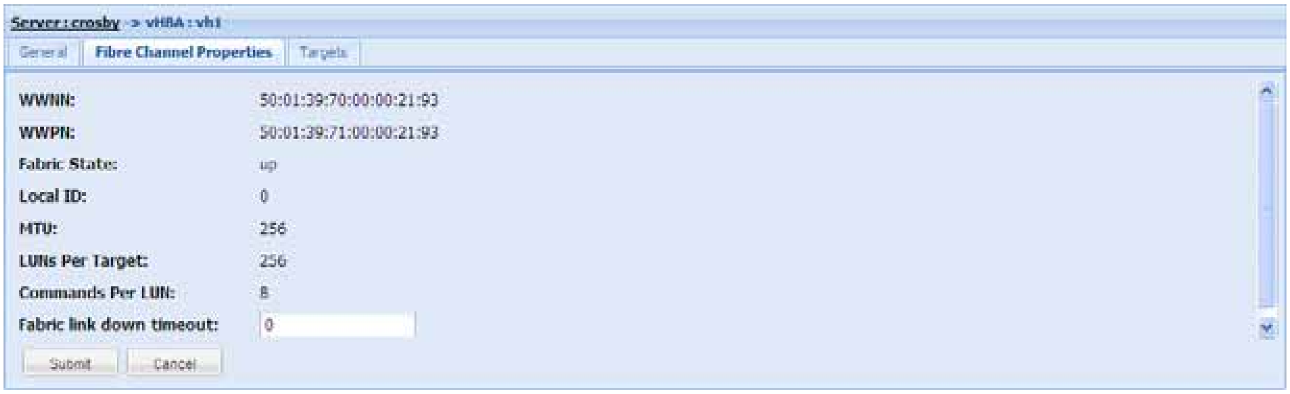
Fabric link down timeout: 0

Figure 18 Physical Servers Details Frame — Fibre Channel Properties Tab

The *Fibre Channel Properties* tab has an ***Edit*** button allows you to unlock the editable fields on the tab to set or change existing properties.

To edit a vHBA's Fibre Channel Properties, follow this procedure:

Step 6 On the *Fibre Channel Properties* tab, click the ***Edit*** button to unlock the editable fields, as shown in Figure 19.



WWNN:	50:01:39:70:00:00:21:93
WWPN:	50:01:39:71:00:00:21:93
Fabric State:	up
Local ID:	0
MTU:	256
LUNs Per Target:	256
Commands Per LUN:	8
Fabric link down timeout:	0

Figure 19 Editable Fibre Channel Properties Tab

Step 7 Edit the fields as needed, then click ***Submit*** to make the changes.

Step 8 Check the *Fibre Channel Properties* tab to verify that the correct properties are configured.

Displaying a vHBA's Targets

A vHBA connects host servers to SAN resources (targets) such as arrays, JBODs, and so on. The vHBA can connect either directly to storage through the Fabric Director, or indirectly through an intervening Fibre Channel switch between the Fabric Director and the storage.

When an I/O Profile is bound to a host server, the vHBA that connects to the storage is deployed on the server. That vHBA provides the connection for read and write data between the host server and the storage.

Fabric Manager tracks the storage connected to a host server through the *Targets* tab on the vHBA Details frame.

To display the storage targets available to a server, follow this procedure:

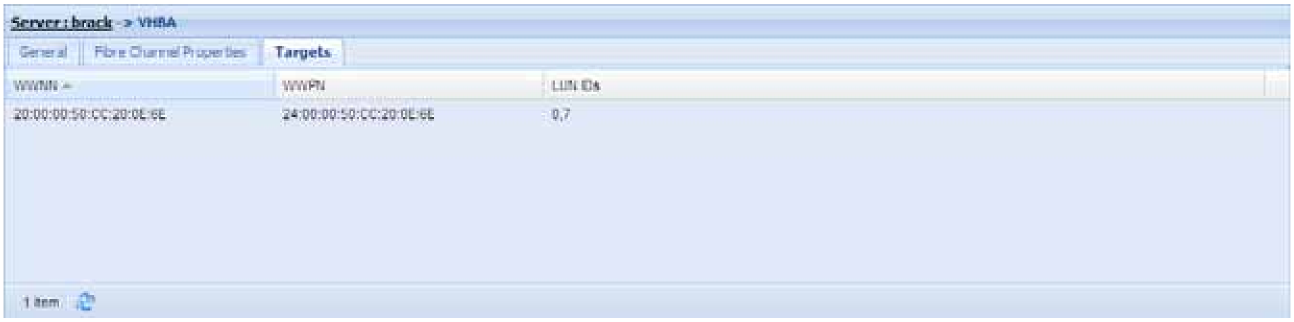
Step 1 Select *Server Resource Manager->Physical Servers* to display the Physical Server Summary.

Step 2 Select a server in the Physical Server Summary to display the server in the details frame.

Step 3 On the Physical Server details frame, click the *vHBAs* tab.

Step 4 On the *vHBAs* tab, click a vHBA name to display the vHBA Details frame for that vHBA.

Step 5 On the vHBA details frame, click the *Targets* tab. Figure 20 shows the *Targets* tab for one of a server's vHBAs.



Server : brack -> VHBA

WWNN	WWPN	LUN IDs
20:00:00:50:CC:20:0E:6E	24:00:00:50:CC:20:0E:6E	0,7

1 item

Figure 20 Physical Servers Details Frame — Targets Tab

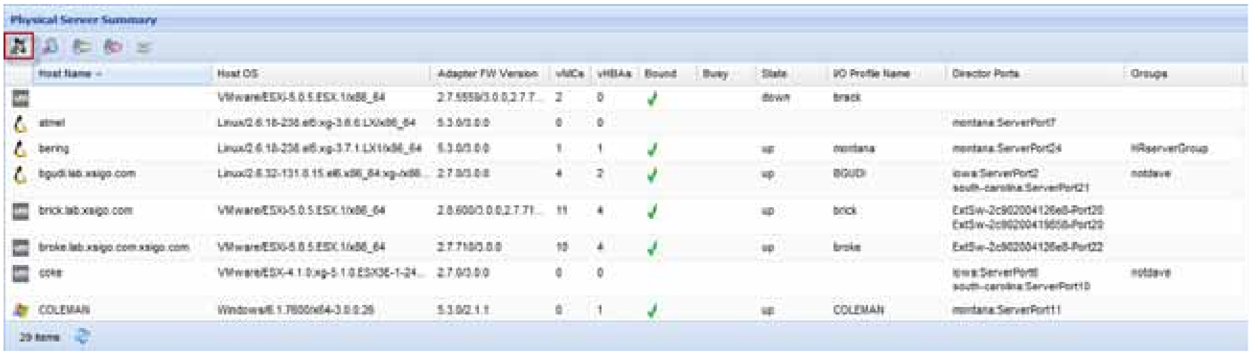
Scanning for New Servers or Removing Stale Servers

When servers are connected to a Fabric Director, they become available on the fabric. Also, if servers drop offline for any reason, or are disconnected from the fabric, scanning will remove them from Fabric Manager. Adding and deleting servers can occur automatically in Fabric Manager, but you can also perform a manual scan for physical servers.

To scan the fabric, follow this procedure:

Step 1 Select *Server Resource Manager->Physical Servers* to display the Physical Server Summary.

Step 2 Click the ***Scan for New or Stale Servers*** button as shown in Figure 21.



Physical Server Summary

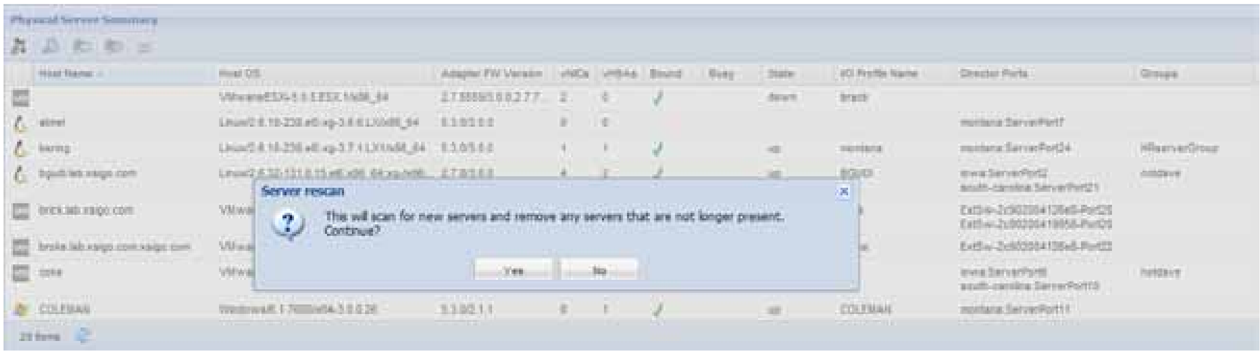
Host Name	Host OS	Adapter FW Version	vNICs	vHBAs	Bound	Busy	State	I/O Profile Name	Director Ports	Groups
	VMware/ESXi-5.0.5.ESX.1/x86_64	2.7.5559/3.0.0.2.7.7...	2	0	✓		down	brack		
atmel	Linux/2.6.18-238.el5.xg-3.6.6.LX/x86_64	5.3.0/3.0.0	0	0					montana:ServerPort7	
bering	Linux/2.6.18-238.el5.xg-3.7.1.LX1/x86_64	5.3.0/3.0.0	1	1	✓		up	montana	montana:ServerPort24	HRserverGroup
bgudi.lab.xsigo.com	Linux/2.6.32-131.0.15.el6.x86_64.xg-/x86...	2.7.0/3.0.0	4	2	✓		up	BGUDI	iowa:ServerPort2 south-carolina:ServerPort21	notdave
brick.lab.xsigo.com	VMware/ESXi-5.0.5.ESX.1/x86_64	2.8.600/3.0.0.2.7.71...	11	4	✓		up	brick	ExtSw-2c902004126e8-Port20 ExtSw-2c90200419658-Port20	
broke.lab.xsigo.com.xsigo.com	VMware/ESXi-5.0.5.ESX.1/x86_64	2.7.710/3.0.0	10	4	✓		up	broke	ExtSw-2c902004126e8-Port22	
coke	VMware/ESX-4.1.0.xg-5.1.0.ESX3E-1-24...	2.7.0/3.0.0	0	0					iowa:ServerPort8 south-carolina:ServerPort10	notdave
COLEMAN	Windows/6.1.7600/x64-3.0.0.26	5.3.0/2.1.1	0	1	✓		up	COLEMAN	montana:ServerPort11	

29 items

Figure 21 Physical Server Summary — Rescan Button

When you click the button, a confirmation dialog is displayed, as shown in Figure 22.

.



Physical Server Summary

	Host Name	Host OS	Adapter FW Version	vNICs	vHBAs	Bound	Busy	State	I/O Profile Name	Director Ports	Groups
		VMwareESXi-5.5.0.ESX.1/x86_64	2.7.55555.0.0.2.7.7...	2	0	✓		down	brack		
	abrel	Linux/2.6.18-238.el5.xg-3.6.6.LX/x86_64	5.3.0/2.0.0	0	0					montana.ServerPort7	
	baring	Linux/2.6.18-238.el5.xg-3.7.1.LX/x86_64	5.3.0/5.0.0	1	1	✓		up	montana	montana.ServerPort24	HRserverGroup
	bgudi.lab.xsigo.com	Linux/2.6.32-131.0.15.el6.x86_64.xg...	2.7.0/3.0.0	4	2	✓		up	BGUDI	iowa.ServerPort2 south-carolina.ServerPort21	hotdave
	brick.lab.xsigo.com	VMwa[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Ext3/w-2c902004126e5-Port25 Ext5/w-2c902004189S8-Port25	
	broke.lab.xsigo.com.xsigo.com	VMwa[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Ext5/w-2c902004126e5-Port22	
	coke	VMwa[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	iowa.ServerPort8 south-carolina.ServerPort13	hotdave
	COLEMAN	Windows/6.1.7600/x64-3.0.0.26	5.3.0/2.1.1	0	1	✓		up	COLEMAN	montana.ServerPort11	

Server rescan

This will scan for new servers and remove any servers that are not longer present. Continue?

Figure 22 Physical Server Summary — Rescan for New or Remove Stale Servers

Step 3 On the confirmation dialog, click ***Yes*** to initiate the rescan. Depending on the number of servers that have been added or the number of stale servers in Fabric Manager, the scan process can take some time. Please be patient and allow the scan to complete.

Saving a Server Configuration as a Template

Oracle's Xsigo Fabric Manager supports saving a server's configuration as an I/O Template. When the configuration is saved as an I/O Template, you can then use that I/O Template for other servers that need the same configuration. By saving the server configuration as an I/O Template, you can great a "master configuration" that can be used to create I/O Profiles as needed. This process is basically cloning one server's configuration, which can then be used (by deploying I/O Profiles) on individual servers that need the same vNIC and vHBAs configuration.

Note

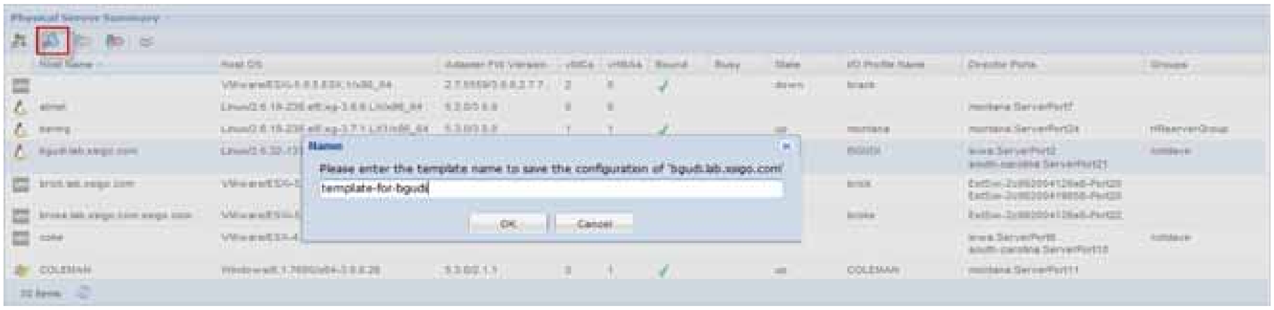
Remember that you can edit individual I/O Templates to change settings.

To assign an I/O Template to a server, follow this procedure:

Step 1 Select *Server Resource Manager->Physical Servers* to display the Physical Server Summary.

Step 2 On the Physical Server Summary, select a physical server that is already bound to an I/O Profile. This step activates the *Save the Selected Server Configuration as an I/O Template* icon.

Step 3 Click the *Assign I/O Template to Server* icon to display the *Name* dialog as shown in Figure 23.



Physical Server Summary

	Host Name	Host OS	Adapter FW Version	vNICs	vHBAs	Bound	Busy	State	I/O Profile Name	Director Ports	Groups
		VMware/ESXi-[illegible]	2.7.550/[illegible]	2	8	✓		down	brack		
	[illegible]	Linux/2.6.18-238.el5.xg-3.6.6.L/x86_64	5.2.0/3.0.0	8	8					montana:ServerPort7	
	[illegible]	Linux/2.6.18-238.el5.xg-3.7.1.L/x86_64	5.3.0/3.0.0	1	1	✓		up	montana	montana:ServerPort24	[illegible]
	bgudi.lab.xsigo.com	Linux/2.6.32-131							BGUDI	iowa:ServerPort2 south-carolina:ServerPort21	[illegible]
	brick.lab.xsigo.com	VMware/ESXi-5							brick	ExtSw-2c902004126e8-Port20 ExtSw-2c90200419858-Port20	
	broke.lab.xsigo.com.xsigo.com	VMware/ESXi-5							broke	ExtSw-2c902004126e8-Port22	
	coke	VMware/ESX-4								iowa:ServerPort6 south-carolina:ServerPort10	[illegible]
	COLEMAN	Windows/6.1.7600/x64-3.0.0.28	5.3.0/2.1.1	3	1	✓		up	COLEMAN	montana:ServerPort11	

22 items

Name

Please enter the template name to save the configuration of 'bgudi.lab.xsigo.com'

template-for-bgudi

OK Cancel

Figure 23 Name the Template

Step 4 On the Name dialog, enter the name that will be given to the I/O Template you are creating from the selected server’s configuration, then click ***OK***.

Step 5 Check the I/O Template Summary to verify that the I/O Template was saved correctly.

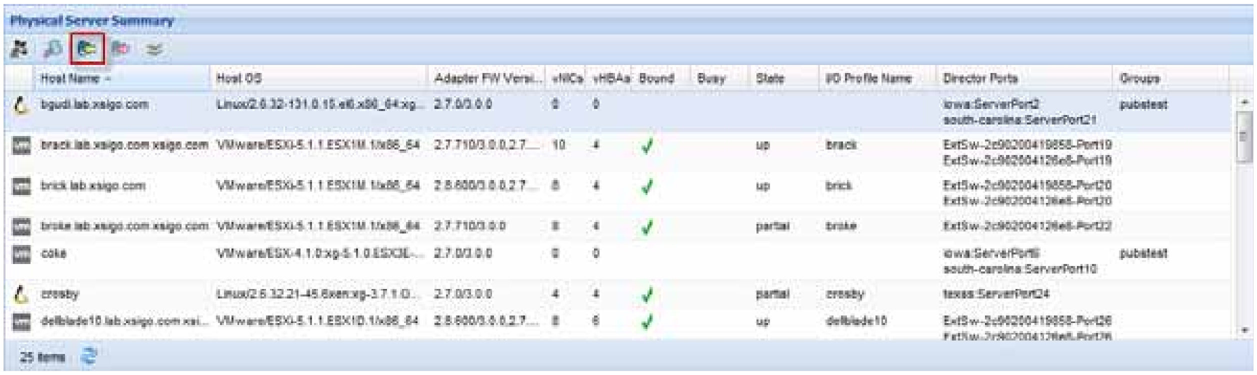
Connecting an I/O Profile to a Server

Configured I/O Profiles do not automatically provide I/O to a server. The I/O Profile must be connected to the server for the server to have the vNICs and vHBAs pushed to the host. If a server is not already connected to an I/O Profile, you can connect it to any I/O Profile in disconnected state. When the I/O Profile is connected to a server, it will take a short time to push the network and storage connectivity to the host. Once established, the I/O Profile transitions from “disconnected” state to “up” state. While in “up” state, traffic can flow to and from the server. If the I/O Profile transitions from “disconnected” state to “partial” state, an error has prevented the I/O Profile from completely connecting to the server. This state requires your attention to fix.

To connect an I/O Profile to a server, follow this procedure:

Step 1 Display the Physical Server summary.

Step 2 Select a physical server that is not bound to an I/O Profile. This step activates the ***Connect I/O Profile to Server*** button, as shown in Figure 24.



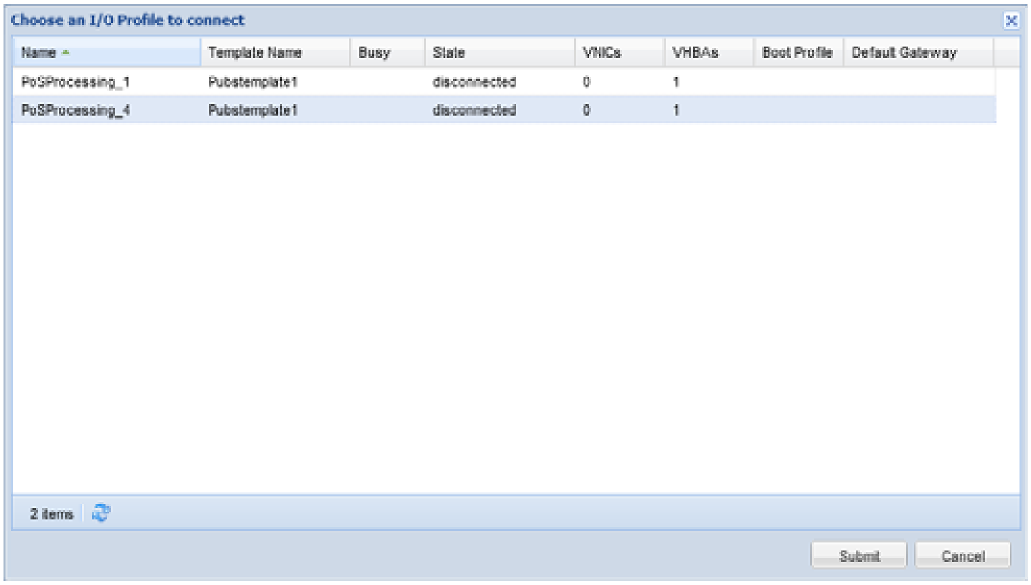
Physical Server Summary

	Host Name	Host OS	Adapter FW Versi...	vNICs	vHBAs	Bound	Busy	State	I/O Profile Name	Director Ports	Groups
	bgudi.lab.xsigo.com	Linux/2.6.32-131.0.15.el6.x86_64.xg...	2.7.0/3.0.0	0	0					iowa:ServerPort2 south-carolina:ServerPort21	pubstest
	brack.lab.xsigo.com.xsigo.com	VMware/ESXi-5.1.1.ESX1M.1/x86_64	2.7.710/3.0.0.2.7....	10	4	✓		up	brack	ExtSw-2c90200419858-Port19 ExtSw-2c902004126e8-Port19	
	brick.lab.xsigo.com	VMware/ESXi-5.1.1.ESX1M.1/x86_64	2.8.600/3.0.0.2.7....	8	4	✓		up	brick	ExtSw-2c90200419858-Port20 ExtSw-2c902004126e8-Port20	
	broke.lab.xsigo.com.xsigo.com	VMware/ESXi-5.1.1.ESX1M.1/x86_64	2.7.710/3.0.0	8	4	✓		partial	broke	ExtSw-2c902004126e8-Port22	
	coke	VMware/ESX-4.1.0:xg-5.1.0.ESX3L-...	2.7.0/3.0.0	0	0					iowa:ServerPort6 south-carolina:ServerPort10	pubstest
	crosby	Linux/2.6.32.21-45.6xen.xg-3.7.1.0...	2.7.0/3.0.0	4	4	✓		partial	crosby	texas:ServerPort24	
	dellblade10.lab.xsigo.com.xsi...	VMware/ESXi-5.1.1.ESX1D.1/x86_64	2.8.600/3.0.0.2.7....	8	6	✓		up	dellblade10	ExtSw-2c90200419858-Port26 ExtSw-2c902004126e8-Port26	

25 items

Figure 24 Physical Server Summary

Step 3 Click the ***Connect I/O Profile to Server*** button to display the choose an I/O Profile to Select dialog. See Figure 25.



Choose an I/O Profile to connect

Name	Template Name	Busy	State	VNICs	VHBAs	Boot Profile	Default Gateway
PoSProcessing_1	Pubstemplate1		disconnected	0	1		
PoSProcessing_4	Pubstemplate1		disconnected	0	1		

2 items

Figure 25 Choose an I/O Profile to Connect

Step 4 Select an I/O Profile that you want to connect to the Physical Server. This step activates the ***Submit*** button.

Step 5 Click ***Submit*** to connect the selected server to the selected I/O Profile.

Disconnecting an I/O Profile from a Server

You can remove an I/O Profile that is already bound to a physical server. When you unbind an I/O Profile, all vNICs and vHBAs that are assigned to the server are completely removed. As a result, all traffic no longer moves between the server and the data and storage networks to which it is connected.

When the I/O Profile is disconnected from a server, that I/O Profile is in the `up/down` state. The server itself remains online, but it is no longer connected to the Fabric Director at the network or storage level. The server is still physically connected to the Fabric Director through the cable between server’s HCA and the Oracle Xsigo Fabric Director.

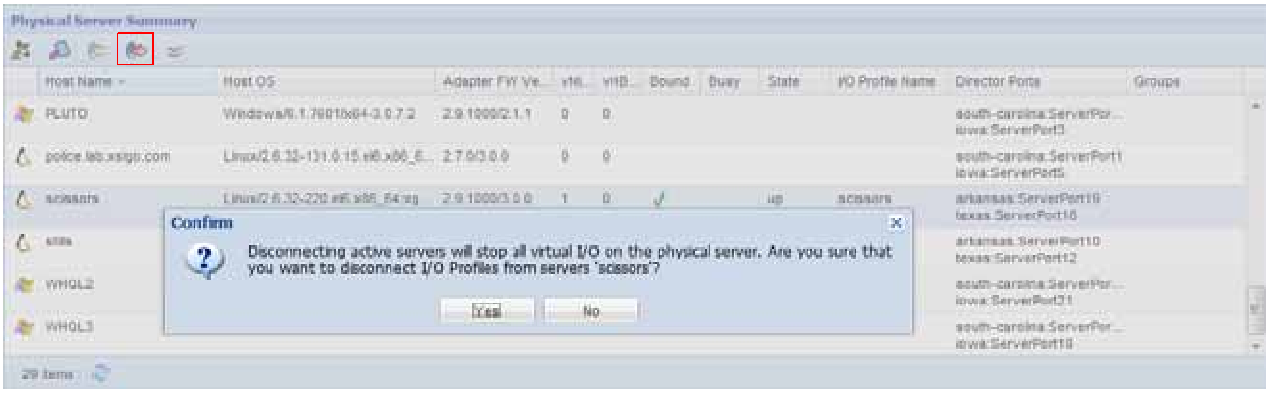
Disconnecting a server is supported through the Physical Server Summary.

To disconnect a currently bound I/O Template, follow this procedure:

Step 1 Select *Server Resource Manager->Physical Servers* to display the Physical Server Summary.

Step 2 On the Physical Server Summary, select a physical server that is already bound to an I/O Template. This step activates the *Unbind Server* button.

Step 3 Click the *Unbind the Server* button to display a message that requires confirmation about unbinding the Server and I/O Template, as shown in figure Figure 26.



Physical Server Summary

Host Name	Host OS	Adapter FW Ve...	vN...	vHB...	Bound	Busy	State	I/O Profile Name	Director Ports	Groups
PLUTO	Windows/6.1.7601/x64-3.0.7.2	2.9.1000/2.1.1	0	0					south-carolina:ServerPor... iowa:ServerPort3	
police.lab.xsigo.com	Linux/2.6.32-131.0.15.el6.x86_6...	2.7.0/3.0.0	0	0					south-carolina:ServerPort1 iowa:ServerPort5	
scissors	Linux/2.6.32-220.el6.x86_64.xg	2.9.1000/3.0.0	1	0	✓		up	scissors	arkansas:ServerPort16 texas:ServerPort16	
stills									arkansas:ServerPort10 texas:ServerPort12	
WHQL2									south-carolina:ServerPor... iowa:ServerPort31	
WHQL3									south-carolina:ServerPor... iowa:ServerPort19	

29 items

Confirm

Disconnecting active servers will stop all virtual I/O on the physical server. Are you sure that you want to disconnect I/O Profiles from servers 'scissors'?

Figure 26 Confirmation of Unbinding a Server and I/O Template

Step 4 On the confirmation dialog, click ***Yes*** to confirm that you want to unbind the selected server from its I/O Template.

Creating a Server Group from Selected Servers

A Server Group is a software construction that enables you to select one or more physical servers and treat them as one logical unit for the purpose of certain management functions. Server Groups allow adding and removing individual servers.

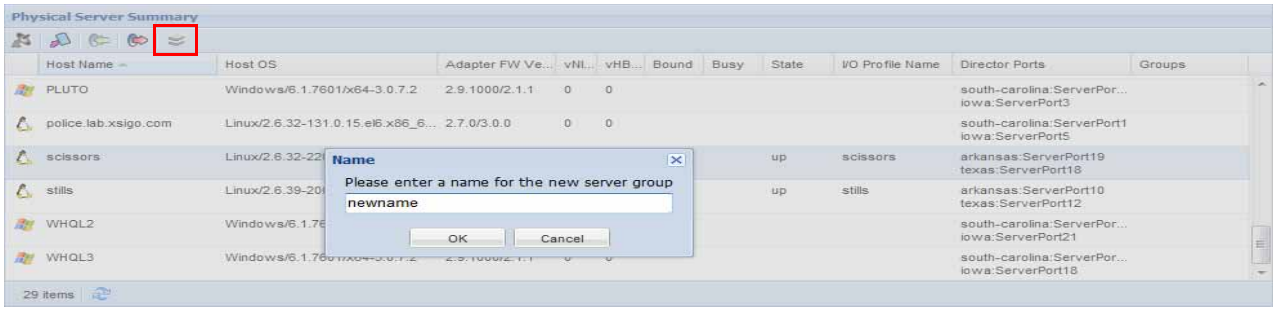
You can create a Server Group through the Physical Server Summary by selecting one or more servers. For more information about Server Groups, see Working with Server Groups.

To create a Server Group, follow this procedure:

Step 1 Select *Server Resource Manager->Physical Servers* to display the Physical Server Summary.

Step 2 On the Physical Server Summary, select one or more physical servers. This step activates the *Create a Server Group from a Set of Servers* icon.

Step 3 Click the *Create a Server Group from a Set of Servers* icon to display the Name dialog as shown in Figure 27.



Physical Server Summary

Host Name	Host OS	Adapter FW Ve...	vNI...	vHB...	Bound	Busy	State	I/O Profile Name	Director Ports	Groups
PLUTO	Windows/6.1.7601/x64-3.0.7.2	2.9.1000/2.1.1	0	0					south-carolina:ServerPor... iowa:ServerPort3	
police.lab.xsigo.com	Linux/2.6.32-131.0.15.el6.x86_6...	2.7.0/3.0.0	0	0					south-carolina:ServerPort1 iowa:ServerPort5	
scissors	Linux/2.6.32-22						up	scissors	arkansas:ServerPort19 texas:ServerPort18	
stills	Linux/2.6.39-20						up	stills	arkansas:ServerPort10 texas:ServerPort12	
WHQL2	Windows/6.1.76								south-carolina:ServerPor... iowa:ServerPort21	
WHQL3	Windows/6.1.7601/x64-3.0.7.2	2.9.1000/2.1.1	0	0					south-carolina:ServerPor... iowa:ServerPort18	

29 items

Name

Please enter a name for the new server group

newname

Figure 27 Name the Server Group

Step 4 In the Name dialog, enter the name for the new Server Group. You must enter the name to activate the ***OK*** button.

Step 5 When the name is specified, click ***OK***.

Step 6 Check the Server Groups Summary (*Server Resource Manager->Server Groups*) to verify that the Server Group is configured.

Working with Server Groups

This chapter documents the following topics:

- Understanding Server Groups
- Displaying Server Groups
- Configuring Server Groups
- Deleting a Server Group

Understanding Server Groups

Server Groups are logical constructions that are assembled from individual servers. Sever groups enable you to use some of Oracle’s Xsigo Fabric Manager’s features to manage multiple servers at once, instead of managing individual servers.

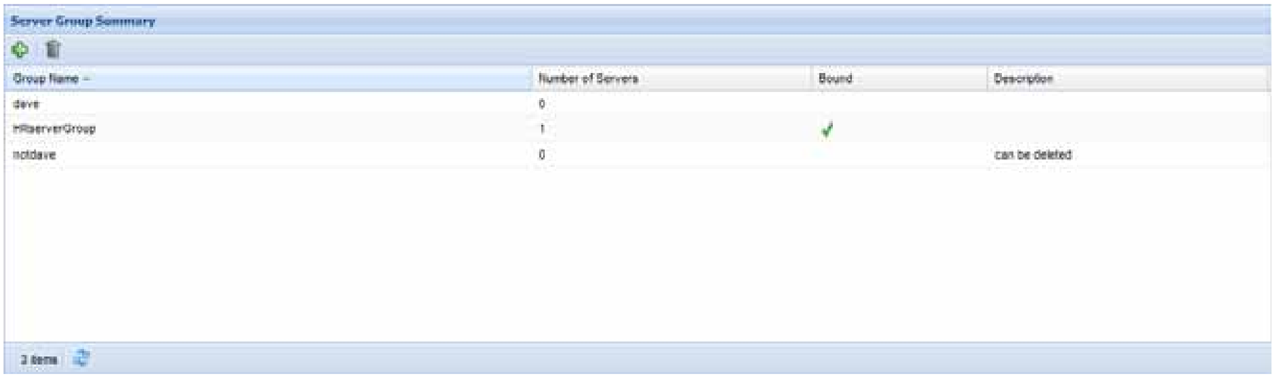
When you create server groups, you are gathering individual servers in the network and putting them together in a logical construction that acts like a container. When server groups are created, all servers in the group are treated as one entity for many configuration and management tasks. For example, you can assign the same I/O Profile to all servers within the group so that all servers have an identical vNIC and vHBA configuration.

You are free to group servers as needed for your network, but it is common to have a unifying theme for the server group. For example, grouping servers by department or business unit, by application type, or by hardware configuration is common.

Displaying Server Groups

When server groups are configured, they are displayed in the Server Group Summary. To display the Server Groups configured in Fabric Manager, follow this procedure:

Step 1 On the navigation frame, select *Server Resource Manager->Server Groups*. Figure 1 shows the Server Group summary.



Server Group Summary

Group Name ⌄	Number of Servers	Bound	Description
dave	0		
HRserverGroup	1	✓	
notdave	0		can be deleted

Figure 1 Server Group Summary

Table 1 shows the Server Group Summary and explains what each field means.

Table 1 Contents of the Storage Targets Summary Table

Field	Indicates...
Group Name	The name of the server group(s) that are configured within Fabric Manager.
Number of Servers	The number of physical servers in each of the listed Server Groups.
Bound	The presence or absence of an I/O Profile on any of the servers in the server group. • A check mark indicates that one or more of the servers in the Server Group has an I/O Profile. • If no check mark is displayed, one or more of the servers has no I/O Profile. Server Groups that do not contain a check mark are viable candidates for receiving virtual resources that will be migrated from another server group.
Description	An optional description for each server group.

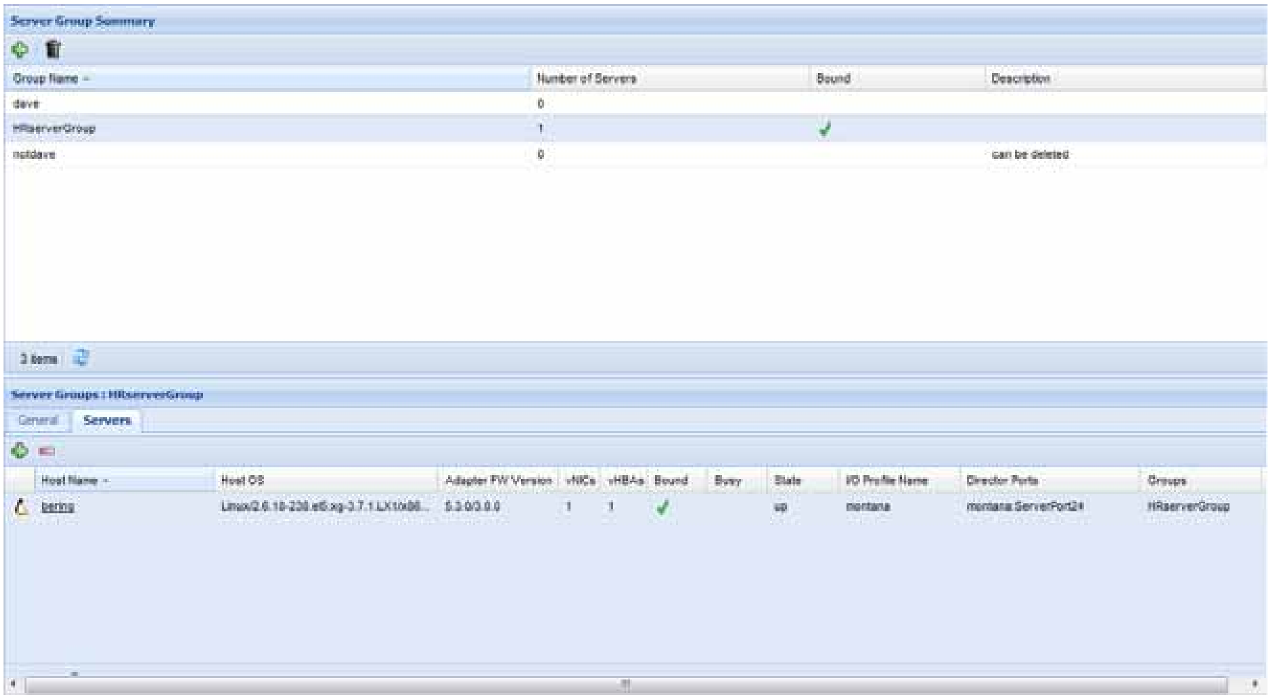
Also, when Server Groups are configured, you can see them in other physical server-based displays within Fabric Manager, for example, the Virtual Topology.

Renaming Server Groups

Fabric Manager supports renaming a server group, which enables you to change the name without having to completely delete and recreate the entire server group. When the server group is renamed, all other properties for the server group are retained, including the server membership for the group. As an option, you can also set or change the description for the Server Group.

You can rename the server group through the Server Group Details frame. To rename the server group, follow this procedure:

Step 1 On the Navigation Frame, select *Server Resource Manager->Server Groups*. Figure 2 shows the Server Group summary.



Server Group Summary

Group Name	Number of Servers	Bound	Description
dave	0		
HRserverGroup	1	✓	
notdave	0		can be deleted

3 items

Server Groups : HRserverGroup

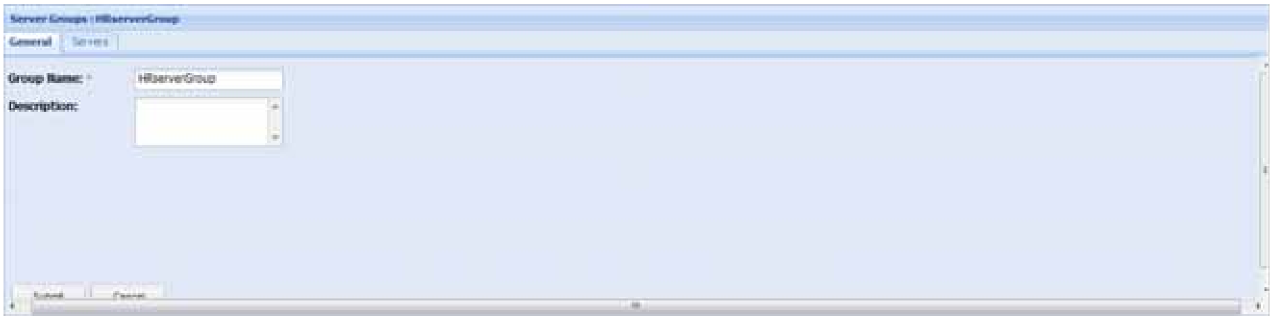
	Host Name	Host OS	Adapter FW Version	vNICs	vHBAs	Bound	Busy	State	I/O Profile Name	Director Ports	Groups
	bering	Linux/2.6.18-238.el5.xg-3.7.1.LX1/x86...	5.3.0/3.0.0	1	1	✓		up	montana	montana.ServerPort24	HRserverGroup

Figure 2 Server Group Summary

Step 2 Select a server group to populate the details frame with its properties.

Step 3 Click the *General* tab to display general properties for the selected server group.

Step 4 On the *General* tab, click the ***Edit*** button to edit the properties of the selected Server Group, as shown in Figure 3.



Server Groups : HRserverGroup

Group Name: HRserverGroup

Description:

Figure 3 Server Group Summary — Editing Details to Rename Server Group

Step 5 In the *Group Name* field, enter the new name for the Server Group.

Step 6 As an option, you also can set or change the description for the selected Server Group.

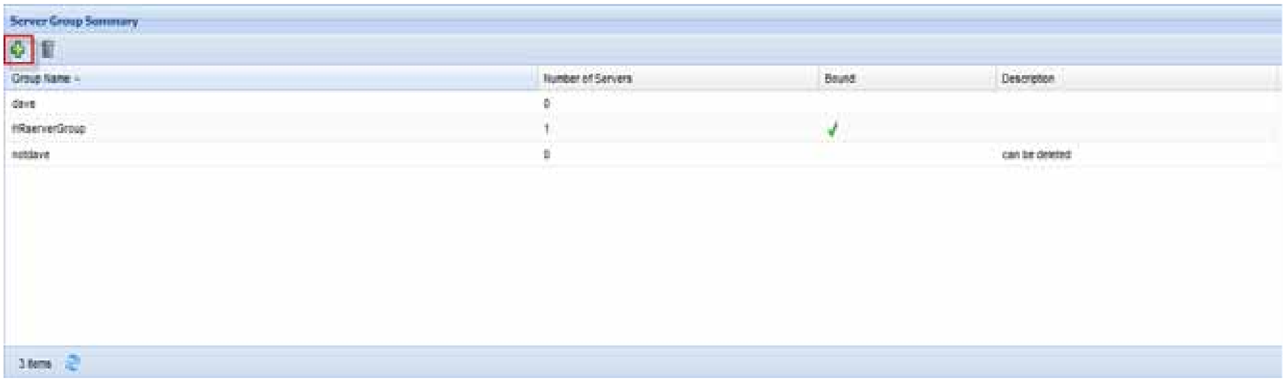
Step 7 When the new name has been specified for the Server Group, click ***Submit***.

Configuring Server Groups

When you configure server groups, you create the logical “container” by selecting one or more servers and naming the server group. After servers are added to the server group, they are still displayable and manageable as individual entities, but since servers in the server group are typically similar in one way, you also gain the ability to manage the servers as one entity.

Server Groups are configurable through the Server Group Summary. To configure a Server Group, follow this procedure:

Step 1 On the navigation frame, select *Server Resource Manager->Server Groups*. Figure 4 shows the Server Group Summary.



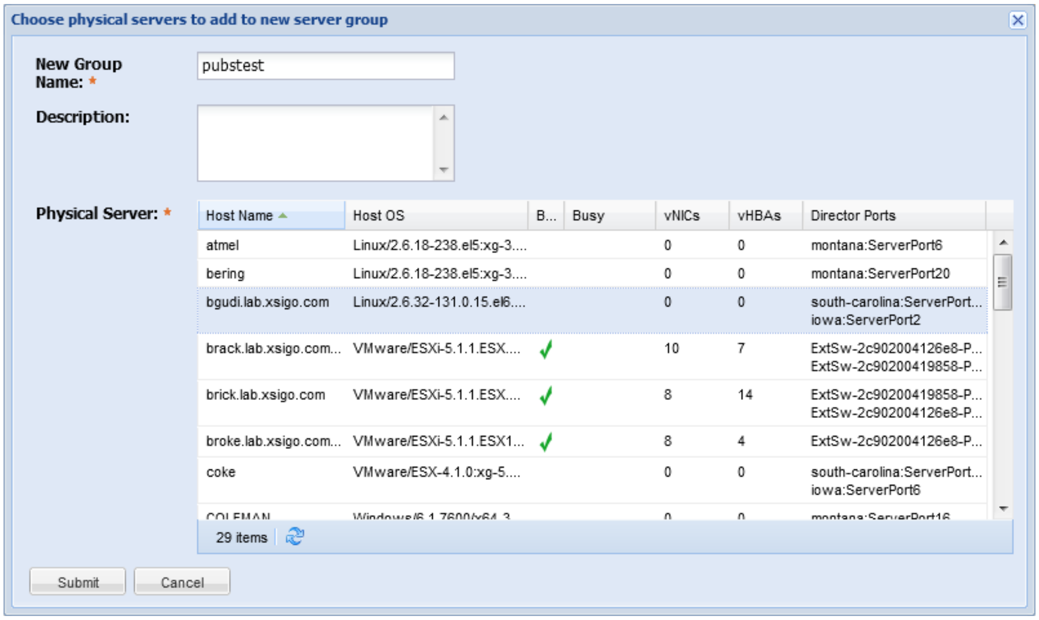
Server Group Summary

Group Name	Number of Servers	Bound	Description
dave	0		
rRserverGroup	1	✓	
notdave	0		can be deleted

3 items

Figure 4 Server Group Summary

Step 2 Click the plus sign to display the Create a Server Group dialog. Figure 5 shows this figure.



Choose physical servers to add to new server group

New Group Name: * pubstest

Description:

Physical Server: *

Host Name	Host OS	B...	Busy	vNICs	vHBAs	Director Ports
atmel	Linux/2.6.18-238.el5:xg-3....			0	0	montana:ServerPort6
bering	Linux/2.6.18-238.el5:xg-3....			0	0	montana:ServerPort20
bgudi.lab.xsigo.com	Linux/2.6.32-131.0.15.el6....			0	0	south-carolina:ServerPort... iowa:ServerPort2
brack.lab.xsigo.com...	VMware/ESXi-5.1.1.ESX....	✓		10	7	ExtSw-2c902004126e8-P... ExtSw-2c90200419858-P...
brick.lab.xsigo.com	VMware/ESXi-5.1.1.ESX....	✓		8	14	ExtSw-2c90200419858-P... ExtSw-2c902004126e8-P...
broke.lab.xsigo.com...	VMware/ESXi-5.1.1.ESX1...	✓		8	4	ExtSw-2c902004126e8-P...
coke	VMware/ESX-4.1.0:xg-5....			0	0	south-carolina:ServerPort... iowa:ServerPort6
COLEMAN	Windows/6.1.7600/x64.3			0	0	montana:ServerPort16

29 items

Figure 5 Server Group — Choose Physical Servers for Server Group

Step 3 In the *New Group Name* field, enter the name of the Server Group that you are creating.

Step 4 As an option, in the *Description* field, you can enter a description for the server group that you are creating.

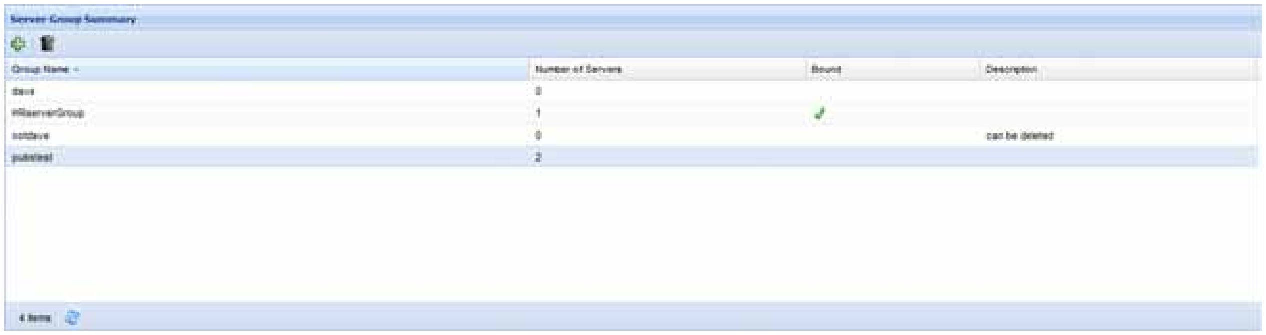
Step 5 From the *Physical Servers* table, select the servers that you want in the server group that you are creating. You can select one server to create the server group, then add more servers. Or, you can select multiple servers at once in the Physical Servers table.

- You can use bound servers to create a server group.
- You can mix bound and unbound servers to create a server group.

Step 6 When the servers are selected, click ***Submit*** to create the server group. When you click ***Submit***, a confirmation dialog is displayed to verify that you want to create the server group from the selected servers.

Step 7 On the confirmation dialog, click ***Yes*** to create the server group. When you click ***Yes***, the Server Group Summary is displayed.

Step 8 Check the Server Group Summary to verify that the server group was created with the correct number of servers, as shown in Figure 6.



Server Group Summary

Group Name ▾	Number of Servers	Bound	Description
dave	0		
rRserverGroup	1	✓	
notdave	0		can be deleted
pubstest	2		

4 items

Figure 6 Server Group Summary

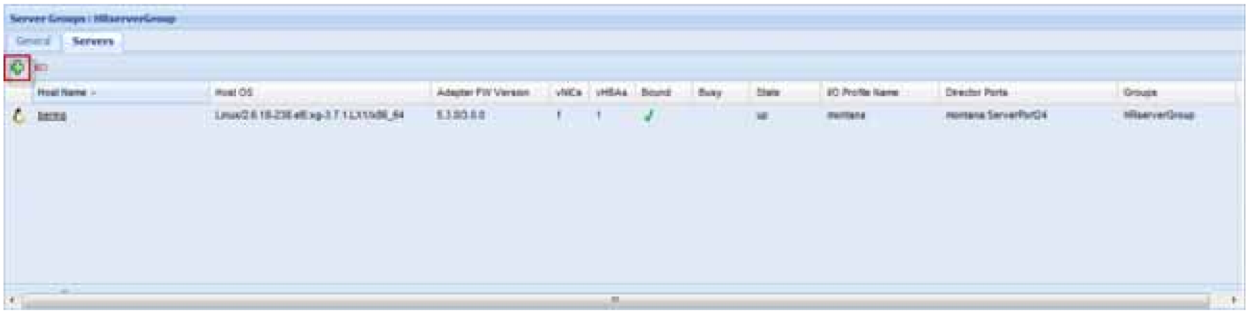
Adding Servers to Server Groups

If a server group is configured, you can add more standalone servers to it. The servers you add can be either unassigned to an existing server group, or part of an existing server group. Servers can be bound or unbound, and of different types, but typically server groups are created from servers that have some kind of similarity (hardware, OS, hypervisor, or function). The following procedure assumes that a server group already exists. If it doesn’t, it must be created before adding more servers to it. (The following procedure is valid even for an “empty” server group, which is a server group that is created with no servers in it.)

To add servers to an existing server group, follow this procedure:

Step 1 On the Server Group Summary, click to select the server group to which you want to add more servers. This step populates the details frame with the information for the server group you select.

Step 2 On the Server Group details frame, click the *Servers* tab to display the Servers in the Server Group. See Figure 7.

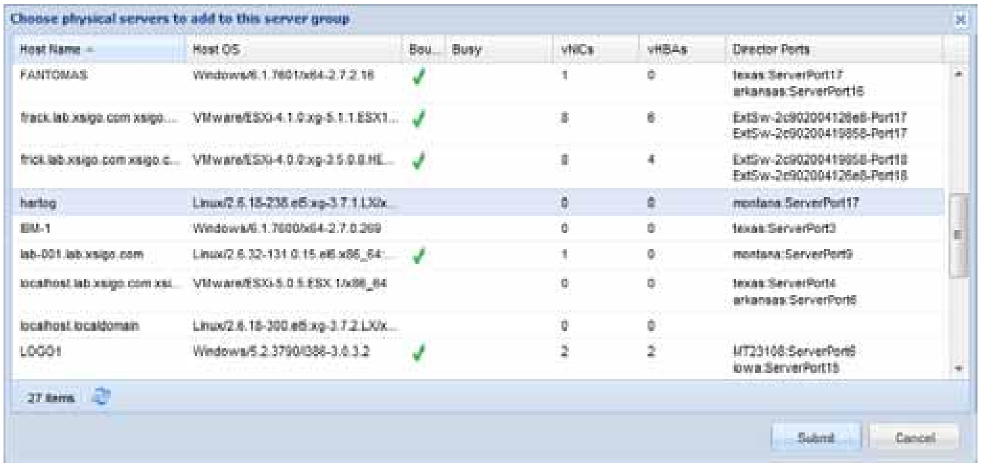


Server Groups : HRserverGroup

Host Name	Host OS	Adapter FW Version	vNICs	vHBAs	Bound	Busy	State	I/O Profile Name	Director Ports	Groups
berma	Linux/2.6.18-238.el5.xg-3.7.1.LX/x86_64	5.3.00.0.0	1	1	✓		up	montana	montana:ServerPort24	HRserverGroup

Figure 7 Server Group Details —Servers in the Server Group

Step 3 On the *Servers* tab, click the plus sign (+) to display the Choose Physical Server to Add to Server Group dialog as shown in Figure 8.



Choose physical servers to add to this server group

Host Name	Host OS	Bou...	Busy	vNICs	vHBAs	Director Ports
FANTOMAS	Windows/6.1.7601/x64-2.7.2.16	✓		1	0	texas:ServerPort17 arkansas:ServerPort16
frack.lab.xsigo.com.xsigo....	VMware/ESXi-4.1.0.xg-5.1.1.ESX1...	✓		8	6	ExtSw-2c902004126e8-Port17 ExtSw-2e90200419858-Port17
frick.lab.xsigo.com.xsigo.c...	VMware/ESXi-4.0.0.xg-3.5.0.8.HE...	✓		8	4	ExtSw-2c90200419858-Port18 ExtSw-2e902004126e8-Port18
hartog	Linux/2.6.18-238.el5.xg-3.7.1.LX/x...			8	8	montana:ServerPort17
EM-1	Windows/6.1.7600/x64-2.7.0.269			0	0	texas:ServerPort3
lab-001.lab.xsigo.com	Linux/2.6.32-131.0.15.el6.x86_64:...	✓		1	0	montana:ServerPort9
localhost.lab.xsigo.com.xsi...	VMware/ESXi-5.0.5.ESX.1/x86_64			0	0	texas:ServerPort4 arkansas:ServerPort6
localhost.localdomain	Linux/2.6.18-300.el5.xg-3.7.2.LX/x...			0	0	
LOGO1	Windows/5.2.3790/i386-3.6.3.2	✓		2	2	MT23108:ServerPort6 iowa:ServerPort15

27 items

Figure 8 Add Server to Server Group

Step 4 When you have selected the sever(s) that you want to add to the existing Server Group, click ***Submit*** to add the selected servers.

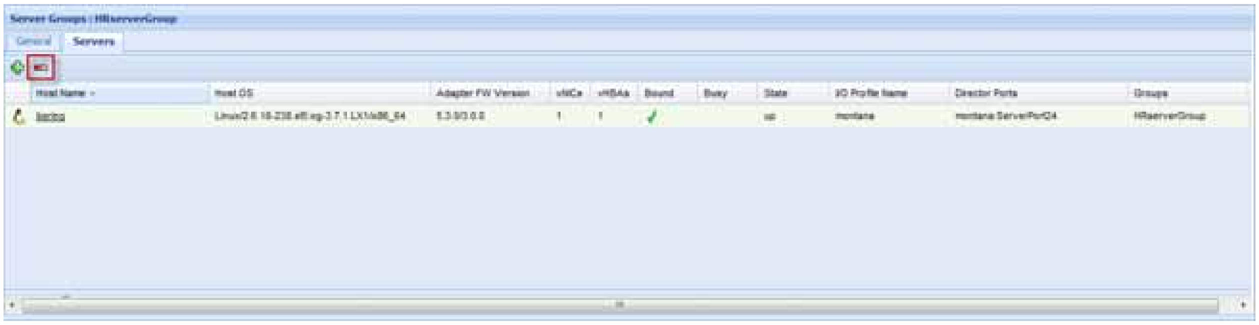
Removing Servers from Server Groups

When a Server Group is configured, you can delete individual servers from the Server Group at any time. When you delete a server, it reverts to being a single, standalone manageable object. When a server is deleted from a Server Group, it remains in the same operating state and has all the same software features (OS/hypervisor, host drivers, vNICs, vHBAs, and so on). The only difference is that it is no longer a member of a Server Group.

To remove servers from an existing server group, follow this procedure:

Step 1 On the Server Group Summary, click to select the server group from which you want to remove one or more servers. This step populates the details frame with the information for the server group you select.

Step 2 On the Server Group details frame, click the *Servers* tab to display the Servers in the Server Group. See Figure 9.



Server Groups : HRserverGroup

Host Name	Host OS	Adapter FW Version	vNICs	vHBAs	Bound	Busy	State	IO Profile Name	Director Ports	Groups
lambo	Linux/2.6.18-238.el5.eg-3.7.1.LX1/x86_64	5.3.0/3.0.0	1	1	✓		up	montana	montana.ServerPort24	HRserverGroup

Figure 9 Server Group Details —Servers in the Server Group

Step 3 On the *Servers* tab, click in the row(s) that contains the server(s) you want to delete. This step activates the ***Delete Server*** button, Do not click the server name or you will go to a different page where you cannot delete the server.

Step 4 When you have selected the sever(s) that you want to add to the existing Server Group, click the ***Delete Server*** button (the red minus sign) to delete the selected server(s) from the Server Group. It is possible to delete all servers from a Server Group. In this case, the Server Group is not deleted. It remains in Oracle's Xsigo Fabric Manager as an empty Server Group, which you can use as needed at any time.

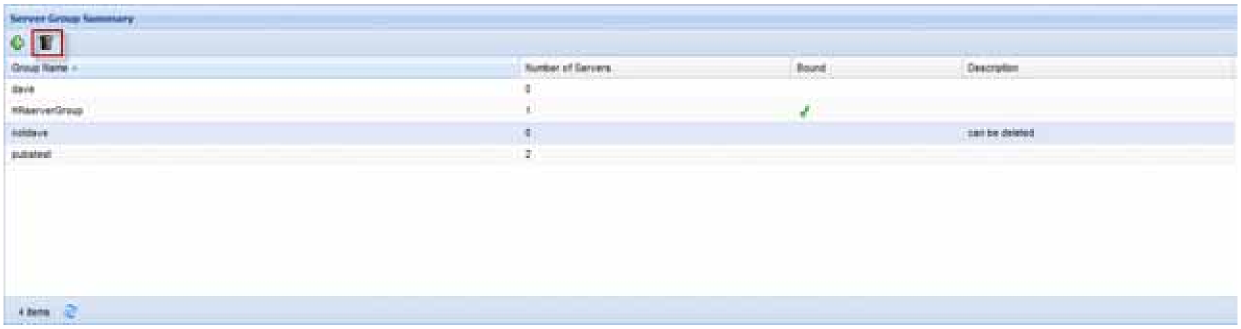
Deleting a Server Group

You can delete a server group at any time after the group is created. Deleting a server group removes the logical container around the servers, and as a result, the servers must be configured or managed individually. The servers are otherwise not affected. For example, any virtual resources that were migrated from servers in one server group to another remain deployed on the target server(s). Any I/O Templates that were assigned to the servers in the Server Group remain assigned.

To delete a server group, follow this procedure:

Step 1 From the navigation frame, display the Server Group Summary (*Server Resource Manager->Server Groups*).

Step 2 Click one or more server groups to select them, then click the garbage can icon as shown in Figure 10.



Server Group Summary

Group Name	Number of Servers	Bound	Description
dave	0		
HRserverGroup	1	✓	
noldave	0		can be deleted
pubstest	2		

4 items

Figure 10 Server Group Summary — Deleting a Server Group

When you click the garbage can icon, a confirmation dialog is displayed to verify that you actually want to delete the selected Server Groups.

Step 3 On the confirmation dialog, click ***Yes*** to accept the deletion and complete removing the selected Server Group(s).

Working with Boot Profiles

This chapter documents the creation and use of SAN Boot Profiles and iSCSI Boot Profiles.

For SAN Booting, this chapter contains the following topics:

- Understanding SAN Boot
- Overview of Setting Up SAN Boot
- Creating a SAN Boot Profile
- Create the Bootable I/O Template
- Displaying SAN Boot Profiles
- Displaying SAN Boot Profile Details
- Deleting a SAN Boot Profile

For iSCSI Booting, this chapter contains the following topics:

- Understanding iSCSI Boot
- Overview of Setting Up iSCSI Boot
- Creating an iSCSI Boot Profile
- Create the Bootable I/O Template
- Create an I/O Profile from the I/O Template
- Displaying the iSCSI Boot Profiles
- Displaying iSCSI Boot Profile Details
- Deleting an iSCSI Boot Profile

Understanding SAN Boot

SAN Boot allows you to boot a server or virtual machine from a SAN disk accessed through a vHBA. The disk is identified by a target World Wide Port Name (WWPN) and Logical Unit Number (LUN) ID on a storage disk array. See Figure 1.

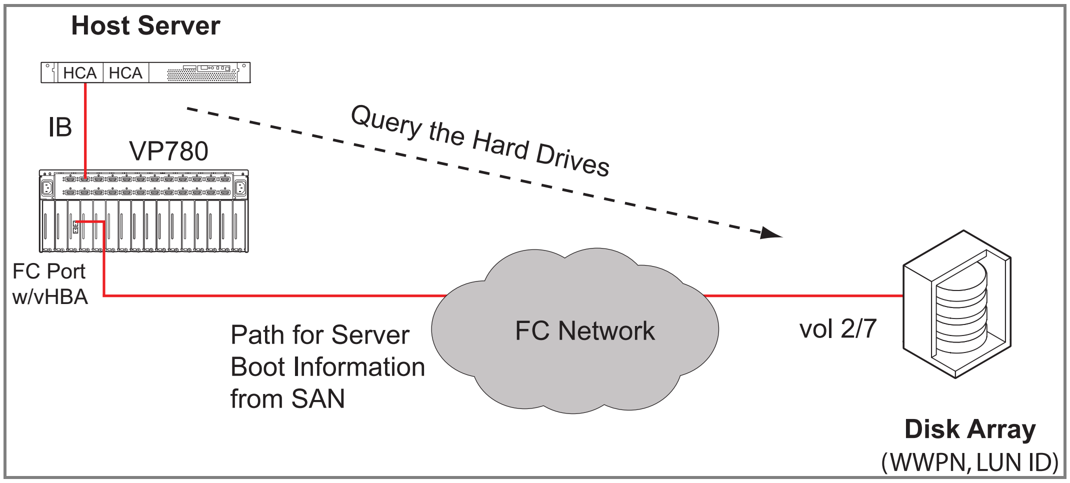
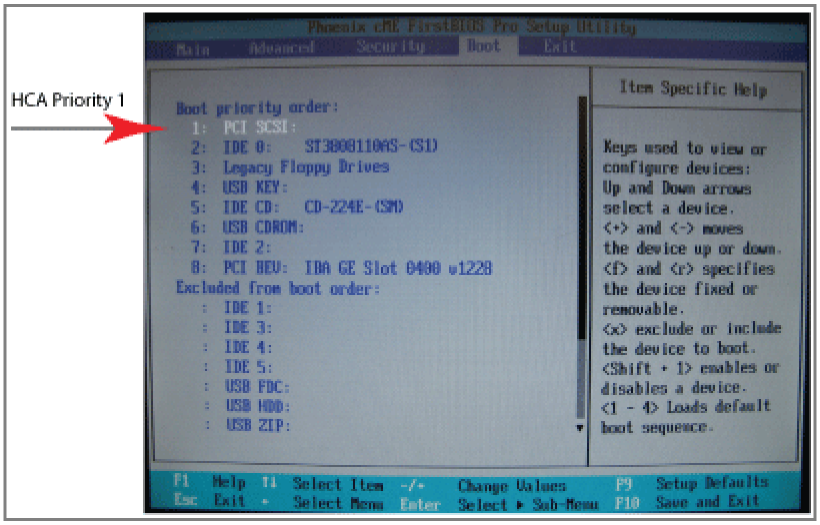


Figure 1 SAN Boot Topology

Understanding the SAN Boot Sequence

All computers boot from local boot devices. However to boot from a “remote” device, you need to make the device appear to be local. Xsigo implemented ROM BIOS extensions for HCA cards that follow these boot-sequence steps:

1. On power up, the server’s BIOS performs basic hardware initialization.
2. The host server establishes a connection to the Oracle Xsigo Fabric Director, where the system determines which vHBA to use and how to set up the communication path from the host server to the hard disk in the storage array.
3. BIOS reads the boot sequence, where the Xsigo HCA is the first boot device (highest priority) in the list. Be sure the Xsigo HCA is moved up from the “Excluded from boot order” list into the “Boot priority order” list. The HCA card appears as a generic “PCI SCSI” device, as shown in Figure 2.



```
Boot priority order:
  1:  PCI SCSI:
  2:  IDE 0:     ST3808110AS-(S1)
  3:  Legacy Floppy Drives
  4:  USB KEY:
  5:  IDE CD:    CD-224E-(SM)
  6:  USB CDROM:
  7:  IDE 2:
  8:  PCI BEV:   IBA GE Slot 0400 v1228
Excluded from boot order:
   :  IDE 1:
   :  IDE 3:
   :  IDE 4:
   :  IDE 5:
   :  USB FDC:
   :  USB HDD:
   :  USB ZIP:
```

```
Keys used to view or
configure devices:
Up and Down arrows
select a device.
<+> and <-> moves
the device up or down.
<f> and <r> specifies
the device fixed or
removable.
<x> exclude or include
the device to boot.
<Shift + 1> enables or
disables a device.
<1 - 4> Loads default
boot sequence.
```

F1 Help ↑↓ Select Item -/+ Change Values F9 Setup Defaults
Esc Exit ↔ Select Menu Enter Select ▸ Sub-Menu F10 Save and Exit

Figure 2 HCA is the “PCI SCSI” Device at Priority 1

4. The OS Loader is installed, which is specific to each OS:

   For Linux, the loader is GRand Unified Bootloader (GRUB). This loader resides in the boot sector of a bootable disk. The software responsible for loading the GRUB loader is held in the Option ROM of the HCA and runs in the context of the BIOS.

   When the loader runs, it typically reads a configuration file from the disk and allows the user to boot the operating system in a number of configurations. For GRUB, this file is called **`grub.conf`**.

   For Linux, GRUB will load the kernel and initrd into memory and begin running the kernel. The root file system (rootfs) given to the kernel will be the initrd. An initial RAM disk (initrd) is a compressed CPIO image (or compressed ext2 image for older kernels).

   The kernel runs a program in the initrd in the location `/init`. Typically this program is a shell script that loads the kernel modules and mounts the real root file system.

5. Interrogate the hard disk to determine if it is present and if the disk is bootable (or not). If the hard disk is bootable, the Xsigo HCA functions as a hard-disk controller. BIOS begins to treat the Xsigo HCA as the local ID controller for the local hard disk.

6. The data (Linux kernel) is sent from the hard disk and loaded into memory. The kernel begins to work and loads all the necessary drivers into the host server.

Additional information about preparing the host server for SAN Booting over a Xsigo vHBA is available through the *Remote Booting Guide*.

Overview of Setting Up SAN Boot

SAN Boot has the following phases:

1. Create the SAN Boot Profile
2. Create a Bootable I/O Template for either a single or dual path vHBA to the LUN that contains the SAN Boot information.
3. Create an I/O Profile.

For this procedure, you will find it helpful to have the following information available before starting the procedure:

- the Server GUID
- the LUN from which the server will be booting. This is the LUN where the server's boot information is located in the SAN. The Xsigo vHBA must be connected to this LUN to provide a path for the boot information to reach the server on which the vHBA is deployed.

Creating a SAN Boot Profile

When the physical server has been installed with a Xsigo HCA with SAN Boot Option ROM, SAN Boot requires a vHBA and a SAN Boot Profile to support server bootup from SAN disk.

As part of creating a SAN Boot Profile, you specify the root file system through a LUN on a target. The SAN Boot Profile supports different ways of mounting the root file system:

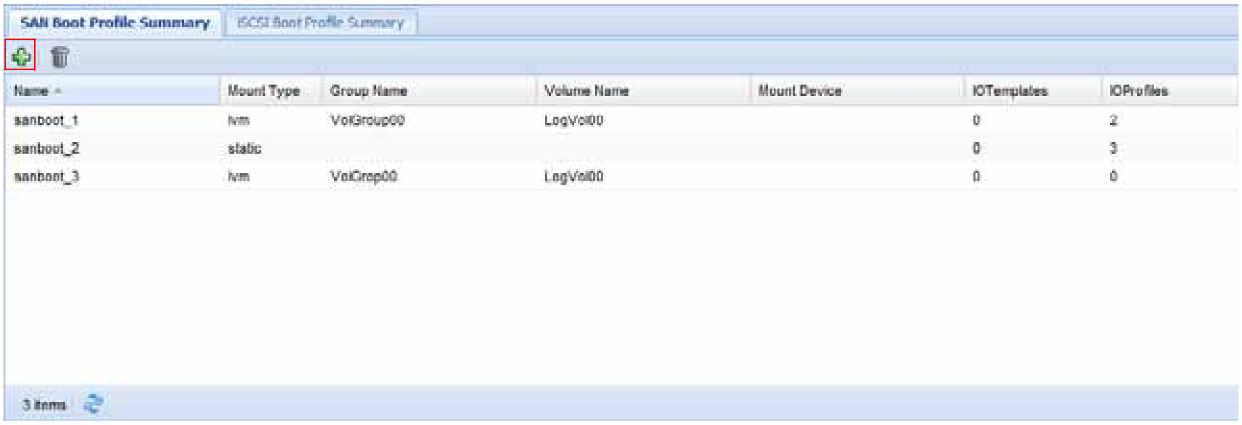
- direct, which allows you to specify a device name for the LUN that contains the boot image and the root file system, and always use that device name. Otherwise, when devices are discovered you cannot guarantee that the SAN boot device is used consistently.
- static, which allows you to manually specify the location of the SAN boot information and configure SAN booting on the host server.
- logical volume manager, which allows you to specify a group and volume that contain the root file system.

Be aware that the boot image must be entirely contained within one LUN. The boot image file cannot be striped across multiple LUNs. The root file system must also be entirely contained within one LUN.

When you configure a SAN Boot vHBA, the vHBA supports both SAN Boot and vHBA functionality.

To create a SAN Boot Profile, follow this procedure:

Step 1 On the navigation panel, select *Server Resource Manager->Boot Profiles->SAN Boot Profile Summary* tab. Figure 3 shows the SAN Boot Profile Summary.

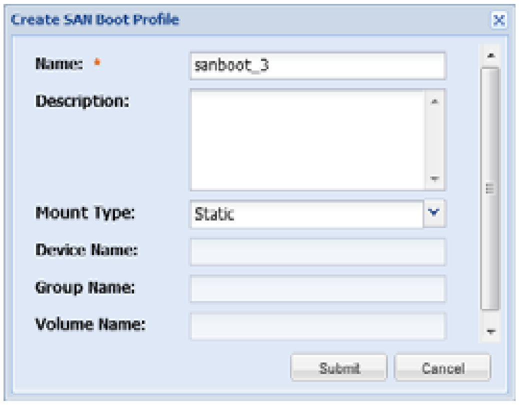


Name	Mount Type	Group Name	Volume Name	Mount Device	IOTemplates	IOProfiles
sanboot_1	lvm	VolGroup00	LogVol00		0	2
sanboot_2	static				0	3
sanboot_3	lvm	VolGrop00	LogVol00		0	0

Figure 3 SAN Boot Profile Summary

Notice that the SAN Boot Profile Summary supports adding a new SAN Boot Profile or deleting a configured SAN Boot Profile through the plus sign (+) and garbage can icon, respectively.

Step 2 Click the plus sign (+) to start the Create SAN Boot Profile dialog. Figure 4 shows this dialog.



Name: * sanboot_3
Description:
Mount Type: Static
Device Name:
Group Name:
Volume Name:

Figure 4 Configure SAN Boot Profile

Mount types Static, Direct Attach, and Logical Volume Manager are supported for SAN Boot Profiles. For more information, see the following sections:

- Creating a Static SAN Boot Profile.
- Creating a Direct-Attach SAN Boot Profile.
- Creating a Logical Volume Manager SAN Boot Profile.

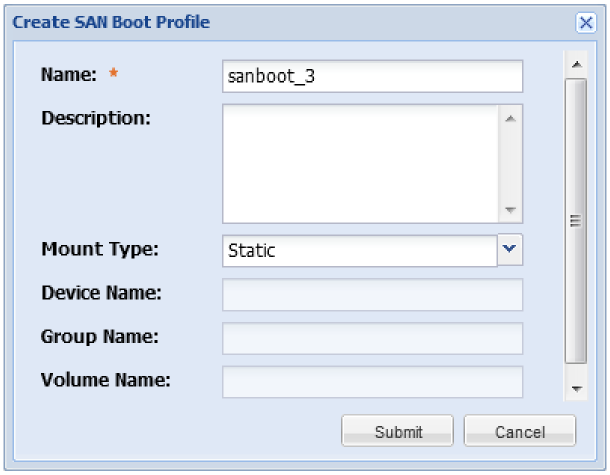
Creating a Static SAN Boot Profile

To configure a static SAN Boot Profile:

Step 3 In the *Name* field, enter the name for the SAN Boot Profile that you are creating. The name can be an alphanumeric character string, and typically relates to the server(s) that use the SAN Boot Profile—for example, `LinuxFinance` for all the Linux servers in the Finance server group.

Step 4 As an option, in the *Description* field, you can enter a description for the SAN Boot Profile that you are creating.

Step 5 From the *Mount Type* dropdown menu, select *Static* as shown in Figure 5.



Create SAN Boot Profile

Name: * sanboot_3

Description:

Mount Type: Static

Device Name:

Group Name:

Volume Name:

Figure 5 Create SAN Boot Profile — Static

Step 6 Click ***Submit*** to create the SAN Boot Profile.

At this point, the SAN Boot Profile is configured. However, for the server to receive the SAN Boot information, it must have a vHBA configured on the server, which occurs by configuring an I/O Profile from the I/O Template that contains the bootable vHBA, then connecting the I/O Profile to the server. For information about I/O Profiles, see Working with I/O Profiles.

Also, the server's BIOS boot order must be edited to insert the Xsigo HCA as the highest priority boot device in the server's boot priority list. See Understanding SAN Boot.

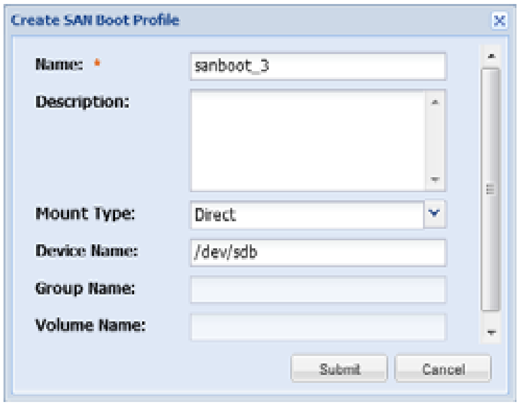
Creating a Direct-Attach SAN Boot Profile

To configure the SAN Boot Profile for Direct Attached storage:

Step 7 In the *Name* field, enter the name for the SAN Boot Profile that you are creating. The name can be an alphanumeric character string, and typically relates to the server(s) that use the SAN Boot Profile—for example, `LinuxFinance` for all the Linux servers in the Finance server group.

Step 8 As an option, in the *Description* field, you can enter a description for the SAN Boot Profile that you are creating.

Step 9 From the *Mount Type* dropdown menu, select *Direct* as shown in Figure 6.



Create SAN Boot Profile

Name: * sanboot_3

Description:

Mount Type: Direct

Device Name: /dev/sdb

Group Name:

Volume Name:

Figure 6 Configure SAN Boot Profile — Direct Boot

Step 10 In the *Device Name* field, enter the name of the server's boot device that will receive the SAN boot information (kernel and initrd) from the SAN.

Step 11 Click ***Submit*** to create the SAN Boot Profile.

At this point, the SAN Boot Profile is configured. However, for the server to receive the SAN Boot information, it must have a vHBA configured on the server, which occurs by configuring an I/O Profile from the I/O Template that contains the bootable vHBA, then connecting the I/O Profile to the server. For information about I/O Profiles, see Working with I/O Profiles.

Also, the server's BIOS boot order must be edited to insert the Xsigo HCA as the highest priority boot device in the server's boot priority list. See Understanding SAN Boot.

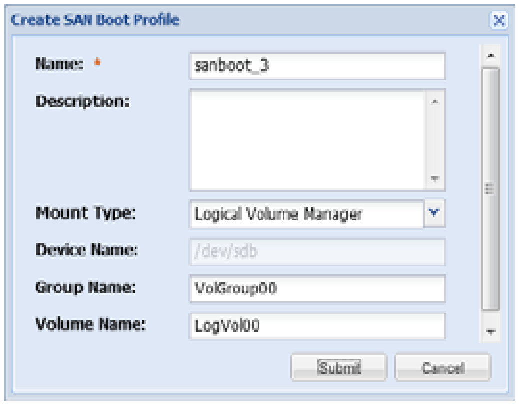
Creating a Logical Volume Manager SAN Boot Profile

To configure the SAN Boot Profile for Logical Volume Manager (LVM):

Step 12 In the *Name* field, enter the name for the SAN Boot Profile that you are creating. The name can be an alphanumeric character string, and typically relates to the server(s) that use the SAN Boot Profile—for example, `LinuxFinance` for all the Linux servers in the Finance server group.

Step 13 As an option, in the *Description* field, you can enter a description for the SAN Boot Profile that you are creating.

Step 14 From the *Mount Type* dropdown menu, select *Logical Volume Manager* as shown in Figure 7.



Create SAN Boot Profile

Name: * sanboot_3

Description:

Mount Type: Logical Volume Manager

Device Name: /dev/sdb

Group Name: VolGroup00

Volume Name: LogVol00

Figure 7 Configure SAN Boot Profile — Direct Boot

Step 15 In the *Group Name* field, enter the name of the Volume Group that contains the volume where SAN Boot information is located.

Step 16 In the *Volume Name* field, enter the name of the volume on which the SAN Boot information is located.

Step 17 Click ***Submit*** to create the SAN Boot Profile.

Step 18 Proceed to the next section.

Also, the server's BIOS boot order must be edited to insert the Xsigo HCA as the highest priority boot device in the server's boot priority list. See Understanding SAN Boot.

Create the Bootable I/O Template

When the SAN Boot Profile is created, you must associate an I/O Template with it. The I/O Template provides the vHBA that connects the LUN in the SAN where the server's boot information (kernel, boot image, and so on) are located. This section documents how to create an I/O Template with a bootable vHBA. After creating the bootable template, you will need to also create an I/O Profile from that I/O Template. For more information about I/O Profiles, see Working with I/O Profiles.

When you create the I/O Template for the SAN Boot Profile, make sure that you select the bootable field. Without this setting the vHBA in the I/O Template will not be able to support SAN Boot functionality. When the bootable option is set, it does not preclude the vHBA from carrying standard read and write data. Instead, the bootable option allows the vHBA to support SAN Booting the server in addition to read and write I/O.

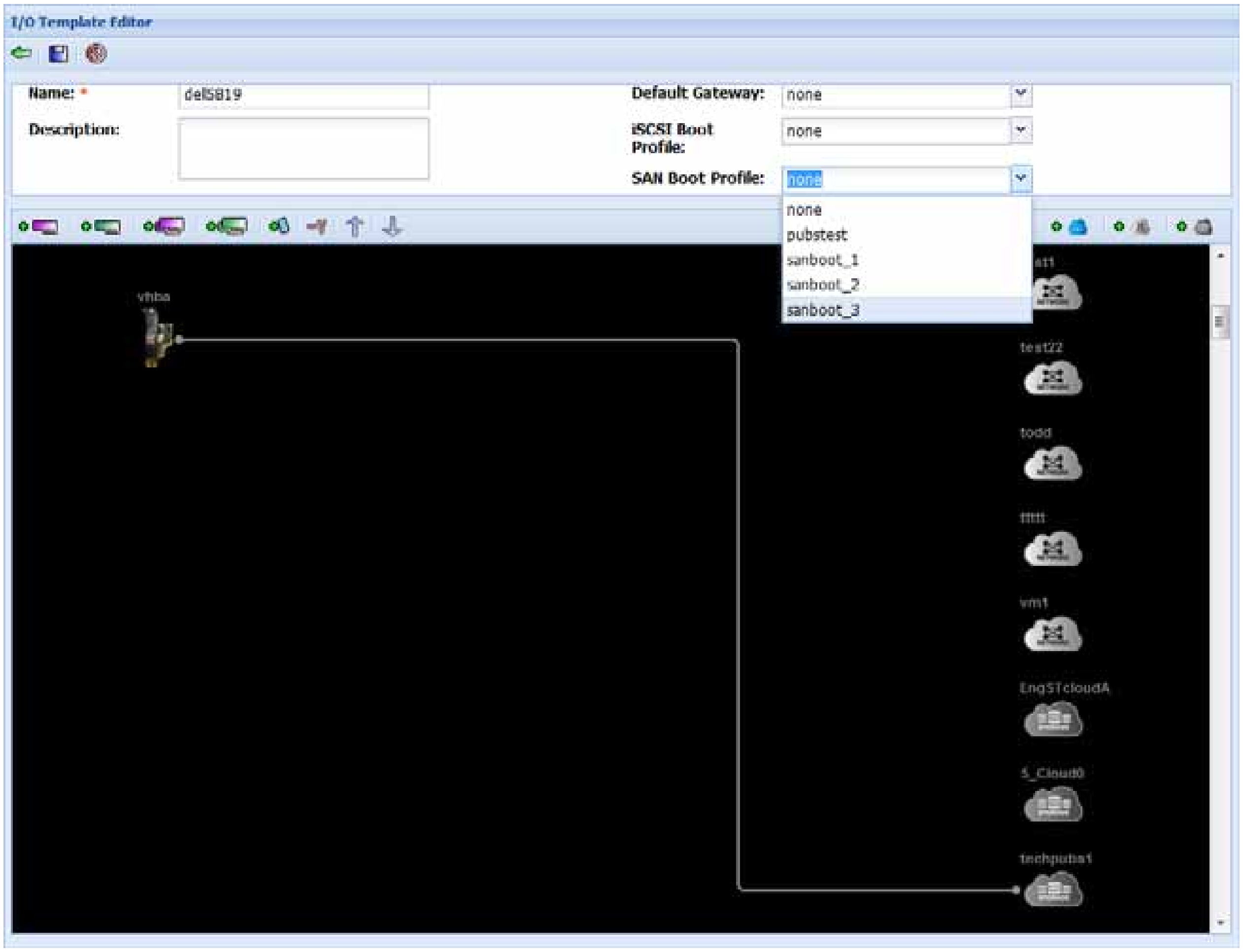
Oracle's Xsigo Fabric Manager supports SAN Boot functionality through one or two paths, which are configured through the I/O Template.

- Single Path Bootable I/O Template
- Dual Path Bootable I/O Template

Single Path Bootable I/O Template

To create the bootable I/O Template, follow this procedure:

Step 1 Select *Server Resource Manager->I/O Templates* to display the I/O Template summary, then click the plus sign (+) to display the I/O Template Editor. Figure 8 shows the I/O Template Editor.



I/O Template Editor

Name: * dell5819

Description:

Default Gateway: none

iSCSI Boot Profile: none

SAN Boot Profile: none

Figure 8 I/O Template, SAN Bootable

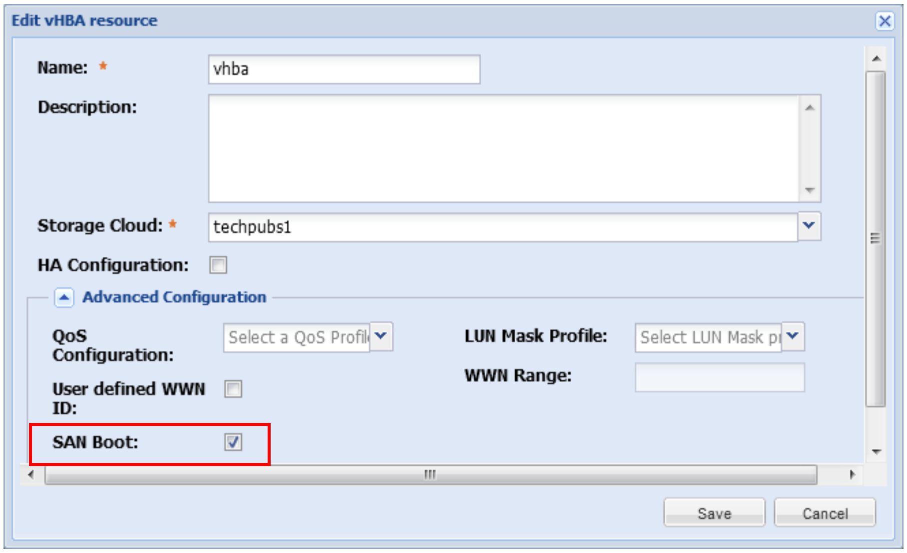
Step 2 In the *Name* field, enter the name of the I/O Template that will be used for SAN Booting.

Step 3 From the SAN Boot Profile dropdown menu, make sure to select the SAN Boot Profile you just created in the preceding section. Without creating the I/O Template as a bootable I/O Template, the server where the vHBA is deployed cannot be SAN Booted.

Step 4 Click and drag the vHBA to the appropriate Storage Cloud to terminate the vHBA on an FC port.

Step 5 Double click the vHBA icon on the I/O Template work space to display the Edit vHBA Resource dialog.

Step 6 On the Edit vHBA Resource dialog, click the ***Advanced Configuration*** button to display the advanced properties for the selected vHBA. Figure 9 shows this dialog.



Edit vHBA resource

Name: * vhba

Description:

Storage Cloud: * techpubs1

HA Configuration: □

Advanced Configuration

QoS Configuration: Select a QoS Profil

LUN Mask Profile: Select LUN Mask pr

User defined WWN ID: □

WWN Range:

SAN Boot: ☑

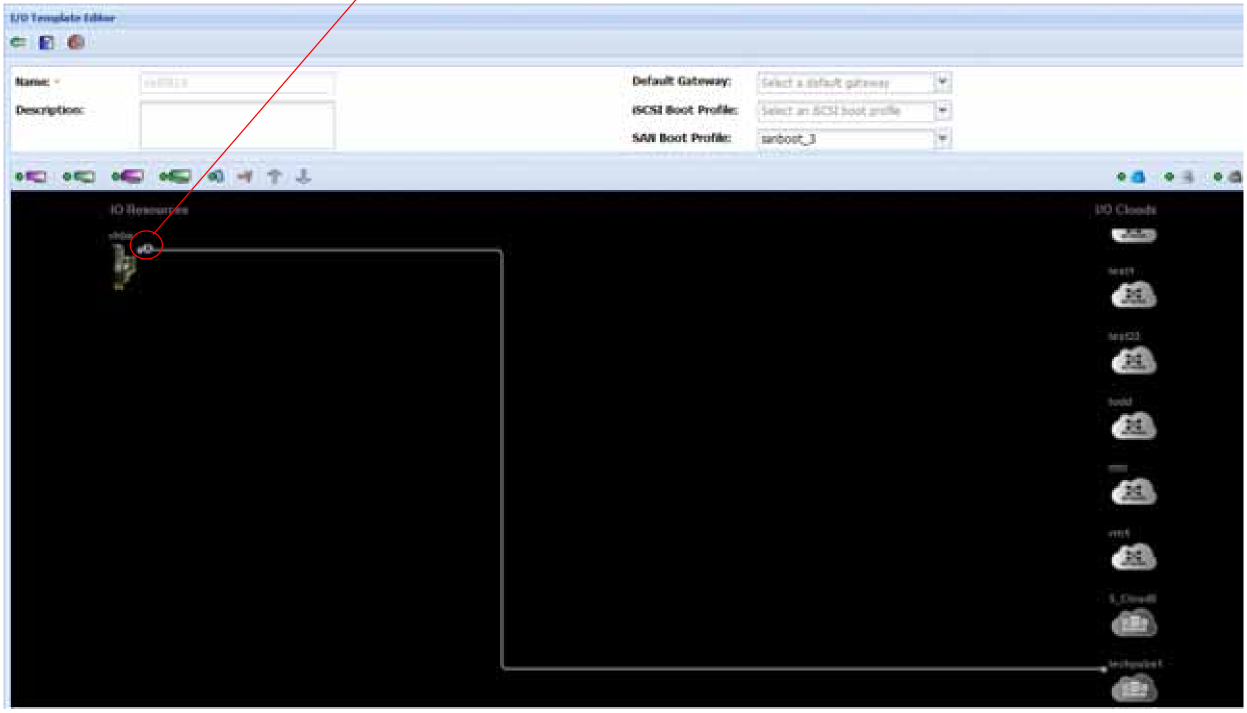
Figure 9 Edit vHBA Resource, Setting a Bootable vHBA

Step 7 Click the *SAN Boot* checkbox. The checkbox must contain a check mark for SAN Booting capabilities to be supported on the vHBA.

Step 8 Click ***Save*** to return to the I/O Template Editor.

Step 9 Check the I/O Template Editor for the bootable icon (a circle with a red “B” within) associated with the server’s boot vHBA. The presence of this icon indicates that the vHBA connected to the host is bootable. Figure 10 shows a bootable vHBA.

Bootable vHBA Icon



Name:

Description:

Default Gateway: Select a default gateway

iSCSI Boot Profile: Select an iSCSI boot profile

SAN Boot Profile: sanboot_3

Figure 10 I/O Template with Single Bootable vHBA

If the “bootable” icon is not present, make sure the SAN Boot checkbox contains a checkmark, as shown in Figure 9.

Step 10 On the I/O Template Editor, click ***Save***. Without saving the I/O Template, all in-progress configuration will be lost.

Step 11 After the bootable I/O Template is configured, proceed to Create an I/O Profile from the I/O Template.

Dual Path Bootable I/O Template

Dual paths provide two paths to the same LUN so that a single point of failure through the Fabric Director’s fabric is eliminated and availability of the SAN Boot information is increased. If one path is not available, the second one usually is.

Be aware that the two paths in dual pathing are not true HA, so there is no automatic failover or failback if one of the paths is not available. Instead, dual pathing simply provides to connections for the server to SAN Boot. If one path is not available, user intervention is required to select the other path through host-side methods, such as multipathing software.

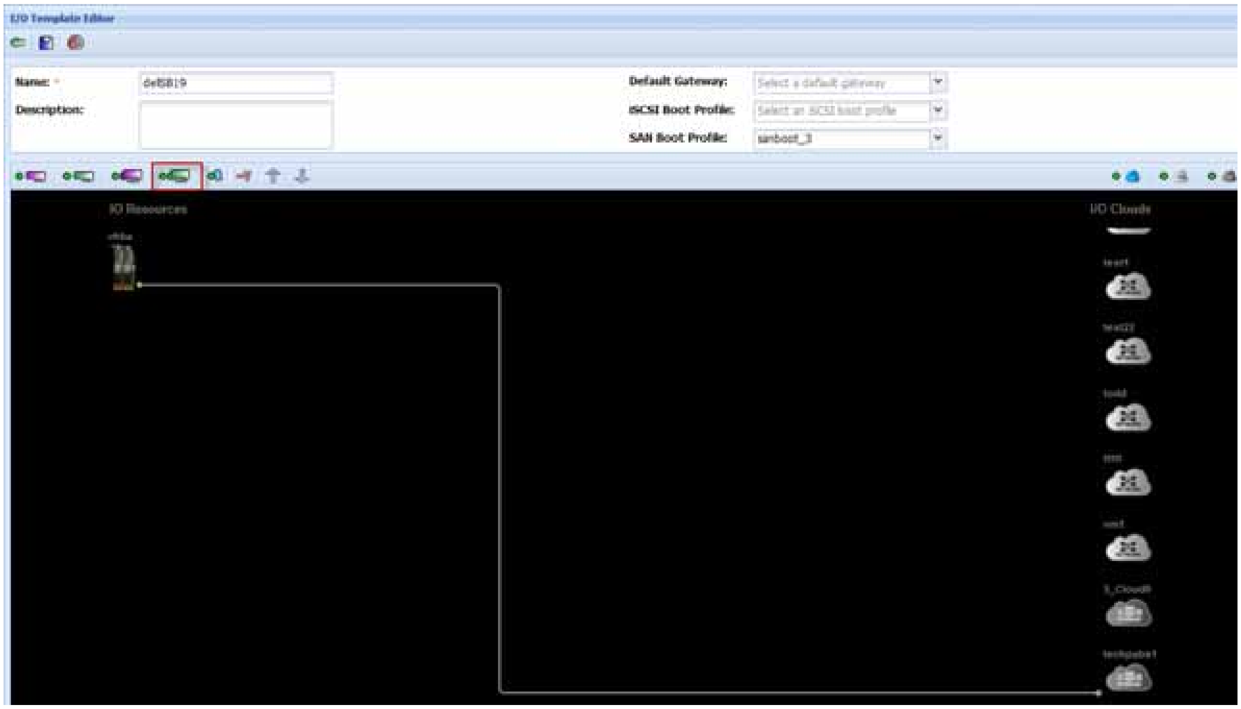
For dual path bootable I/O Tempaltes, two vHBAs are configured with the following considerations:

- Two fibre channel ports must be configured in the Storage Cloud. The HA vHBA cannot be created unless a minimum of two ports exist in the Storage Cloud. Depending on how you want the dual pathing to work, you can have storage ports on the same module or Fabric Director as long as the minimum of two ports exist in the Storage Cloud.
- On the I/O Template Editor, you must use the HA vHBAs option instead of creating two single vHBAs.
- The two vHBAs must connect to the *same LUN*. You cannot put the server's SAN Boot information on multiple LUNs. Since the two vHBAs will be connected to the same LUN, you will terminate the two vHBAs in the same Storage Cloud.

To create a dual path bootable I/O Template, follow this procedure:

Step 1 Select *Server Resource Manager->I/O Templates* to display the I/O Template summary, then click the plus sign (+) to display the I/O Template Editor.

Step 2 Click the ***Add an HA vHBA to Template*** button, then click and drag to connect the vHBA to the appropriate storage cloud, as shown in Figure 11.



I/O Template Editor

Name: * dell819

Description:

Default Gateway: Select a default gateway

iSCSI Boot Profile: Select an iSCSI boot profile

SAN Boot Profile: sanboot_3

Figure 11 I/O Template, Dual Path SAN Bootable

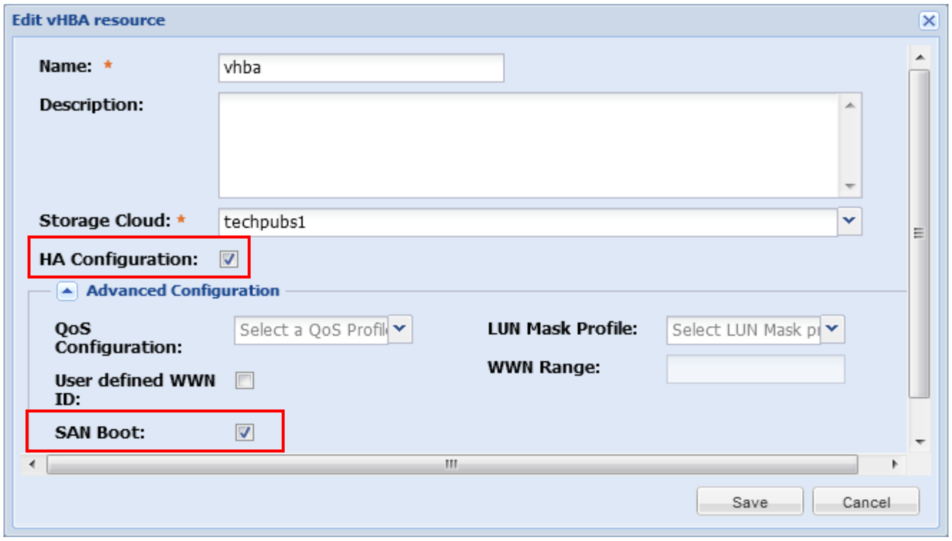
Step 3 In the *Name* field, enter the name of the I/O Template that will be used for SAN Booting.

Step 4 From the *SAN Boot Profile* dropdown menu, make sure to select the SAN Boot Profile you just created in the preceding section. Without creating the I/O Template as a bootable I/O Template, the server where the vHBA is deployed cannot be SAN Booted.

Step 5 Click and drag the vHBA to the appropriate Storage Cloud to terminate the vHBA on an FC port.

Step 6 Double click the vHBA icon on the I/O Template work space to display the Edit vHBA Resource dialog.

Step 7 On the Edit vHBA Resource dialog, click the ***Advanced Configuration*** button to display the advanced properties available to the HA vHBA that you are creating. Figure 12 shows this dialog.



Name: * vhba
Description:
Storage Cloud: * techpubs1
HA Configuration: ☑
QoS Configuration: Select a QoS Profil
LUN Mask Profile: Select LUN Mask pr
User defined WWN ID: □
WWN Range:
SAN Boot: ☑

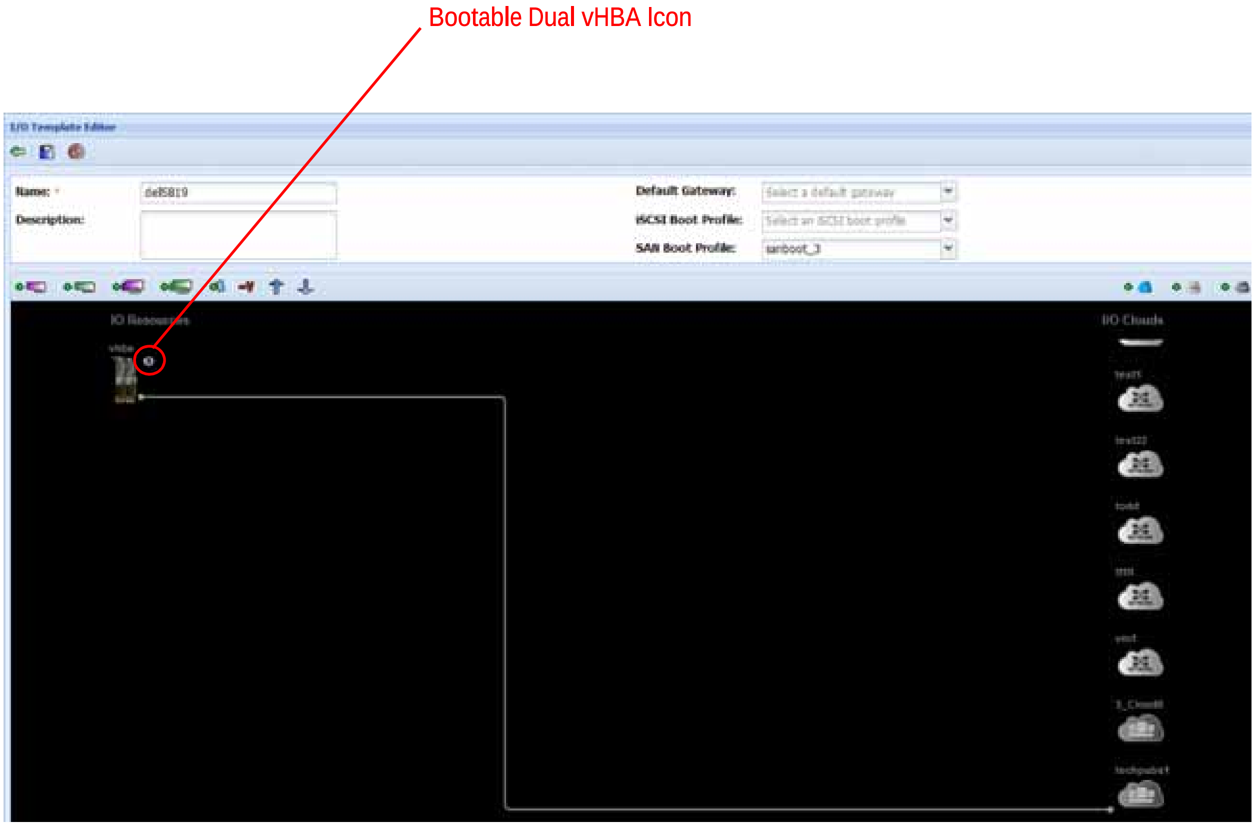
Figure 12 Edit vHBA Resource, Setting a Bootable vHBA

Step 8 On the Edit vHBA Resource dialog, make sure that the *HA Configuration* checkbox contains a checkmark. If it does not, click it now. Without this checkbox properly set, only one vHBA (and therefore one path) will be supported for SAN Booting the server.

Step 9 Click the *SAN Boot* checkbox. The checkbox must contain a check mark for SAN Booting capabilities to be supported on the vHBA.

Step 10 Click ***Save*** to return to the I/O Template Editor.

Step 11 Check the I/O Template Editor for the bootable icon (a circle with a red “B” within) associated with the server’s boot vHBAs. The presence of this icon indicates that the dual vHBAs connected to the host are bootable. Figure 13 shows a bootable vHBA pair.



Name: * del5819

Description:

Default Gateway: Select a default gateway

iSCSI Boot Profile: Select an iSCSI boot profile

SAN Boot Profile: sanboot_3

Figure 13 I/O Template with Single Bootable vHBA

If the “bootable” icon is not present, make sure the SAN Boot checkbox contains a checkmark, as shown in Figure 9.

Step 12 On the I/O Template Editor, click ***Save***. Without saving the I/O Template, all in-process configuration will be lost.

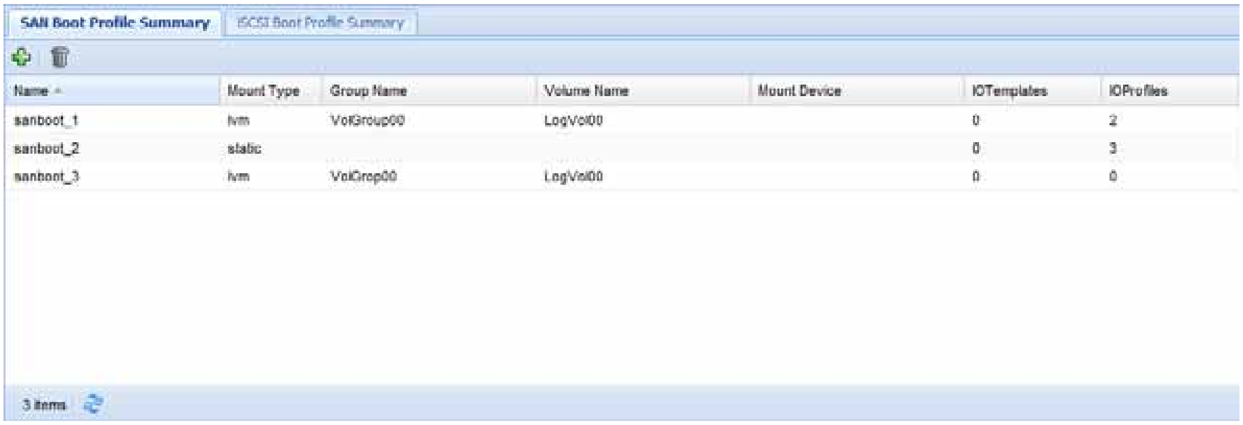
Step 13 After the bootable I/O Template is configured, proceed to Create an I/O Profile from the I/O Template.

Displaying SAN Boot Profiles

The SAN Boot Profiles are displayed in the SAN Boot Profile Summary, which contains information about all the SAN Boot Profiles that have been created through Fabric Manager. The table shows general information about the SAN Boot Profile such as the server profile and vHBA that support the connection to the SAN disk that contains the server’s kernel and initrd.

The SAN Boot Profile Summary also contains a link to the SAN Boot Details page where additional information about the configuration is available for the vHBA that is supporting the connection to the SAN disk that contains the server’s kernel and initrd.

Figure 14 shows the SAN Boot Profile Summary which is available through the *Server Resource Manager->Boot Profiles->SAN Boot Profile Summary.*



Name	Mount Type	Group Name	Volume Name	Mount Device	IOTemplates	IOProfiles
sanboot_1	lvm	VolGroup00	LogVol00		0	2
sanboot_2	static				0	3
sanboot_3	lvm	VolGrop00	LogVol00		0	0

Figure 14 SAN Boot Profile Summary

Table 1 shows the contents of the SAN Boot Profile Summary and explains what each field means.

Table 1 Contents of the SAN Boot Profile Summary

Field	Indicates
Name	The name of the SAN Boot Profile.
Mount Type	The type of mount configured on the SAN Boot vHBA. Valid values are: • static, for a Static SAN Boot Profile. • lvm, for the Logical Volume Manager. • direct, for assigning the device name that has the root file system.
Group Name	The logical volume manager (LVM) group name. If the mount type is LVM, this field displays the group name. If the mount type is other than LVM, no value is displayed.
Volume Name	The name of the logical volume that LVM uses for the root file system mount point.
Mount Device	The name of the device that contains the root file system mount point for the SAN Boot Profile.
I/O Template	The number of I/O Templates that are assigned to each SAN Boot Profile.
I/O Profiles	The number of I/O Profiles that are associated with each SAN Boot Profile.

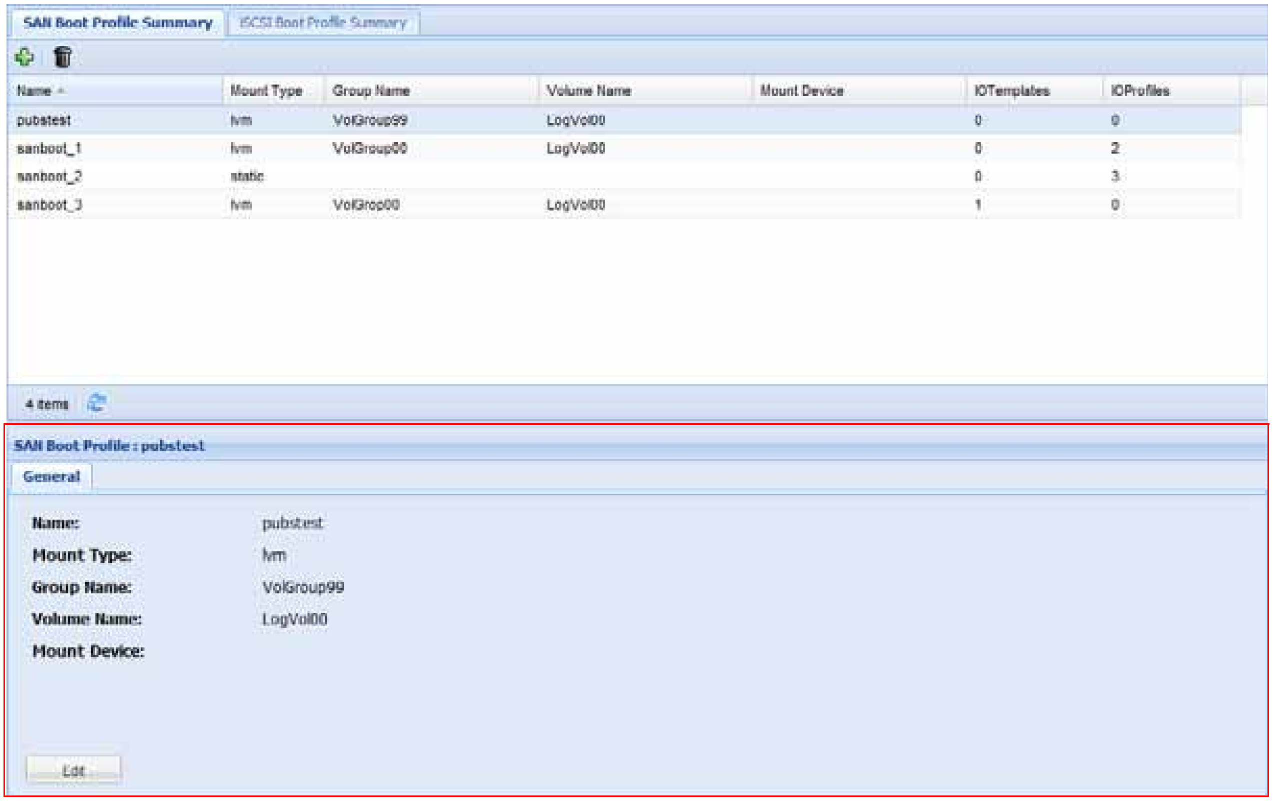
Displaying SAN Boot Profile Details

The SAN Boot Profile Details frame contains information about any configured SAN Boot Profiles. The SAN Boot Details frame contains only one instance of a SAN Boot, which is determined by the SAN Boot Profile that you select in the SAN Boot Profile Summary. By clicking a specific SAN Boot Profile in the summary, all of its corresponding details are available in the details frame.

Through the SAN Boot Profile Details Frame you can also edit a configured SAN Boot Profile to make changes to the profile without having to delete then re-add the profile. Be aware that:

- changes to the profile might also require resetting the server, or making changes to the server's configuration (for example, if a new boot device is specified, you might need to change the order of boot devices in the server's boot priorities list.)
- editing a SAN Boot Profile is allowed only when the SAN Boot Profile is not currently associated with an I/O Template.

The SAN Boot Profile Details Frame is in the Fabric Manager GUI just below the SAN Boot Summary Profile. Figure 15 shows the SAN Boot Profile Details frame.



Name	Mount Type	Group Name	Volume Name	Mount Device	IOTemplates	IOProfiles
pubstest	lvm	VolGroup99	LogVol00		0	0
sanboot_1	lvm	VolGroup00	LogVol00		0	2
sanboot_2	static				0	3
sanboot_3	lvm	VolGrop00	LogVol00		1	0

4 items

SAN Boot Profile : pubstest

Name:	pubstest
Mount Type:	lvm
Group Name:	VolGroup99
Volume Name:	LogVol00
Mount Device:	

Figure 15 SAN Boot Profile Details Frame

Table 2 shows the contents of the SAN Boot Profile Details frame, and explains what each field means. Not all fields will be populated based on the options specified during the configuration of the SAN Boot Profile. For example, if you created a direct connect SAN Boot Profile, none of the fields for logical volume manager will contain information.

Table 2 Contents of the SAN Boot Profile Details Frame

Field	Means
Name	The name assigned to the selected SAN Boot Profile.
Mount Type	The method used to mount the SAN location of the server’s SAN Boot information: • Direct • Static • Logical Volume Manager
Group Name	For Logical Volume Manager mount types, this field shows the logical group that contains the SAN location of the server’s SAN boot information.
Volume Name	For Logical Volume Manager mount types, this field shows the logical volume that contains the SAN location of the server’s SAN boot information.
Mount Device	For Direct mount types, this field shows the device that contains the root file system mount point for the server’s SAN Boot information.
I/O Template	The number of I/O Templates that are assigned to each SAN Boot Profile.
I/O Profiles	The number of I/O Profiles that are associated with each SAN Boot Profile.

Create an I/O Profile from the I/O Template

If you are setting up SAN Boot for a server that has already booted up and connected to the Fabric Director, you can now create an I/O Profile from the I/O Template. When the I/O Profile is created, it will contain the bootable vHBA that you created. You can create one more I/O Profiles from the same I/O Template.

For information about creating an I/O Profile, follow the procedure for creating an I/O Profile as documented in Creating an I/O Profile.

Connect the I/O Profile to a Physical Server

When you assign the I/O Profile to the server, you begin pushing the bootable vHBA and the associated SAN Boot Profile to the server.

To assign the I/O Template to a server, follow this procedure for connecting an I/O Profile to a Physical server, as documented in Connecting an I/O Profile to a Server.

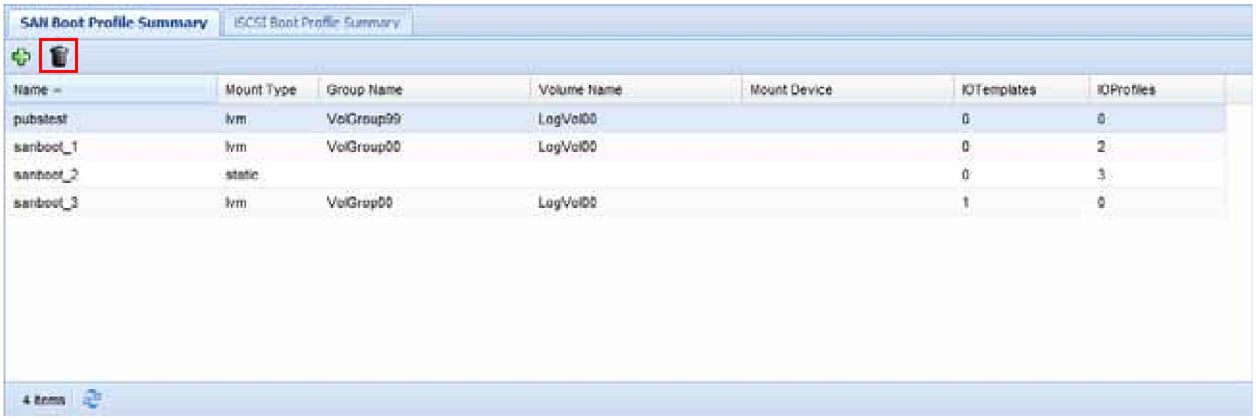
Deleting a SAN Boot Profile

Through the SAN Boot Profile Summary, you can delete a SAN Boot Profile. To delete a SAN Boot Profile, follow this procedure:

Step 1 On the navigation panel, click *Server Resource Manager->Boot Profiles->SAN Boot Profile Summary.* This step displays the SAN Boot Profile Summary.

Step 2 On the SAN Boot Profile Summary, select the SAN Boot Profile that you want to delete. This step activates the garbage can icon. You can select multiple SAN Boot profiles through standard keyboard conventions, for example by pressing the ***CTRL*** + click or ***Shift*** + click.

Step 3 Click the garbage can icon to delete the selected SAN Boot Profile as shown in Figure 16.



Name	Mount Type	Group Name	Volume Name	Mount Device	IOTemplates	IOProfiles
pubstest	lvm	VolGroup99	LogVol00		0	0
sanboot_1	lvm	VolGroup00	LogVol00		0	2
sanboot_2	static				0	3
sanboot_3	lvm	VolGrup00	LogVol00		1	0

Figure 16 Deleting a SAN Boot Profile

When you click the garbage can icon, a confirmation page is displayed to verify that you actually want to delete the selected SAN Boot Profile.

Step 4 Click ***OK*** to delete the selected SAN Boot Profile(s), or ***Cancel*** to abort the deletion.

Understanding iSCSI Boot

The I/O Director supports booting an ESX server over a vNIC using an iSCSI connection. Figure 17 illustrates the topology used to achieve iSCSI booting.

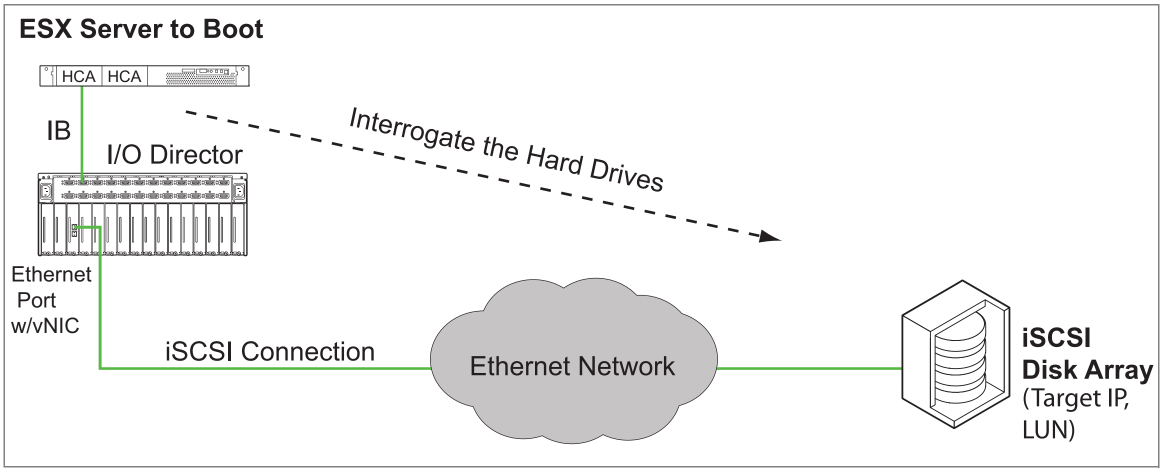


Figure 17 Linux Server iSCSI Boot Topology

Table 3 lists some terminology specific to iSCSI booting.

Table 3 iSCSI Boot Terms

Term	Definition
initiator	The host server that is booting over an iSCSI connection
target	The iSCSI array
IQN	An iSCSI qualified name of an initiator or target
target IP	The IP address of the target filer or array

Understanding the iSCSI Boot Procedure

When configuring iSCSI boot, you perform the same general steps as for any remote booting setup:

1. Install the SAN volume with the necessary bits.

   — iSCSI boot uses the same initrd that Linux SAN Boot uses. You cannot use the supported Linux installers over iSCSI. You can find additional affirmation about patching the Anaconda installer and installing the boot disk in the *Remote Booting Guide*'s “iSCSI Booting” chapter.

   — Alternatively, you can install over FC to the disk and then have your server boot over iSCSI. The iSCSI install options require a temporary FC or Ethernet connection to the volume.

2. Configure the I/O Director with the required virtual I/O resources.

   Create a vNIC and server profile, using either DHCP or static addressing.

3. Configure the host server with drivers and firmware to enable remote booting.

Overview of Setting Up iSCSI Boot

Setting up iSCSI Boot has the following phases:

1. Create the iSCSI Boot Profile
2. Create a Bootable I/O Template for either a single or dual path to the LUN that contains the SAN Boot information.
3. Create an I/O Profile. While the I/O Profile is being pushed to the host, you will be prompted to provide pertinent information, such as the iSCSI initiator to complete connecting the I/O Profile while the iSCSI Boot configuration is being pushed to the server.

For this procedure, you will find it helpful to have the following information available before starting the procedure:

- the Server GUID
- the LUN from which the server will be booting. This is the LUN where the server's boot information is located on the iSCSI storage array. The Xsigo vNIC must be connected to this LUN to provide a path for the boot information to reach the server on which the vNIC is deployed.
- the target IQN (T-IQN), which you can get by logging into the storage.
- the initiator IQN (I-IQN), which you can get by displaying the vNIC properties. On the Fabric Director, you can get this information by issuing the **`show server-profile`** `<profile-name>` **`iscsi-boot -detail`** command. The **`-detail`** qualifier is required to display the I-IQN.

Creating an iSCSI Boot Profile

Creating an iSCSI Boot Profile enables the host server to access its boot information over a boot capable vNIC which connects the server to its boot information. The iSCSI boot information is supported on the server through a Xsigo HCA and option ROM, which must be present in the host server that will be iSCSI booting. If the Xsigo HCA and option ROM are not yet installed, install them now. This section documents how to create an iSCSI Boot Profile.

When an iSCSI Boot Profile is created, the necessary information is available for booting the server over a vNIC that connects to its boot information on iSCSI storage. However, the bootable vNIC that connects the server to the network is not configured as part of creating an iSCSI Boot Profile. The iSCSI Boot Profile must be connected to an I/O Template which contains a valid bootable vNIC for iSCSI booting. For information about creating an I/O Template, see Working with I/O Templates.

As part of creating an iSCSI Boot Profile, you specify the root file system through a LUN on a target. The iSCSI Boot Profile supports different ways of mounting the root file system:

- direct, which allows you to specify a device name for the LUN that contains the boot image and the root file system, and always use that device name. Otherwise, when devices are discovered you cannot guarantee that the iSCSI boot device is used consistently.
- static, which allows you to manually specify the location of the iSCSI boot information and configure iSCSI booting on the host server.
- logical volume manager, which allows you to specify a group and volume that contain the root file system.

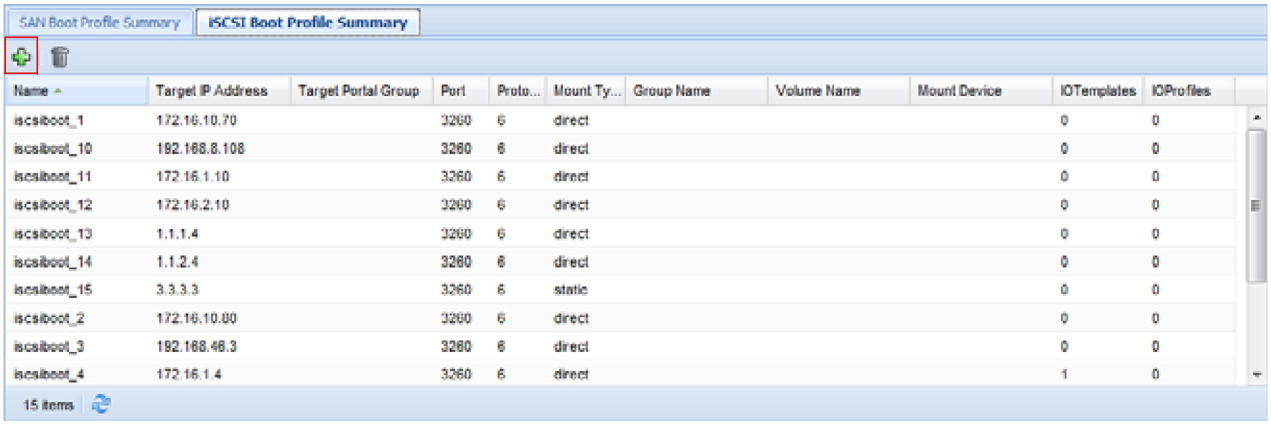
Be aware that the boot image must be entirely contained within one LUN. The boot image file cannot be striped across multiple LUNs. The root file system must also be entirely contained within one LUN.

You also must specify the target IP Address Group, which is the IP address of the target filer or array.

When you configure an iSCSI Boot vNIC, the vNIC supports both iSCSI Boot and standard virtual I/O functionality.

To create an iSCSI Boot Profile, follow this procedure:

Step 1 On the navigation panel, select *Server Resource Manager->Boot Profiles->iSCSI Boot Profile Summary* tab. Figure 18 shows the iSCSI Boot Profile Summary.

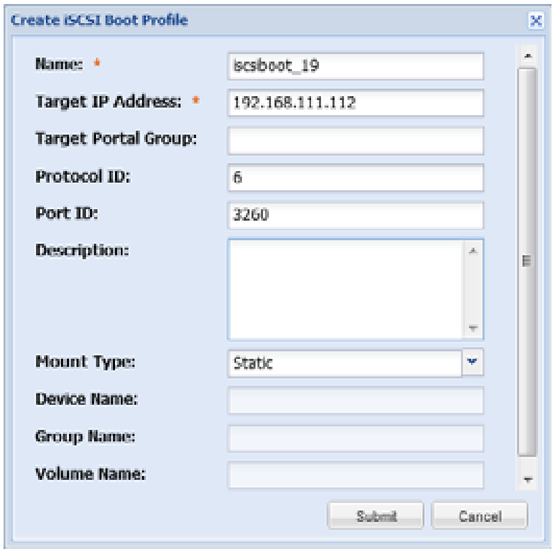


Name	Target IP Address	Target Portal Group	Port	Proto...	Mount Ty...	Group Name	Volume Name	Mount Device	IOTemplates	IOProfiles
iscsiboot_1	172.16.10.70		3260	6	direct				0	0
iscsiboot_10	192.168.8.108		3260	6	direct				0	0
iscsiboot_11	172.16.1.10		3260	6	direct				0	0
iscsiboot_12	172.16.2.10		3260	6	direct				0	0
iscsiboot_13	1.1.1.4		3260	6	direct				0	0
iscsiboot_14	1.1.2.4		3260	6	direct				0	0
iscsiboot_15	3.3.3.3		3260	6	static				0	0
iscsiboot_2	172.16.10.80		3260	6	direct				0	0
iscsiboot_3	192.168.48.3		3260	6	direct				0	0
iscsiboot_4	172.16.1.4		3260	6	direct				1	0

Figure 18 iSCSI Boot Profile Summary

Through the iSCSI Profile Summary, you can add a new iSCSI Boot Profile or delete a selected iSCSI Boot Profile through the plus sign (+) and garbage can icon, respectively.

Step 2 Click the plus sign to display the Create iSCSI Boot Profile dialog. Figure 19 shows this dialog.


Create iSCSI Boot Profile

Name: * iscsiboot_19
Target IP Address: * 192.168.111.112
Target Portal Group:
Protocol ID: 6
Port ID: 3260
Description:
Mount Type: Static
Device Name:
Group Name:
Volume Name:

Figure 19 Create iSCSI Boot Profile

Step 3 In the *Name* field, enter an alphanumeric character string that will name the iSCSI Boot Profile that you are creating.

Step 4 In the *Target IP Address* field, enter the IP Address group for the filer or array that contains the server’s iSCSI Boot information.

Step 5 In the *Target Portal Group* field, enter the IP address for the iSCSI Portal Group. Depending on your iSCSI storage array, this field might not be required.

Step 6 In the *Protocol ID* field, enter the number of the protocol that will be supporting iSCSI communication. This field is populated with a default value, but you can change the communication protocol number if you need to.

Step 7 In the *Port ID* field, enter the port number that will support the iSCSI communication between the server and the location of the server’s iSCSI Boot information. This field is populated with a default value, but you can change the communication port number if you need to.

Step 8 As an option, in the *Description* field, you can enter an alphanumeric character string that describes the iSCSI Boot Profile that you are creating.

Step 9 From the *Mount Type* dropdown menu, select one of the following methods of mounting the location of the server’s SAN Boot Profile:

- *Static*, in which the iSCSI Boot profile connects to the statically assigned storage through the same vNIC. To configure this iSCSI Boot Profile, proceed to Creating a Static iSCSI Boot Profile.
- *Direct*, in which the iSCSI Boot Profile connects to the same server boot device. To configure this iSCSI Boot Profile, proceed to Creating a Direct Attach iSCSI Boot Profile.
- *Logical Volume Manager*, which contains a pointer to a LUN and Volume Group that contains the iSCSI Boot information. To configure this iSCSI Boot Profile, proceed to Creating a Logical Volume Manager iSCSI Boot Profile.

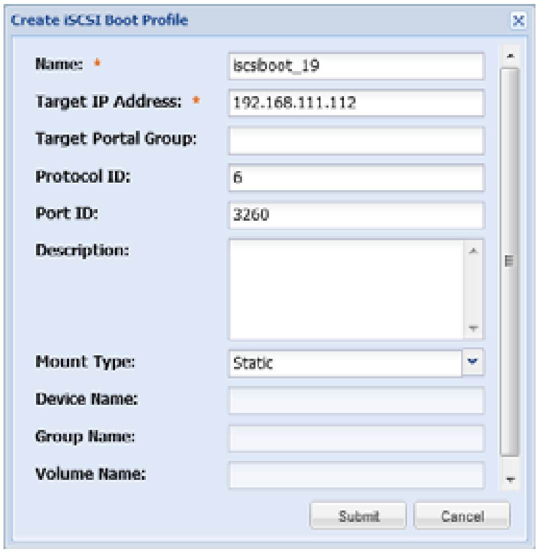
Creating a Static iSCSI Boot Profile

To configure a static iSCSI Boot Profile:

Step 10 In the *Name* field, enter the name for the iSCSI Boot Profile that you are creating. The name can be an alphanumeric character string, and typically relates to the server(s) that use the iSCSI Boot Profile.

Step 11 As an option, in the *Description* field, you can enter an alphanumeric character string that describes the iSCSI Boot Profile that you are creating.

Step 12 From the *Mount Type* dropdown menu, select *Static* as shown in Figure 20.



Name: * iscsboot_19
Target IP Address: * 192.168.111.112
Target Portal Group:
Protocol ID: 6
Port ID: 3260
Description:
Mount Type: Static
Device Name:
Group Name:
Volume Name:

Figure 20 Create SCSI Boot Profile — Static

Step 13 Click ***Submit*** to create the iSCSI Boot Profile.

At this point, the iSCSI Boot Profile is configured. However, for the server to receive the iSCSI Boot information, it must have a bootable vNIC configured on the server, which occurs by configuring an I/O Profile from the I/O Template that contains the bootable vNIC, then connecting the I/O Profile to the server. For information about I/O Profiles, see Working with I/O Profiles.

Also, the server's BIOS boot order must be edited to insert the Xsigo HCA as the highest priority boot device in the server's boot priority list. See Understanding SAN Boot.

Step 14 Proceed to Create the Bootable I/O Template.

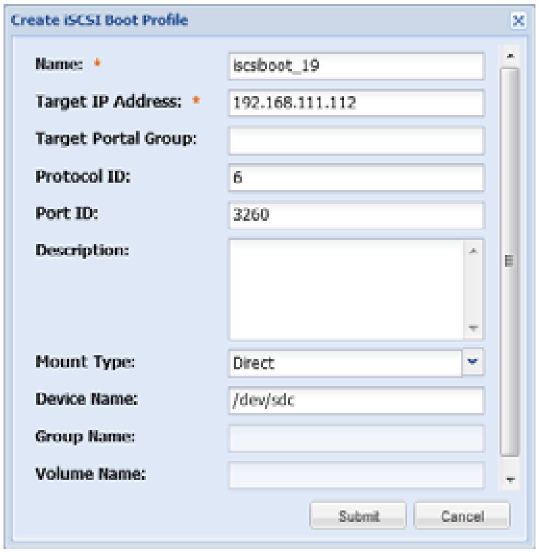
Creating a Direct Attach iSCSI Boot Profile

To configure a direct attach iSCSI Boot Profile:

Step 15 In the *Name* field, enter the name for the iSCSI Boot Profile that you are creating. The name can be an alphanumeric character string, and typically relates to the server(s) that use the iSCSI Boot Profile.

Step 16 As an option, in the *Description* field, you can enter an alphanumeric character string that describes the iSCSI Boot Profile that you are creating.

Step 17 From the *Mount Type* dropdown menu, select *Direct* as shown in Figure 21. This step activates the *Device Name* field.



Create iSCSI Boot Profile

Name: *	iscsiboot_19
Target IP Address: *	192.168.111.112
Target Portal Group:	
Protocol ID:	6
Port ID:	3260
Description:	
Mount Type:	Direct
Device Name:	/dev/sdc
Group Name:	
Volume Name:	

Figure 21 Configure SCSI Boot Profile — Direct Boot

Step 18 In the *Device Name* field, enter the name of the server's boot device that will receive the iSCSI boot information.

Step 19 Click ***Submit*** to create the iSCSI Boot Profile.

At this point, the iSCSI Boot Profile is configured. However, for the server to receive the iSCSI Boot information, it must have a bootable vNIC configured on the server, which occurs by configuring an I/O Profile from the I/O Template that contains the bootable vNIC, then connecting the I/O Profile to the server. For information about I/O Profiles, see Working with I/O Profiles.

Also, the server's BIOS boot order must be edited to insert the Xsigo HCA as the highest priority boot device in the server's boot priority list. See Understanding SAN Boot.

Step 20 Proceed to Create the Bootable I/O Template.

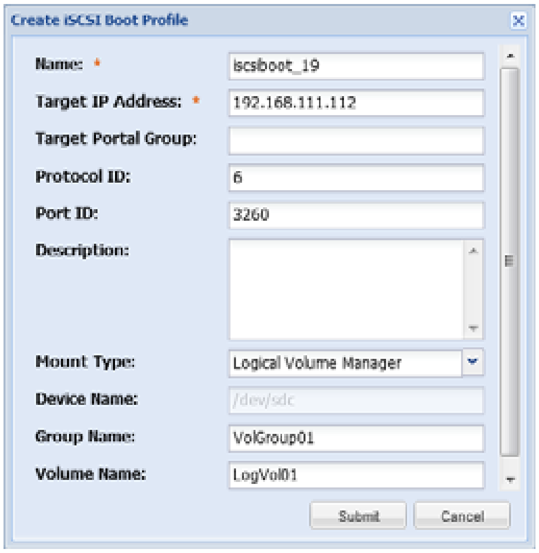
Creating a Logical Volume Manager iSCSI Boot Profile

To configure the iSCSI Boot Profile to use a logical volume manager:

Step 21 In the *Name* field, enter the name for the iSCSI Boot Profile that you are creating. The name can be an alphanumeric character string, and typically relates to the server(s) that use the iSCSI Boot Profile.

Step 22 As an option, in the *Description* field, you can enter an alphanumeric character string that describes the iSCSI Boot Profile that you are creating.

Step 23 From the *Mount Type* dropdown menu, select *Logical Volume Manager* as shown in Figure 22. This step activates the *Group Name* and *Volume Name* fields.



Create iSCSI Boot Profile

Name: *	iscsboot_19
Target IP Address: *	192.168.111.112
Target Portal Group:	
Protocol ID:	6
Port ID:	3260
Description:	
Mount Type:	Logical Volume Manager
Device Name:	/dev/sdc
Group Name:	VolGroup01
Volume Name:	LogVol01

Figure 22 Configure SCSI Boot Profile — Direct Boot

Step 24 In the *Group Name* field, enter the name of the Volume Group that contains the volume where the server’s iSCSI Boot information is located.

Step 25 In the *Volume Name* field, enter the name of the volume on which the server’s iSCSI Boot information is located.

Step 26 Click ***Submit*** to create the iSCSI Boot Profile.

At this point, the iSCSI Boot Profile is configured. However, for the server to receive the iSCSI Boot information, it must have a bootable vNIC configured on the server, which occurs by configuring an I/O Profile from the I/O Template that contains the bootable vNIC, then connecting the I/O Profile to the server. For information about I/O Profiles, see Working with I/O Profiles.

Also, the server’s BIOS boot order must be edited to insert the Xsigo HCA as the highest priority boot device in the server’s boot priority list. See Understanding SAN Boot.

Step 27 Proceed to Create the Bootable I/O Template.

Create the Bootable I/O Template

When the iSCSI Boot Profile is created, you must associate an I/O Template with it. The I/O Template provides the vNIC that connects the server to the LUN on the iSCSI storage array where the server’s boot information (kernel, boot image, and so on) are located. This section documents how to create an I/O Template with a bootable vNIC. For more information about I/O Templates, see Working with I/O Templates.

When you create the I/O Template for the iSCSI Boot Profile, make sure that you select the bootable field. Without this setting, the vNIC in the I/O Template will not be able to support iSCSI Boot functionality. When the bootable option is set, it does not preclude the vNIC from carrying standard network traffic. Instead, the bootable option allows the vNIC to support iSCSI Booting the server in addition to standard Ethernet and Gigabit Ethernet network traffic.

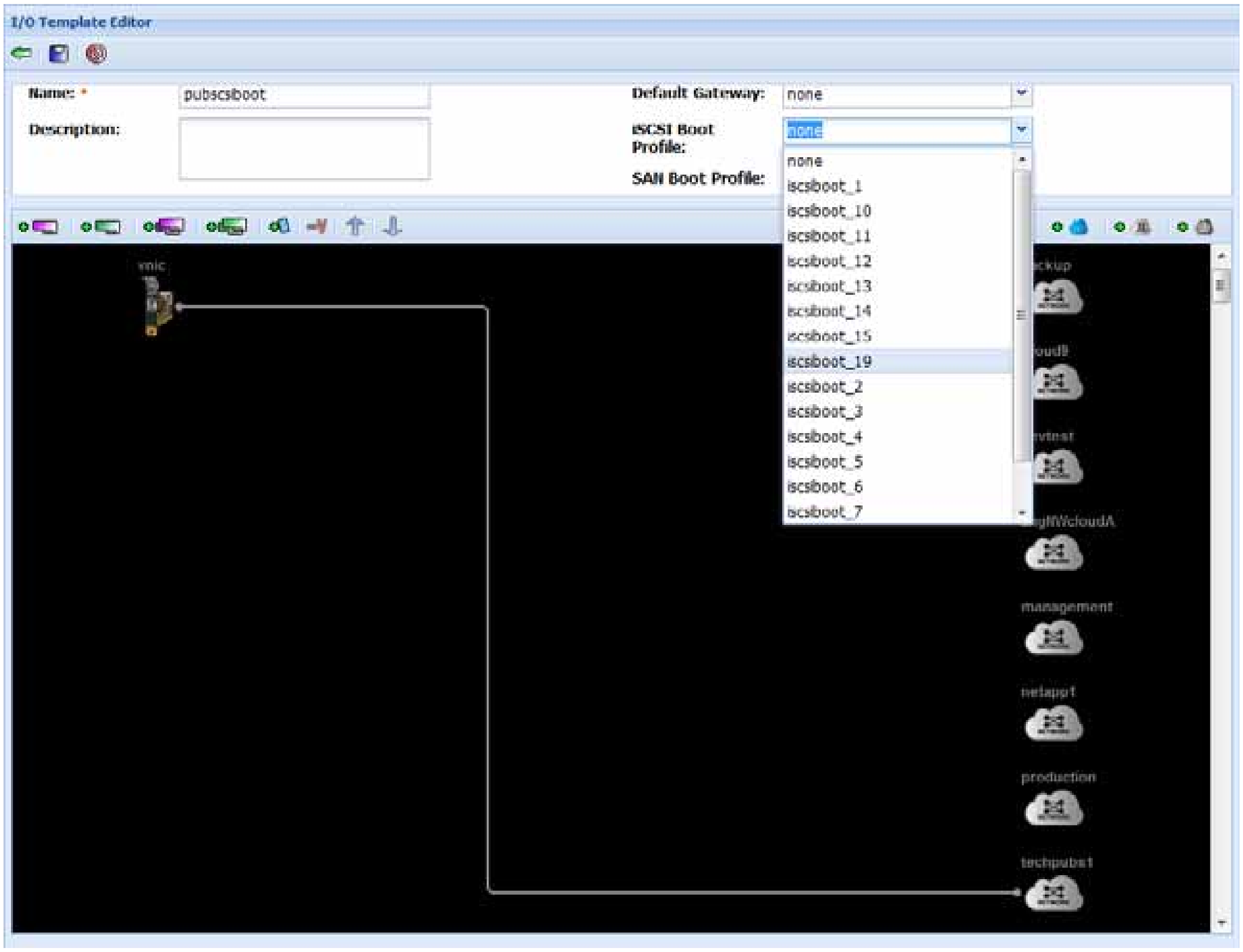
Fabric Manager supports iSCSI Boot functionality through one or two paths, which are configured through the I/O Template.

- Single Path Bootable I/O Template
- Dual Path Bootable I/O Template

Single Path Bootable I/O Template

To create the bootable I/O Template, follow this procedure:

Step 1 Select *Server Resource Manager->I/O Templates* to display the I/O Template summary, then click the plus sign (+) to display the I/O Template Editor. Figure 23 shows the I/O Template Editor.



I/O Template Editor

Name: * pubscsiboot

Description:

Default Gateway: none

iSCSI Boot Profile: none

SAN Boot Profile:

Figure 23 I/O Template, SCSI Bootable

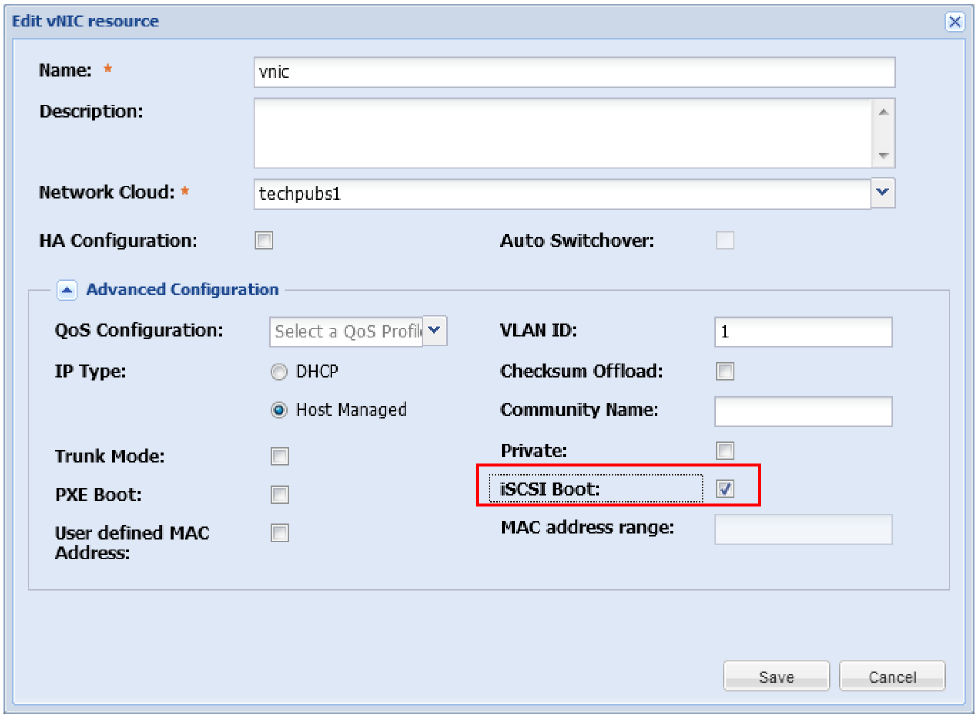
Step 2 In the *Name* field, enter the name of the I/O Template that will be used for SAN Booting.

Step 3 From the *iSCSI Boot Profile* dropdown menu, make sure to select the iSCSI Boot Profile you just created in the preceding section. Without creating the I/O Template as a bootable I/O Template, the server where the vNIC is deployed cannot be iSCSI Booted.

Step 4 Click and drag the vNIC to the appropriate Network Cloud to terminate the vNIC on an Ethernet port.

Step 5 Double click the vNIC icon on the I/O Template work space to display the Edit vNIC Resource dialog.

Step 6 On the Edit vNIC Resource dialog, click the *Advanced Configuration* button to display additional options for the vNIC—including the *iSCSI Boot* checkbox. Figure 24 shows this dialog.



Name: * vnic

Description:

Network Cloud: * techpubs1

HA Configuration: □ Auto Switchover: □

QoS Configuration: Select a QoS Profil

VLAN ID: 1

IP Type: ○ DHCP ● Host Managed

Checksum Offload: □

Community Name:

Trunk Mode: □

Private: □

PXE Boot: □

iSCSI Boot: ☑

User defined MAC Address: □

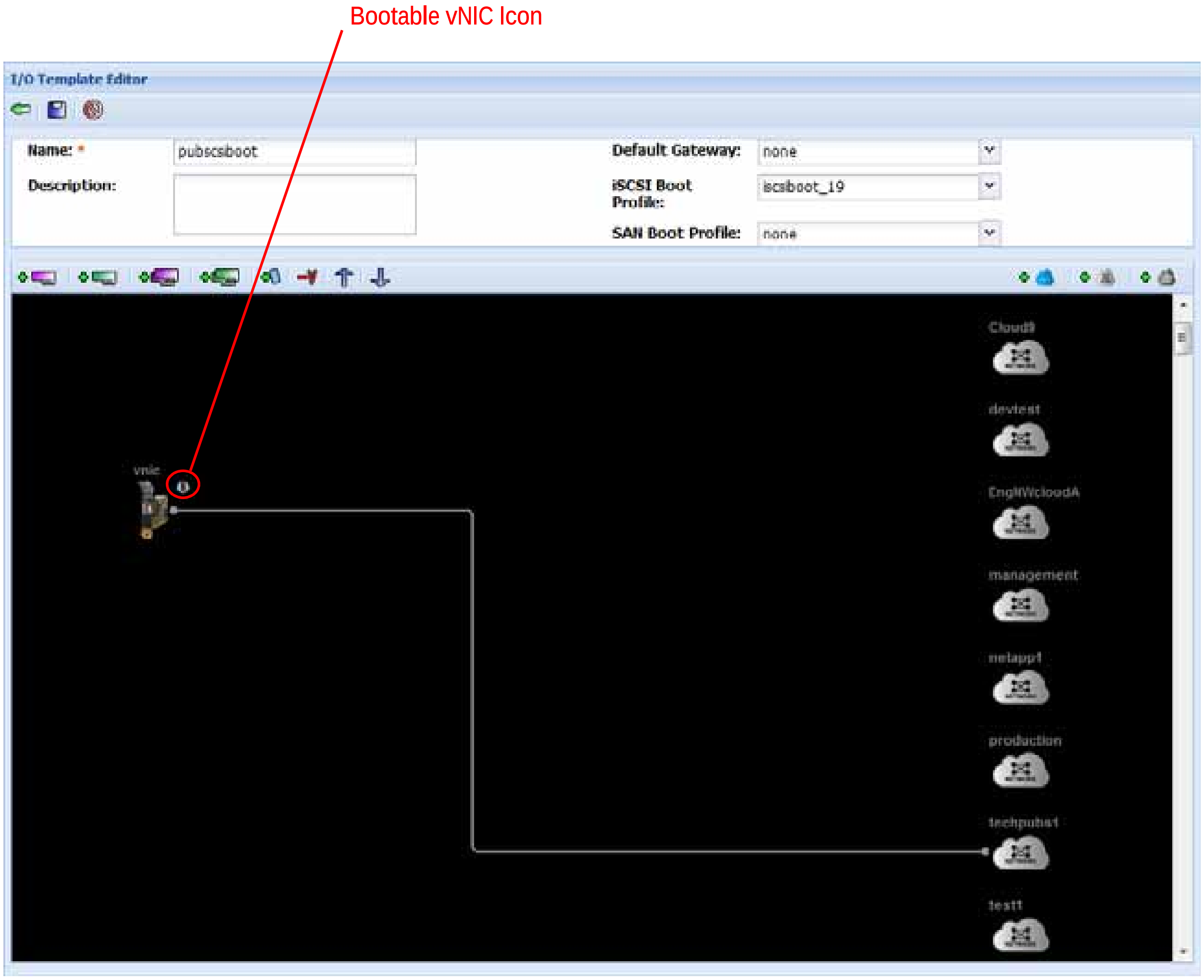
MAC address range:

Figure 24 Edit vNIC Resource, Setting a Bootable vNIC

Step 7 Click the *iSCSI Boot* checkbox. The checkbox must contain a check mark for iSCSI Booting capabilities to be supported on the vNIC.

Step 8 Click ***Save*** to return to the I/O Template Editor.

Step 9 Check the I/O Template Editor for the bootable icon (a circle with a red “B” within) associated with the server’s boot vNIC. The presence of this icon indicates that the vNIC connected to the host is bootable. Figure 25 shows a bootable vNIC.



Bootable vNIC Icon

I/O Template Editor

Name: *	pubscsiboot
Description:	
Default Gateway:	none
iSCSI Boot Profile:	iscsiboot_19
SAN Boot Profile:	none

Figure 25 I/O Template with Single Bootable vNIC

If the “bootable” icon is not present, make sure the iSCSI Boot checkbox contains a checkmark, as shown in Figure 24.

Step 10 On the I/O Template Editor toolbar, click ***Save***. Without saving the I/O Template, the pending I/O Template configuration will be lost.

Step 11 After the bootable I/O Template is configured, proceed to Create an I/O Profile from the I/O Template.

Dual Path Bootable I/O Template

Dual path provides two paths to the same LUN so that a single point of failure through the Fabric Director's fabric is eliminated and availability of the iSCSI Boot information is increased. If one path is not available, the second one is.

Be aware that the two paths in dual pathing are not true HA, so there is no automatic failover or failback if one of the paths is not available. Instead, dual pathing simply provides two connections for the server to iSCSI Boot. If one path is not available, user intervention is required to select the other path through host-side methods, such as multipathing software.

For dual path bootable I/O Tempaltes, two vNICs are configured with the following considerations:

- On the I/O Template Editor, you must use the HA vNICs option instead of creating two single vNICs.
- The two vNICs must connect to the *same LUN*. You cannot put the server's iSCSI Boot information on multiple LUNs. Since the two vNICs will be connected to the same LUN, you will terminate the two vNICs in the same Network Cloud.

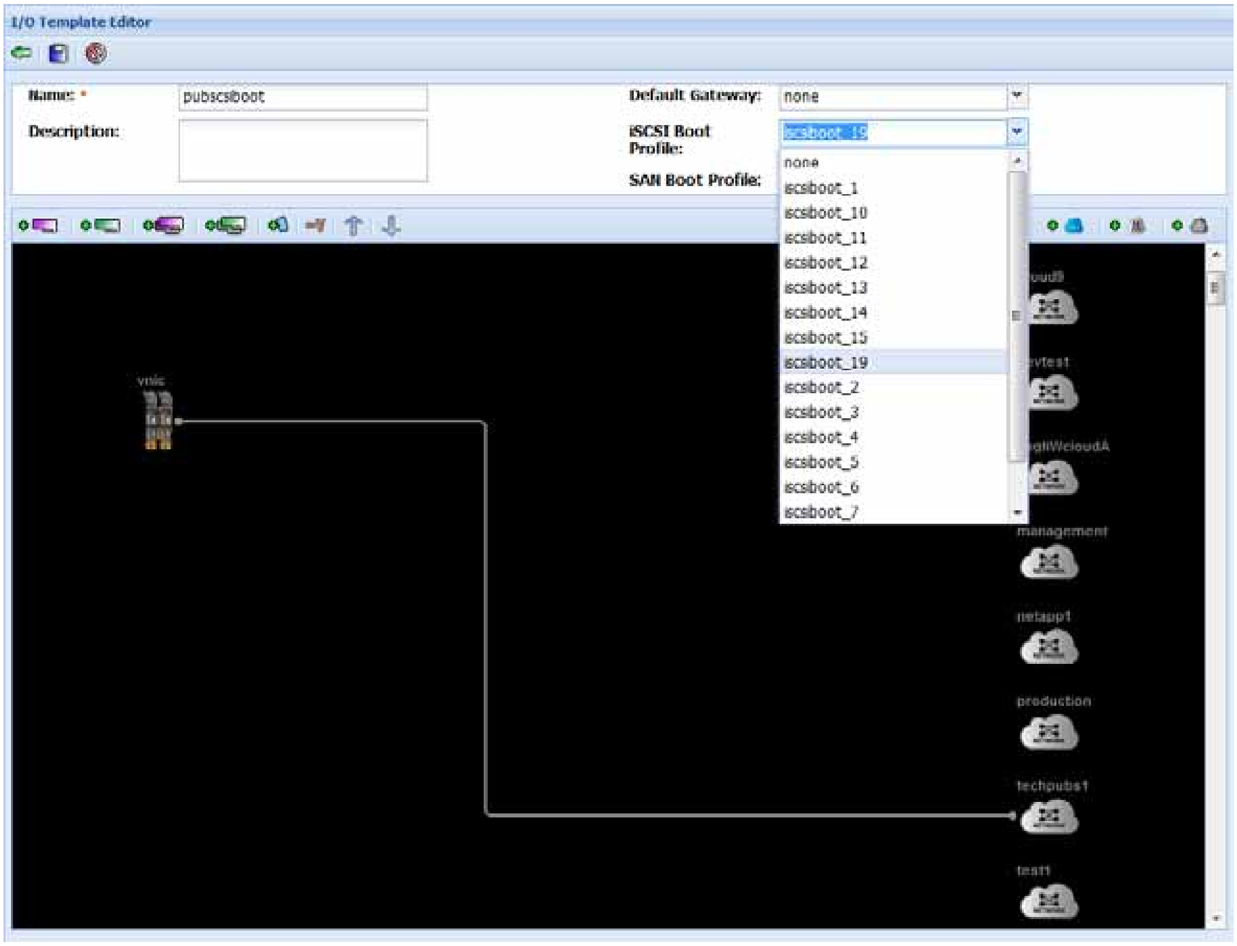
To create a dual path bootable I/O Template, follow this procedure:

Step 1 Select *Server Resource Manager->I/O Templates* to display the I/O Template summary, then click the plus sign (+) to display the I/O Template Editor.

Step 2 Click the ***Add an HA vNIC to Template*** button, then click and drag to connect the vNIC to the appropriate Network Cloud, as shown in Figure 26.

Note

To terminate an HA vNIC, the Network Cloud must have more than one Gigabit Ethernet port in it.



I/O Template Editor

Name: * pubscsiboot

Description:

Default Gateway: none

iSCSI Boot Profile: iscsiboot_19

SAN Boot Profile:

Figure 26 I/O Template, Dual Path iSCSI Bootable

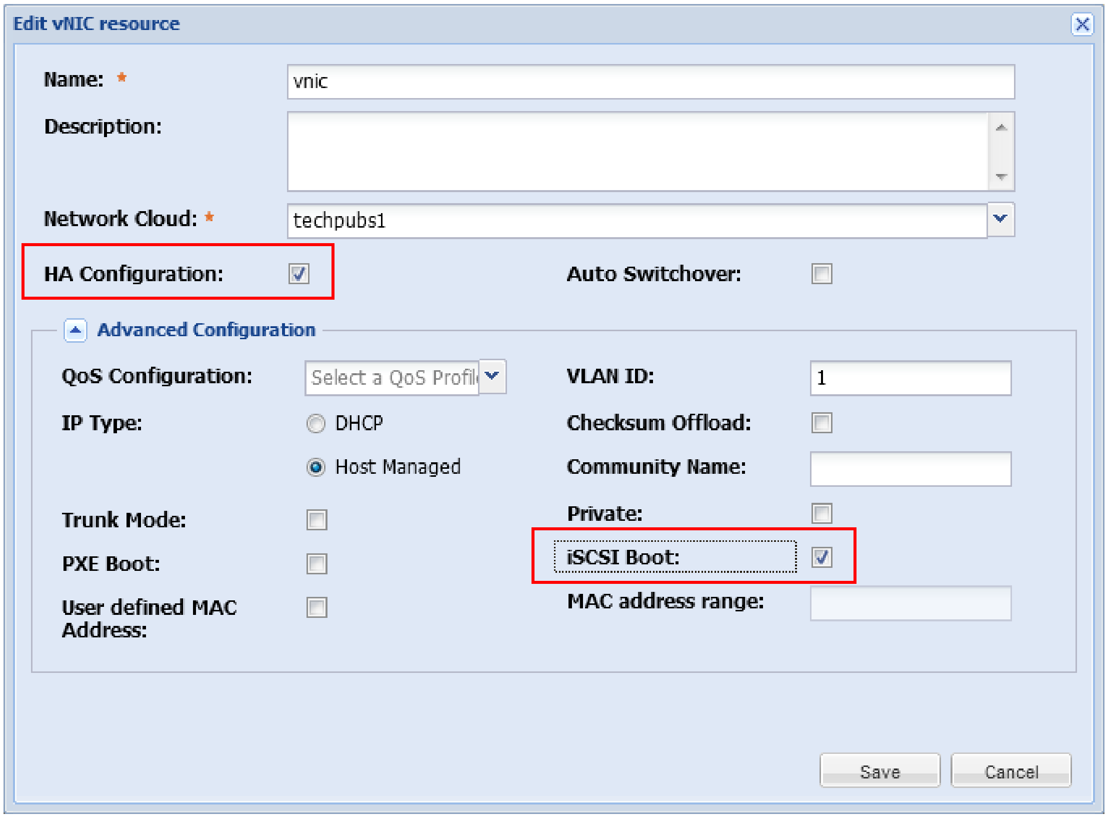
Step 3 In the *Name* field, enter the name of the I/O Template that will be used for iSCSI Booting.

Step 4 From the *iSCSI Boot Profile* dropdown menu, make sure to select the iSCSI Boot Profile you just created in the preceding section. Without creating the I/O Template as a bootable I/O Template, the server where the vNICs are deployed cannot be iSCSI Booted.

Step 5 Click and drag the vNICs to the appropriate Network Cloud to terminate the vNICs on Ethernet ports.

Step 6 Double click the vNIC icon on the I/O Template work space to display the Edit vNIC Resource dialog.

Step 7 Click the *Advanced Configuration* checkbox to display the additional configuration options for the HA vNIC—including the *iSCSI Boot* checkbox. Figure 27 shows this dialog.



Edit vNIC resource

Name: * vnic

Description:

Network Cloud: * techpubs1

HA Configuration: ☑

Auto Switchover: □

Advanced Configuration

QoS Configuration: Select a QoS Profil

VLAN ID: 1

IP Type: ○ DHCP ● Host Managed

Checksum Offload: □

Community Name:

Trunk Mode: □

Private: □

PXE Boot: □

iSCSI Boot: ☑

User defined MAC Address: □

MAC address range:

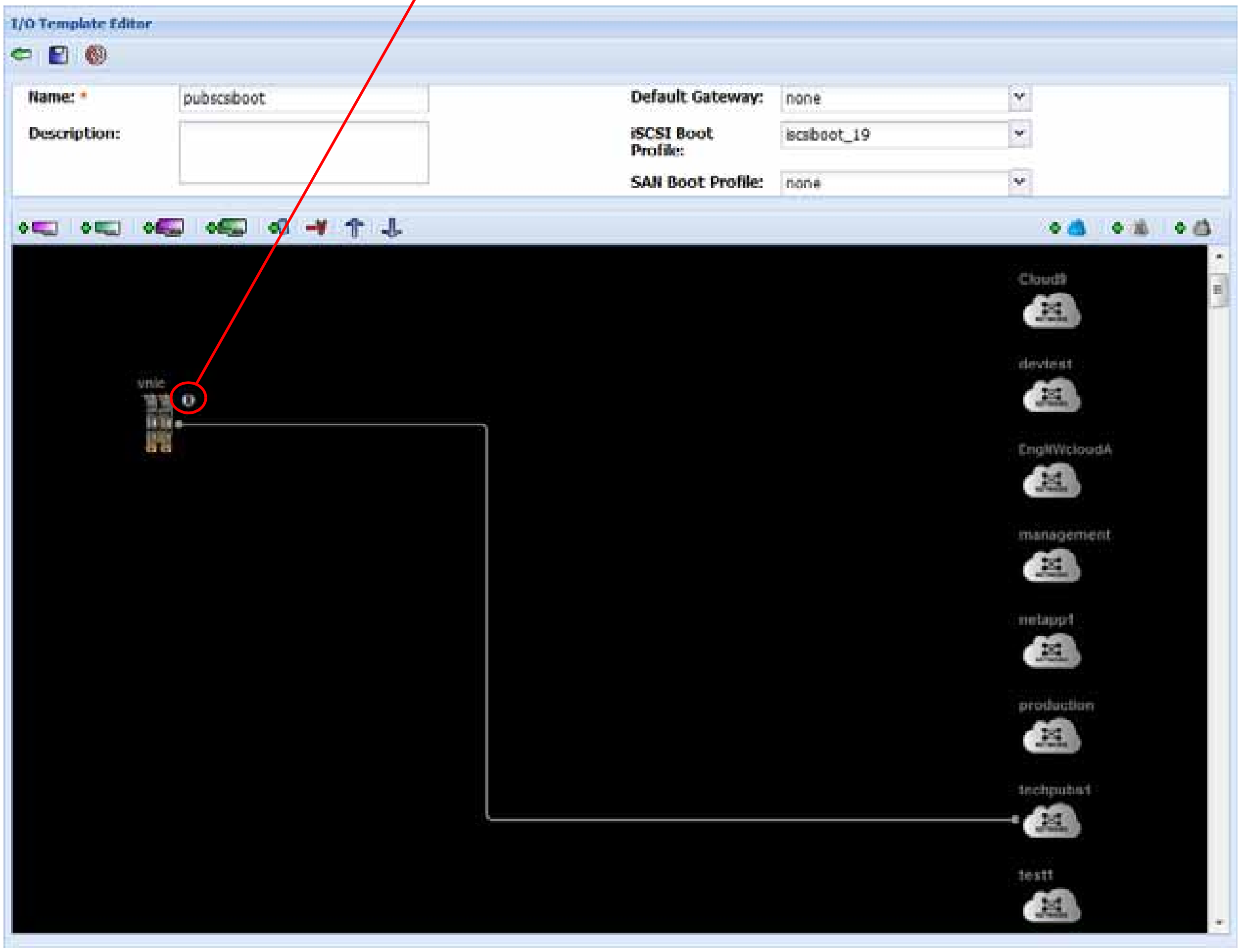
Figure 27 Edit vNIC Resource, Setting a Bootable vNIC

Step 8 On the Edit vNIC Resource dialog, make sure that the *HA Configuration* checkbox contains a checkmark. If it does not, click it now. Without this checkbox properly set, only one vNIC (and therefore one path) will be supported for iSCSI Booting the server.

Step 9 Click the *iSCSI Boot* checkbox. This checkbox must contain a checkmark for the HA vNICs to support iSCSI boot of the server where the vNICs are deployed.

Step 10 Click ***Save*** to return to the I/O Template Editor.

Step 11 Check the I/O Template Editor for the bootable icon (a circle with a red “B” within) associated with the server’s boot vNIC. The presence of this icon indicates that the vNIC connected to the host is bootable. Figure 28 shows a bootable vNIC.



Bootable Dual vNIC Icon

I/O Template Editor

Name: * pubscsiboot

Description:

Default Gateway: none

iSCSI Boot Profile: iscsiboot_19

SAN Boot Profile: none

Figure 28 I/O Template with Dual Bootable vNICs

Step 12 On the I/O Template Editor, click ***Save***. Without saving the I/O Template, all pending I/O Template configuration will be lost.

Step 13 After the bootable I/O Template is configured, proceed to Create an I/O Profile from the I/O Template.

Create an I/O Profile from the I/O Template

If you are setting up iSCSI Boot for a server that has already booted up and connected to the Oracle Xsigo Fabric Director, you can now create an I/O Profile from the I/O Template. When the I/O Profile is created, it will contain the bootable vNIC that you created. You can create multiple I/O Profiles from the same I/O Template if needed.

For information about creating an I/O Profile, follow the procedure for creating an I/O Profile as documented in Working with I/O Profiles.

Connect the I/O Profile to a Physical Server

When you assign the I/O Profile to the server, you begin pushing the bootable vNIC and the associated iSCSI Boot Profile to the server.

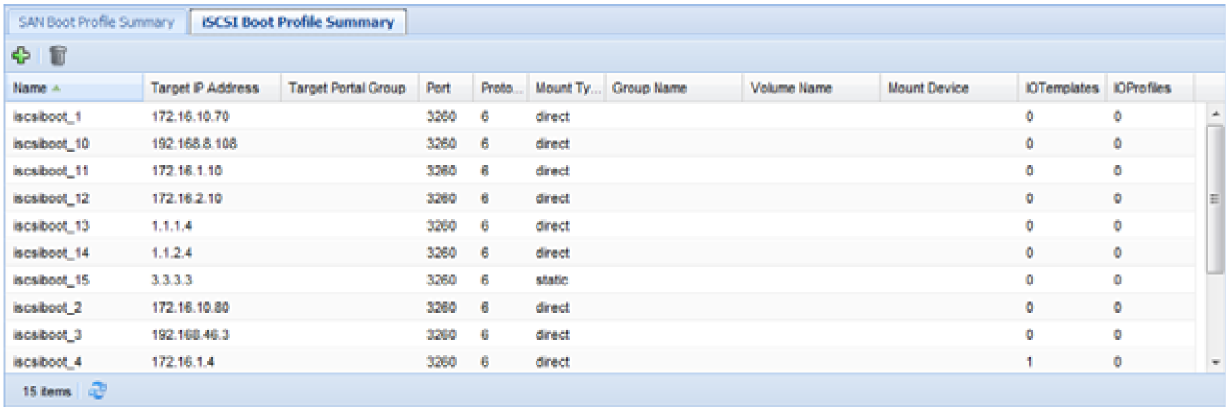
While Fabric Manager is pushing the iSCSI bootable vNIC and iSCSI Boot Profile to hosts, it prompts you for IQN information to complete the path between the host and the LUN containing the host's iSCSI boot information. When needed, Fabric Manager prompts you for the necessary information through a series of popup dialogs. IQN information is required for either a single path or dual path iSCSI configuration. Answer the prompts as needed to complete assigning the I/O Profile to the relevant servers.

To assign the I/O Profile to a server, follow the procedure documented in Connecting an I/O Profile to a Server.

Displaying the iSCSI Boot Profiles

The iSCSI Boot Profiles are displayed in the iSCSI Boot Profile Summary, which contains information about all the iSCSI Boot Profiles that have been created through Fabric Manager. The table shows general information about the iSCSI Boot Profile such as the IP address of the device containing the server's boot information and the mount type that will be used to access the boot information, kernel, and initrd.

Figure 29 shows the iSCSI Boot Profile Summary which is available through the *Server Resource Manager->Boot Profiles->iSCSI Boot Profile Summary.*



Name	Target IP Address	Target Portal Group	Port	Proto...	Mount Ty...	Group Name	Volume Name	Mount Device	IOTemplates	IOProfiles
iscsiboot_1	172.16.10.70		3260	6	direct				0	0
iscsiboot_10	192.168.8.108		3260	6	direct				0	0
iscsiboot_11	172.16.1.10		3260	6	direct				0	0
iscsiboot_12	172.16.2.10		3260	6	direct				0	0
iscsiboot_13	1.1.1.4		3260	6	direct				0	0
iscsiboot_14	1.1.2.4		3260	6	direct				0	0
iscsiboot_15	3.3.3.3		3260	6	static				0	0
iscsiboot_2	172.16.10.80		3260	6	direct				0	0
iscsiboot_3	192.168.46.3		3260	6	direct				0	0
iscsiboot_4	172.16.1.4		3260	6	direct				1	0

Figure 29 iSCSI Boot Profile Summary

Table 4 shows the contents of the iSCSI Boot Profile Summary and explains what each field means.

Table 4 Contents of the iSCSI Boot Profile Summary

Field	Indicates
Name	The name of the iSCSI Boot Profile.
Target IP Address	Shows the IP address of the storage target filer or array where the server's iSCSI Boot information is located.
Target Portal Group	Shows the name of the target portal group (if any) in which the server's iSCSI Boot information is located.
Port	Shows the port number on which the iSCSI communication between the server and the target containing the iSCSI boot information.
Protocol	Shows the protocol number used for communication between the server and the target containing its iSCSI boot information.
Mount Type	The type of mount configured on the iSCSI Boot vNIC. Valid values are: • static, for a Static iSCSI Boot Profile. • lvm, for the Logical Volume Manager. • direct, for assigning the device name that has the root file system.
Group Name	The logical volume manager (LVM) group name. If the mount type is LVM, this field displays the group name. If the mount type is other than LVM, no value is displayed.
Volume Name	The name of the logical volume that LVM uses for the root file system mount point.
Mount Device	The name of the device that contains the root file system mount point for the iSCSI Boot Profile.
I/O Template	The number of I/O Templates that are assigned to each iSCSI Boot Profile.
I/O Profiles	The number of I/O Profiles that are associated with each iSCSI Boot Profile.

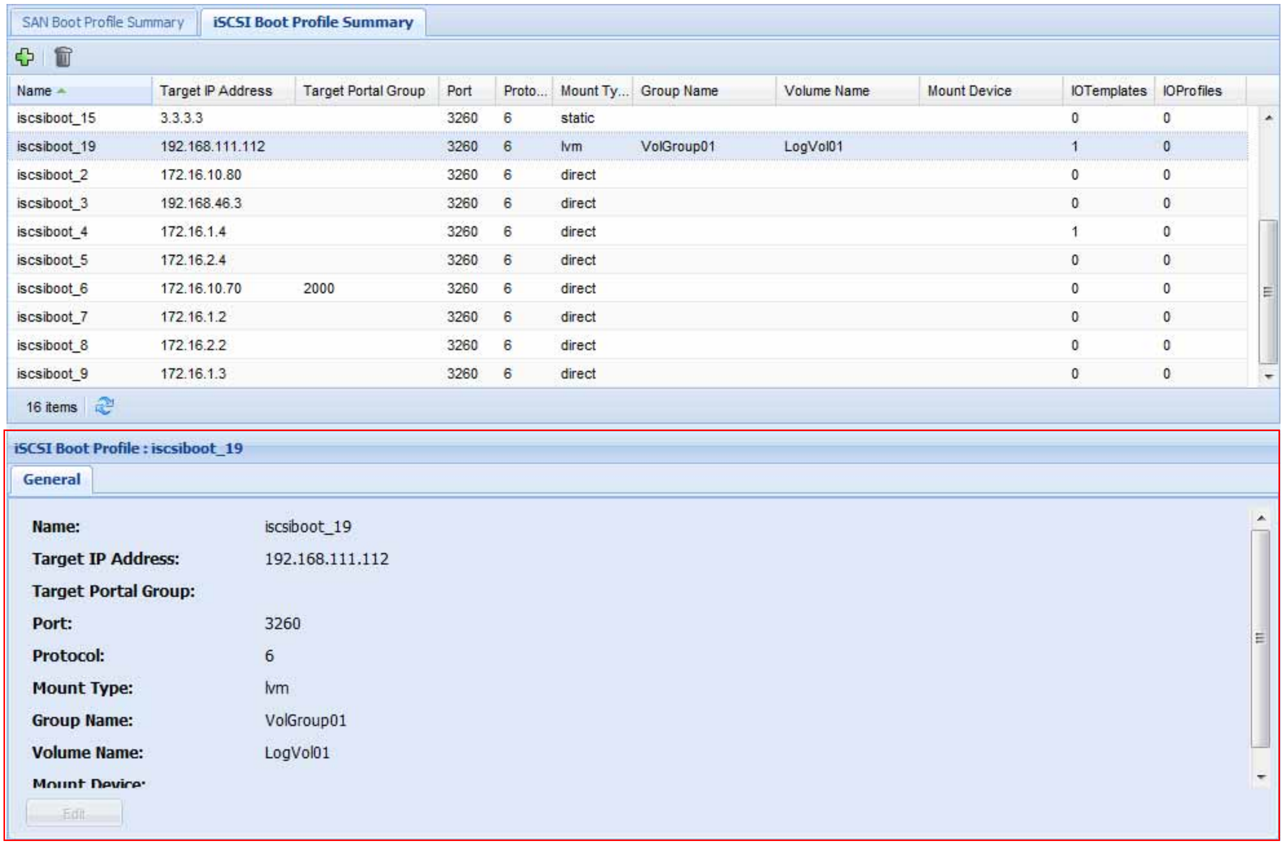
Displaying iSCSI Boot Profile Details

The iSCSI Boot Profile Details frame contains information about any configured iSCSI Boot Profiles. The iSCSI Boot Profile Details frame contains only one instance of an iSCSI Boot Profile, which is determined by the iSCSI Boot Profile that you select in the iSCSI Boot Profile Summary. By clicking a specific iSCSI Boot Profile in the summary, all of its corresponding details are available in the details frame.

Through the iSCSI Details Frame you can also edit a configured iSCSI Boot Profile to make changes to the profile without having to delete then re-add the profile. Be aware that:

- changes to the profile might also require resetting the server, or making changes to the server's configuration (for example, if a new boot device is specified, you might need to change the order of boot devices in the server's boot priorities list).
- editing an iSCSI Boot Profile is allowed only when the iSCSI Boot Profile is not currently associated with an I/O Template.

The iSCSI Boot Profile Details Frame is in Oracle’s Xsigo Fabric Manager GUI just below the iSCSI Boot Summary Profile. Figure 30 shows the iSCSI Boot Profile Details frame.



Name	Target IP Address	Target Portal Group	Port	Proto...	Mount Ty...	Group Name	Volume Name	Mount Device	IOTemplates	IOProfiles
iscsiboot_15	3.3.3.3		3260	6	static				0	0
iscsiboot_19	192.168.111.112		3260	6	lvm	VolGroup01	LogVol01		1	0
iscsiboot_2	172.16.10.80		3260	6	direct				0	0
iscsiboot_3	192.168.46.3		3260	6	direct				0	0
iscsiboot_4	172.16.1.4		3260	6	direct				1	0
iscsiboot_5	172.16.2.4		3260	6	direct				0	0
iscsiboot_6	172.16.10.70	2000	3260	6	direct				0	0
iscsiboot_7	172.16.1.2		3260	6	direct				0	0
iscsiboot_8	172.16.2.2		3260	6	direct				0	0
iscsiboot_9	172.16.1.3		3260	6	direct				0	0

Name:	iscsiboot_19
Target IP Address:	192.168.111.112
Target Portal Group:	
Port:	3260
Protocol:	6
Mount Type:	lvm
Group Name:	VolGroup01
Volume Name:	LogVol01
Mount Device:	

Figure 30 iSCSI Boot Profile Details Frame

When the iSCSI Boot Details frame is populated with an iSCSI Boot Profile, you can edit the profile to make changes to the current profile without having to delete and re-add the profile.

Table 5 shows the contents of the iSCSI Boot Profile Details frame, and explains what each field means. Not all fields will be populated based on the options specified during the configuration of the iSCSI Boot Profile. For example, if you created a direct connect iSCSI Boot Profile, none of the fields for logical volume manager will contain information.

Table 5 Contains of the iSCSI Boot Profile Details Frame

Field	Means
Name	The name assigned to the selected iSCSI Boot Profile.
Target IP Address	Shows the IP address of the storage target filer or array where the server's iSCSI Boot information is located.
Target Portal Group	Shows the name of the target portal group (if any) in which the server's iSCSI Boot information is located.
Port	Shows the port number on which the iSCSI communication between the server and the target containing the iSCSI boot information.
Protocol	Shows the protocol number used for communication between the server and the target containing its iSCSI boot information.
Mount Type	The method used to mount the SAN location of the server's iSCSI Boot information: • Direct • Static • Logical Volume Manager
Group Name	For Logical Volume Manager mount types, this field shows the logical group that contains the SAN location of the server's iSCSI boot information.
Volume Name	For Logical Volume Manager mount types, this field shows the logical volume that contains the SAN location of the server's iSCSI boot information.
Mount Device	For Direct mount types, this field shows the device that contains the root file system mount point for the server's iSCSI Boot information.
I/O Template	The number of I/O Templates that are assigned to each iSCSI Boot Profile.
I/O Profiles	The number of I/O Profiles that are associated with each iSCSI Boot Profile.

Deleting an iSCSI Boot Profile

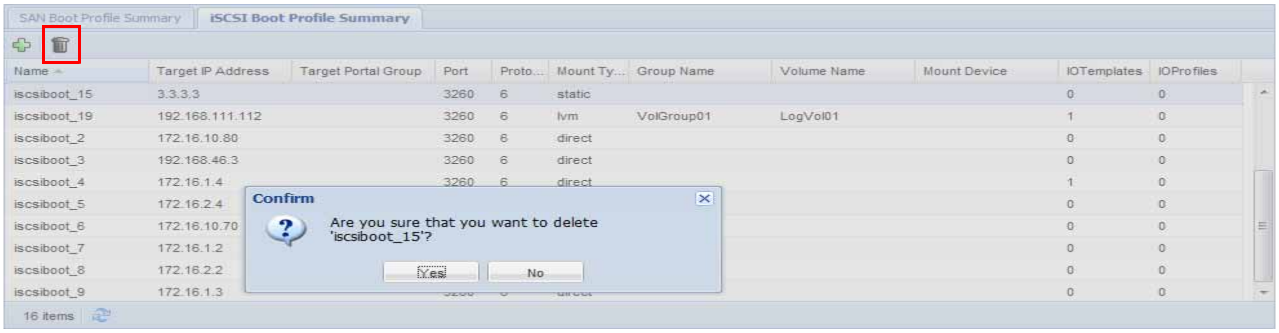
Through the iSCSI Boot Profile Summary, you can delete an iSCSI Boot Profile. Any iSCSI Boot Profile that is not associated with an I/O Template or a physical server can be deleted.

To delete an iSCSI Boot Profile, follow this procedure:

Step 1 On the navigation panel, click *Server Resource Manager->Boot Profiles->iSCSI Boot Profile Summary* tab. This step displays the iSCSI Boot Profile Summary.

Step 2 On the iSCSI Boot Profile Summary, select the iSCSI Boot Profile that you want to delete. This step activates the garbage can icon. You can select multiple iSCSI Boot profiles through standard keyboard conventions, for example by pressing the ***CTRL*** + click or ***Shift*** + click.

Step 3 Click the garbage can icon to delete the selected iSCSI Boot Profile as shown in Figure 31.



Name	Target IP Address	Target Portal Group	Port	Proto...	Mount Ty...	Group Name	Volume Name	Mount Device	IOTemplates	IOProfiles
iscsiboot_15	3.3.3.3		3260	6	static				0	0
iscsiboot_19	192.168.111.112		3260	6	lvm	VolGroup01	LogVol01		1	0
iscsiboot_2	172.16.10.80		3260	6	direct				0	0
iscsiboot_3	192.168.46.3		3260	6	direct				0	0
iscsiboot_4	172.16.1.4		3260	6	direct				1	0
iscsiboot_5	172.16.2.4								0	0
iscsiboot_6	172.16.10.70								0	0
iscsiboot_7	172.16.1.2								0	0
iscsiboot_8	172.16.2.2								0	0
iscsiboot_9	172.16.1.3								0	0

16 items

Confirm

Are you sure that you want to delete 'iscsiboot_15'?

Figure 31 Deleting an iSCSI Boot Profile

When you click the garbage can icon, a confirmation page is displayed to verify that you actually want to delete the selected iSCSI Boot Profile.

Step 4 Click ***OK*** to delete the selected iSCSI Boot Profile(s), or ***Cancel*** to abort the deletion.

Working with the Topology

This chapter contains the following topics:

- Understanding the Topology
- Displaying the Topology Overview
- Displaying the Server Cloud View
- Displaying the Director Cloud View
- Displaying the Server Director View
- Displaying the Target Topology View
- Displaying Performance Meters
- Switching Between Physical and Virtual Views

Understanding the Topology

The Topology is a series of network illustrations of connectivity from different perspectives. Each perspective is called a "view." When you are displaying the Topology, you are displaying how different parts of the datacenter that Oracle's Xsigo Fabric Manager is managing are connected together over Xsigo virtual I/O and other products.

The Topology is different than the Physical Topology, which displays a diagram of how Oracle's Xsigo Fabric Director and physical hosts are physically connected (cabled) together.

Displaying Detailed Information for the Topology

In addition to the top-level information available on the Topology, you can drill-down to lower, more detailed levels of information about the contents of the Topology. The detailed information is displayed based on the context of the view you are in. For example, if you are in Server Director view, details displayed will be in the context of the servers' connections to one or more Fabric Directors including any connections through intermediary switches. If you are in Server Cloud view, the detailed information will be displayed in the context of the servers' connections to clouds.

You can display detailed information by double-clicking individual elements (servers, clouds, Fabric Directors, and so on) within each view. Additional information is documented in the sections for each view.

Displaying the Topology Overview

The general topology is displayed through the Topology Overview, and shows the virtual connections (vNICs and vHBAs) for each Network and Storage Cloud to all the connected hosts. In the Topology Overview, toolbar controls are available for:

- Displaying Performance Meters

Figure 1 shows the Topology Overview.

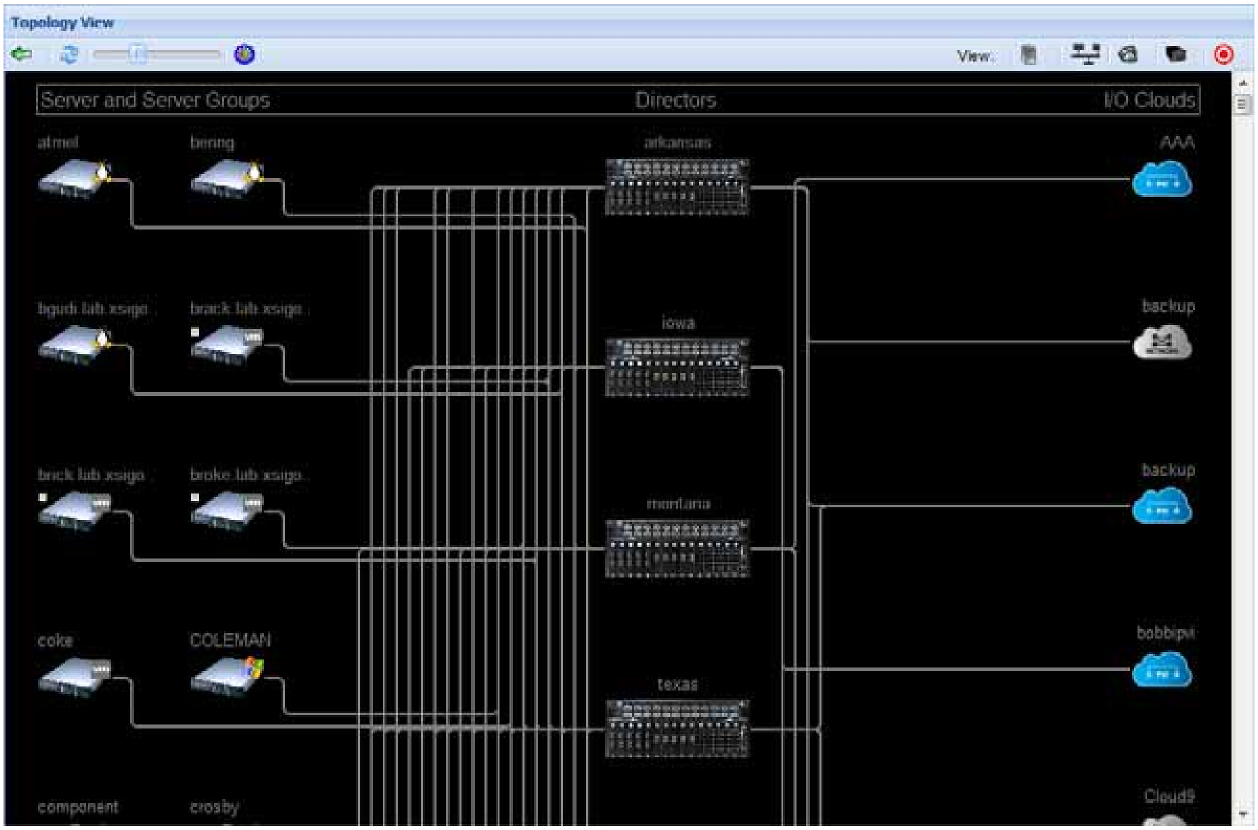


Figure 1 Topology Overview

Through the toolbar on the Topology Overview, you can control various aspects of how the Topology Overview contents are displayed:

- — a button toggles the display of performance meters for each server in the Topology Overview. (See Displaying Performance Meters.)
- — a slider controls zooming in and out on the Topology. Zooming in enables you to focus in on a smaller area of the Topology and enlarge that area. Zooming out enables you to pan out to a wider view of the Topology and reduce the size of the individual elements in the Topology.

- the right side of the toolbar contains controls for displaying different views of the Topology page, including:
  - — the Topology view, which shows the overall topology from the Network and Storage Cloud through the Fabric Director to the discovered host servers.
  - — the Server Cloud view, which shows connectivity between hosts and clouds. The Fabric Directors providing connectivity are not shown.
  - — the Director Cloud view, which shows connectivity between the clouds and the Fabric Directors that are providing the connections. Host servers are not displayed.
  - — the Server Director view, which shows connectivity between the physical servers and server groups and the Fabric Directors. The connectivity to the network and storage clouds is not displayed.

— the Target Topology view, which shows the connectivity of individual vHBAs and their respective targets. The Fabric Directors and hosts are not displayed.

- the main area of the Topology also shows whether or not a Server has an I/O Profile bound to it. A small icon to the upper left of each server or server group indicates whether the server or group has Xsigo I/O bound to it or not. Figure 2 shows which servers have I/O Profiles bound.

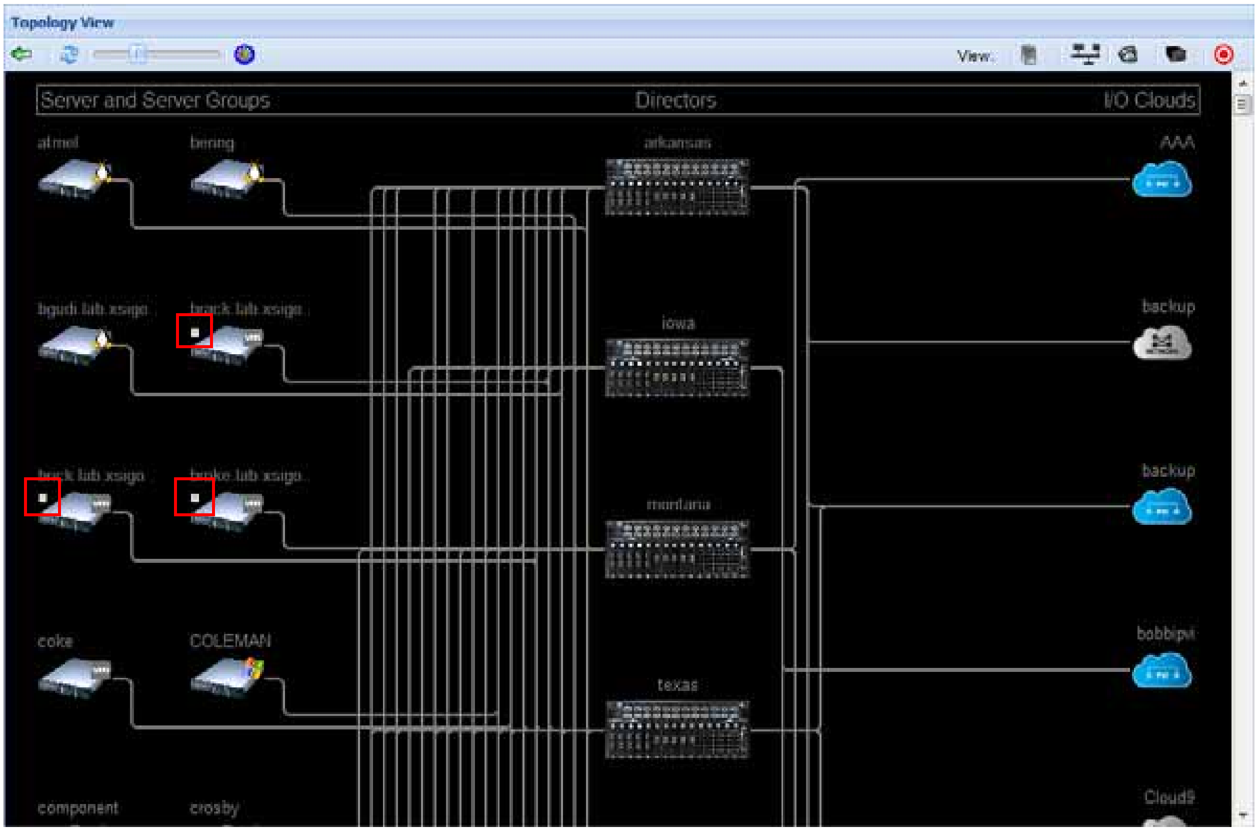


Figure 2 Topology Overview — Servers Bound to an I/O Profile

Vertically Scrolling Columns on the Topology

In the main work area of each view in the Topology, elements (such as servers, Fabric Directors, and Clouds) are arranged in vertical columns. Column headings on the Topology indicate the individual columns. Usually, two or three columns are displayed on the work area. In a larger deployment, these elements can scroll off the Topology, and it can become difficult to see all the elements of the topology on one page even if you zoom out to the widest display. Each vertical column on the Topology supports a vertical click and drag to scroll that column up and down.

To click and drag a column, follow this procedure:

Step 1 Hover with the mouse near the element in that vertical column until the mouse pointer switches to a hand icon, as shown in Figure 3.

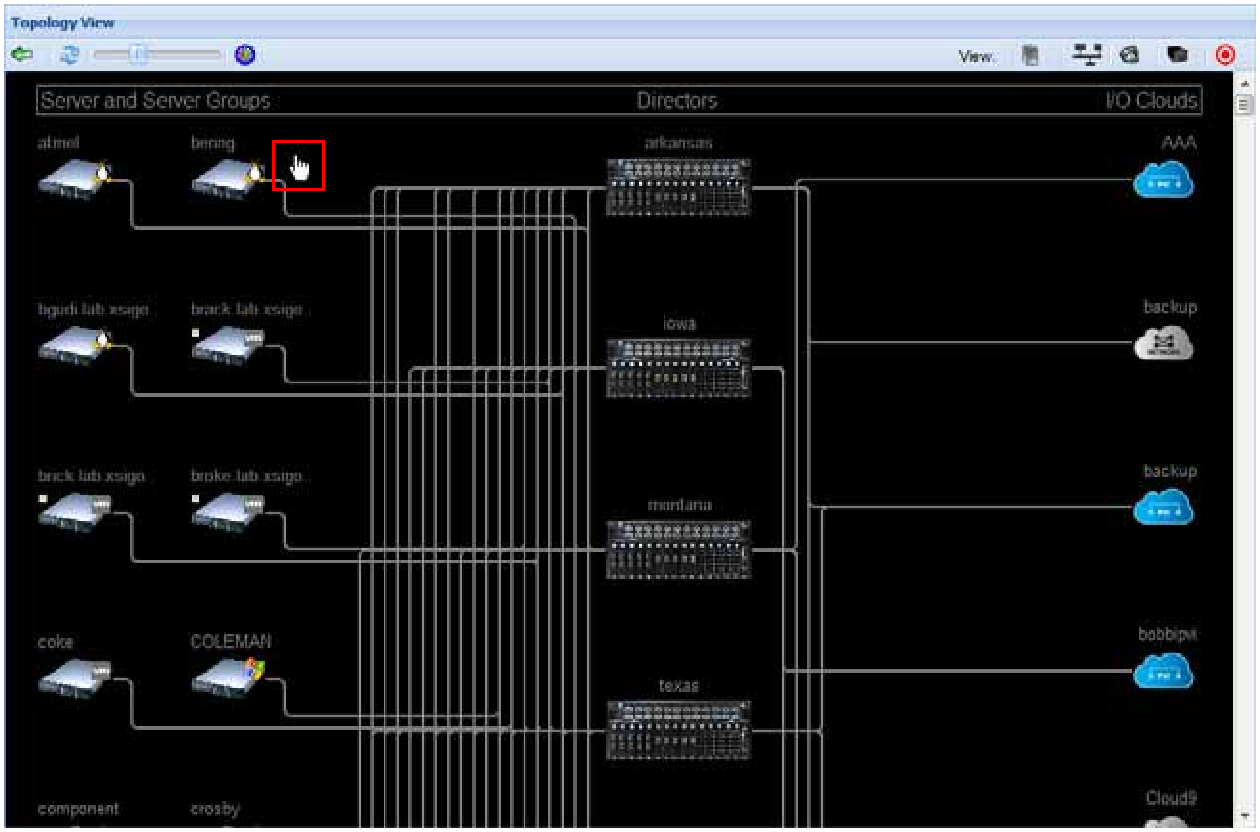


Figure 3 Selecting a Column for Vertical Scrolling

Step 2 At that point, you can click with the mouse and drag the column up or down. Figure 4 shows an example of vertically scrolling the contents of the *Server and Server Group* column on the Topology.

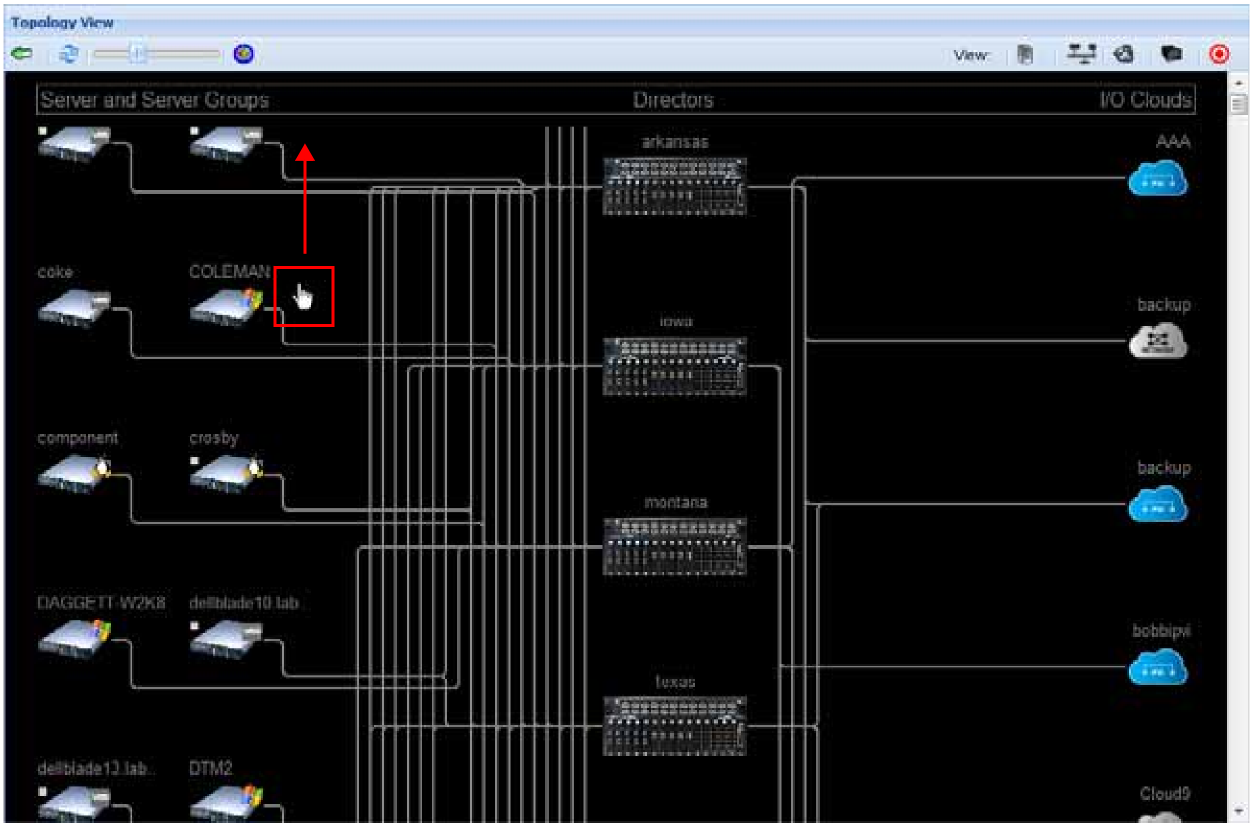


Figure 4 Vertically Scrolling a Column

Each column is individually controllable, so you can arrange each column until you get all elements arranged so that they show the information you need.

Displaying the Physical Server Details

Through the Topology overview, you can get additional information about server connections to clouds by double-clicking a server. For information, see Displaying Detailed Information about Individual Servers.

Displaying the Server Group Details

Through the Topology overview, you can get additional information about the connections from a server group to clouds by double-clicking a server group. For information, see Displaying Detailed Information about Server Groups.

Displaying Physical Connectivity for the Topology Overview

Through the Topology Details, you can display physical connectivity information for the Fabric Director physical ports that connect vNICs and vHBAs to servers. The information displayed shows the same connectivity as the Server Cloud view. For more information, see Displaying Physical Connectivity for Server Cloud View.

Displaying the Server Cloud View

The Server Cloud view shows information about which server(s) are connected to which Network and Storage Clouds. This view shows individual servers as well as server groups.

In Server Director view, two options are available as toolbar buttons:

- Displaying Performance Meters
- Displaying Physical Connectivity for Server Cloud View

Figure 5 shows an example of the Server Cloud view.

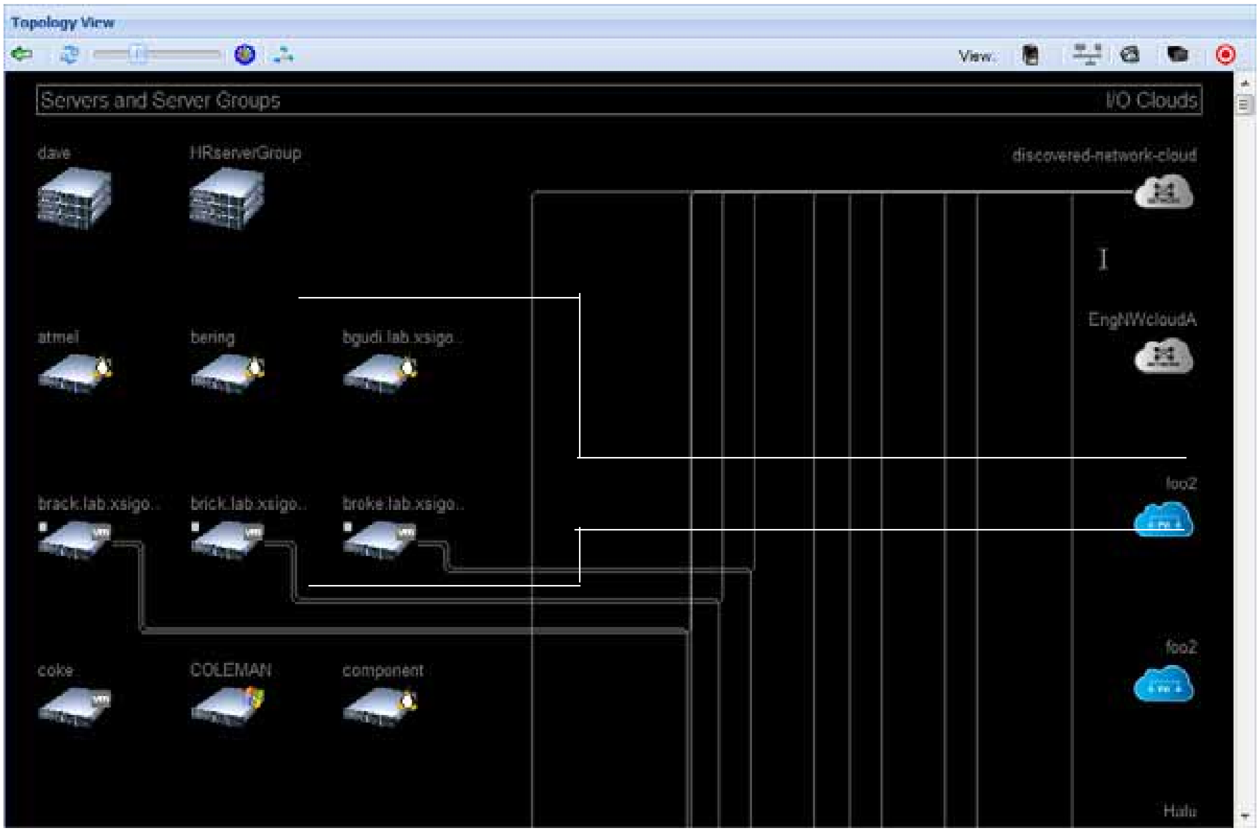


Figure 5 Topology — Server Cloud View

Displaying Detailed Information about Server Groups

A server group is logical collection of individual servers that you have created. (For information see, Working with Server Groups.) The Topology supports displaying information about server groups, including:

- which servers constitute the server group
- whether servers in the server group are bound to an I/O Profile
- how individual servers in the server group are connected to individual clouds

To display the Server Group details, double-click a server group on the Topology from either Server Cloud view or the Topology Overview. See Figure 6.

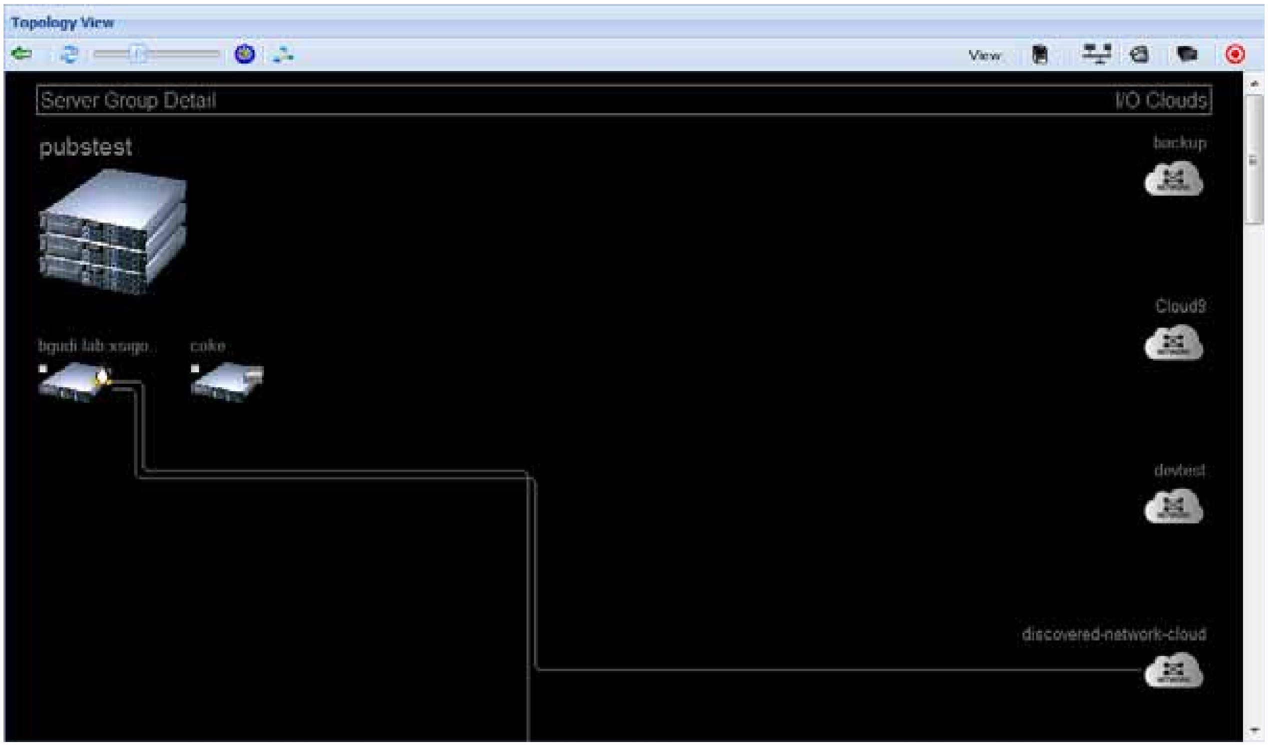


Figure 6 Server Group Details

In this example, you can see that the Server Group “pubtest” consists of the servers bgudi and coke. Each server is bound to an I/O Profile (as indicated by the icon to the upper right of each server), and each server is connected to two clouds. In this example, the only connection shown is from bgudi to the “discovered-network-cloud”.

Displaying Detailed Information about Individual Servers

Detailed information is available for individual servers that are managed by Fabric Manager. Through the Topology, you can see the following detailed information for individual servers:

- the individual server
- individual vNICs and vHBA connections from the server
- how individual vNICs and vHBAs on the server are connected to individual clouds

Note

Additional details about physical servers are available based on the context of the view you are in. For example, if you are in Server Director view, details displayed will be in the context of the servers’ connections to one or more Fabric Directors including any connections through intermediary switches.

To display the details for individual servers, double-click a server group on the Topology from either Server Cloud view or the Topology Overview. See Figure 7.

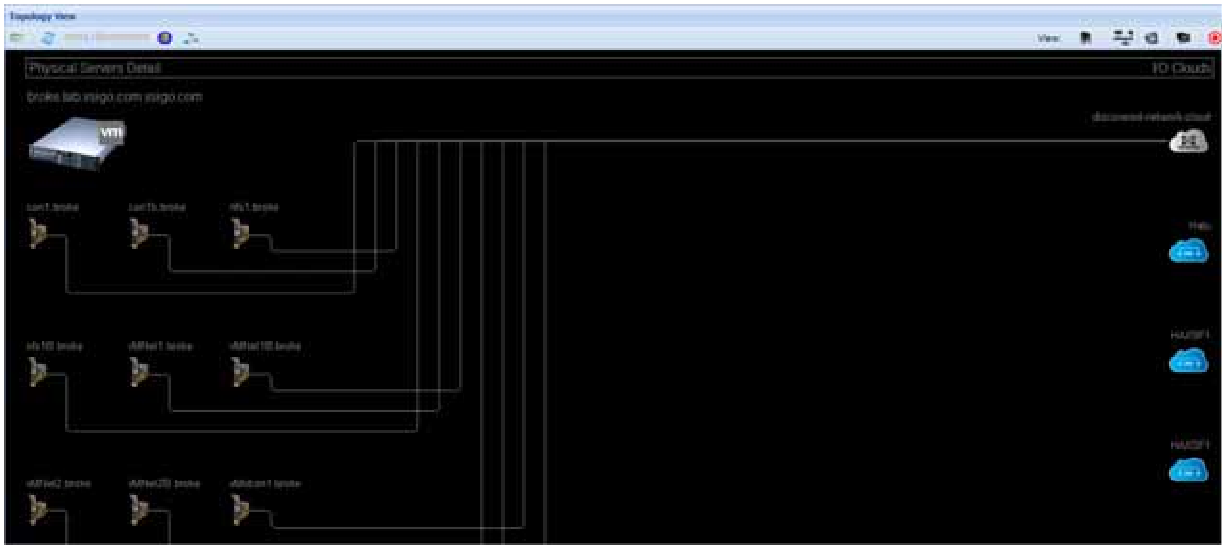


Figure 7 Physical Server Details

In this example, the server “broke” has multiple vNICs and vHBAs. In this example, vNICs are shown connected to discovered-network-cloud, and also to another Network Cloud (not displayed, but connections to it run off the bottom of the Physical Server Details page).

Displaying Physical Connectivity for Server Cloud View

The Server Cloud Details contains an option to show physical connection information, such as what the server(s) in the server group are connected to on one or more Fabric Directors. The ***Show Physical View*** toolbar button is supported on the toolbar for the Server Cloud view and the Server Cloud Details. Different information is displayed based on which view is used when the Show Physical View toolbar button is clicked.

- On the Server Cloud view, the Show Physical View button shows the same information as the Server Director view. For information, see Figure 12.
- On the Server Cloud Details page enables you to see which port on which Fabric Director each server in the group is connected to. See Figure 8.

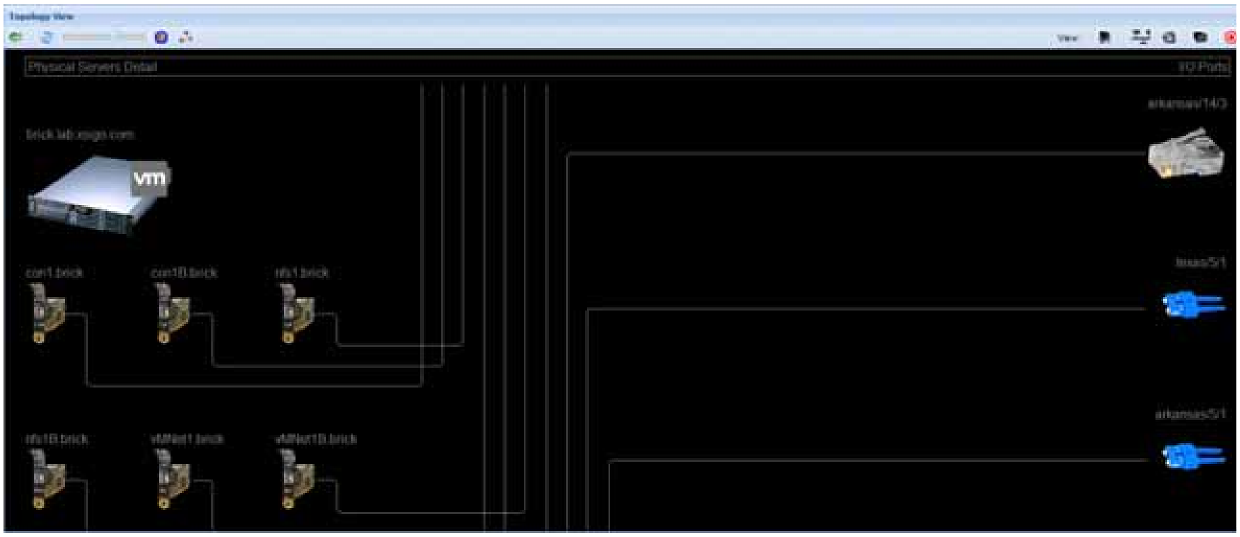


Figure 8 Server Cloud Details — Physical Port Connections

In this example, you can see the individual vHBAs in the server “brick.” Some of these vHBAs are connected to physical port 14/3 and 5/1 on Fabric Director “arkansas” and physical port 5/1 on Fabric Director “texas” among others.

Displaying the Director Cloud View

The Director Cloud view shows information about which Fabric Director(s) are connected to which Network and Storage Clouds.

Figure 9 shows an example of the Director Cloud view.

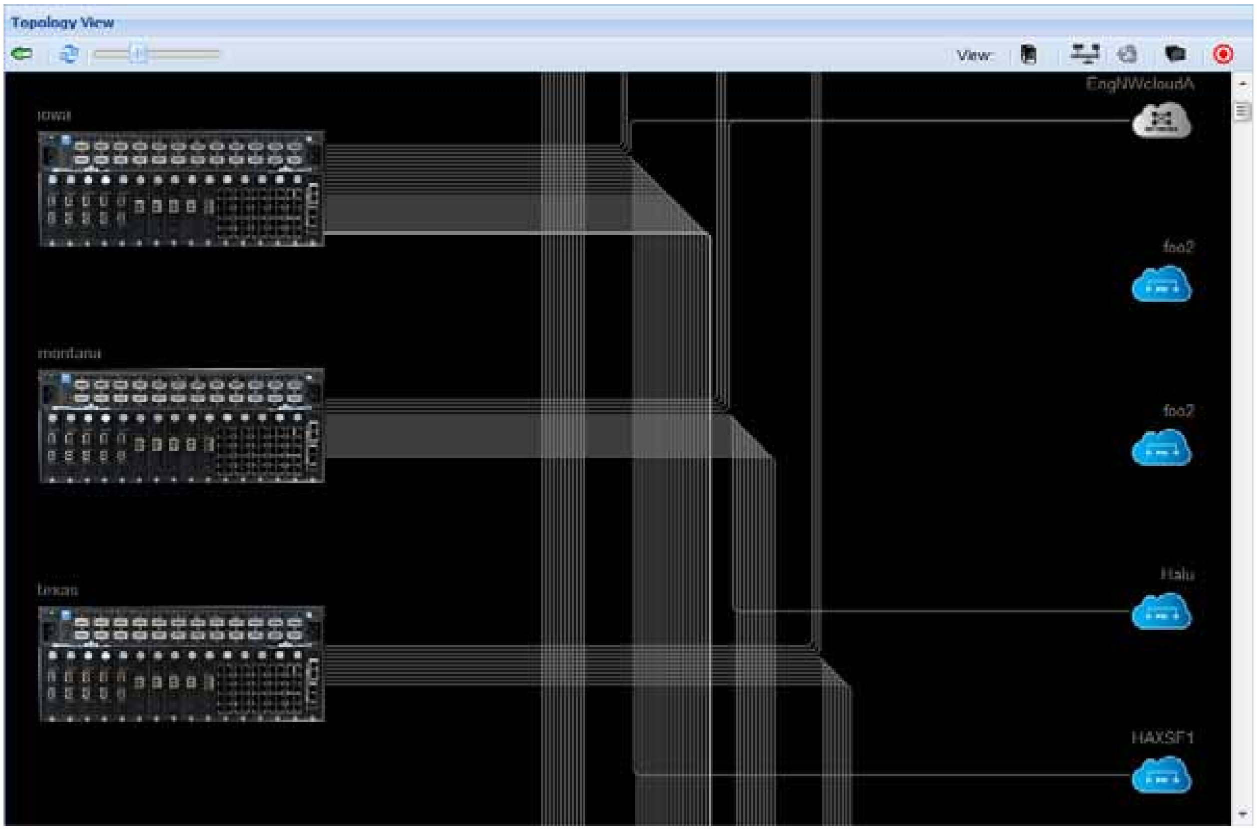


Figure 9 Topology — Director Cloud View

Through the Director Cloud view, you can configure and manage Fabric Directors, Network Clouds, and Storage Clouds through right clicking on these objects. Some basic management functions are also available through the ***Assign Virtual I/O Resources*** button.

Displaying the Director Details

Detailed information about the Fabric Directors in the Topology are available. Through the Director Details, you can view information about a selected Fabric Director, including:

- the number and type of I/O Modules in the Fabric Director. All installed I/O Modules are displayed regardless of whether or not they are currently supporting a vNIC or vHBA connection.
- The connection from each I/O Module to the cloud where the module’s vNIC or vHBA is terminated. Only modules that are currently supporting a vNIC or vHBA connection are displayed.
- The cloud(s) to which the I/O Module is connected through the listed I/O Module(s).

To display the Director details, double-click a Fabric Director on the Director Cloud view. Figure 10 shows the Director details.

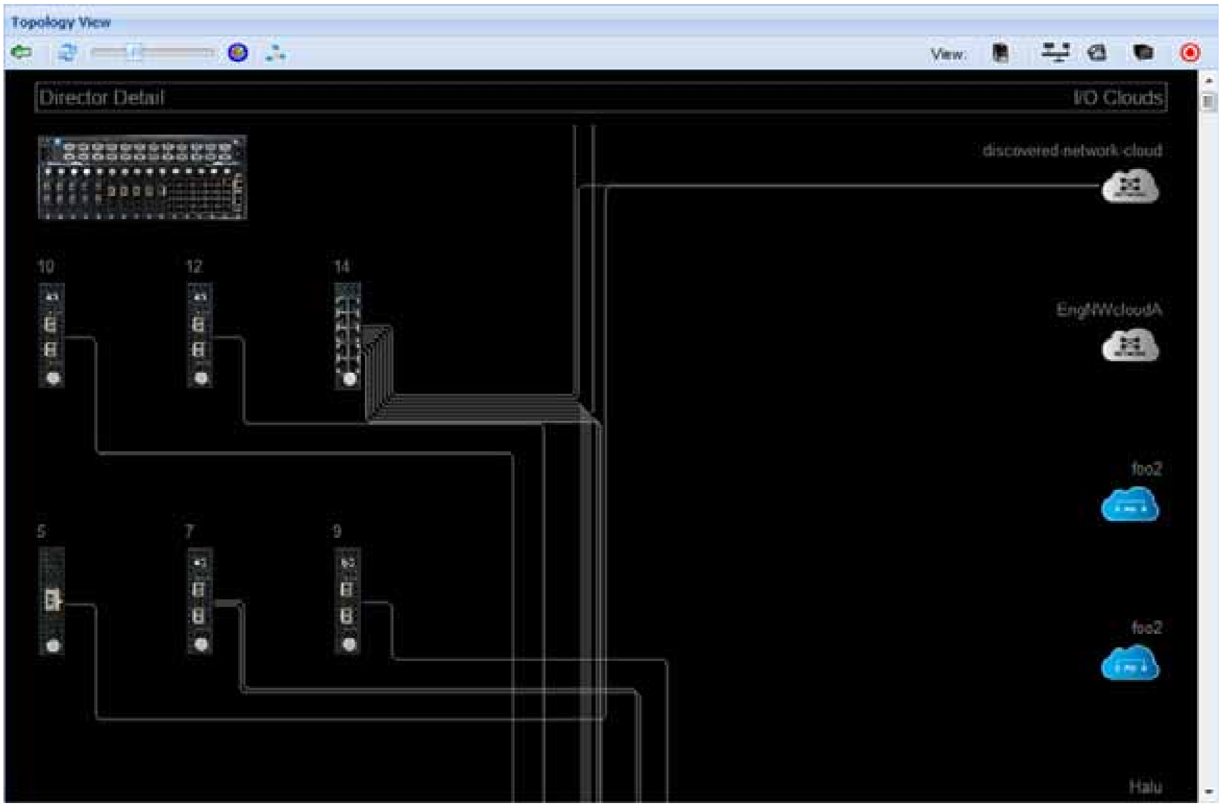


Figure 10 Director Cloud View — Director Details

In this example, the Fabric Director “arkansas” is displayed. This Fabric Director has multiple network and storage I/O modules:

- Three 4 Gbps fibre channel modules in slots 10, 12, and 7 are connected to Storage Clouds (not shown)
- One 10 Gbps Ethernet I/O Module in slot 14 is connected to the discovered-network-cloud
- Additional module exist in slots 4 and 5

By hovering over the module or a cloud, Fabric Manager highlights the connection between the module and a cloud.

Displaying Physical Connectivity for Director Cloud View

Through the Topology, you can display a diagram of physical connections between the Fabric Directors and physical servers that Fabric Manager is managing. This physical connection diagram also includes intervening InfiniBand switches if any are present. Through the ***Show Physical View*** toolbar button on the Director Cloud Details view, you can display physical connections. See Figure 11.

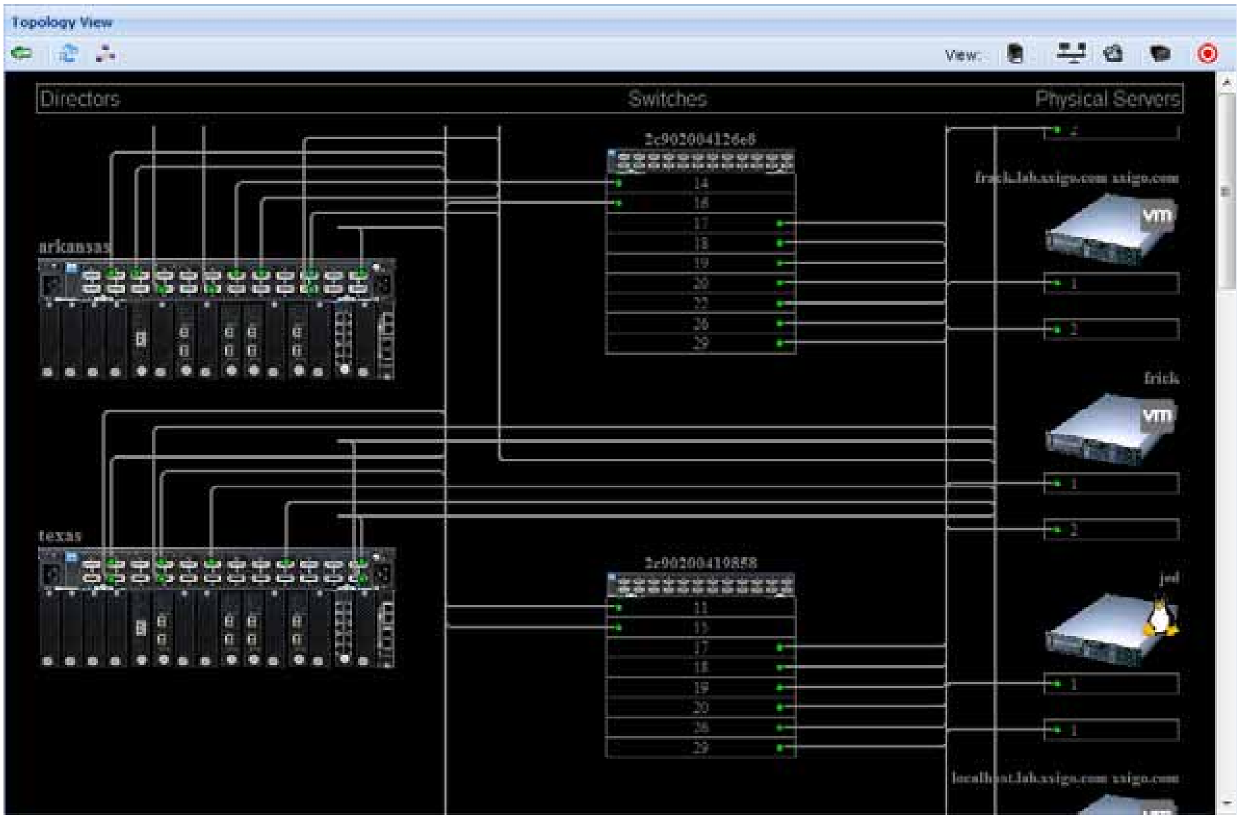


Figure 11 Director Cloud Details — Show Physical Connections

In this example, all physical connections from the Fabric Director server ports to individual servers are displayed. The diagram shows each physical port's connection either directly to a server or through an intervening InfiniBand switch. By hovering over Fabric Directors, Fabric Director ports, InfiniBand ports, or servers, you can trace either parts of the physical connection, or the entire end-to-end path.

Displaying the Server Director View

The Server Director view shows information about which physical servers are connected to which Fabric Director(s). If a Fabric Director is not displayed in this view, it is not managed by Fabric Manager. Also, if a Fabric Director is not connected to any server, it will still be displayed in the Topology, but it will appear unconnected (no lines leading to other equipment) in the Server Director view. Since a server must contain a server profile and at least one vNIC or vHBA, you can use this display to determine if a server has been deployed with virtual I/O. If the server has no line connecting it to a Fabric Director, that server has no virtual I/O deployed.

In Server Director view, two options are available as toolbar buttons:

- Displaying Physical Connectivity for Director Cloud View
- Displaying Performance Meters

Figure 12 shows the Server Director view.

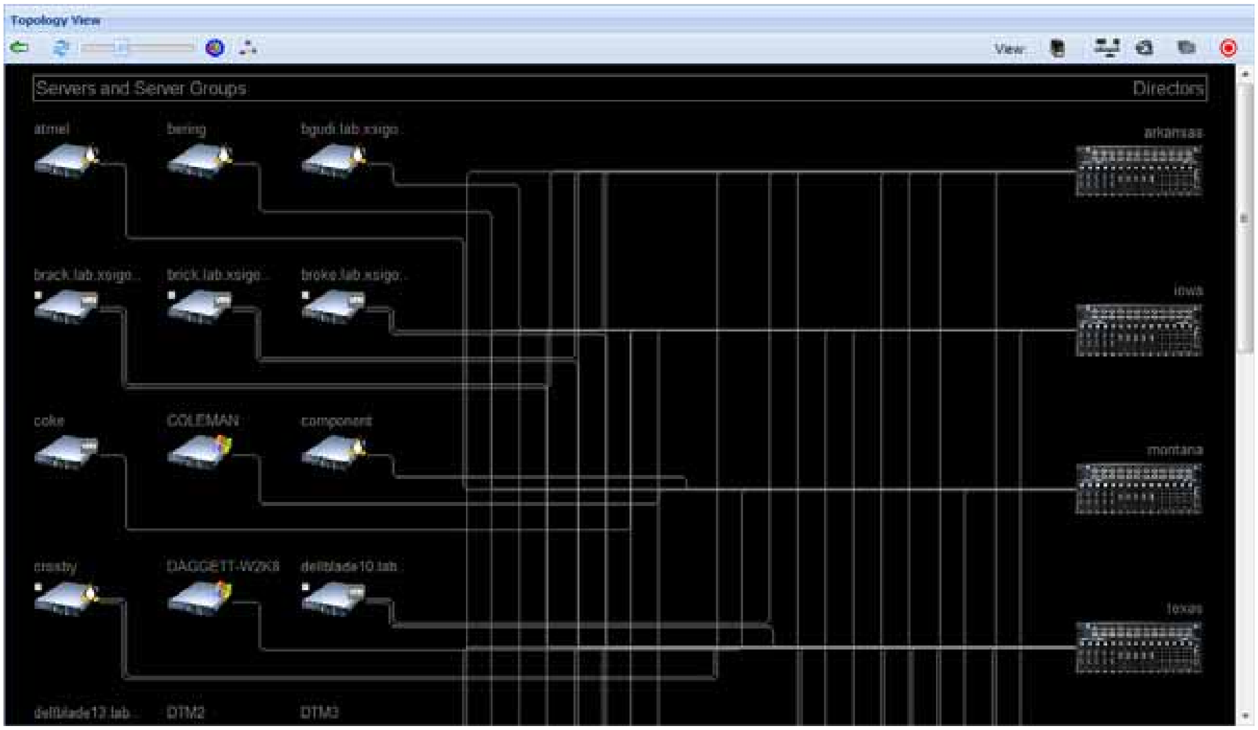


Figure 12 Topology — Server Director View

Through the Server Director view, you can configure and manage host servers and Fabric Directors through right clicking on these objects. Some basic management functions are also available through the ***Assign Virtual I/O Resources*** button.

Displaying Detailed Connectivity Information

Through the Server Director view you can see detailed connection diagrams for the Fabric Directors and servers in your data center. The detailed connectivity information shows a diagram of how the Fabric Director is cabled to servers.

The detailed information shows:

- a server or server groups that is connected to Fabric Directors, and the port number on which the server is connected
- Fabric Directors that are providing connection to the server or server group, and the IB server port on the Fabric Director that is connected to the server or server group
- IB switches (if any) that are connecting the servers to the Fabric Directors, and the switch ports that are providing the connections.

You can display the detailed connectivity information by double-clicking a server in the Server Director view. See Figure 13.

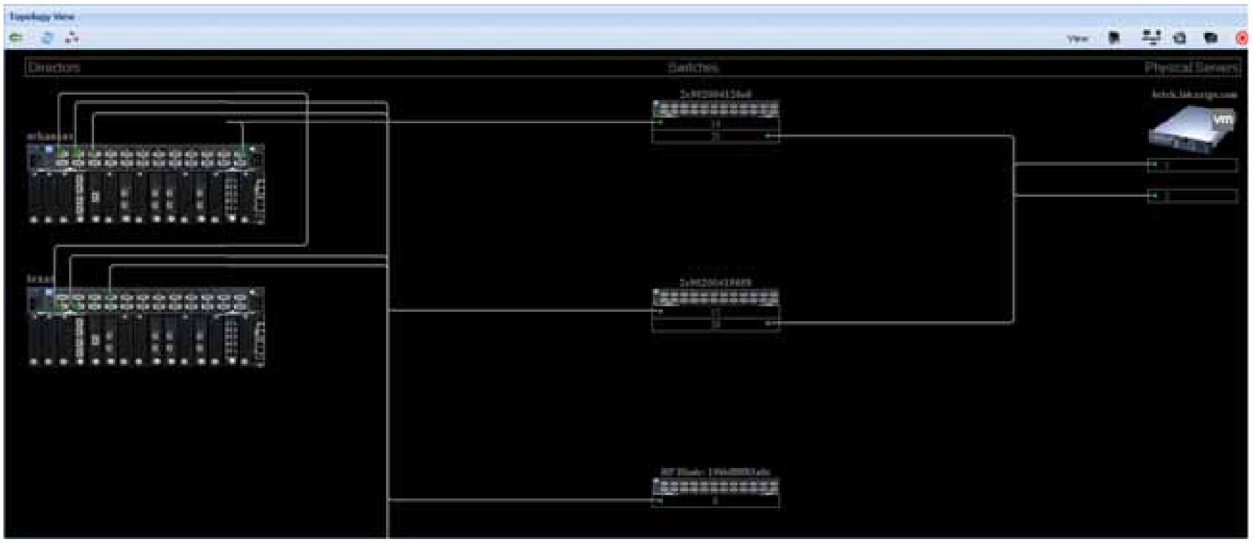


Figure 13 Server Director View—Connection Details

In this example, two Fabric Directors (“arkansas” and “texas”) are connected together in a shared IB fabric from server port 1 on “texas” to server port 13 on “arkansas”. The Fabric Director “arkansas” is connected to the first IB switch from Director port 24 to switch port 14, and the server “brick” is connected to the same IB switch from switch port 20 to server port 1.

The Fabric Director “texas” is connected to the second IB switch from Director port 2 to switch port 15, and the server “brick” is connected to the same IB switch from switch port 20 to server port 2.

Displaying Virtual Connectivity for Server Director View

By default, physical connections are shown in the Server Director view. You can display the virtual connections between servers and their clouds, by clicking the ***Show Virtual View*** toolbar button. This button is available on either the top-level Server Director view or the Server Director Details:

- On the Server Director view, when you can click the ***Show Virtual View*** toolbar button, the virtual connections displayed are the same as the Director Cloud view. See Figure 9.
- On Server Director Details page, when you click the ***Show Virtual View*** toolbar button, the virtual connections displayed are the same as the Server Cloud view. See Figure 5.

Displaying the Target Topology View

The Target Topology view shows information about which storage targets (listed by WWN) are connected to which vHBAs. This view can be displayed by clicking the far right button in the View bar. The Target Topology button looks like a red target or bull’s-eye.

Through the Target Topology view, you can determine if a vHBA is currently connected. The presence of a line between the target and a vHBA indicates that the vHBA is currently connected. If the line is absent, the vHBA is not currently connected to any storage target.

You can highlight the connection between a vHBA and its storage by mousing over either the storage target icon or the vHBA icon.

Figure 14 shows the Target Topology view.

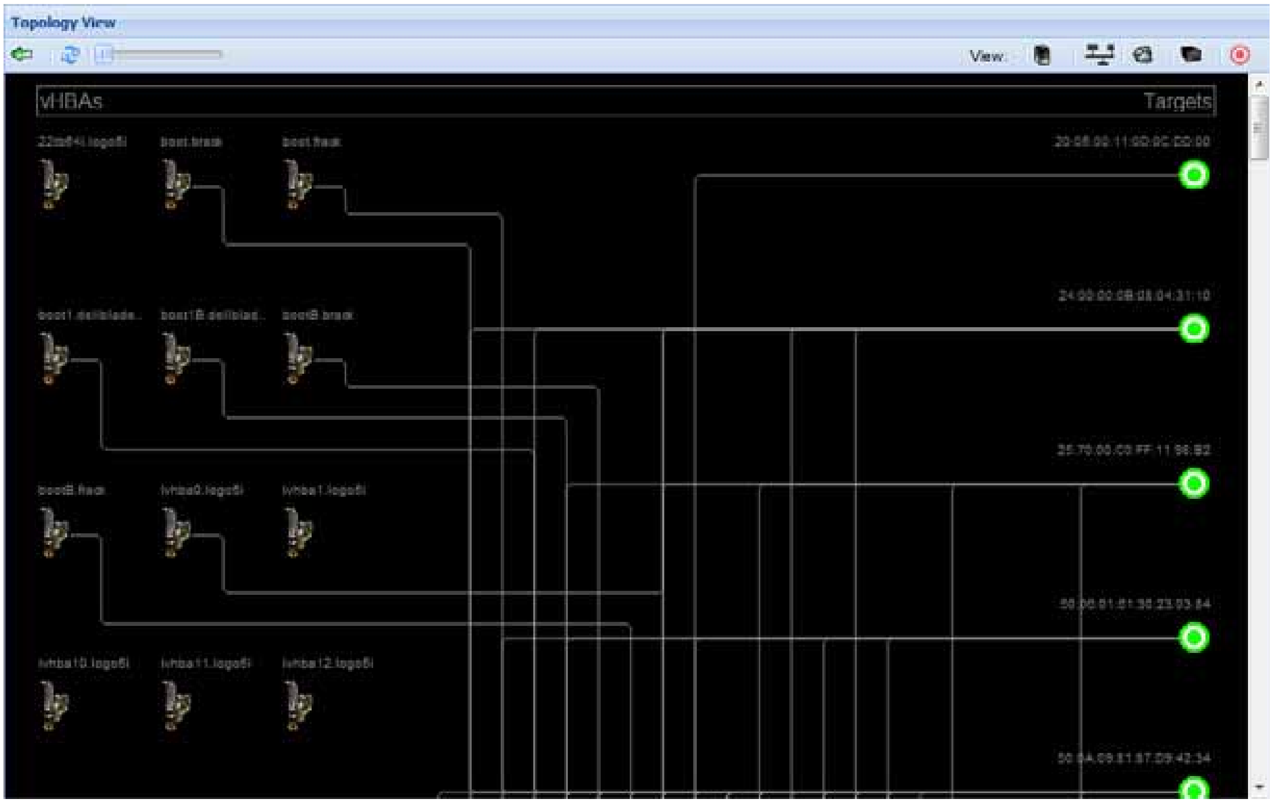


Figure 14 Topology — Target Topology View

Through the Target Topology view, you can configure and manage vHBAs and the storage targets to which they are connected through right clicking on these objects. Some basic management functions are also available through the ***Assign Virtual I/O Resources*** button.

Displaying Detailed Target Information

Through the Topology you can display detailed information about which vHBAs are connected to which LUNs on a specific target. The detailed information includes:

- a list of all vHBAs connected to a particular fibre channel storage target
- a list of all LUNs on that target, and how each vHBA is connected

By hovering over a vHBA you will highlight its connection to a particular LUN. Also, by clicking one of the listed LUNs, you will highlight all of its connections to listed vHBAs.

You can double-click a target in the Storage Topology view to display the detailed target information. See Figure 15.

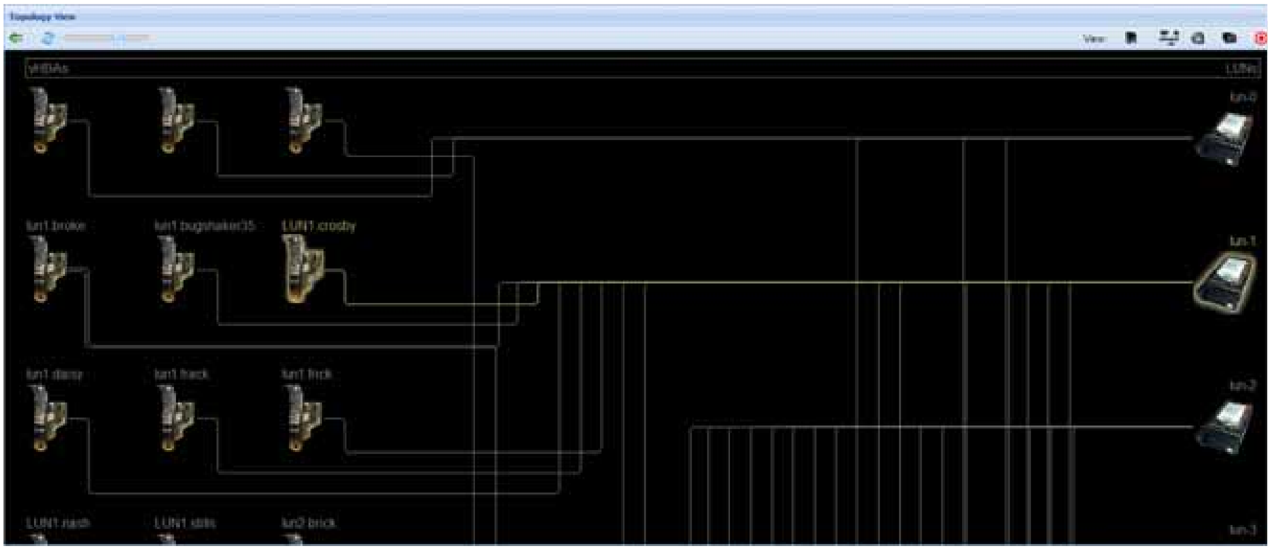


Figure 15 Storage Topology View — vHBA Details

In this example, all vHBAs connections are displayed for the storage target that you clicked. Also, the LUNs within that target are displayed. For this example, the mouse was hovered over the vHBA named “LUN1.crosy” to highlight how that vHBA is connected. You can see that it is connected to `lun-1`, so the server “crosby” which is where vHBA “LUN1.crosby” exists is connected to `lun-1` on the selected target.

Displaying Performance Meters

Through the Topology, you can display performance meters for individual servers through a toolbar button. Through the meters you can display aggregate network and storage throughput for servers in the topology or I/O modules connected to clouds.

Performance meters are available on most pages in the Topology where elements with measurable throughput are present (typically, servers or I/O Modules). Table 1 shows which views have performance meters available.

Table 1 Performance Meter Availability

View	Shows
Topology Overview	Throughput of servers in the Topology
Topology Server Details	Double-click a server in the Topology, and performance meters are available to show throughput for that particular server.
Server Cloud view	Throughput of servers in the Server Cloud view
Server Cloud Details	Double-click a server in the Topology, and performance meters are available to show throughput for that particular server.
Director Cloud Details	Double-click a Fabric Director in the Director Cloud view, and performance meters are available to show throughput for individual I/O Modules in that Fabric Director.
Server Director view	Throughput of servers in the Server Director view

Figure 16 shows an example of the Topology Overview without performance meters, and the location of the Show Performance Meters toolbar button.

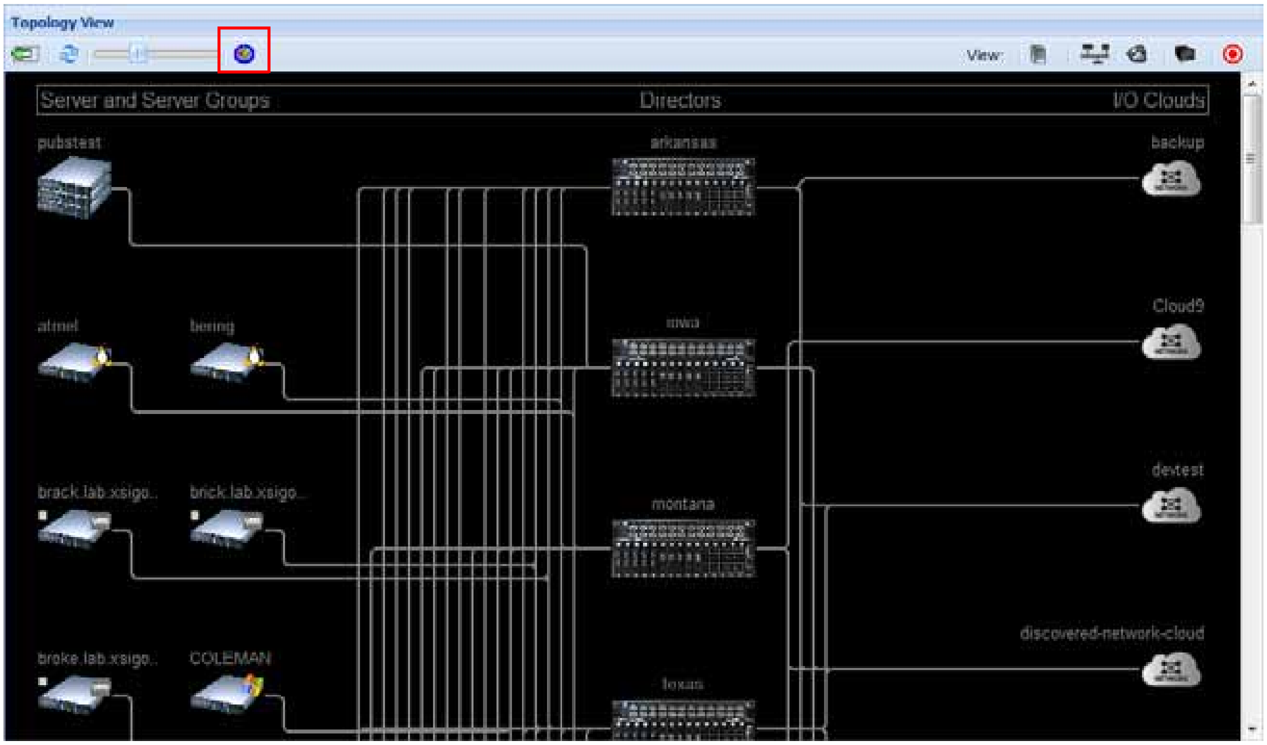


Figure 16 Topology Toolbar — Show Performance Meters Button

By default, the meters are not displayed as shown in Figure 16. However, since this button is a toggle, click it once to display the performance meters as shown in Figure 17, and click once again to hide the performance meters.

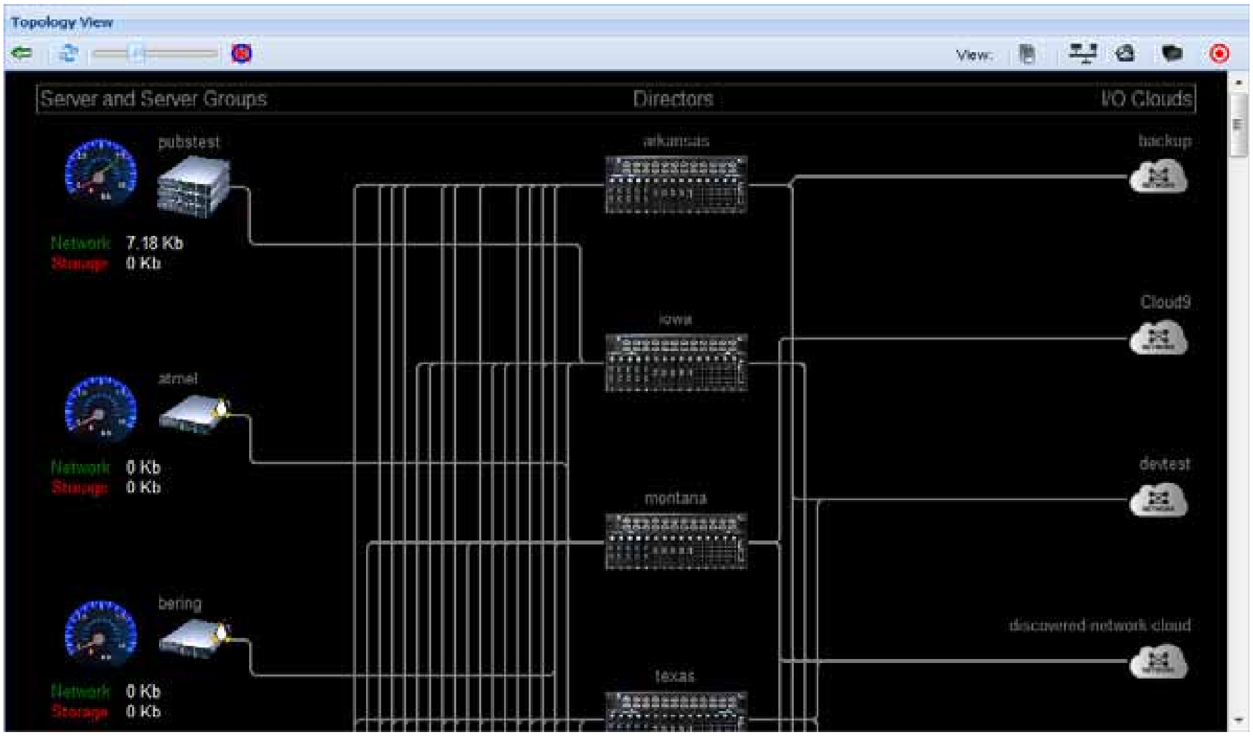


Figure 17 Topology — Per-Server Performance Meters

As shown, each performance meter consists of two needles on a speedometer. The Green needle represents the total network throughput across vNICs on the server. The red needle represents the total I/O across all vHBAs on the server.

When you no longer want to see the performance meters, click the ***Hide Performance Meters*** button as shown in Figure 18.

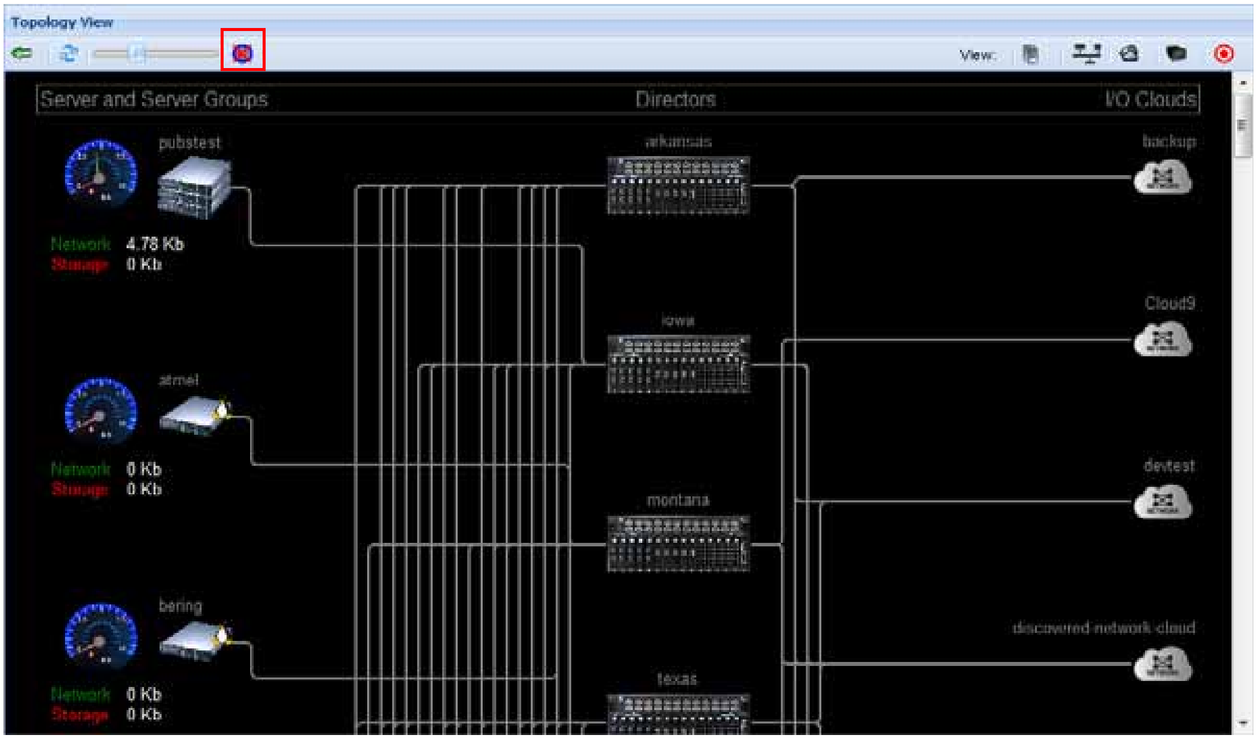


Figure 18 Topology — Hide Per-Server Performance Meters Button

Switching Between Physical and Virtual Views

Many of the individual pages in the Topology show virtual connections from Xsigo resources to other devices, but you might also want to know how a physical connection exists in your data center. For this reason, Oracle's Xsigo Fabric Manager offers a toggle to show physical and virtual connections through the ***Show Physical View*** or ***Show Virtual View*** toolbar button that exists on many of the Topology pages. Table 2 shows the pages that contain the toolbar button and explains what the button does.

Table 2 Physical and Virtual Toggle

View	Toggle	See...
Topology Details	Default: Server virtual connections to clouds. Use ***Show Physical View*** toolbar button to show the physical ports on the Fabric Director to which HCAs are connected.	Displaying Physical Connectivity for the Topology Overview
Server Cloud view	Default: Server virtual connections to clouds. Use ***Show Physical View*** toolbar button to show the Fabric Director to which servers are connected.	Displaying Physical Connectivity for Server Cloud View
Server Cloud Details	Default: HCA virtual connections to clouds. Use ***Show Physical View*** toolbar button to show the physical ports on the Fabric Director to which HCAs are connected.	Displaying Physical Connectivity for Server Cloud View
Director Cloud Details	Default: One Fabric Director's virtual connections to clouds. Use ***Show Physical View*** to show the InfiniBand server ports connections to individual servers and InfiniBand switches (if present)	Displaying Physical Connectivity for Director Cloud View
Server Director view	Default: Shows physical connections between servers and Fabric Directors. Use ***Show Virtual View*** to show the virtual connections for all servers to their clouds	Displaying Virtual Connectivity for Server Director View
Server Director Details	Default: Shows the physical connection between servers and Fabric Director ports including connections to InfiniBand switches (if present). Use ***Show Virtual View*** to show the virtual connections between servers and Oracle's Xsigo Fabric Director.	Displaying Virtual Connectivity for Server Director View

Working with Discovery Subnets

This chapter contains the following topics:

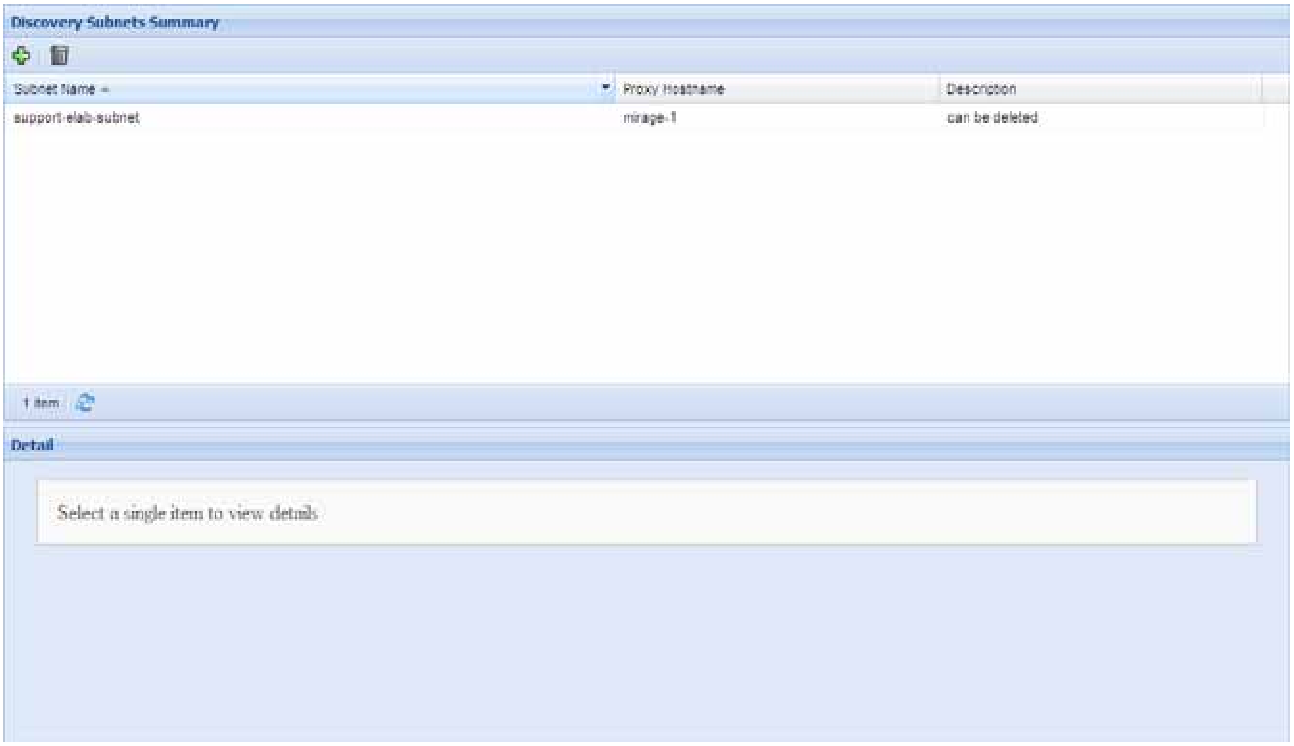
- Displaying the Discovery IP Subnet
- Displaying Discovery Subnet Details
- Adding a Discovery Subnet

Displaying the Discovery IP Subnet

By default, Oracle's Xsigo Fabric Manager discovers the IP subnet that it is currently on. However, there might be a need to discover other subnets. In this case, Fabric Manager can query the remote IP subnet through the use of a proxy Oracle Xsigo Fabric Director you specify in that remote network. This query occurs only for the purpose of discovering devices on other subnets. The discovery subnet shows the IP-connected devices that can be found on that subnet, but not all subnets, so if you want to discover other subnets, you must manually discover them individually.

To display the discovery subnet, follow this procedure:

Step 1 From the Navigation frame, select *Fabric Director->Discovery Subnet* to display the Discovery Subnet Summary. Figure 1 shows the Discovery Subnet Summary.



Subnet Name	Proxy Hostname	Description
support-elab-subnet	mirage-1	can be deleted

Select a single item to view details

Figure 1 Discovery Subnet Summary

Notice that through the Discovery Subnet Summary, you can add new discovery subnets or delete existing discovery subnets.

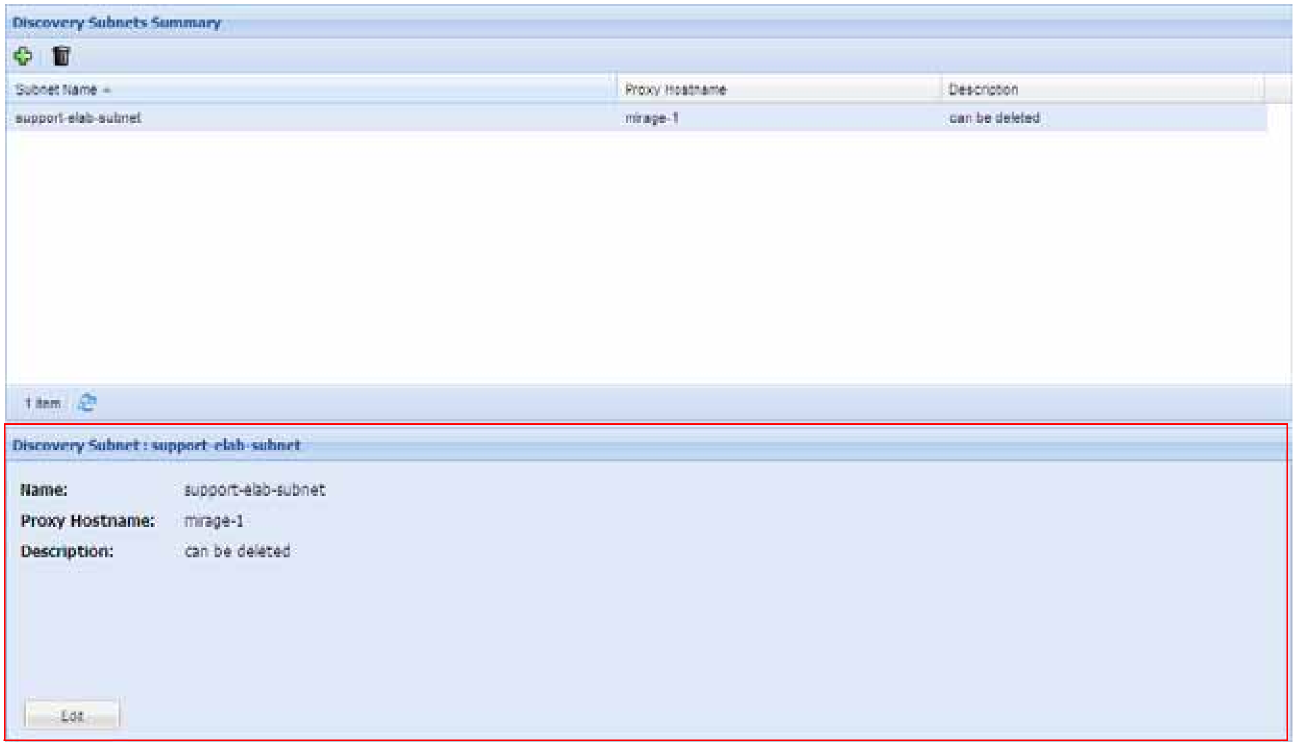
Displaying Discovery Subnet Details

The IP Discovery Subnet has a details frame that displays additional information for a configured discovery subnet. Through the IP Discovery Subnet Details frame, you can also edit selected parameters.

To display details for a discovery subnet, follow this procedure:

Step 1 From the Navigation frame, select *Fabric Director->Discovery Subnet* to display the Discovery Subnet Summary.

Step 2 Click an IP Discovery Subnet in the Discovery Subnet Summary to display the selected item in the details frame as shown in Figure 2.



Discovery Subnets Summary

Subnet Name	Proxy Hostname	Description
support-elab-subnet	mirage-1	can be deleted

1 item

Discovery Subnet : support-elab-subnet

Name: support-elab-subnet
Proxy Hostname: mirage-1
Description: can be deleted

Figure 2 Discovery Subnet Details Frame

Notice that on the Discovery Subnet details frame, you can edit the details to change the proxy host name used for discovery, or the description.

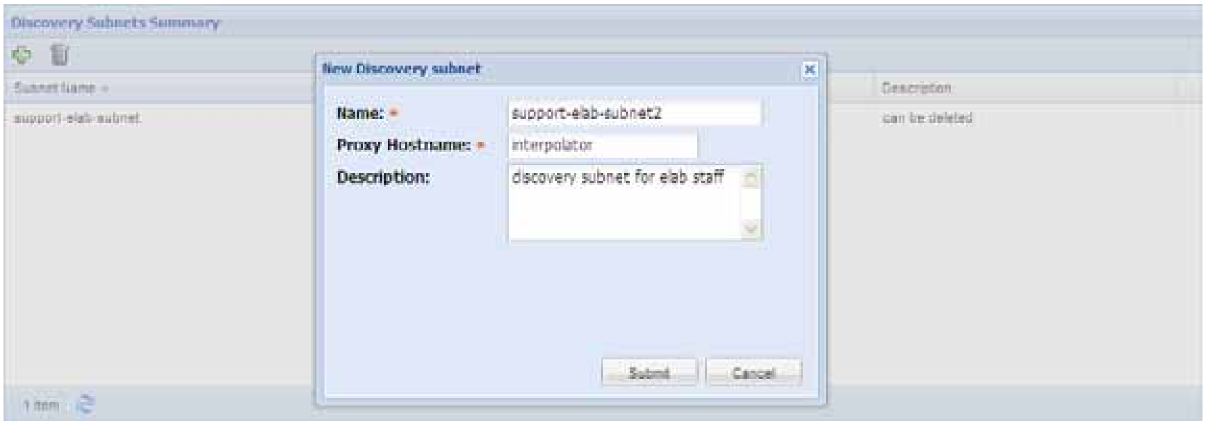
Adding a Discovery Subnet

Through the Discovery Subnet Summary you can add additional discovery subnet profiles so that Fabric Manager can scan additional IP subnets. By adding a discovery subnet, you allow Fabric Manager to learn about hosts and other network devices that are connected on a different subnet than the Oracle Xsigo Fabric Manager Server.

You can add multiple discovery subnets by creating multiple discovery subnet profiles. To add a discovery subnet, follow this procedure:

Step 1 From the Navigation frame, select *Fabric Director->Discovery Subnet* to display the Discovery Subnet Summary.

Step 2 Click the plus sign to display the New Discovery Subnet dialog as shown in Figure 3.



Discovery Subnets Summary

Subnet Name	Description
support-elab-subnet	can be deleted

New Discovery subnet

Name: * support-elab-subnet2

Proxy Hostname: * interpolator

Description: discovery subnet for elab staff

Figure 3 New Discovery Subnet

Step 3 In the *Name* field, enter a name for the discovery subnet profile that you are configuring.

Step 4 In the *Proxy Hostname* field, enter the name of the proxy device that will be used to discover devices on the IP subnet. The Proxy host name can be either a DNS resolvable name or an IP address.

Step 5 As an option, in the *Description* field, enter a description for the discovery subnet.

Step 6 When the Discovery Subnet profile’s parameters have been specified, click ***Submit*** to configure the discovery subnet profile.

Working with VMware Servers

This chapter documents the following topics:

- Supported VMware Virtual Infrastructures
- Integrating Fabric Manager into VMware Virtual Infrastructure
- Starting the Fabric Manager VMware Extension Through VI Client

Supported VMware Virtual Infrastructures

Oracle's Xsigo Fabric Manager can be integrated into a VMware server running any of the following virtual infrastructure components:

- VMware Virtual Center (VC) Server
- VMware vSphere

To integrate Fabric Manager into VMware virtual infrastructure, the VMware operating system must be up and running on the ESX server, and Fabric Manager must already be fully installed on the Fabric Manager server.

Integrating Fabric Manager into VMware Virtual Infrastructure

By default, when Fabric Manager is installed, it is not registered with any VMware VI infrastructure client. Until Fabric Manager is registered, Fabric Manager is not available as an extension of the VMware VI Client, and Xsigo virtual I/O cannot be managed through any VMware virtual infrastructure clients.

Note

If you are upgrading the Fabric Manager Server, see Meeting Minimum Requirements for important information.

When you register Fabric Manager, it is a supported service running on the VC Server. As a result, the ***Virtual I/O*** tab appears in the VI Client's interface.

Note

When you are entering information for the Fabric Manager VMware Extension Installer, at any prompt that requires a host name, do not enter the "localhost" name. Use only the real name of a server running the vCenter or vSphere virtual infrastructure clients.

To register Fabric Manager as a VMware Extension, the following requirements must be met:

- the Fabric Manager must already be installed. If you have not installed Fabric Manager, do so now by following the instructions documented in this chapter.
- all Virtual Center clients must be closed before beginning the process of registering the Fabric Manager Extension with the VC Server. After Fabric Manager is successfully registered, you can open VC clients again.

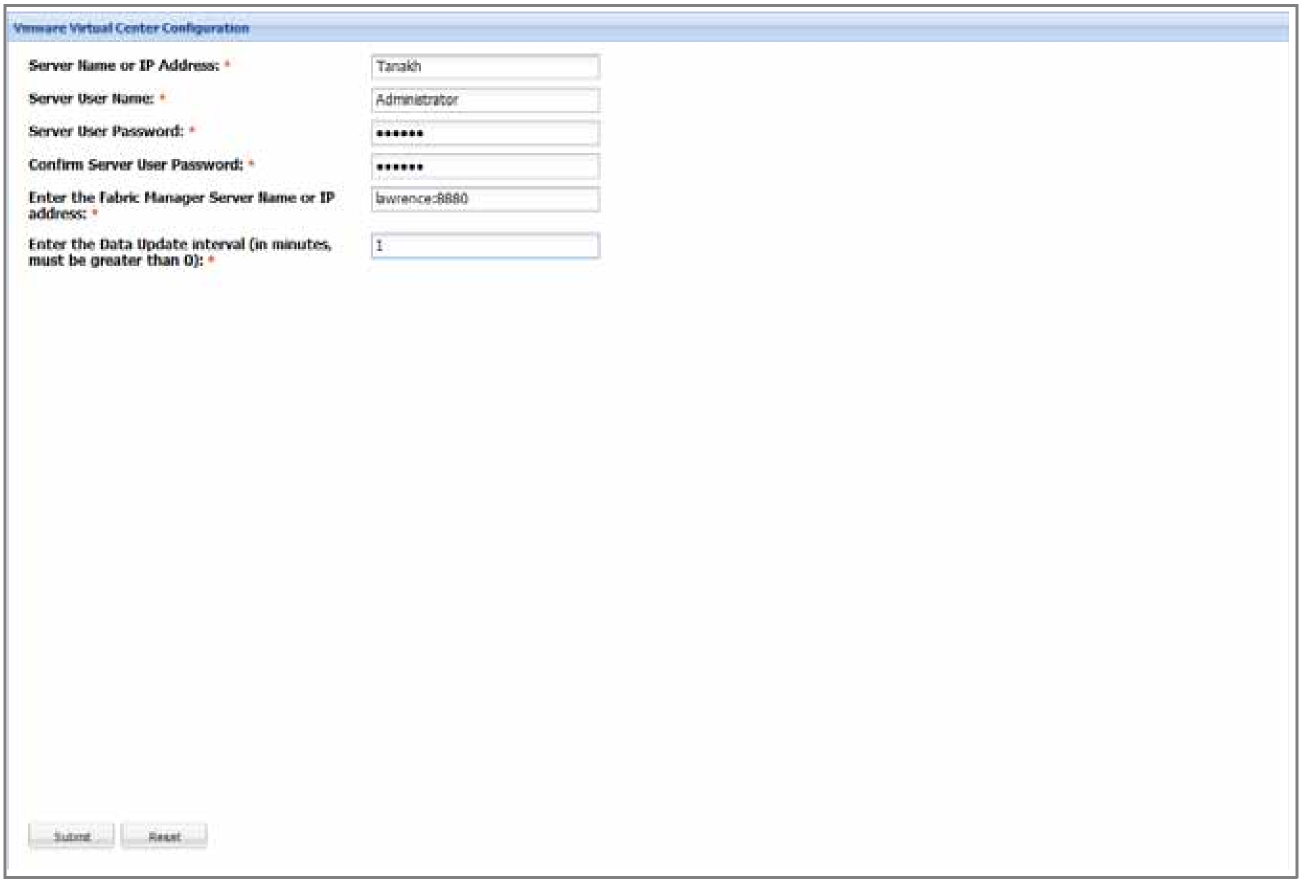
When Fabric Manager is installed, follow this procedure:

Step 1 Open Fabric Manager in a browser window, by pointing the browser to port 8880 on the Fabric Manager Server. For example, if the Fabric Manager server is a device named "Gorilla" you would enter the address:

```
http://Gorilla:8880/xms
```

Step 2 Log in to Fabric Manager by entering the user name and password.

Step 3 From the navigation panel, select *Integration Manager->VMware Integration* to display the VMware Virtual Center Configuration page. Figure 1 shows this page.



Server Name or IP Address: *	Tanakh
Server User Name: *	Administrator
Server User Password: *	••••••
Confirm Server User Password: *	••••••
Enter the Fabric Manager Server Name or IP address: *	lawrence:8880
Enter the Data Update interval (in minutes, must be greater than 0): *	1

Figure 1 VMware Integration Page

Notice that by default the “Register the Fabric Manager Server in VirtualCenter Server” option is set to false.

Step 4 In the *Server Name or IP address* field, enter the device name or IP address of the VMware server.

Step 5 In the *Server User Name* field, enter the name of the user account that can log into the VC server.

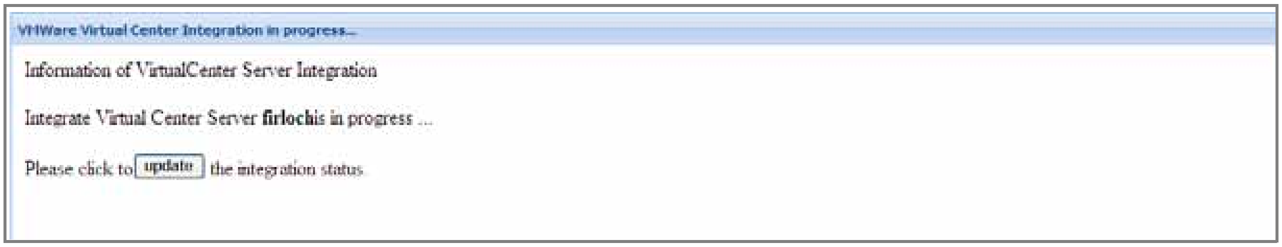
Step 6 In the *Server User Password* field, enter the password for the user account that can log into the VC server.

Step 7 In the *Confirm Server User Password* field, enter the password for the user account again, and make sure that the same password is entered. If the passwords are different, you will be prompted to re-enter them until they match.

Step 8 In the *Enter the Fabric Manager Server Name or IP Address* field specify either the hostname or IP address of the Fabric Manager server that will be integrated into the VMware virtual infrastructure.

Step 9 In the *Enter the Data Update Interval (minutes)* field, enter a value from 1 to 60 that determines the number of minutes that pass between each refresh of VC information through Fabric Manager. This field controls when the Fabric Manager and VI Client sync up information. The default polling interval is 5 minutes.

Step 10 Click ***Submit*** to register the Fabric Manager server with the VC Server. The Integration might take some time to complete, so be patient. A progress dialog is displayed that shows the in-progress integration, as shown in Figure 2.



VMWare Virtual Center Integration in progress...

Information of VirtualCenter Server Integration

Integrate Virtual Center Server **firlochis** in progress ...

Please click to update the integration status

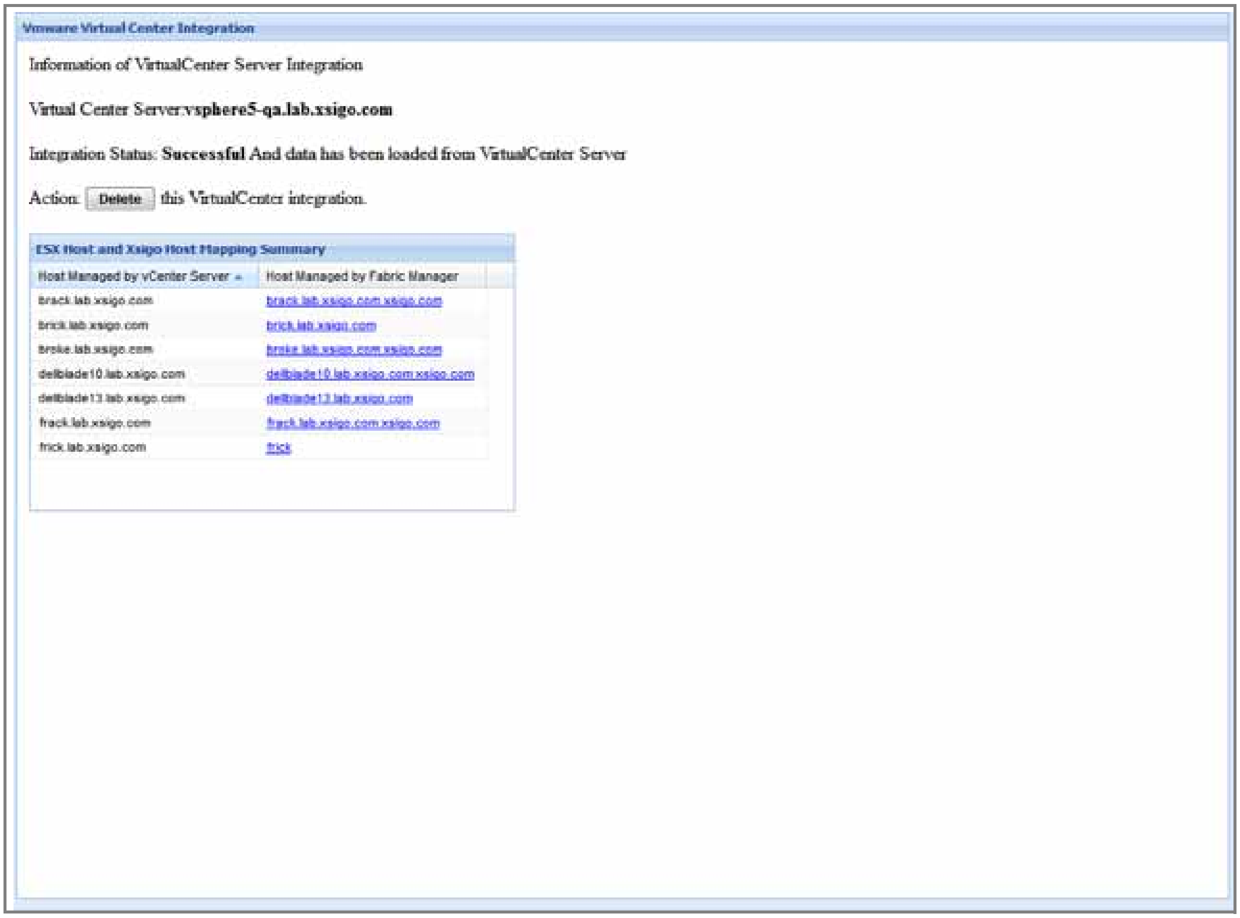
Figure 2 VMware Integration, In Progress

Step 11 After registering Fabric Manager with the VC Server, check the VMware Integration page to make sure that the Fabric Manager server is displayed.

Note

You might need to wait for the first Data Update Interval to complete for the first data sync between Fabric Manager and the VC Server.

If the Fabric Manager server has registered with the VC Server, the ESX Host and Xsigo Host Mapping table is displayed. Figure 3 shows this table.



Vmware Virtual Center Integration

Information of VirtualCenter Server Integration

Virtual Center Server:**vsphere5-qa.lab.xsigo.com**

Integration Status: **Successful** And data has been loaded from VirtualCenter Server

Action: Delete this VirtualCenter integration.

ESX Host and Xsigo Host Mapping Summary

Host Managed by vCenter Server	Host Managed by Fabric Manager
brack.lab.xsigo.com	brack.lab.xsigo.com.xsigo.com
brick.lab.xsigo.com	brick.lab.xsigo.com
broke.lab.xsigo.com	broke.lab.xsigo.com.xsigo.com
dellblade10.lab.xsigo.com	dellblade10.lab.xsigo.com.xsigo.com
dellblade13.lab.xsigo.com	dellblade13.lab.xsigo.com
frack.lab.xsigo.com	frack.lab.xsigo.com.xsigo.com
frick.lab.xsigo.com	frick

Figure 3 VMware Integration Page — Fabric Manager Server Registered with VirtualCenter Server

This table is the combination of two sets of data, the hosts that are learned by the VC Server, and the hosts that are learned by the Fabric Manager. Typically, the table contains the same information for both hosts. However, a difference can occur between the two columns.

When the Fabric Manager registers with the VC Server, it learns the hosts that the VC Server knows about. In this case, the two columns should contain the exact same host names. The two-column display contains information about the hosts managed by both Fabric Manager and the ESX server. If the Hosts are managed by Fabric Manager, you can map them to an ESX Server, by using the Map dropdown list.

A few considerations:

- The Xsigo Hosts column requires a host name, not an IP address. VI Client can support registering hosts by IP address, and if the host is registered by IP address, the host name will not be learned by Fabric Manager and consequently, will not appear in the Xsigo Hosts column.
- You can manually enter the host name in the Xsigo Hosts field. If you do, the name must be exactly as it appears in the VI Client. You cannot use aliases, short names (without the domain or suffix), and you cannot use IP addresses.

Notice that the Xsigo host name (which indicates the hosts that Fabric Manager can manage) contains links to the Server Details page for the named host.

Note

When the Fabric Manager Server is registered with the VC Server, Xsigo Server Profiles, vNICs, and vHBAs are available for configuration and management through the ***Virtual I/O*** tab in the VI Client. If you do not see the button, you can repeat this procedure to make sure that the Fabric Manager Server was correctly registered with the VC Server. For information about using Fabric Manager through VI Client, see Starting the Fabric Manager VMware Extension Through VI Client.

Starting the Fabric Manager VMware Extension Through VI Client

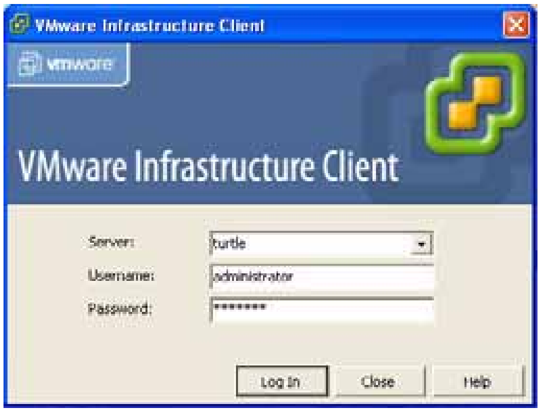
If you have installed the Fabric Manager VMware Extension, you can start the Fabric Manager GUI from within the VI Client.

Note

If you have installed stand-alone Fabric Manager (without the VMware Extension), you can start the Fabric Manager GUI by pointing your browser at an Oracle Xsigo Fabric Director.

To start Fabric Manager from the VI Client, follow this procedure:

Step 1 Double-click the VI Client icon to run the VMware® Virtual Infrastructure Client. Figure 4 shows the Virtual Infrastructure Client Login page.



Server: turtle

Username: administrator

Password: ********

Figure 4 Log In Page

Step 2 Log in with the surname and password you specified when you installed VMware VirtualCenter Management server or vSphere server.

Step 3 On the VI Client toolbar, click the ***Virtual I/O*** tab to display the Fabric Manager Login page. Figure 5 shows the ***Virtual I/O*** tab.

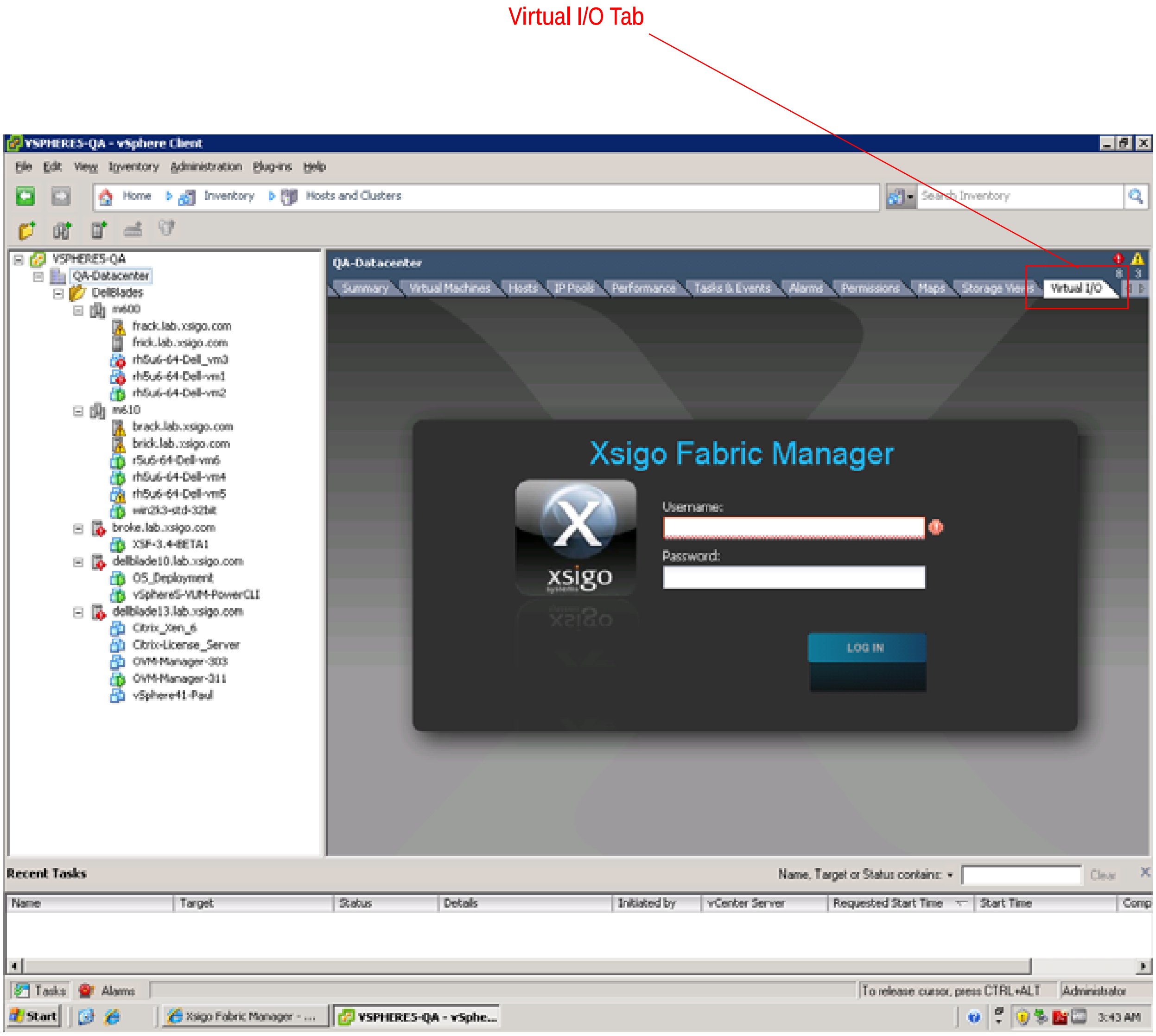


Figure 5 Virtual I/O Tab in vSphere

Note

If the ***Virtual I/O*** tab is not displayed, follow this procedure to manage plug-ins from within the VMware® Virtual Infrastructure Client:
1.) Select *Plug-ins->Manage Plug-ins...* to display the Plugin Manager window.
2.) Click the *Installed* tab.
3.) In the Xsigo Fabric Manager section, click the *Enabled* checkbox to display the Fabric Manager plug-in.
4.) Click ***OK*** to close the Plugin Manager window.
The ***Virtual I/O*** tab should now visible in Virtual Infrastructure Client.

Step 4 Click the ***Virtual I/O*** tab, to start Oracle's Xsigo Fabric Manager in a separate browser window and display the login screen. See Figure 4.

Step 5 Complete Step 2 (enter a user name) and discover Oracle Xsigo Fabric Directors as documented in Working with the Fabric Director.

Working with Alarms

This chapter contains the following topics:

Understanding the Alarm Summary

Alarms are posted to the Alarm Summary, which contains instances of existing alarms. Alarms in the Alarm Summary remain until they are explicitly cleared. When cleared, the “cleared” alarm is no longer present in the Alarm Summary. It is possible for an alarm to be cleared, then reoccur in the Alarm Summary. However, for this to happen, the condition(s) that spawned the alarm must occur again.

Displaying the Alarm Summary

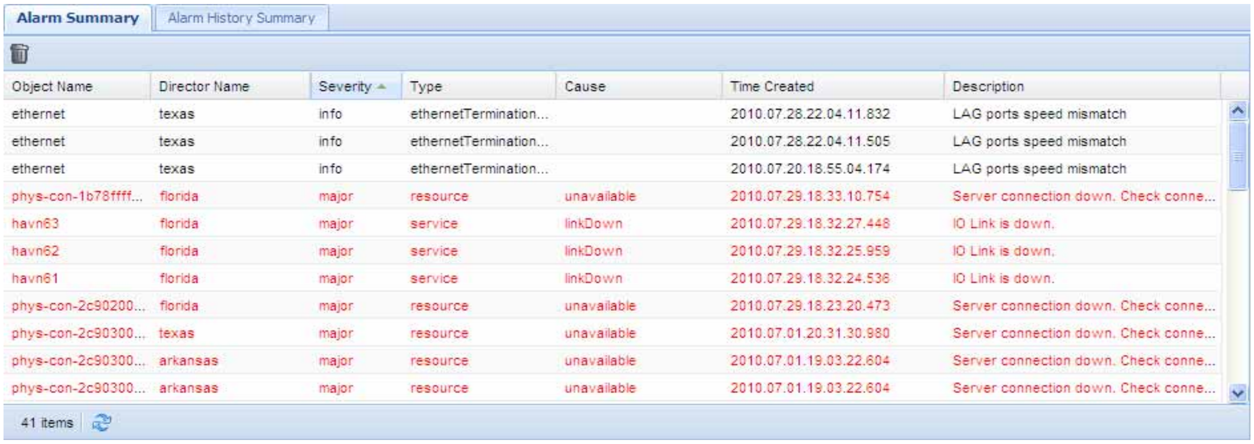
Oracle’s Xsigo Fabric Manager tracks system events and network management alarms and displays them in a table called the Alarm Summary. The Alarm Summary contains real-time information about alarms and events. An alarm is a network management fault of one of the following severities as defined by the TMN TMF model:

- Critical
- Major
- Warning
- Indeterminate
- Minor
- Info
- Conditional

Through the *Filter* menu, you can control the displayed contents of the Alarm Summary, by filtering based on any of these severities.

To display the Alarm Summary, follow this procedure:

Step 1 From the navigation panel, select *General->Alarms*. This step displays the Alarm Summary. Figure 1 shows the Alarm Summary.



Object Name	Director Name	Severity ▲	Type	Cause	Time Created	Description
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.832	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.505	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.20.18.55.04.174	LAG ports speed mismatch
phys-con-1b78ffff...	florida	major	resource	unavailable	2010.07.29.18.33.10.754	Server connection down. Check conne...
havn63	florida	major	service	linkDown	2010.07.29.18.32.27.448	IO Link is down.
havn62	florida	major	service	linkDown	2010.07.29.18.32.25.959	IO Link is down.
havn61	florida	major	service	linkDown	2010.07.29.18.32.24.536	IO Link is down.
phys-con-2c90200...	florida	major	resource	unavailable	2010.07.29.18.23.20.473	Server connection down. Check conne...
phys-con-2c90300...	texas	major	resource	unavailable	2010.07.01.20.31.30.980	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.604	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.604	Server connection down. Check conne...

41 items

Figure 1 Alarm Summary

Table 1 shows the contents of the Alarm Summary and indicates what each field means.

Table 1 Contents of Alarm Summary

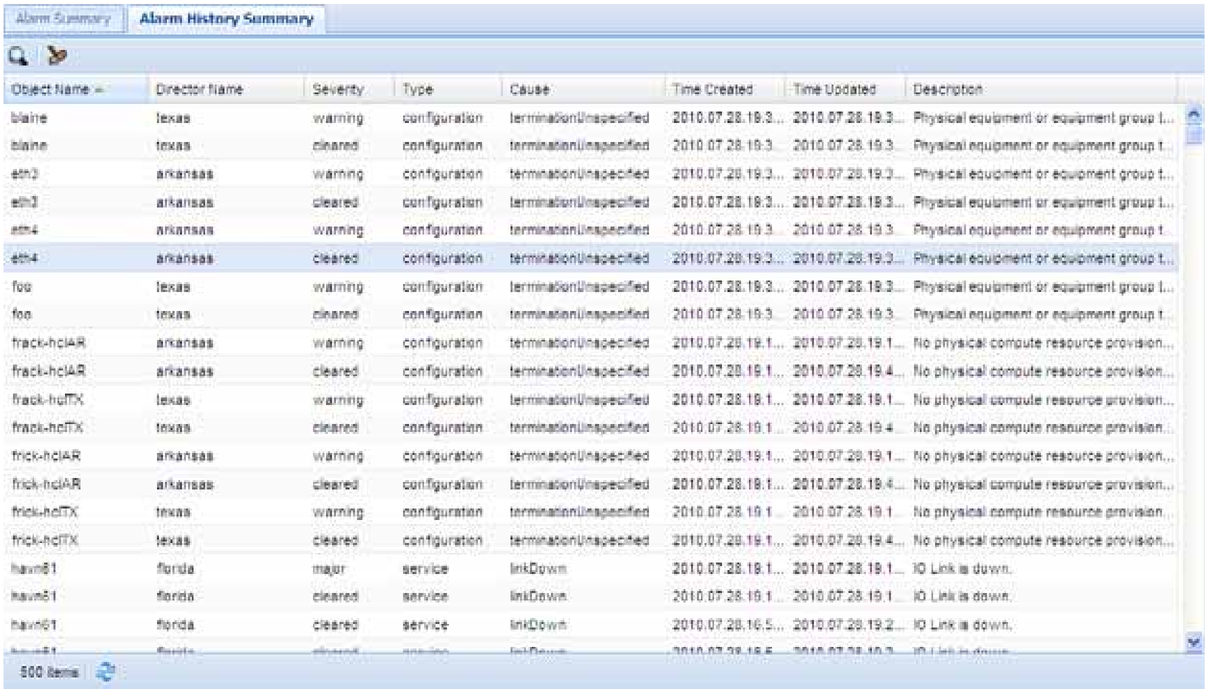
Field	Indicates
Object Name	The object in the Xsigo model on which the alarm occurred. This field typically contains server profile names, vNIC or vHBA names, or physical server names.
Director Name	The name of the Oracle Xsigo Fabric Director where the alarm condition occurred.
Severity	The level of alarm that was raised.
Type	The type of error that occurred.
Cause	The cause of the alarm.
Time Created	The date and time stamp of when the alarm occurred.
Description	A brief description of the alarm condition.

Displaying the Alarm History Summary

Through the Alarm History you can display a history of all alarms reported to Fabric Manager. This information is displayed through the *Alarm History Summary* tab, which contains a table of each alarm's activity and any state changes that have occurred for each alarm. The Alarm Summary History tracks alarm historical information between Fabric Manager reboots, so if the server is rebooted (for example, as part of a software upgrade) the Alarm History Summary will be cleared. However, if the alarm condition still exists, it will be reported to Fabric Manager, and in turn, the Alarm History Summary will begin filling again.

You can display the Alarm History Summary by selecting *Service Manger->Alarms*, then clicking the *Alarm History Summary* tab.

Figure 2 shows the Alarm History Summary.



Object Name	Director Name	Severity	Type	Cause	Time Created	Time Updated	Description
blaine	texas	warning	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
blaine	texas	cleared	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
eth3	arkansas	warning	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
eth3	arkansas	cleared	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
eth4	arkansas	warning	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
eth4	arkansas	cleared	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
foo	texas	warning	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
foo	texas	cleared	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
frack-hclAR	arkansas	warning	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.1...	No physical compute resource provision...
frack-hclAR	arkansas	cleared	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.4...	No physical compute resource provision...
frack-hclTX	texas	warning	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.1...	No physical compute resource provision...
frack-hclTX	texas	cleared	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.4...	No physical compute resource provision...
frick-hclAR	arkansas	warning	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.1...	No physical compute resource provision...
frick-hclAR	arkansas	cleared	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.4...	No physical compute resource provision...
frick-hclTX	texas	warning	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.1...	No physical compute resource provision...
frick-hclTX	texas	cleared	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.4...	No physical compute resource provision...
havn61	florida	major	service	linkDown	2010.07.28.19.1...	2010.07.28.19.1...	IO Link is down.
havn61	florida	cleared	service	linkDown	2010.07.28.19.1...	2010.07.28.19.1...	IO Link is down.
havn61	florida	cleared	service	linkDown	2010.07.28.16.5...	2010.07.28.19.2...	IO Link is down.
havn61	florida	cleared	service	linkDown	2010.07.28.16.5	2010.07.28.19.3	IO Link is down.

500 items

Figure 2 Alarm History Summary

Because the Alarm History Summary can contain a large number of entries, you can filter the entries to display pertinent information, and you can also manually clear one or more alarm entries from the table.

The Alarm History Summary has no corresponding Alarm History Details frame. However, you can display alarm history information for individual alarms. See Viewing an Alarm’s Historical Information.

Filtering the Alarm History Summary

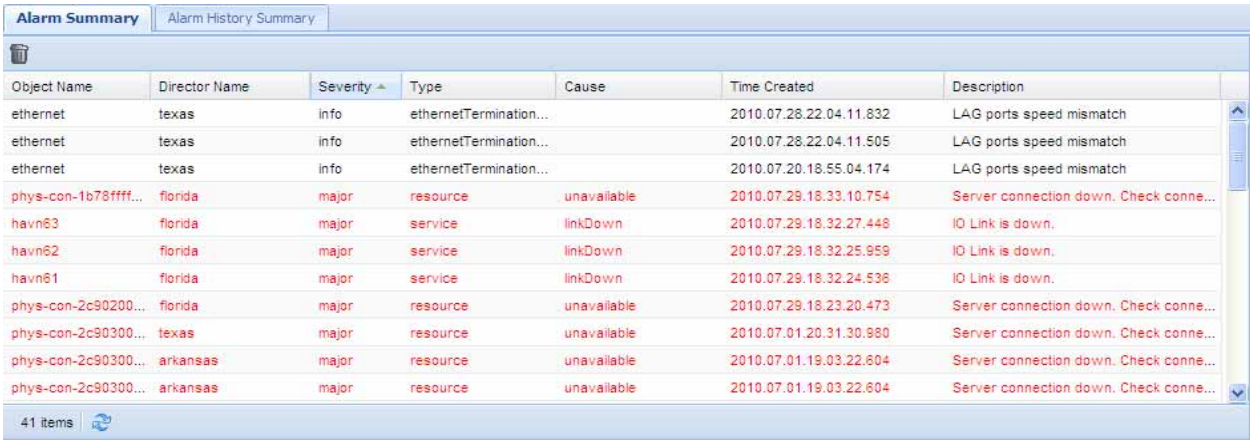
The Alarm History Summary can be filtered by clicking the magnifying glass icon, which allows you to select pre-defined date options for filtering. When you specify filtering criteria, you select a starting date and an ending date that creates a date range. All alarms that occurred during that date range are then displayed with a highlight.

Using these options, you can create the date range to use for filtering. For example, setting the start date as yesterday, and the ending date as today creates a 1-day date range, and all alarms that occurred from yesterday to today would be displayed.

You can filter the Alarm History Summary by using the Filter dialog.

To filter the Alarm History Summary, follow this procedure:

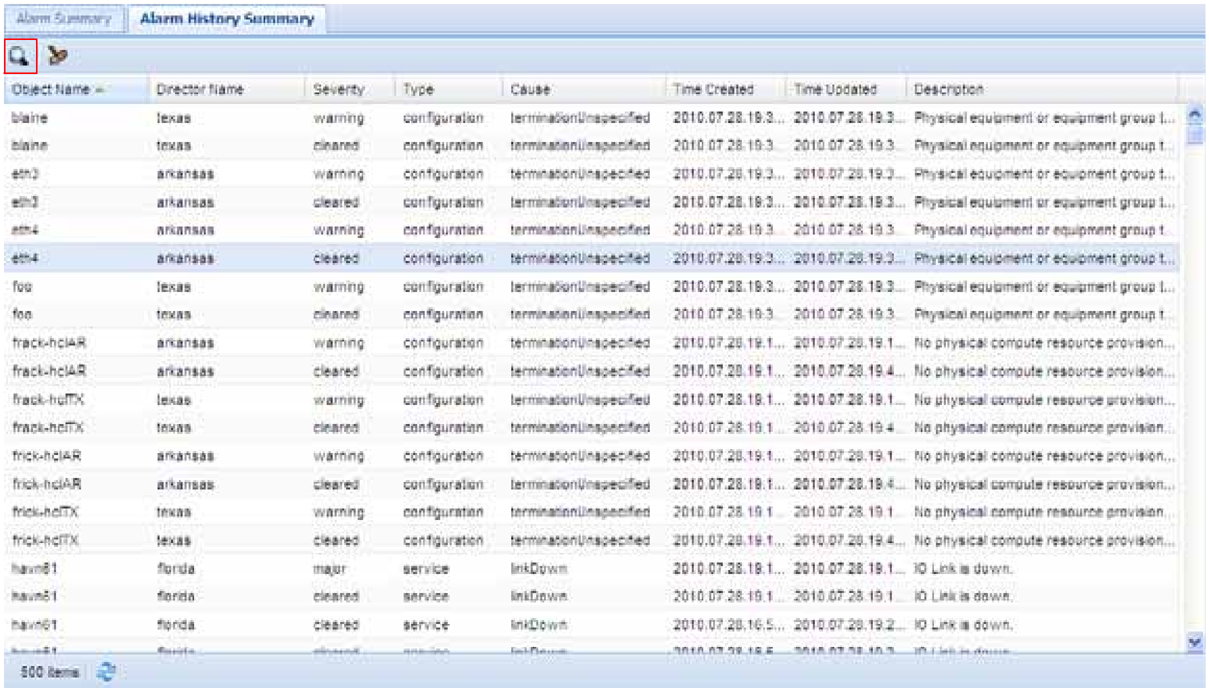
Step 1 From the navigation panel, select *General->Alarms*. This step displays the Alarm Summary. Figure 3 shows the Alarm Summary.



Object Name	Director Name	Severity	Type	Cause	Time Created	Description
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.832	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.505	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.20.18.55.04.174	LAG ports speed mismatch
phys-con-1b78ffff...	florida	major	resource	unavailable	2010.07.29.18.33.10.754	Server connection down. Check conne...
havn63	florida	major	service	linkDown	2010.07.29.18.32.27.448	IO Link is down.
havn62	florida	major	service	linkDown	2010.07.29.18.32.25.959	IO Link is down.
havn61	florida	major	service	linkDown	2010.07.29.18.32.24.536	IO Link is down.
phys-con-2c90200...	florida	major	resource	unavailable	2010.07.29.18.23.20.473	Server connection down. Check conne...
phys-con-2c90300...	texas	major	resource	unavailable	2010.07.01.20.31.30.980	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.604	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.604	Server connection down. Check conne...

Figure 3 Alarm Summary

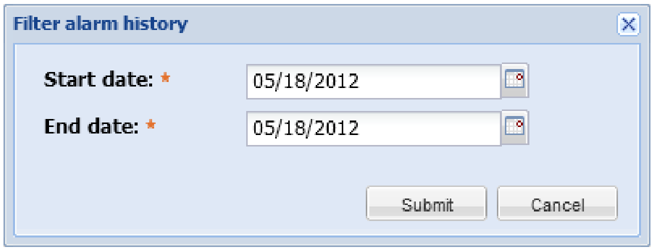
Step 2 On the Alarm Summary, click the *Alarm History Summary* tab to display the Alarm History Summary. Figure 4 shows this tab.



Object Name	Director Name	Severity	Type	Cause	Time Created	Time Updated	Description
blaine	texas	warning	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
blaine	texas	cleared	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
eth3	arkansas	warning	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
eth3	arkansas	cleared	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
eth4	arkansas	warning	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
eth4	arkansas	cleared	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
foo	texas	warning	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
foo	texas	cleared	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
frack-hclAR	arkansas	warning	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.1...	No physical compute resource provision...
frack-hclAR	arkansas	cleared	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.4...	No physical compute resource provision...
frack-hclTX	texas	warning	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.1...	No physical compute resource provision...
frack-hclTX	texas	cleared	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.4...	No physical compute resource provision...
frick-hclAR	arkansas	warning	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.1...	No physical compute resource provision...
frick-hclAR	arkansas	cleared	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.4...	No physical compute resource provision...
frick-hclTX	texas	warning	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.1...	No physical compute resource provision...
frick-hclTX	texas	cleared	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.4...	No physical compute resource provision...
havn61	florida	major	service	linkDown	2010.07.28.19.1...	2010.07.28.19.1...	IO Link is down.
havn61	florida	cleared	service	linkDown	2010.07.28.19.1...	2010.07.28.19.1...	IO Link is down.
havn61	florida	cleared	service	linkDown	2010.07.28.16.5...	2010.07.28.19.2...	IO Link is down.

Figure 4 Alarm History Summary

Step 3 On the Alarm History Summary, click the magnifying glass icon to display the Filter dialog. Figure 5 shows this dialog.



Start date: * 05/18/2012

End date: * 05/18/2012

Figure 5 Filter Alarm History Dialog

Step 4 From the *Start Date* dropdown menu, click to start the calendar utility, and select the start date from the calendar. As an alternative, you can manually enter the start date in the format shown.

Step 5 In the *End Date* dropdown menu, click to start the calendar utility, and select the end date from the calendar. As an alternative, you can manually enter the end date in the format shown.

Step 6 When the Filter dialog is completed, click ***Submit***.

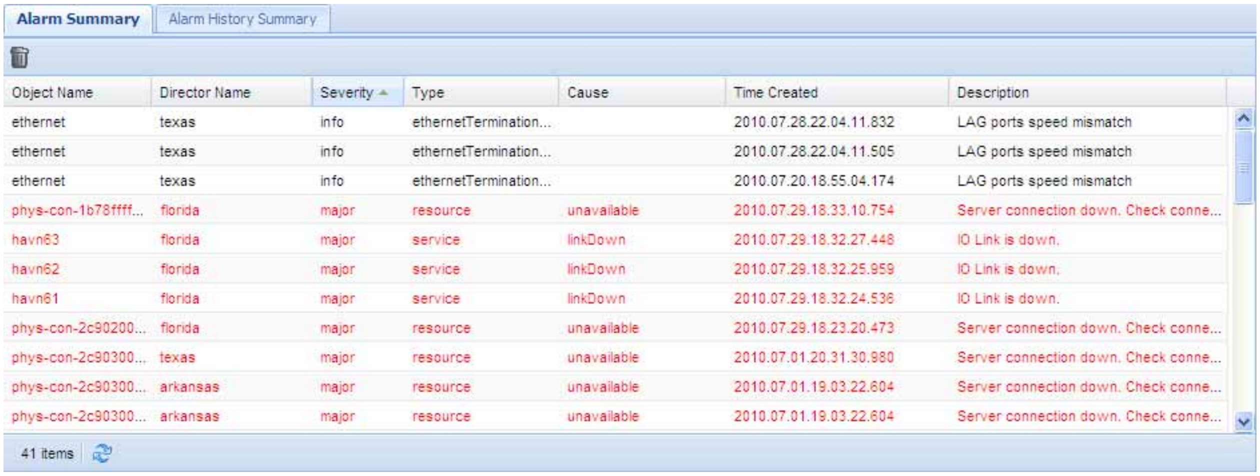
Step 7 Check the Alarm History Summary, which displays the filtered results.

Displaying Detailed Alarm Information

The Alarm Details page contains additional information about network alarms. Detailed alarm information is available through the Alarm Details page.

To display detailed alarm information, follow this procedure:

Step 1 From the navigation panel, select *General->Alarms* to display the Alarm Summary. Figure 6 shows the Alarm Summary.

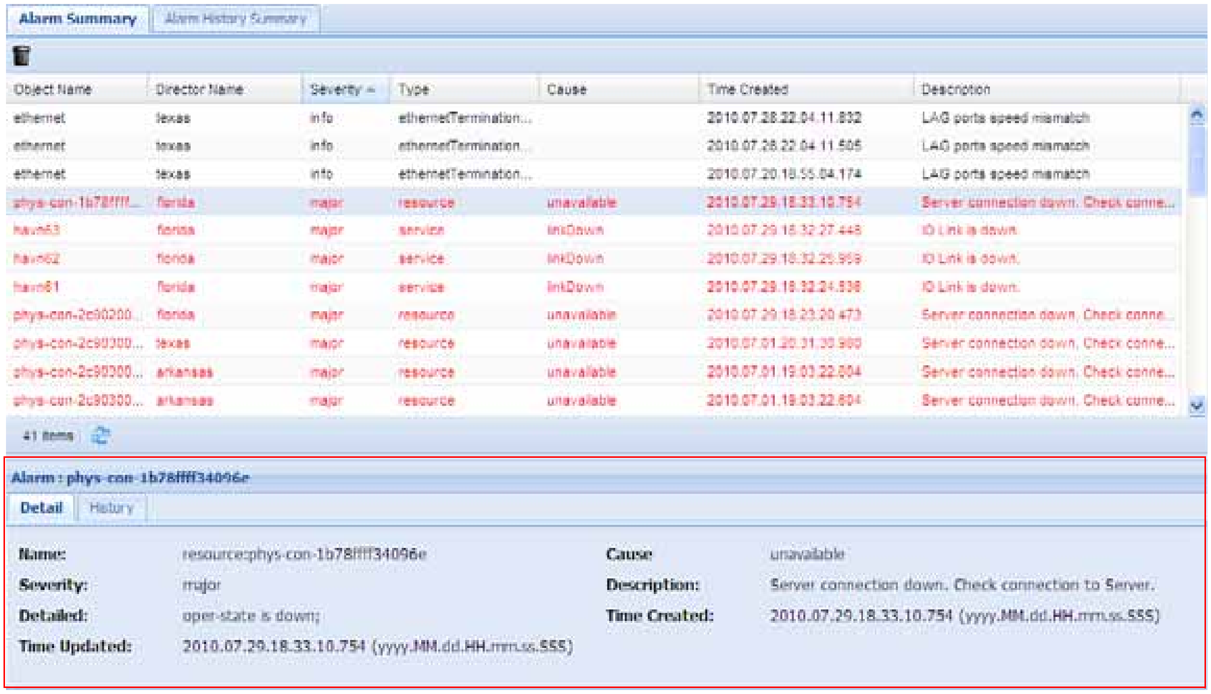


Object Name	Director Name	Severity ▲	Type	Cause	Time Created	Description
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.832	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.505	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.20.18.55.04.174	LAG ports speed mismatch
phys-con-1b78ffff...	florida	major	resource	unavailable	2010.07.29.18.33.10.754	Server connection down. Check conne...
havn63	florida	major	service	linkDown	2010.07.29.18.32.27.448	IO Link is down.
havn62	florida	major	service	linkDown	2010.07.29.18.32.25.959	IO Link is down.
havn61	florida	major	service	linkDown	2010.07.29.18.32.24.536	IO Link is down.
phys-con-2c90200...	florida	major	resource	unavailable	2010.07.29.18.23.20.473	Server connection down. Check conne...
phys-con-2c90300...	texas	major	resource	unavailable	2010.07.01.20.31.30.980	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.604	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.604	Server connection down. Check conne...

41 items

Figure 6 Alarm Summary

Step 2 In the *Object Name* field, click the name of the alarm (as shown) to display detailed information for that alarm. When you click the object name, the Alarm Details page is displayed, as shown in Figure 7.



Object Name	Director Name	Severity	Type	Cause	Time Created	Description
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.832	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.505	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.20.18.55.04.174	LAG ports speed mismatch
phys-con-1b78ffff...	florida	major	resource	unavailable	2010.07.29.18.33.10.754	Server connection down. Check conne...
havn63	florida	major	service	linkDown	2010.07.29.18.32.27.448	IO Link is down.
havn62	florida	major	service	linkDown	2010.07.29.18.32.25.959	IO Link is down.
havn61	florida	major	service	linkDown	2010.07.29.18.32.24.538	IO Link is down.
phys-con-2c90200...	florida	major	resource	unavailable	2010.07.29.18.23.20.473	Server connection down. Check conne...
phys-con-2c90300...	texas	major	resource	unavailable	2010.07.01.20.31.30.980	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.204	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.604	Server connection down. Check conne...

41 items

Alarm : phys-con-1b78ffff34096e

Name: resource:phys-con-1b78ffff34096e
Severity: major
Detailed: oper-state is down;
Time Updated: 2010.07.29.18.33.10.754 (yyyy.MM.dd.HH.mm.ss.SSS)
Cause unavailable
Description: Server connection down. Check connection to Server.
Time Created: 2010.07.29.18.33.10.754 (yyyy.MM.dd.HH.mm.ss.SSS)

Figure 7 Alarm Details Frame

Notice that the Alarms Details frame contains the Detail and History tabs:

- *Detail* shows the general properties for the alarm.
- *History* shows detailed historical information about changes that have occurred for the selected alarm.

Viewing an Alarm’s General Properties

Through the Alarm Details frame, you can display general properties about a single alarm. The general properties display additional pertinent information about the selected alarm. An alarm’s general properties can be displayed through the *Detail* tab, and historical information about the selected alarm can be displayed through the *History* tab.

To display an Alarm’s general properties, follow this procedure:

Step 1 From the navigation panel, select *General->Alarms* to display the Alarm Summary. Figure 1 shows the Alarm Summary.

Step 2 In the *Object Name* field, click the name of the alarm (as shown) to display detailed information for that alarm. When you click the object name, the Alarm Details frame is displayed, as shown in Figure 7.

Table 2 shows the contents of the Alarm Details page and explains what each field means.

Table 2 Contents of Alarm Details Frame

Field	Indicates
Name	The object on which the alarm was raised.
Cause	The cause of the alarm.
Severity	The level of alarm that was raised.
Description	A brief description of the alarm condition.
Detailed	More information (if available) about the error condition on the object that spawned the alarm.
Time Created	The date and time stamp of when the alarm occurred.
Time Updated	The date and time stamp of when the alarm was last posted to the Alarm Summary.

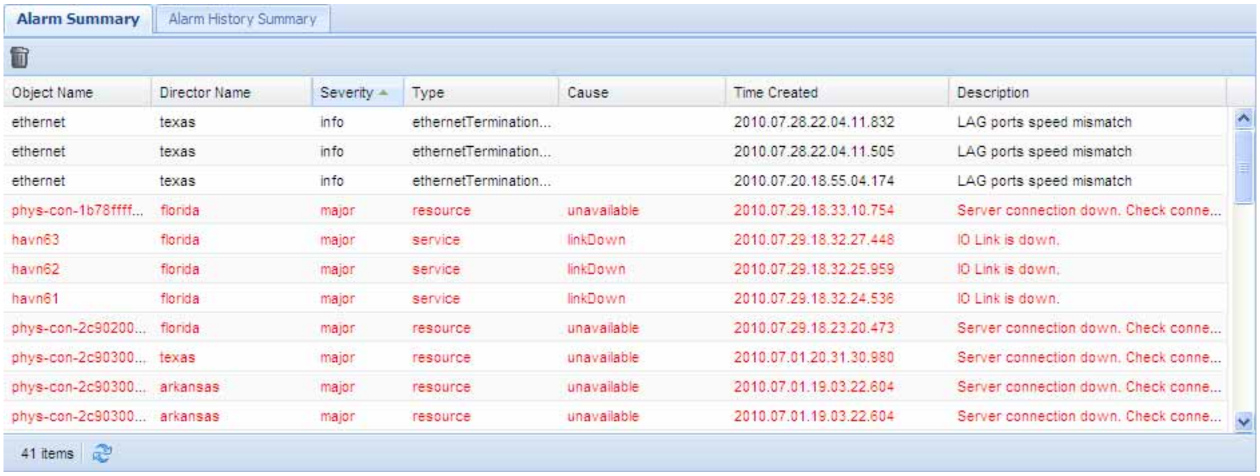
Viewing an Alarm’s Historical Information

Through the Alarm Details frame, you can display historical information about a single alarm. The historical information is a table that lists each time an alarm was modified, such as when an alarm has changed state, or an admin has materially changed the alarm so that a new record is added to the table due to its new status resulting from the change to the alarm.

An alarm’s historical information can be displayed through the *Details* tab, and historical information about the selected alarm can be displayed through the *History* tab.

To display an alarm’s historical information, follow this procedure:

Step 1 From the navigation panel, select *General->Alarms* to display the Alarm Summary. Figure 8 shows the Alarm Summary.

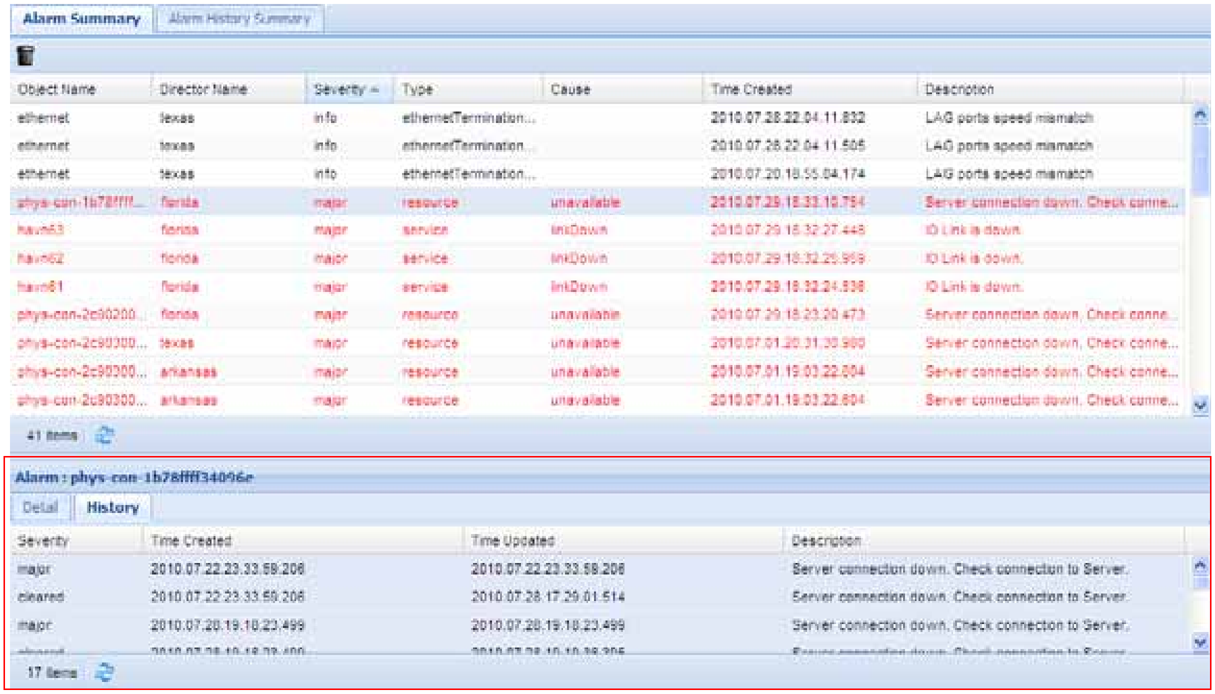


Object Name	Director Name	Severity ▲	Type	Cause	Time Created	Description
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.832	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.505	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.20.18.55.04.174	LAG ports speed mismatch
phys-con-1b78ffff...	florida	major	resource	unavailable	2010.07.29.18.33.10.754	Server connection down. Check conne...
havn63	florida	major	service	linkDown	2010.07.29.18.32.27.448	IO Link is down.
havn62	florida	major	service	linkDown	2010.07.29.18.32.25.959	IO Link is down.
havn61	florida	major	service	linkDown	2010.07.29.18.32.24.536	IO Link is down.
phys-con-2c90200...	florida	major	resource	unavailable	2010.07.29.18.23.20.473	Server connection down. Check conne...
phys-con-2c90300...	texas	major	resource	unavailable	2010.07.01.20.31.30.980	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.604	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.604	Server connection down. Check conne...

41 items

Figure 8 Alarm Summary

Step 2 In the *Object Name* field, click the name of the alarm (as shown) to display detailed information for that alarm. When you click the object name, the Alarm Details page is displayed, as shown in Figure 9.



Object Name	Director Name	Severity	Type	Cause	Time Created	Description
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.832	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.505	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.20.18.55.04.174	LAG ports speed mismatch
phys-con-1b78ffff...	florida	major	resource	unavailable	2010.07.29.18.33.10.754	Server connection down. Check conne...
havn63	florida	major	service	linkDown	2010.07.29.18.32.27.448	IO Link is down.
havn62	florida	major	service	linkDown	2010.07.29.18.32.25.959	IO Link is down.
havn61	florida	major	service	linkDown	2010.07.29.18.32.24.538	IO Link is down.
phys-con-2c90200...	florida	major	resource	unavailable	2010.07.29.18.23.20.473	Server connection down. Check conne...
phys-con-2c90300...	texas	major	resource	unavailable	2010.07.01.20.31.30.900	Server connection down. Check conne...
phys-con-2c90200...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.204	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.604	Server connection down. Check conne...

Severity	Time Created	Time Updated	Description
major	2010.07.22.23.33.58.206	2010.07.22.23.33.58.206	Server connection down. Check connection to Server.
cleared	2010.07.22.23.33.58.206	2010.07.28.17.29.01.514	Server connection down. Check connection to Server.
major	2010.07.28.19.18.23.499	2010.07.28.19.18.23.499	Server connection down. Check connection to Server.

Figure 9 Alarm Details Frame

The *History* tab shows the history of changes made to the selected alarm, including the action that cleared the alarm. Historical records for an alarm are arranged oldest to newest so that the most recent changes to an alarm are at the bottom of the list.

Table 3 shows the contents of the Alarm Details History tab, and explains what each field on the tab means.

Table 3 Contents of Alarm Details History Tab

Field	Indicates
Severity	The level of alarm that was raised.
Time Created	The date and time stamp of when the alarm occurred.
Time Updated	The date and time stamp of when the alarm was last posted to the Alarm Summary.
Description	A brief description of the alarm condition.

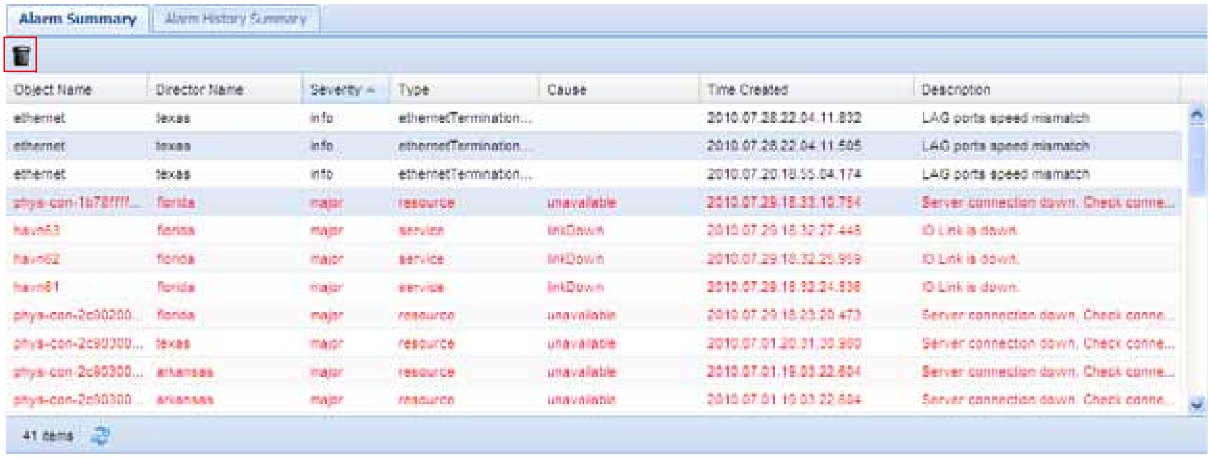
Clearing Alarms from the Alarm Summary

When the condition that created the alarm has been fixed, you can remove the alarm from the Alarm Summary by deleting the entry. An alarm that has been removed from the Alarm Summary is considered a cleared alarm. When an alarm is cleared, it is no longer displayed in the Alarm Summary, but is still displayed in the Alarm History Summary.

To clear alarms from the Alarm Summary, follow this procedure:

Step 1 From the navigation panel, select *General->Alarms*. This step displays the Alarm Summary.

Step 2 On the Alarm Summary, click one or more alarms to select them as shown in Figure 10. The selected alarm(s) will be cleared.



Object Name	Director Name	Severity	Type	Cause	Time Created	Description
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.832	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.505	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.20.18.55.04.174	LAG ports speed mismatch
phys-con-1b78ffff...	florida	major	resource	unavailable	2010.07.29.18.33.10.754	Server connection down. Check conne...
havn63	florida	major	service	linkDown	2010.07.29.18.32.27.448	IO Link is down.
havn62	florida	major	service	linkDown	2010.07.29.18.32.25.959	IO Link is down.
havn61	florida	major	service	linkDown	2010.07.29.18.32.24.538	IO Link is down.
phys-con-2c90200...	florida	major	resource	unavailable	2010.07.29.18.23.20.473	Server connection down. Check conne...
phys-con-2c90300...	texas	major	resource	unavailable	2010.07.01.20.31.30.980	Server connection down. Check conne...
phys-con-2c80300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.804	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.804	Server connection down. Check conne...

Figure 10 Alarm Summary

Step 3 Click the garbage can icon to delete the selected alarms. When you click the garbage can, a confirmation dialog is displayed to verify that you want to actually delete the selected alarm(s).

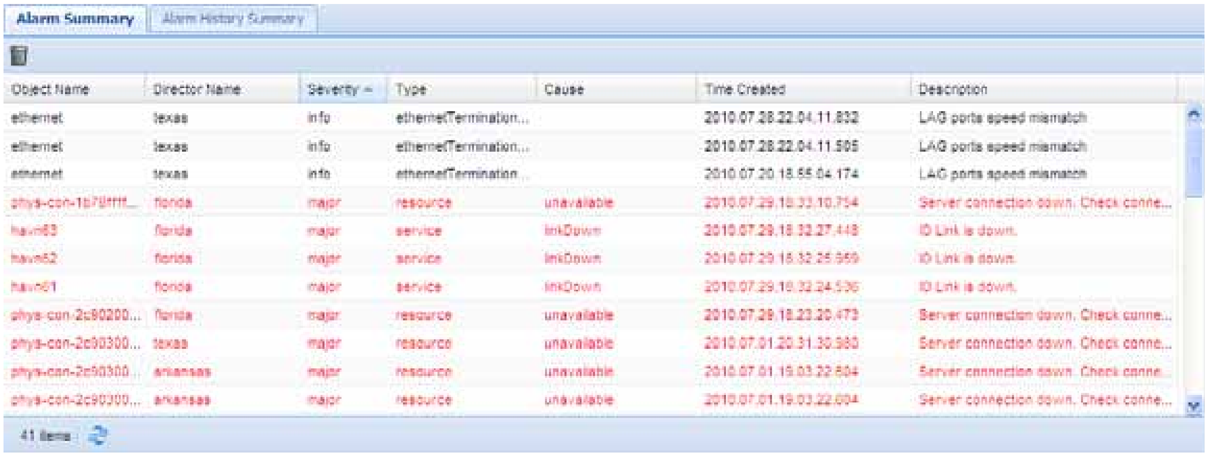
Step 4 On the Confirmation dialog, select ***Yes*** to delete the selected alarm, or ***No*** to abort deleting the selected alarm.

Clearing Alarms from the Alarm History

The Alarm History Summary contains a table of historical information for all alarms reported to Oracle's Xsigo Fabric Manager. Since all alarms are kept for historical reference, the Alarm History Summary can grow to a large size. You can manually clear the Alarm History Summary to keep it at a manageable size. The Alarm History Summary does not automatically delete entries.

To clear alarms from the Alarm History summary, follow this procedure:

Step 1 From the navigation panel, select *General->Alarms*. This step displays the Alarm Summary. Figure 11 shows the Alarm Summary.



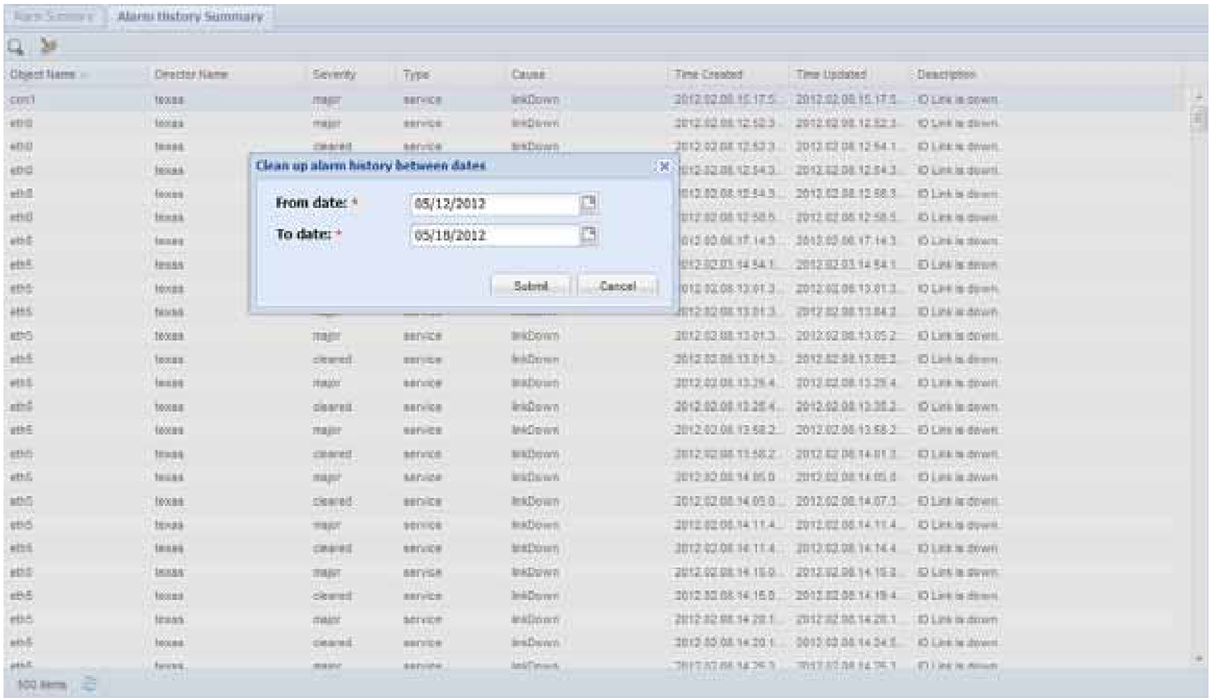
Object Name	Director Name	Severity	Type	Cause	Time Created	Description
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.832	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.505	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.20.18.55.04.174	LAG ports speed mismatch
phys-con-1b78ffff...	florida	major	resource	unavailable	2010.07.29.18.33.10.754	Server connection down. Check conne...
havn63	florida	major	service	linkDown	2010.07.29.18.32.27.448	IO Link is down.
havn62	florida	major	service	linkDown	2010.07.29.18.32.25.959	IO Link is down.
havn61	florida	major	service	linkDown	2010.07.29.18.32.24.536	IO Link is down.
phys-con-2c90200...	florida	major	resource	unavailable	2010.07.28.18.23.20.473	Server connection down. Check conne...
phys-con-2c90300...	texas	major	resource	unavailable	2010.07.01.20.31.30.380	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.604	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.604	Server connection down. Check conne...

41 items

Figure 11 Alarm History Summary

Step 2 Click the *Alarm History Summary* tab.

Step 3 Click the eraser icon to display the Clean Up Alarm History dialog as shown Figure 12.



Clean up alarm history between dates

From date: * 05/12/2012

To date: * 05/18/2012

Object Name	Director Name	Severity	Type	Cause	Time Created	Time Updated	Description
con1	texas	major	service	linkDown	2012.02.08.15.17.5...	2012.02.08.15.17.5...	IO Link is down.
eth0	texas	major	service	linkDown	2012.02.08.12.52.3...	2012.02.08.12.52.3...	IO Link is down.
eth0	texas	cleared	service	linkDown	2012.02.08.12.52.3...	2012.02.08.12.54.1...	IO Link is down.
eth0	texas				2012.02.08.12.54.3...	2012.02.08.12.54.3...	IO Link is down.
eth8	texas				2012.02.08.12.54.3...	2012.02.08.12.58.3...	IO Link is down.
eth0	texas				2012.02.08.12.58.5...	2012.02.08.12.58.5...	IO Link is down.
eth8	texas				2012.02.08.17.14.3...	2012.02.08.17.14.3...	IO Link is down.
eth4	texas				2012.02.03.14.54.1...	2012.02.03.14.54.1...	IO Link is down.
eth5	texas				2012.02.08.13.01.3...	2012.02.08.13.01.3...	IO Link is down.
eth5	texas				2012.02.08.13.01.3...	2012.02.08.13.04.2...	IO Link is down.
eth5	texas	major	service	linkDown	2012.02.08.13.01.3...	2012.02.08.13.05.2...	IO Link is down.
eth5	texas	cleared	service	linkDown	2012.02.08.13.01.3...	2012.02.08.13.05.2...	IO Link is down.
eth5	texas	major	service	linkDown	2012.02.08.13.25.4...	2012.02.08.13.25.4...	IO Link is down.
eth5	texas	cleared	service	linkDown	2012.02.08.13.25.4...	2012.02.08.13.35.2...	IO Link is down.
eth5	texas	major	service	linkDown	2012.02.08.13.58.2...	2012.02.08.13.58.2...	IO Link is down.
eth5	texas	cleared	service	linkDown	2012.02.08.13.58.2...	2012.02.08.14.01.3...	IO Link is down.
eth5	texas	major	service	linkDown	2012.02.08.14.05.0...	2012.02.08.14.05.0...	IO Link is down.
eth5	texas	cleared	service	linkDown	2012.02.08.14.05.0...	2012.02.08.14.07.3...	IO Link is down.
eth5	texas	major	service	linkDown	2012.02.08.14.11.4...	2012.02.08.14.11.4...	IO Link is down.
eth5	texas	cleared	service	linkDown	2012.02.08.14.11.4...	2012.02.08.14.14.4...	IO Link is down.
eth5	texas	major	service	linkDown	2012.02.08.14.15.0...	2012.02.08.14.15.0...	IO Link is down.
eth5	texas	cleared	service	linkDown	2012.02.08.14.15.0...	2012.02.08.14.19.4...	IO Link is down.
eth5	texas	major	service	linkDown	2012.02.08.14.20.1...	2012.02.08.14.20.1...	IO Link is down.
eth5	texas	cleared	service	linkDown	2012.02.08.14.20.1...	2012.02.08.14.24.5...	IO Link is down.
eth5	texas	major	service	linkDown	2012.02.08.14.25.1...	2012.02.08.14.25.1...	IO Link is down.

Figure 12 Alarm History Summary — Selecting Date Range for Alarm Clean Up

Step 4 In the *From Date* field, click the calendar utility and select the start date for the time range in which alarms will be cleaned out of the Alarm History. As an alternative, you can manually enter the start date in the format shown.

Step 5 In the *To Date* field, click the calendar utility and select the start date for the time range in which alarms will be cleaned out of the Alarm History. As an alternative, you can manually enter the end date in the format shown.

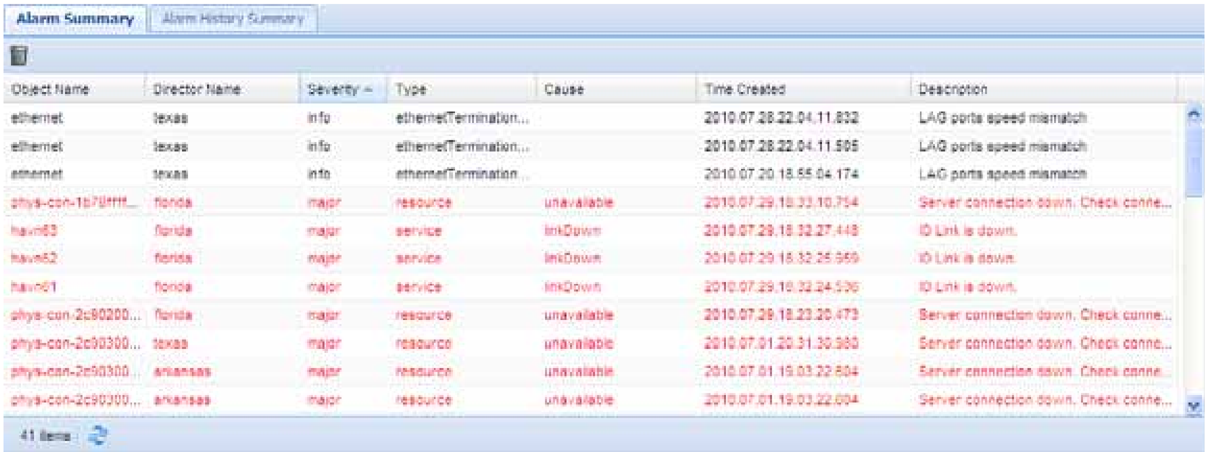
Step 6 When the dates are entered, click ***Submit*** to clean alarms that fall within the date range out of the Alarm History.

Filtering the Alarm History Summary

When the Alarm History Summary is large, finding specific alarm entries can be difficult. To facilitate finding the appropriate information in the Alarm History Summary, you can use the filtering tool. The filtering tool allows you to specify a starting date and an ending date that create a range. When you apply the filter, the Alarm History Summary displays the alarms for only that date range. All other alarm history summary entries are not displayed.

To filter the Alarm History Summary, follow this procedure:

Step 1 From the navigation panel, select *General->Alarms*. This step displays the Alarm Summary. Figure 13 shows the Alarm Summary.

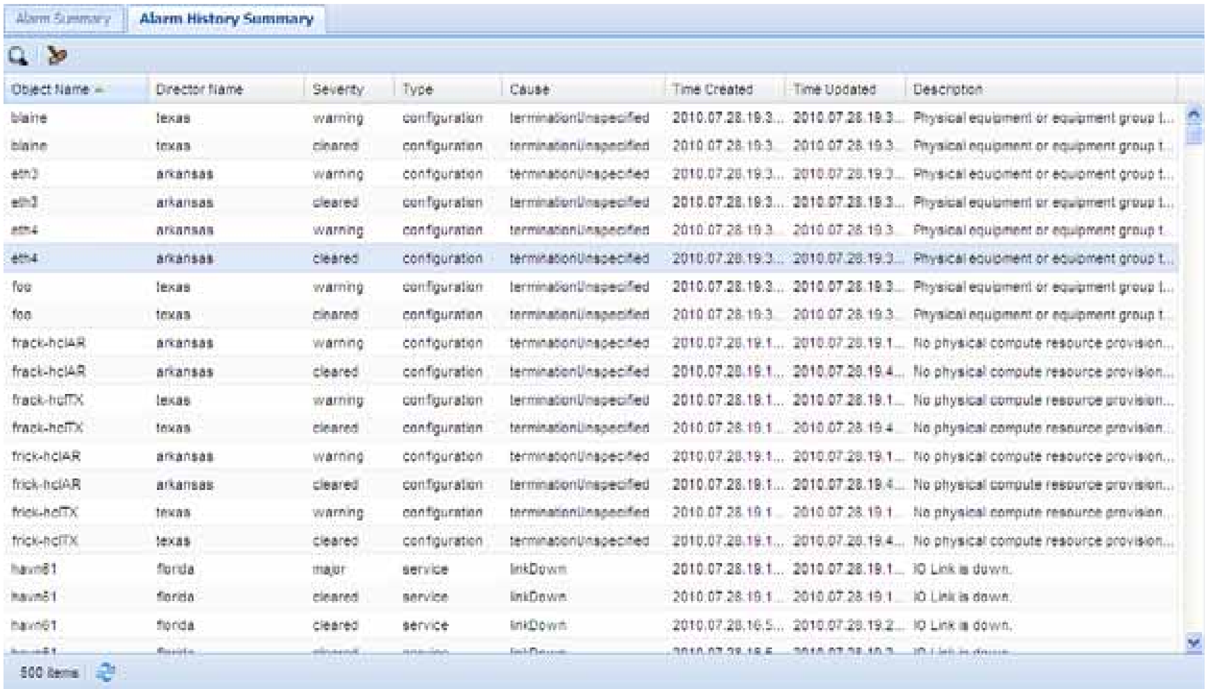


Object Name	Director Name	Severity	Type	Cause	Time Created	Description
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.832	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.28.22.04.11.505	LAG ports speed mismatch
ethernet	texas	info	ethernetTermination...		2010.07.20.18.55.04.174	LAG ports speed mismatch
phys-con-1b78ffff...	florida	major	resource	unavailable	2010.07.29.18.33.10.754	Server connection down. Check conne...
havn63	florida	major	service	linkDown	2010.07.29.18.32.27.448	IO Link is down.
havn62	florida	major	service	linkDown	2010.07.29.18.32.25.969	IO Link is down.
havn61	florida	major	service	linkDown	2010.07.29.18.32.24.536	IO Link is down.
phys-con-2c90200...	florida	major	resource	unavailable	2010.07.28.18.23.20.473	Server connection down. Check conne...
phys-con-2c90300...	texas	major	resource	unavailable	2010.07.01.20.31.30.980	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.604	Server connection down. Check conne...
phys-con-2c90300...	arkansas	major	resource	unavailable	2010.07.01.19.03.22.604	Server connection down. Check conne...

41 items

Figure 13 Alarm History Summary

Step 2 Click the *Alarm History Summary* tab. Figure 14 shows the Alarm History Summary.

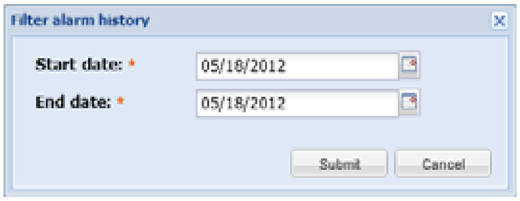


Object Name	Director Name	Severity	Type	Cause	Time Created	Time Updated	Description
blaine	texas	warning	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
blaine	texas	cleared	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
eth3	arkansas	warning	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
eth3	arkansas	cleared	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
eth4	arkansas	warning	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
eth4	arkansas	cleared	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
foo	texas	warning	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
foo	texas	cleared	configuration	terminationUnspecified	2010.07.28.19.3...	2010.07.28.19.3...	Physical equipment or equipment group t...
frack-hcIAR	arkansas	warning	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.1...	No physical compute resource provision...
frack-hcIAR	arkansas	cleared	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.4...	No physical compute resource provision...
frack-hcITX	texas	warning	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.1...	No physical compute resource provision...
frack-hcITX	texas	cleared	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.4...	No physical compute resource provision...
frick-hcIAR	arkansas	warning	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.1...	No physical compute resource provision...
frick-hcIAR	arkansas	cleared	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.4...	No physical compute resource provision...
frick-hcITX	texas	warning	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.1...	No physical compute resource provision...
frick-hcITX	texas	cleared	configuration	terminationUnspecified	2010.07.28.19.1...	2010.07.28.19.4...	No physical compute resource provision...
havn61	florida	major	service	linkDown	2010.07.28.19.1...	2010.07.28.19.1...	IO Link is down.
havn61	florida	cleared	service	linkDown	2010.07.28.19.1...	2010.07.28.19.1...	IO Link is down.
havn61	florida	cleared	service	linkDown	2010.07.28.16.5...	2010.07.28.19.2...	IO Link is down.

500 items

Figure 14 Alarm History Summary

Step 3 Click the magnifying glass icon to display the Filter Alarm History dialog as shown in Figure 15.



Start date: * 05/18/2012

End date: * 05/18/2012

Figure 15 Alarm History Summary — Deleting an Entry

Step 4 From the *Start Date* dropdown menu, select the first date in the range you will use for filtering.

Step 5 From the *End Date* dropdown menu, select the last date in the range you will use for filtering.

Step 6 When the correct timestamp range is specified, click ***Submit***. All alarm history entries that comply with the date range are displayed as highlighted rows in the Alarm History Summary.

Working with High Availability Fabric Manager

This chapter documents the following topics:

- Understanding High Availability Fabric Manager
- Configuring HA Fabric Manager Servers
- Setting an HA Partner’s Mode
- Setting a Sync Interval
- Forcing Sync Up
- Performing Failover and Failback
- Displaying HA Fabric Manager Information
- Displaying HA Partner Detailed Information
- Deleting an HA Partner

Understanding High Availability Fabric Manager

Fabric Manager supports high availability mode, in which multiple Fabric Manager servers are associated with each other to provide a system of Fabric Manager servers that operate in active/passive roles. This high availability Fabric Manager (HA Fabric Manager) system consists of the following components:

- one active Fabric Manager server, and one passive Fabric Manager server. Together, the two servers are called HA partners
- a Fabric Manager server configuration (for the primary Fabric Manager server)
- an HA configuration (one for each of the HA partners)

When HA Fabric Manager partners are configured for a Fabric Manager server, the active and passive partner work together as a pair to retain the same configuration (or an extremely close match) to provide high availability to the Fabric Directors and virtual resources configured within the HA Fabric Manager deployment. After initial configuration, the active partner syncs up automatically with the passive partner. From that point forward, all the HA partners keep in contact with the active partner by sending HA ping packets which verify connectivity between the partners. (Note that HA pings are a separate proprietary message, not a standard ICMP ping.) All nodes use pings to verify each other’s mode, and also to update their records with information about changes made since the last ping. Through the pings, HA partners can determine if one of the Fabric manager servers in the HA system has gone offline, and will update that server’s state in the Fabric Manager user interface so that you can take any corrective action.

Note

Currently, if an HA partner is determined to be not operational, there is no alarm or notification that the server. Also, there is no recovery or self-healing algorithm to get the offline server back online. If an HA partner is determined to be offline, you must take actions to get the server back online.

Also, the active partner periodically syncs a backup file to all passive nodes to ensure that the HA system has the same configuration. On the passive partner, the backup file is stored in the xms-backups directory. You can customize the sync interval through the Fabric Manager user interface if your network requires a quicker or slower sync between the passive and active partners.

Requirements

The High Availability Fabric Manager system has the following requirements:

- the OS installed must be the same on both servers
- the version of Java Runtime Environment (JRE) must be the same on both servers
- both servers must be pingable by host name
- For HA Fabric Managers with Fabric Performance Monitor running on both servers, you must install the PostgreSQL data on a separate server that is reachable by both partners in the HA system. For more information, see Configuring HA Fabric Manager Servers.

Consideration for HA Fabric Manager and Plug-Ins

Fabric Manager supports numerous additional robust tools as plug-ins to the Fabric Manager core graphical user interface. However, with HA Fabric Manager, two instances of Fabric Manager are running—one on the active partner, and one on the passive partner.

If you will be using plug-ins in your HA Fabric Manager system, it is a best practice to install the plug ins on both the partners. To do so, completely install the plug ins on both Fabric Manager servers before connecting them together in an HA system.

By doing installing the plug ins on both servers that will be in the HA system, both servers are “active” at that time. As a result, you ensure that important information, such as config files, application files, and database records, are backed up when the active partner syncs with the passive partner. Also, in the unlikely event that the active partner becomes unavailable, the same applications will be available to the passive partner after it is promoted to the new active node. By installing plug ins on both servers in the HA system before configuring them in the HA system, you retain identical functionality after a failover event, and minimize downtime. If you already have HA Fabric Manager configured and need to install one or more plug-ins on the passive partner, see Installing Plug-ins on the Passive Server.

Fabric Performance Monitoring in HA Fabric Manager Environment

For HA Fabric Manager, if you will be installing Fabric Performance Monitoring, be aware that you will need to install the PostgreSQL database on a separate server that is reachable by both HA partners. This requirement exists to allow the database to be available to both servers during a failover. As part of this requirement, you should follow the PostgreSQL best practices to install and backup the database. Documentation for such best practices is out of the scope of this documentation, but is available in the public domain such as on the web.

In an HA system, if the PostgreSQL database is installed on only the active server, a failover can cause the Fabric Performance Monitoring application with current information to move away from the PostgreSQL database. But, when the PostgreSQL database is installed on a commonly accessible sever, Fabric Performance Monitoring survives a failover. Consider the following example.

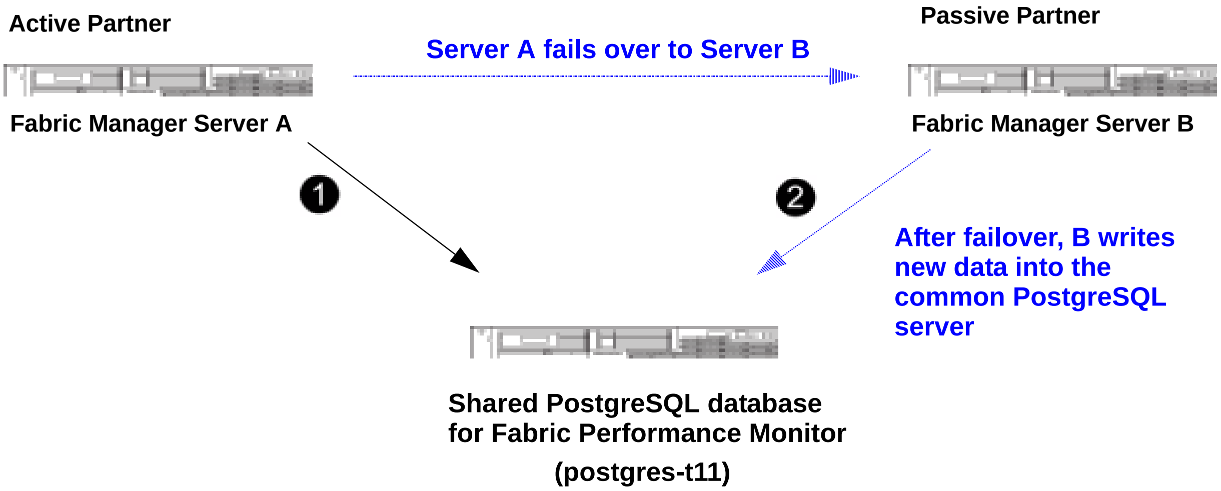

Active Partner
Server A fails over to Server B
Passive Partner
Fabric Manager Server A
Fabric Manager Server B
1
2
After failover, B writes new data into the common PostgreSQL server
Shared PostgreSQL database for Fabric Performance Monitor
(postgres-t11)

Figure 1 Shared Server for Fabric Performance Monitoring in HA Fabric Manager Deployment

However, by installing the PostgreSQL database on a shared server and pointing both servers to shared server’s IP address, the database remains available after the failover regardless of which HA partner is active. During normal runtime operation (see “1” in Figure 1) the active HA partner writes information to the PostgreSQL database. However, when the active HA partner “Server A” fails over, (see “2” in Figure 1), the PostgreSQL database is still online and available on the shared PostgreSQL server (“postgres-t11”). As long as both HA partners point to the shared server as the location of Fabric Performance Monitoring’s PostgreSQL database. The database will be available to both the HA partners. As a result, after you bring “Server B” back online, it can access the PostgreSQL database and Fabric Performance Monitoring can easily resume operation.

Note

This requirement exists only on an HA system. On a stand-alone server (non-HA), the PostgreSQL database is available on the same server where Fabric Performance Monitoring is installed and running. As long as that server remains up and running, the database is available.

Edit the PostgreSQL File to Include the HA Partners

In order to allow both partners to access PostgreSQL database, you will need to configure the database with either the specific IP addresses of the Fabric Manager servers, or the subnet address on which the Fabric Manager servers are configured. Specifying this information determines what nodes are authorized to access the database.

To do so, you will need to edit the PostgreSQL Client Authentication Configuration File (`pg_hba.conf.conf`) file to add the Fabric Manager server IP information.

- On Windows Fabric Manager servers, the file is located in `C:\Program Files\PostgreSQL\9.1\data`
- On Linux Fabric Manager servers, the file is located in `opt/postgres/9.1/data`

Using any common file editor, you will need to open the `pg_hba.conf.conf` file and edit it to include either the specific IP addresses of each of the Fabric Manager servers in the HA Fabric Manager system, or add the subnet and mask on which the servers are configured.

The following example `pg_hba.conf.conf` file is provided for reference. The blue text shows an example of the server IP address information that you will need to add.

```
#### start change xsigo
# TYPE  DATABASE        USER            ADDRESS                 METHOD
host    all             all             192.168.38.131          md5
host    all             all             192.168.38.132          md5
#### end change xsigo
```

Failover and Failback

With HA Fabric Managers, you have two servers with the same configuration, which provides a level of high availability. If one server is goes offline, the other server can continue operating as the Fabric Manager server controlling your deployment by using a manual failover. Manual failover is a corrective action that you can take when the active partner goes offline. When the original active partner goes down, you can manually promote the passive partner to become the active partner so that configuration and management experiences a minimum of interruption. In a manual failover, it might be required to manually restore a backup file to bring the latest configuration onto the new active partner.

Note

In the HA Fabric Manager system, failover does not occur automatically, so you must take action to move the configuration and resolve the condition that caused the HA partner to go offline.

A failback occurs when the offline server is brought back online and the configuration is moved back to the original server. Failback is not mandatory. You can keep the existing active partner, and bring the original active partner online as a passive node. For information about performing the failover and failback procedure, see Performing Failover and Failback.

Local Host and Remote Host

HA Fabric Manager consists of two servers (hosts) that are either the localhost or the remote host. At initial configuration, and upgrade, both servers are the local host. As local host, each server has a record added to the database. The name of the record is the fully-qualified name for the host. At this point, both servers are independent servers that are seen as “active” role servers.

When you connect the two servers into an HA system, you will add them by name. You must use the exact name for each localhost server as it was entered into the configuration database—for example, the DNS server name. If you enter a different name, then the HA system will not be correctly configured between the two servers. For example, if you have a server with a DNS name of larry.lab.companyA, you cannot use “larry” when you add that server into the HA system because the database record associated with that server is “larry.lab.company”

After the HA system is configured the localhost is not tied a specific server. Instead, the local host is the server where you currently have the management session. The other server is the remote host. For example, if you are currently on the active server, it is the localhost and the passive server is the remote host. But, if you are on the passive server then it is localhost and the active server is the remote host.

It is important to understand local host and remote host because some functions in the HA Fabric Manager system are started from the local host but actually run on the remote host. For example, displaying statistics occurs when a command is sent from the local host to the remote host. The statistics are gathered from the remote host and sent back to the local host where they are displayed. Even though the statistics are displayed on the local host, they are from the “other” server which is the remote host.

HA States

HA Fabric Manager has different states that depend on the presence of HA partners and their state. Displaying the operational state of HA Fabric Manager is supported through the HA toolbar object on the Fabric Manager toolbar. This object also is a dropdown menu which supports configuration of the current instance of HA Fabric Manager, as well as configuring HA Partners. Figure 2 shows the HA object on the Fabric Manager toolbar, which is also a dropdown menu that is the first step in configuring the HA Fabric Manager system.

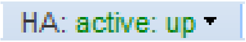


Figure 2 HA Object on the Fabric Manager Toolbar

The state is partially derived from a number of factors, including the presence or absence of the remote partner. When the state is determined, it is displayed as a concatenation to two information elements:

- the first information element indicates which partner
- the second information element indicates the actual administrative state of that partner.

So, for example, `active:up` as shown in Figure 2 indicates that the active partner is in “up” state. In the user interface, the states in the table are color coded to indicate any error. Red text indicates some kind of error, and green text indicates no error (correct functionality). The only correct states, which is shown in green text, are `active:up` and `passive:up`. Table 1 shows the HA states and explains what each means.

Table 1 States for HA Fabric Manager

HA State...	Means...
active: up	The active node is present and HA is correctly configured for HA Fabric Manager. In this state, the number of remote partners detected is equal to the number of remote partners connected to the active partner. This state is a correct runtime state for the active partner.
active:down	The active node is present but HA is not correctly configured. In this state, a partner might be detected, but that partner is not connected to the current active server. This is an error state.
active: not configured	The active node is present and HA is not configured because no remote partners are defined in the current instance of HA. This situation occurs typically when the passive node is not present. This is an error state.
active: remote node not configured	The active node is present, but the HA configuration is only half complete because the local host has a configuration for the remote host, but the remote host does not have a configuration for the local host. In this state, the active partner knows detects the remote partner and can ping it, but the remote partner does not respond to the pings. This situation can occur when the both partners are present, but the intended passive partner is not yet in “passive” mode. This is an error state.
active: more than 1 active partner	The active node is present and HA is not correctly configured because too many active partners exist. The HA Fabric Manager system supports a 1:1, active-passive configuration. If more than one active server exists in the HA system, a conflict occurs. This situation can occur during a failback, when the previous active partner has been brought back online, and the interim active partner has not yet been demoted to its original passive role. This is an error state.
passive: up	The passive node is present and HA Fabric Manager is configured, and the node is connected to its active partner. In this state, the passive server is synced up with is active node. This state is the correct runtime state for the passive partner. On the passive server, the Fabric Manager navigation frame is disabled. Any configuration or management must occur through the active server. After configuration or management tasks are complete, it is a recommended that you perform a backup so that the passive partner’s configuration is a close match to the active partner.
passive:down	The passive node is present but HA is not correctly configured. In this state, a partner might be detected, but that partner is not connected to the current passive server. This is an error state.
passive: not configured	The passive node is present and HA is not configured because no remote partners are detected. This situation occurs typically when the active node is not present. This is an error state.

Table 1 (continued) States for HA Fabric Manager

HA State...	Means...
passive: remote node not configured	The passive node is present and configured but HA is not configured correctly. In this state, the passive partner detects the remote partner and can ping it, but the remote partner does not respond to the pings. This situation can occur when the both partners are present, but the remote partner is not correctly configured. This is an error state.
passive: no active partner	The remote node is present and HA is not configured because no active partner is connected. In this state, no active partner exists, and as a result, the passive mode has nothing to sync up with. This situation can occur when an active node has been changed to passive and two passive servers exist—for example, if a failover has occurred without promoting the original passive to active. This is a serious error state because configuration and management tasks are supported on the active partner only. In this state, both HA partner are effectively read-only.
passive: more than 1 active partner	The passive node is present and HA is not correctly configured because too many active partners exist. The HA Fabric Manager system supports a 1:1, active-passive configuration. If more than one active server exists in the HA system, a conflict occurs. This situation can occur when too many servers in the HA system have been configured with the active role. This is an error state.

Configuring HA Fabric Manager Servers

HA Fabric Managers work as a pair of servers that retain configuration information and allow a standby servers (the passive server) to take over if the primary server (the active server) becomes unavailable as long as the servers have been synced up at least once.

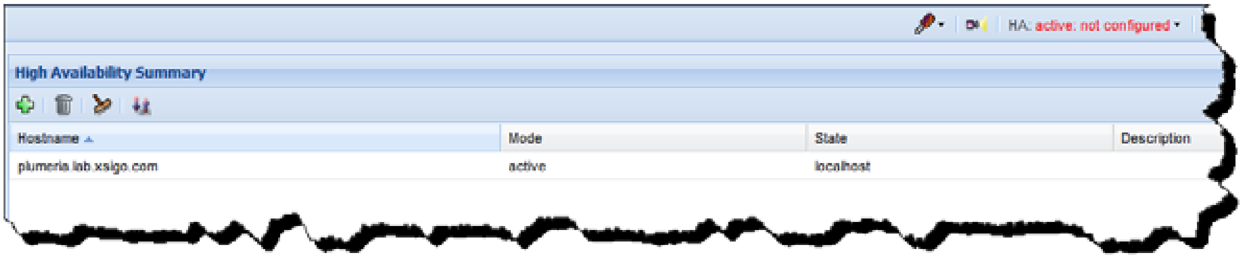
Each HA partner must be specified by a host name., and communication between the HA Partners occurs through a secure connection. When an HA pair is configured, both the Fabric Manager Server and its HA partner are online. One of the servers is active and the other is passive.

Configuring the Active Server

HA Partners can be in either active or passive states. The Active partner is the one on which commands are issued, and the server on which the sync up is initiated. When the active HA partner is configured, it can push data to the passive HA partner to complete a backup. Configuring the Active HA partner occurs through the HA dropdown menu on the Fabric Manager toolbar.

To configure the active HA partner, follow this procedure which requires two Fabric Manager servers and assumes the first server will be the active HA partner.

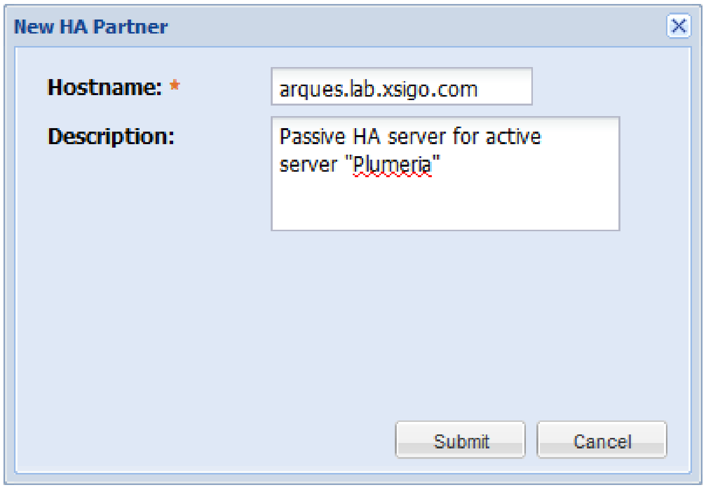
Step 1 Log in to the first Fabric Manager server. By default, this server is the active server and the HA feature is not yet configured as shown in Figure 3.



Hostname	Mode	State	Description
plumeria.lab.xsigo.com	active	localhost	

Figure 3 High Availability Summary

Step 2 On the first server’s toolbar, click the ***Add Servers*** button (the plus sign) to display the New HA Partner dialog. See Figure 4.



New HA Partner

Hostname: * arques.lab.xsigo.com

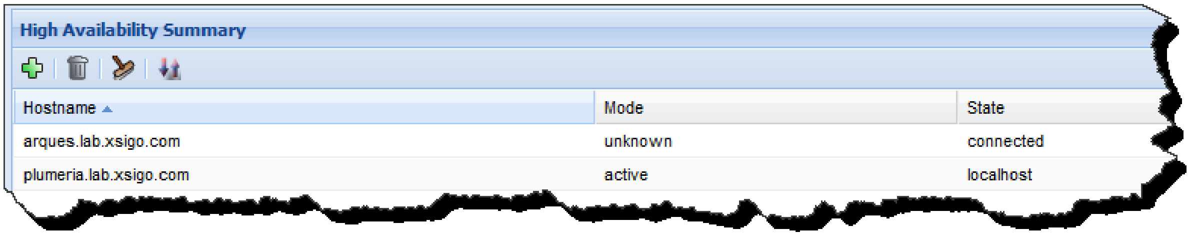
Description: Passive HA server for active server "Plumeria"

Figure 4 Add New HA Partner

Step 3 In the *HostName* field, enter the name of the server that you are configuring as the active HA partner.

Step 4 As an option, in the *Description* field, enter an alphanumeric string that describes the HA partner you are adding.

Step 5 Click ***Submit*** to add the partner the High Availability Summary as shown in Figure 5.



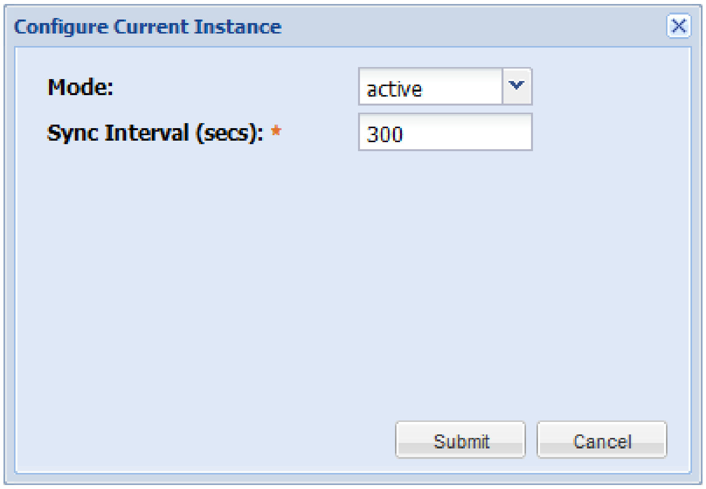
High Availability Summary

Hostname	Mode	State
arques.lab.xsigo.com	unknown	connected
plumeria.lab.xsigo.com	active	localhost

Figure 5 HIgh Availability Summary

The HA partner you added should be present. This partner will be unknown as shown in Figure 5.

Step 6 On the HA toolbar icon, select *HA->Configure Current Instance* to display the Configure HA Partner dialog as shown in Figure 6.



Mode: active

Sync Interval (secs): * 300

Figure 6 Configure Current Instance

Step 7 From the *Mode* dropdown menu. select active.

Step 8 Click ***Submit*** to add the server as the active HA Partner

Configuring the Passive Server

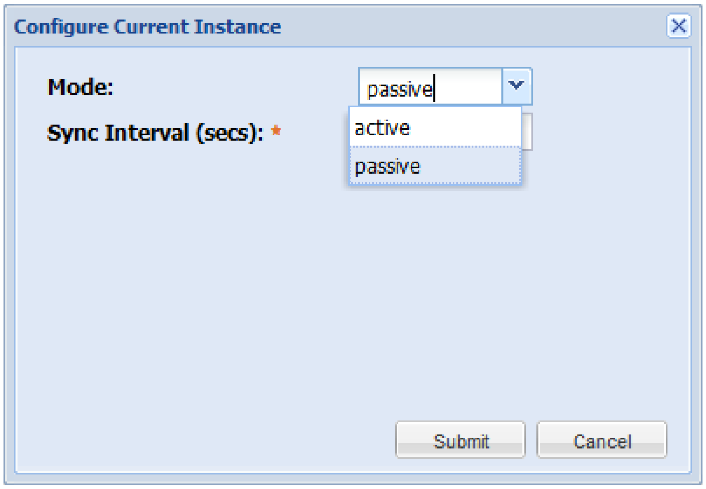
The passive HA partner is the second server in the HA Fabric Manager system. After it syncs up with the active partner, the passive HA partner has a copy of the Fabric Manager config, and the server provides high availability by being an online backup server. The passive server is easily recognizable by checking the navigation panel. If the configuration options are disabled (greyed out), then that node is the passive server.

After configuring the active HA partner, you must configure the passive HA server. To do so, follow this procedure:

Step 1 Log in to the second Fabric Manager server.

Step 2 Repeat Step 2 through Step 5 on page 391 to add the current server to the High Availability Summary.

Step 3 On the HA toolbar icon, select *HA->Configure Current Instance* to display the Configure HA Partner dialog as shown in Figure 7.



Configure Current Instance

Mode: passive

Sync Interval (secs): *

Figure 7 Configure Current Instance

Step 4 From the *Mode* dropdown menu. select passive.

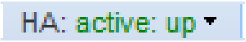
Step 5 Click ***Submit*** to add the server as the passive HA Partner.

Note

At this point, one active HA partner and one passive HA partner should be present. The two HA partners should automatically sync up after both are added to the High Availability Summary. You can also initiate a manual sync up. For information, see Forcing Sync Up.

Step 6 After the sync up occurs, log back in to both Fabric Manager servers in the system and check the HA icon on the toolbar to verify that the state of HA is configured:

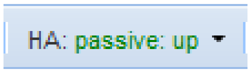
- On the active HA partner, the HA toolbar icon should show `active:up` as shown in figure Figure 8.



HA: active: up

Figure 8 HA Status — Active Partner

- On the passive HA partner, the HA toolbar icon should show `passive:up` as shown in figure Figure 9.



HA: passive: up

Figure 9 HA Status — Passive Partner

Setting an HA Partner’s Mode

The mode of an HA partner indicates how it participates in the HA Fabric Manager system:

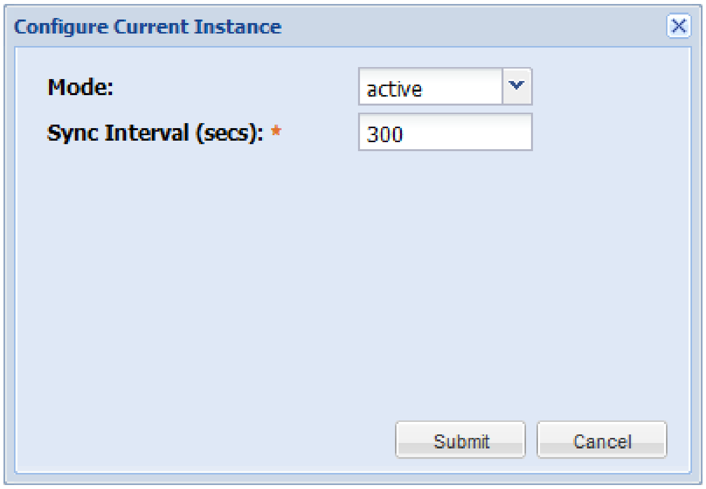
- If the mode is active, this Fabric Manager server is the online server that is used to manage your Fabric Directors and support virtual I/O connections to host servers. Only one active HA Partner is supported in each HA Fabric Manager system.
- If the mode is passive, this Fabric Manager servers is the standby that acts as a redundant server in your deployment. In passive mode, the Fabric Manager servers is not used for configuration and management of Fabric Directors and servers. In fact, the objects on the navigation frame are greyed out to indicate that you cannot use the passive server for network management functions.
- In this release, one passive HA partner is supported in each HA Fabric Manager system.

Changing an HA Partner’s mode is useful in situations where one of the Fabric Manager servers in the HA system becomes unavailable. For example, assume partner A is the active-mode server, and partner B is the passive-mode server and both servers are online and configured. If server A becomes unavailable, you can change partner B’s mode to “promote” it to the active server, then add another server (partner C) as the passive partner to regain high availability. Setting an HA partner’s mode also is useful for predictable tasks such as scheduled maintenance of a Fabric Manager server when you manually trigger a failover and failback. (For more information about failover and failback, see Failover and Failback).

- If you change the HA mode from active to passive, Fabric Manager disconnects from the Fabric Directors that it is managing, and you are prompted to log out to allow the state change to complete. During the state change, the partner is reported to other partners as passive. When you log back in, the Fabric Manager navigation frame is disabled to prevent configuration and management from the passive server.
- If you change the HA mode from passive to active, Fabric Manager verifies that no other active partners exist since there can be only one. Then, the most recent sync up is stored through Fabric Manager’s backup and restore feature. (For information, see “Backing up the Fabric Manager Config”). Fabric Manager connects to all the Fabric Directors that were managed by the original active partner, then prompts you to log out to allow the state change to complete. During the state change, the partner is reported to other partners as the new active node. When you log back in, the new active partner begins to take periodic backups and send them to the other nodes.

Setting an HA Partner’s mode occurs through the HA toolbar icon. To set an HA Partner’s mode, follow this procedure:

Step 1 From the server’s toolbar, select ***HA->Configure Current Instance*** to display the Configure Current Instance dialog. See Figure 10.



Mode: active

Sync Interval (secs): * 300

Figure 10 Configure Current Instance

Step 2 From the ***Mode*** dropdown menu, select the mode that you want to assign to the current server.

Note: Remember that within an HA Fabric Manager system, only one active server is supported.

Step 3 In the *Sync Interval (secs)* field, specify the sync up interval (if needed).

Step 4 When the mode is set, click ***Submit*** to complete setting the server mode.

Setting a Sync Interval

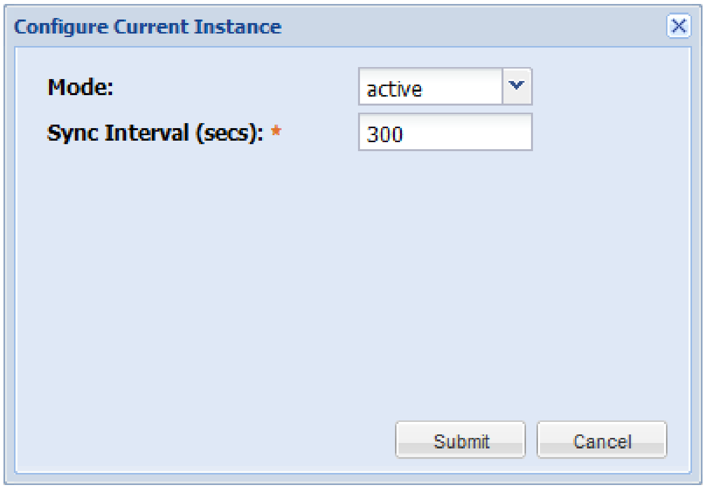
The sync intervals determines the periodicity of sending sync messages from the active node to the passive node. By default, the sync interval between the active and passive HA partners is set to 300 seconds (5 minutes). However, you can set any sync interval that is required in your network. The sync interval can be set to a non-default value at initial configuration time, or at any time after the HA partners have been configured.

Setting a custom sync interval can be beneficial to your deployment based on network conditions. For example:

- Setting a custom sync interval can be useful in highly volatile environments where frequent backups are required. For example, in such an environment you can set the sync interval to a lower number so that backups occur more frequently. Be aware that a smaller sync interval requires more overhead due to sync up occurring more frequently.
- Setting a custom sync interval can be useful also in stable networks or low latency environments where frequent backups are not required. For example, in such an environment you can set the sync interval to a higher number so that backups occur less frequently. Be aware that a larger sync interval creates a larger window between syncs, and as a result, more data can be lost if the active partner goes down.

Setting a sync interval is supported through the *HA->Configure Current Instance* dialog. To set a custom sync interval, follow this procedure:

Step 1 From the server's toolbar, select *HA->Configure Current Instance* to display the Configure Current Instance dialog. See Figure 11.



Mode: active

Sync Interval (secs): * 300

Figure 11 Configure Current Instance

Step 2 In the ***Sync Interval (secs)*** field, you can enter the number of seconds that you want to pass between configuration synchronizations. In most cases, the default value will be sufficient. However, this value is customizable. To set a non-default value, enter a number of seconds that indicate the amount of time that passes before HA partners sync up. You must enter at least 10 seconds.

Note

When configuring the *Sync Interval*, make sure that you set a realistic value. It is possible to set an interval large enough that configurations are not synced up in a timely manner, and the result is that configurations might not be the same on both partners. In most cases, the default value will be acceptable.

Step 3 When you have set the new sync interval, click ***Submit*** to complete the change.

Step 4 Login in to the other HA partner and repeat this procedure making sure to set the same sync interval.

Forcing Sync Up

By default, all partners sync up automatically based on the sync interval specified when you configured each instance. When the sync interval is complete, the active partner pushes a backup file to the passive node(s). For example, with a sync interval of 60 seconds, the backup file is pushed from the active node to all passive nodes every minute.

However, there might be instances when you want to manually sync up databases. For example, if a passive node was taken offline for maintenance, you might want to sync it up immediately after it comes back online to get redundant Fabric

Manager servers as soon as possible. In such cases, you can manually synchronize the HA partners through the Force Sync Up button on the HA Summary.

You can force a manual sync up at any time as long as multiple Fabric Manager servers are online and the HA status is `active:up`. To manually sync up, follow this procedure:

Step 1 Log in to one of the HA partners.

Step 2 On the Fabric Manager toolbar, select *HA->Configure HA Partners*. See Figure 12.

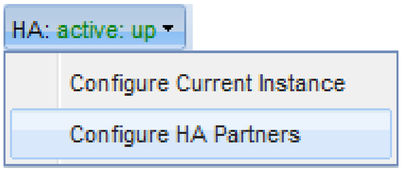
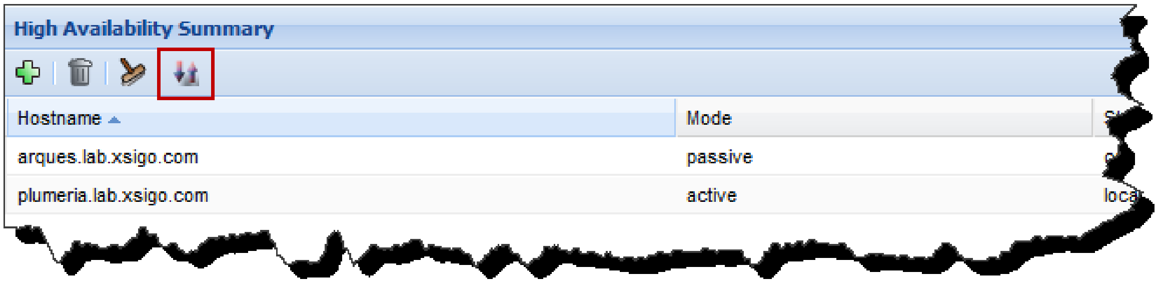


Figure 12 Configure HA Partners

When select Configure HA Partners, the High Availability Summary is displayed.

Step 3 On the High Availability Summary, click the ***Force Sync Up*** button as shown in Figure 13.



High Availability Summary

Hostname ▲	Mode	S
arques.lab.xsigo.com	passive	o
plumeria.lab.xsigo.com	active	loca

Figure 13 HIgh Availability Summary — Force Sync Up

When you click the ***Force Sync*** button, a short amount of time passes while information is exchanged between the Fabric Manager servers. When complete, a popup dialog indicates that the partners synced up and no errors occurred.

Performing Failover and Failback

This section describes the procedure to manually failover from an active node that has gone offline to its partner, then failback to the original active node when you have brought it back online.

Failover

During a a failover, the active node goes offline, and the other partners will see no active partner. Configuration sync up cannot occur between the offline server and the partners. However, after an active partner is detected, the most recent sync up will be restored. Failover is a manual process.

To perform a failover, follow this procedure:

Step 1 When you notice the active partner is down, start a browser and login to the passive partner.

Step 2 On the toolbar, select *HA-> Configure Current Instance* as shown in Figure 14.

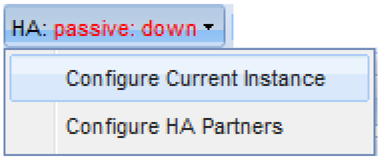


Figure 14 HA Toolbar — Configure Current Instance

Step 3 From the Mode dropdown, select active to promote this node the active node. At this point, you can use this node to configure and managed Fabric Directors through Fabric Manger if needed.

Step 4 Click ***Submit***.

Note

Remember that at this point only one server is operating, so you will want to resolve the issue on the offline Fabric Manager server as soon as possible to regain redundancy. If another Fabric Manager server is available, you can add it as an interim passive node. For information, see Configuring the Passive Server.

Failback

After the original server is brought back online, the server reads its database to determine its role. Because the server was the active partner when it went offline, it comes back online as the active partner.

Note

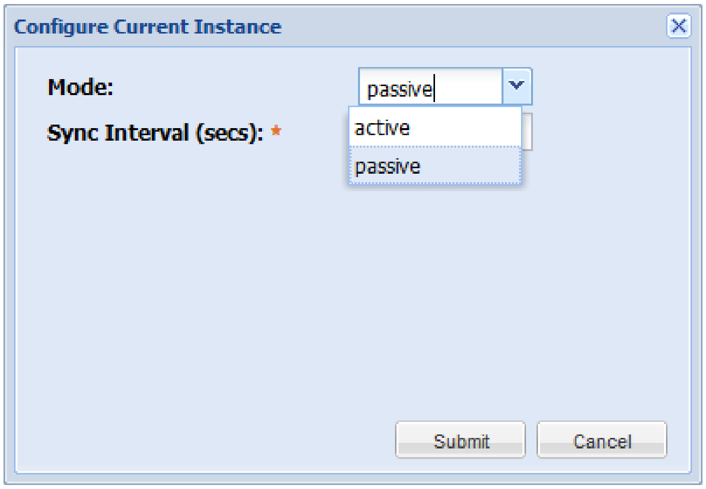
If you have an interim Fabric Manager server acting as the passive node and you do not want that server in the HA system when the original active server comes back online, delete the server now as documented in Deleting an HA Partner.

To perform a failback to use the original active partner again, follow this procedure:

Step 1 Make sure that both HA instances are running. At this point, both partners are active so you'll see an error.

Step 2 As an option, take a backup on both nodes. Although this is optional, it is recommended. For information, see "Backing up the Fabric Manager Configuration."

Step 3 On the node that just came back online, set the mode to "passive" as shown in Figure 15.


Configure Current Instance

Mode: passive

Sync Interval (secs): *

Figure 15 Configure Current Instance — Set Partner to Passive Mode

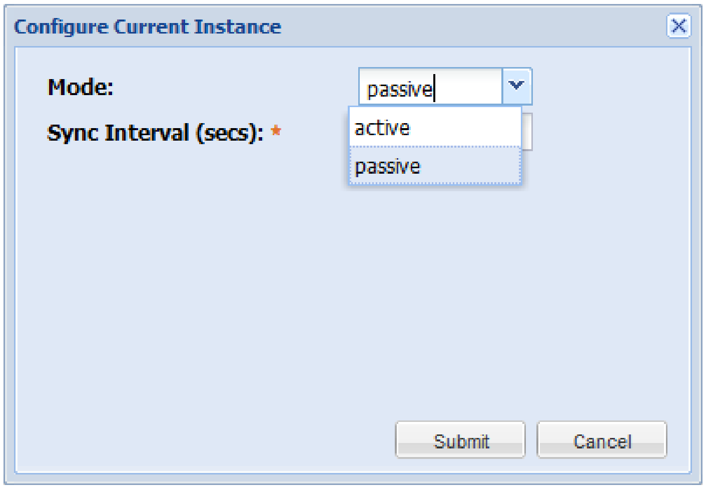
At this point, the HA status (on the toolbar) should be correct since the HA Fabric Manager system has one active node and one passive node.

Note

Make sure that the sync interval is the same between the servers.

Step 4 From the active node, initiate a sync up. For information, see Forcing Sync Up.

Step 5 On the *active* node, set the mode to passive as shown in Figure 16.



Configure Current Instance

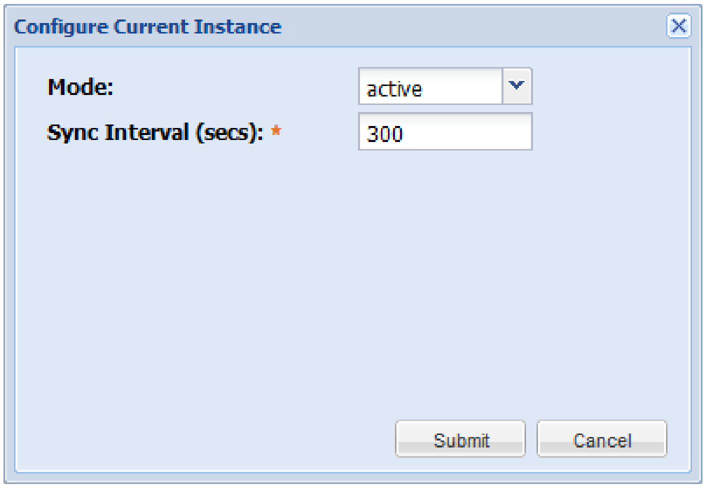
Mode: passive

Sync Interval (secs): *

Figure 16 Configure Current Instance — Set Active Partner to Passive Mode

At this point, the HA status (on the toolbar) should show an error because both nodes are passive.

Step 6 On the original active node, set the mode to active as shown in Figure 17.



Configure Current Instance

Mode: active

Sync Interval (secs): * 300

Figure 17 Configure Current Instance — Set Preferred Partner to Active Mode

At this point, the HA status (on the toolbar) should show `active:up` state because the HA Fabric Manager system has one active node and one passive node.

Installing Plug-ins on the Passive Server

Both servers in the HA Fabric Manager system must have the exact same plug-ins installed. It is a best practice to make sure that both Fabric Manager servers are identically configured before creating the HA pair. However, in some deployments, this is not always possible. The procedure in this section documents how to install the plug-ins on a passive HA Fabric Manager server that is already configured in an HA Fabric Manager pair.

To install the plug-ins, you will need to have them available to you. Before attempting this procedure, make sure that you have the correct plug-ins and versions ready for installation on the passive server.

The procedure for installing the plug-ins on the passive server require you to stop the HA connection, promote the passive server to active, install the necessary plug-ins, then revert the server back to passive mode. Follow this procedure:

Step 1 On both Fabric Manager servers, take a Fabric Manager backup as documented in Backing Up The Fabric Manager Configuration.

Step 2 On the passive server, set the mode to active as documented in Setting an HA Partner’s Mode. As a result of changing the mode to active, you will need to log back in.

Step 3 On the server, which is now in active mode, check the navigation panel. The icons should no longer be greyed out. If the icons are still greyed out, the server is not in active mode.

Step 4 Install the necessary plug-in(s). Make sure that the versions you install match the same versions in use on the other server. For information about installing the plug-ins, see the “Installation” chapter of the user guide that accompanied your plug-in(s).

At this point, the plug-in has been installed on the server, but it has not yet been added to Fabric Manager.

Step 5 On the new active server, click ***Apps->App Manager*** to display the Installed Applications Summary.

Step 6 On the Installed Applications Summary, click the plus sign (+) to add the plug-in to Fabric Manager.

Step 7 When all the necessary plug-ins are installed, set the server’s mode back to passive as documented in Setting an HA Partner’s Mode. You will need to log in to fully reset the state to passive.

Step 8 Log back in to the passive server and check the navigation panel. The icons should be greyed out since this is no longer an active server.

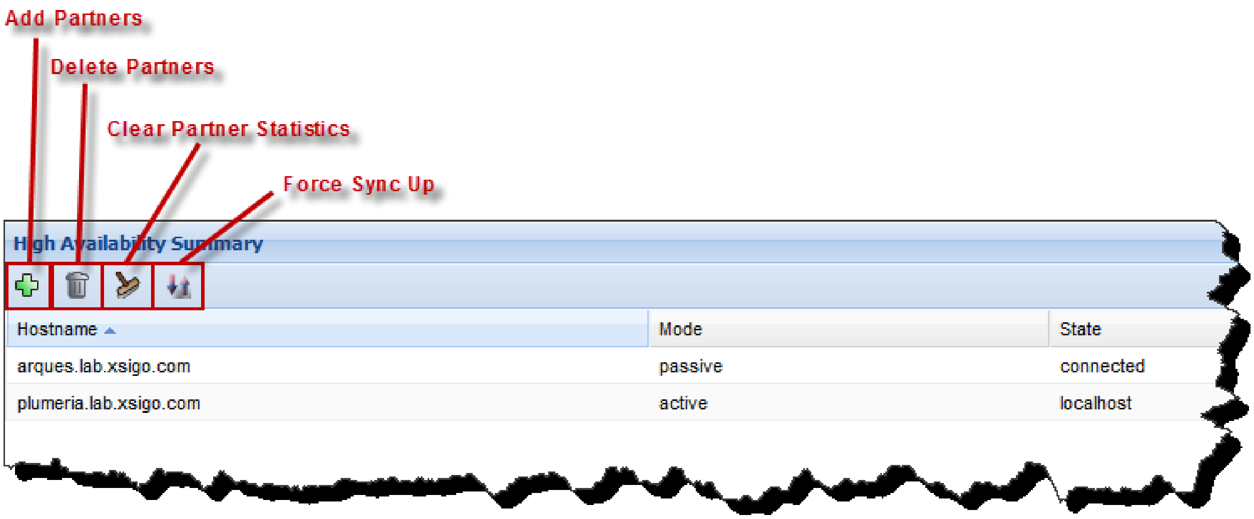
Step 9 Force a sync up as documented in Forcing Sync Up to get the two servers synchronized.

Step 10 Take a backup of the new configuration as documented in Backing Up The Fabric Manager Configuration

Displaying HA Fabric Manager Information

The HA configuration for Fabric Manager is displayed through the High Availability Summary, which contains a list of all the configured HA Partners for the current Fabric Manager Server. Be aware that the HA Summary shows all configured HA Partners for the current Fabric Manager Server, but does not show any specific logical group or connection mapping.

Figure 18 shows the High Availability Summary.



Hostname	Mode	State
arques.lab.xsigo.com	passive	connected
plumeria.lab.xsigo.com	active	localhost

Figure 18 High Availability Summary

Notice that through the High Availability Summary you can add or delete new HA Partners by using the plus sign or garbage can icon, respectively. You can also clear operational and performance statistics for management traffic between the HA partners, as well as initiate a sync up between the HA partners.

Table 2 shows the contents of the High Availability Summary, and explains what each field means.

Table 2 Contents of the High Availability Summary

Field	Means...
Host Name	The host name of the server that is the HA Partner
Mode	The mode (either active or passive) for each HA Partner
State	The operational state of the HA Partner. Valid states are: • Connected, when the HA Partners recognize each other and are correctly connected and configured. • Retrying (the connection is not up yet, but is trying) • Unknown, when the configuration is partial or not yet complete • Not Configured, when an HA Partner does not have a mode (either active or passive) assigned to it. • Not Connected • Down, when one of the HA Partners is not connected to the other, or that HA Partner is not operational.
Description	An optional alphanumeric character string that describes the HA Partner or the team of Fabric Manager Server and HA Partner.

Displaying HA Partner Detailed Information

In addition to the summary information available for each HA partner through High Availability Summary, you can also display additional information through the details frame of each server in the HA Fabric Manager system.

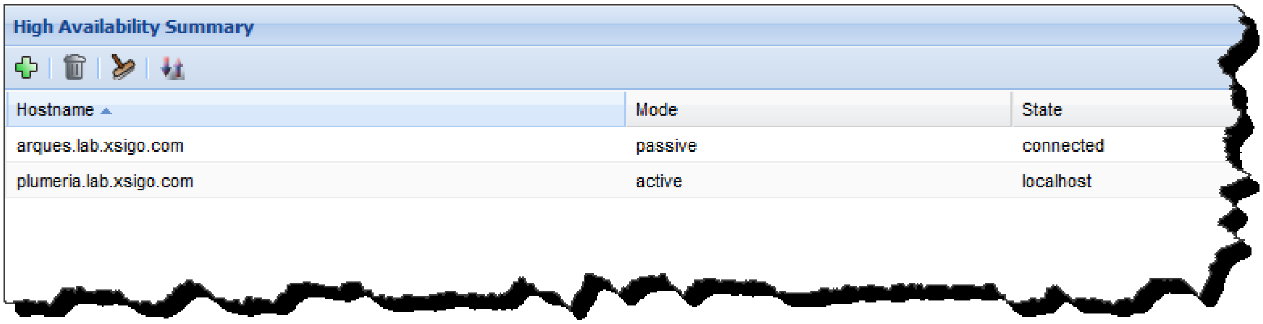
Each server contains information about the general properties configured for the HA Fabric Manager system. This information is available through the *General* tab. This tab is available on both the local host and the other HA partner (remote host). For information, see Displaying General Properties for an HA Partner.

However, the following additional information is available, but is conditional based on a combination of which HA partner you are currently administering (the local host), and which partner you select on the High Availability Summary:

- Unsynced Commands, which are available through Unsynced Commands tab. This tab is available on the local host (when your browser is on a server and you select that server in the High Availability Summary). For information, see Displaying Unsynced Commands for HA Fabric Manager.
- Statistics, which are available through the Statistics tab. This tab is available on the local host when you select the other HA partner. For information, see Displaying Statistics for HA Fabric Manager.

To display details for the HA Fabric Manager configuration, follow this procedure:

Step 1 From the Fabric Manager toolbar, select the *HA* object to display the High Availability Summary. Figure 19 shows this dialog.



High Availability Summary

Hostname	Mode	State
arques.lab.xsigo.com	passive	connected
plumeria.lab.xsigo.com	active	localhost

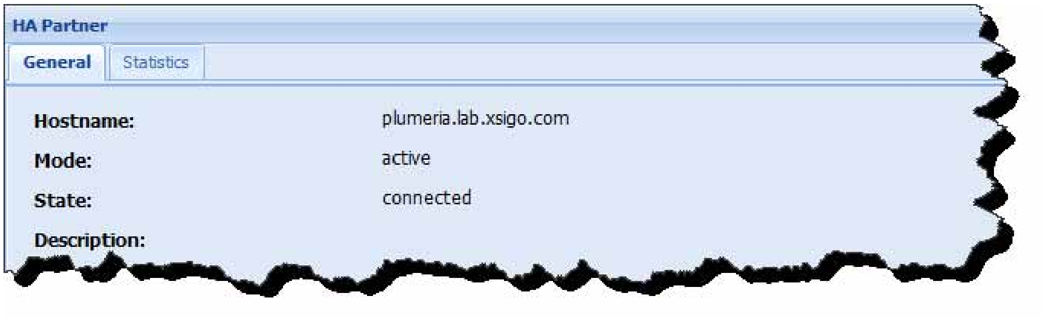
Figure 19 High Availability Summary

Step 2 Select the HA Partner for which you want to display detailed information. When the HA Partner is selected, the High Availability details frame is populated with the following types of data:

- General Properties. For more information, see Displaying General Properties for an HA Partner.
- Statistics. For information see, Displaying Statistics for HA Fabric Manager.
- Unsynced Commands. For more information, see Displaying Unsynced Commands for HA Fabric Manager.

Displaying General Properties for an HA Partner

General properties for the current HA partner are displayed through the General tab. After selecting the HA partner in the High Availability Summary, click the *General* tab to display the general properties as shown in Figure 20.



Hostname: plumeria.lab.xsigo.com
Mode: active
State: connected
Description:

Figure 20 HA Partner Details Frame

Table 3 shows the contents in the HA Partner Details frame and explains what each field means.

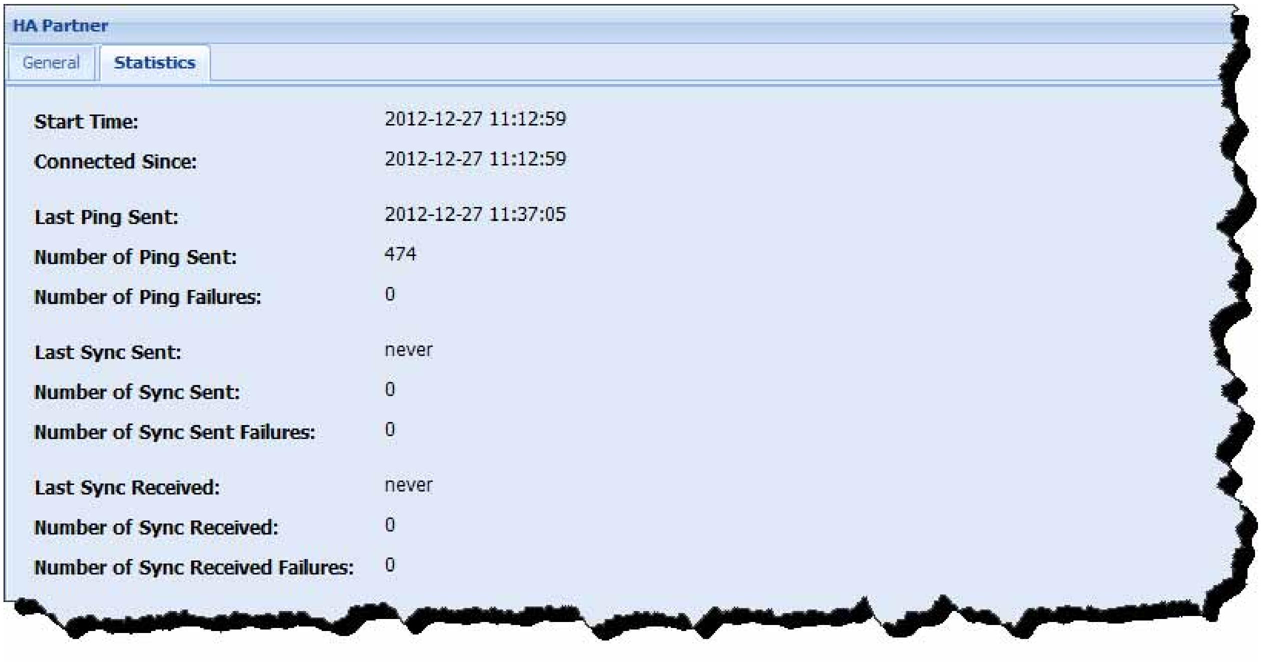
Table 3 Contents of the HA Partner Details Frame

Field	Means
Host Name	The host name of the Fabric Manager server
Mode	The mode in which the host is currently operating. Valid values are: • active, for the Fabric Manager server that is maintaining real-time information and pushing that information to the Standby HA • passive, for the Fabric Manager server that is the passive standby partner in the HA configuration. • unknown, for a Fabric Manager server with a mode that is not recognizable as either active or passive
State	The current state of the Fabric Manager server in the HA environment. Valid values are: • connected • not connected • localhost
Description	An optional alphanumeric character string that describes the HA Partner(s), or combination of Fabric Manager Server and HA Partner(s).

Displaying Statistics for HA Fabric Manager

Fabric Manager shows operational and performance statistics for management traffic sent between HA partners. Statistics and counters for information such as sync up functions, pings, errors, and partner changes are tracked through the non local host partner's *Statistics* tab.

After selecting the HA partner in the High Availability Summary, click the *Statistics* tab to display the HA Fabric Manager statistics as shown in Figure 21.



Start Time: 2012-12-27 11:12:59
Connected Since: 2012-12-27 11:12:59

Last Ping Sent: 2012-12-27 11:37:05
Number of Ping Sent: 474
Number of Ping Failures: 0

Last Sync Sent: never
Number of Sync Sent: 0
Number of Sync Sent Failures: 0

Last Sync Received: never
Number of Sync Received: 0
Number of Sync Received Failures: 0

Figure 21 HA Partner Details Frame — Statistics

Table 4 show the contents of the Statistics tab for HA Fabric Manager environments and explains what each field means.

Table 4 Contents of the HA Partner Statistics Tab

Field	Means...
Start Time	The time and date stamp that indicates when the local host successfully connected to the remote host for the first time.
Connected Since	The time and date stamp since the HA pings have consecutively been successful
Last Ping Sent	The time and date stamp of the last ping sent from the local host.
Number of Pings Sent	The total number of pings sent from the local host to the remote host. This counter is tracked continuously while HA Fabric Manager is running, but it resets after such actions as restoring a backup, restarting Fabric Manager, or forcing a sync up.

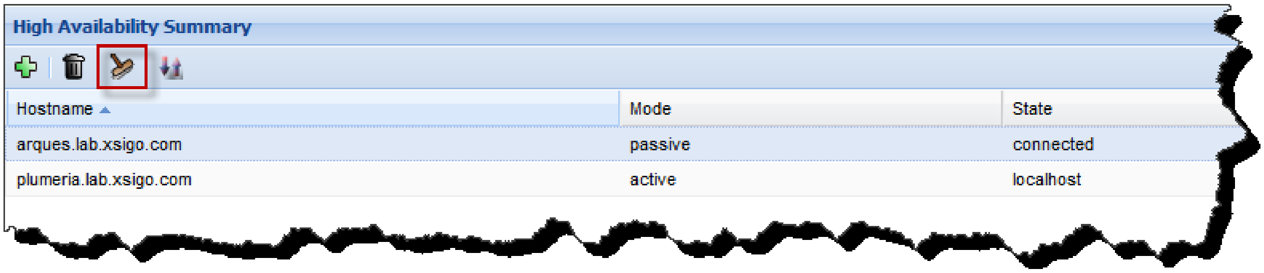
Table 4 (continued) Contents of the HA Partner Statistics Tab

Field	Means...
Number of Ping Failures	The total number of pings failures during failover/failback, and when the statistics are cleared by using the ***Clear Partner Statistics*** button on the High Availability Summary page.
Last Sync Sent	The time and date stamp of the last sync sent from the local host to the remote host during automatic sync up and forced sync up.
Number of Syncs Sent	The total number of synchronizations sent from the local host to the remote host during automatic sync up and forced sync up.
Number of Sync Sent Failures	The total number of failed synchronizations sent from the local host to the remote host during automatic sync up and forced sync up. Sync failures can occur for various reasons, but one common reason is that remote host is not present or connected to the local host.
Last Sync Received	The time and date stamp of the last synchronization successfully received by the local host.
Number of Syncs Received	The total number of synchronizations received by the local host.
Number of Sync Received Failures	The total number of Synchronization received failures on the local host.

Clearing Partner Statistics

When statistics exist, you can clear them at any time. Clearing statistics can be helpful when you have brought an HA Fabric Manager server back online (for example, as part of a failover and failback) to see how the HA partners are communicating.

Clearing partner statistics is supported through the High Availability Summary, as shown in Figure 22.



High Availability Summary

Hostname	Mode	State
arques.lab.xsigo.com	passive	connected
plumeria.lab.xsigo.com	active	localhost

Figure 22 High Availability Summary — Clear Partner Statistics

To clear the partner statistics, follow this procedure:

Step 1 Display the High Availability Summary.

Step 2 On the High Availability Summary, select the HA partner (not the local host). This step activates the ***Clear Partner Stats*** button (the broom icon). See Figure 22.

Step 3 Click the ***Clear Partner Statistics*** button.

Step 4 When you do, a popup dialog prompts you for confirmation. Click ***Yes*** to complete clearing the statistics.

Displaying Unsynced Commands for HA Fabric Manager

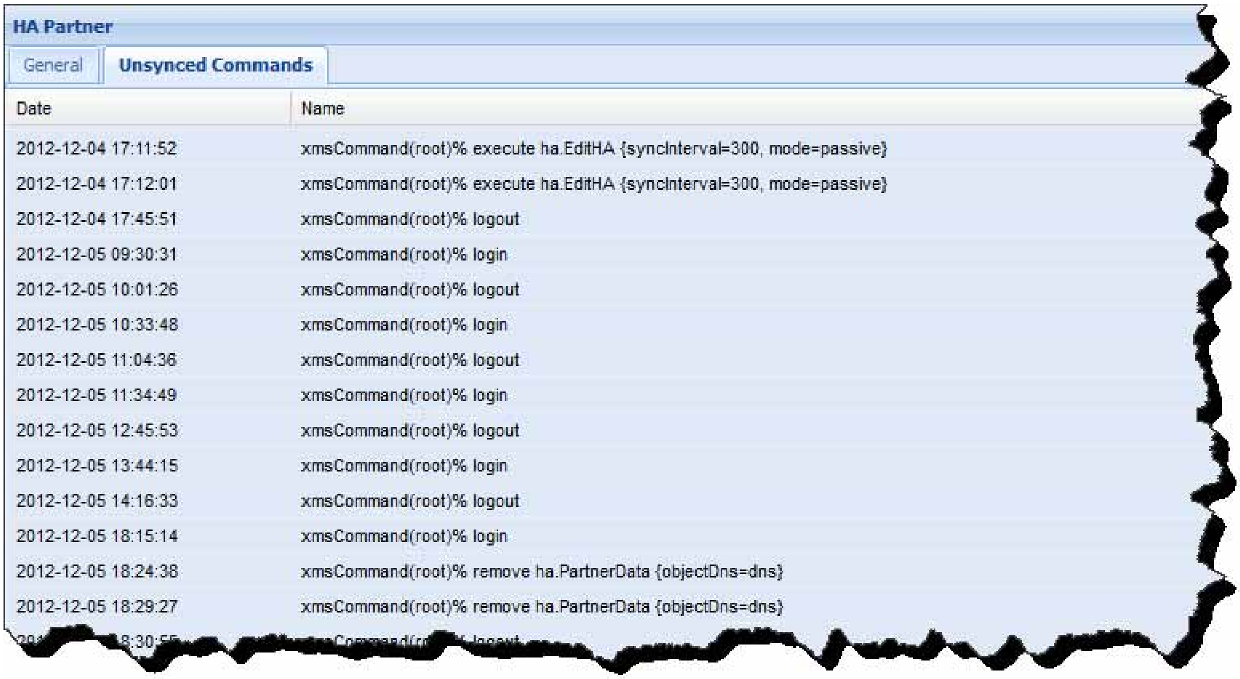
Commands and management traffic between the HA partners are displayed through the *Unsynced Commands* tab. By seeing unsynced commands, in the unlikely event that the active partner goes offline, the passive node will have some record of changes that occurred on the active node since the last sync up.

Due to the periodic sync up between the active and passive partners, the possibility exists that some data can be lost if the active partner goes offline right before the scheduled sync interval has completed. By using the Unsynced Commands tab, you have a way to see the unsynced content, and manually recreate it after the passive partner is promoted to the new active partner.

After selecting an HA partner on the High Availability Summary, click the *Unsynced Commands* tab to display the unsynced commands table as shown in Figure 23.

Note

This option is available on the local host when you select the local host in the High Availability Summary.



Date	Name
2012-12-04 17:11:52	xmsCommand(root)% execute ha.EditHA {syncInterval=300, mode=passive}
2012-12-04 17:12:01	xmsCommand(root)% execute ha.EditHA {syncInterval=300, mode=passive}
2012-12-04 17:45:51	xmsCommand(root)% logout
2012-12-05 09:30:31	xmsCommand(root)% login
2012-12-05 10:01:26	xmsCommand(root)% logout
2012-12-05 10:33:48	xmsCommand(root)% login
2012-12-05 11:04:36	xmsCommand(root)% logout
2012-12-05 11:34:49	xmsCommand(root)% login
2012-12-05 12:45:53	xmsCommand(root)% logout
2012-12-05 13:44:15	xmsCommand(root)% login
2012-12-05 14:16:33	xmsCommand(root)% logout
2012-12-05 18:15:14	xmsCommand(root)% login
2012-12-05 18:24:38	xmsCommand(root)% remove ha.PartnerData {objectDns=dns}
2012-12-05 18:29:27	xmsCommand(root)% remove ha.PartnerData {objectDns=dns}

Figure 23 HA Partner Details Frame — Unsynced Commands

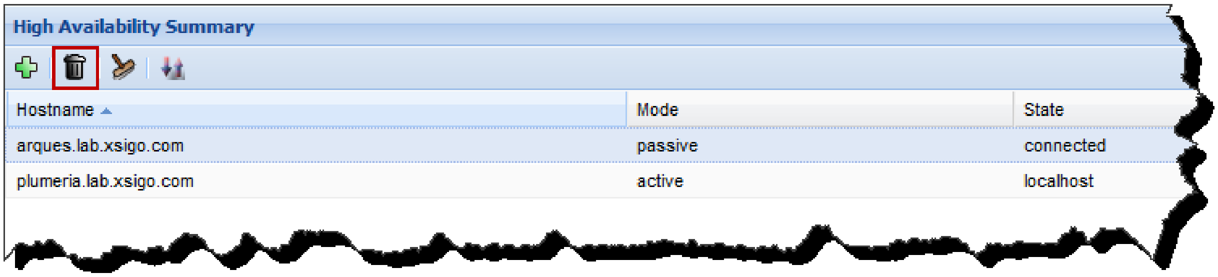
Deleting an HA Partner

If you no longer want high availability for your Fabric Manager Servers, you can remove this functionality by deleting all the HA Partner(s). When the HA partner is deleted, it reverts to a single server running Fabric Manager:

- configuration changes made to the previous Fabric Manager Server are no longer synchronized
- the deleted HA Partner, which is now a stand-alone Fabric Manager Server, has a baseline configuration which is the last config sent from the previous Fabric Manager Server when the HA Partner was still the HA Fabric Manager system.
- the deleted HA Partner, which is now a stand-alone Fabric Manager Server, can be used to manage I/O, just like any other Fabric Manager Server. No reboot is required on either of the servers (the previous Fabric Manager Server or the previous HA Partner).

The HA Partner can be deleted at anytime through the High Availability Summary. To delete an HA Partner and return it to the role of a stand-alone Fabric Manager Server, follow this procedure:

Step 1 From the Fabric Manager toolbar, select *HA->Configure HA Partners* to display the High Availability Summary. Figure 24 shows this dialog.



High Availability Summary

Hostname ▲	Mode	State
arques.lab.xsigo.com	passive	connected
plumeria.lab.xsigo.com	active	localhost

Figure 24 High Availability Summary

Step 2 Select the HA Partner that you want to delete from the HA Fabric Manager system.

Step 3 Click the garbage can icon to delete the HA Partner from the High Availability Summary. When you click the garbage can icon, a confirmation dialog is displayed to verify that you want to delete the HA Partner from the HA Fabric Manager system.

Step 4 On the confirmation dialog, click ***Yes*** to complete deleting the HA Partner from the HA Fabric Manager system, or ***No*** to abort the deletion and leave the selected HA Partner in the HA Fabric Manager setup.

Working with Live Monitoring

This chapter documents the following topics:

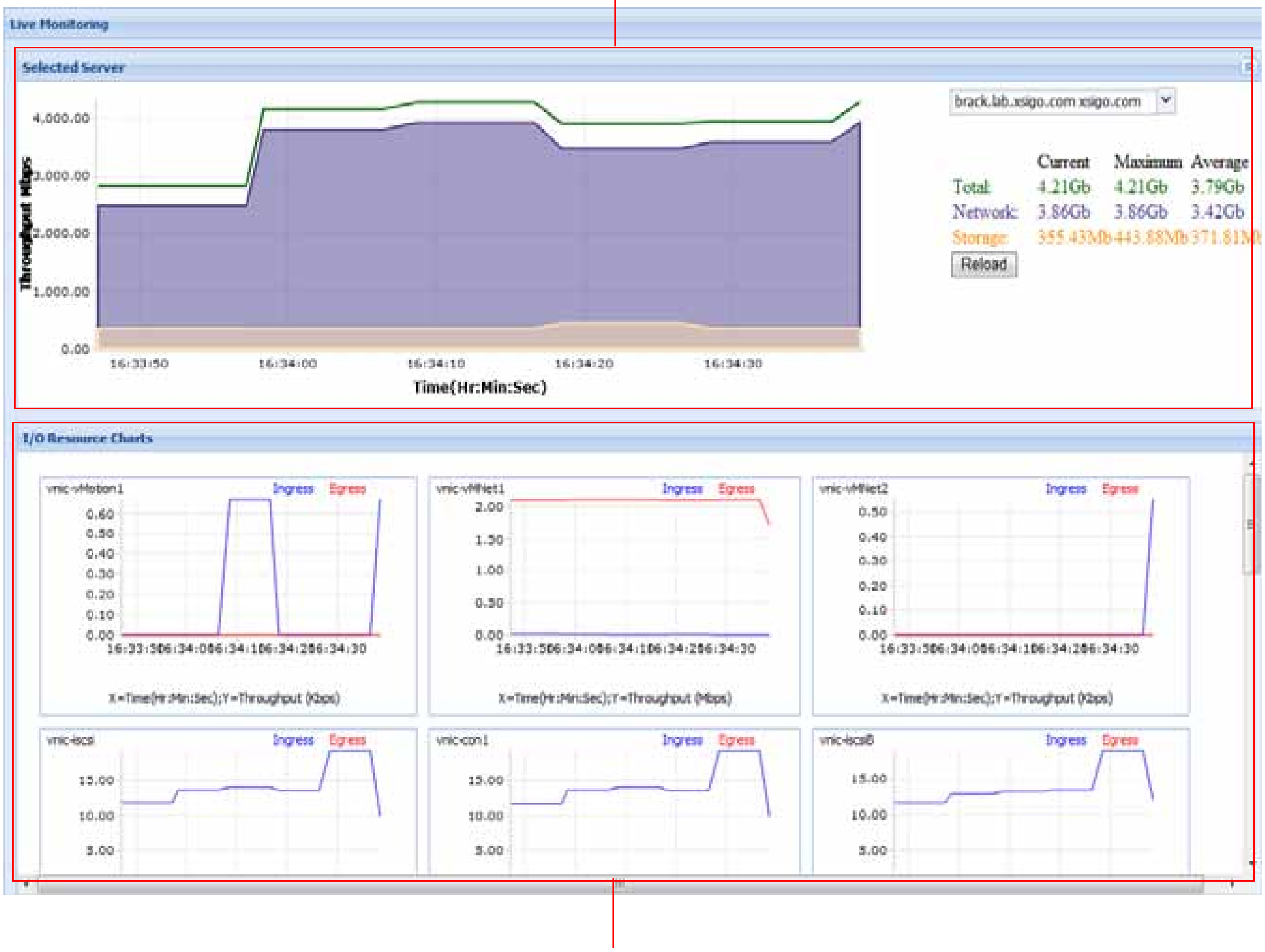
Understanding Live Monitoring

Live Monitoring is a statistics grapher built into Oracle's Xsigo Fabric Manager GUI that supports monitoring of live, real-time statistics and usage. Live Monitoring is divided into two main sections:

- The Selected Server frame, which contains information about a single server that you select.
- The Virtual Resources frame, which is subdivided into individual charts for each vNIC or vHBA deployed on the physical server.

Figure 1 shows the Live Monitoring Summary.

Selected Server Frame



	Current	Maximum	Average
Total:	4.21Gb	4.21Gb	3.79Gb
Network:	3.86Gb	3.86Gb	3.42Gb
Storage:	355.43Mb	443.88Mb	371.81M

I/O Resource Charts for vNICs and vHBAs

Figure 1 Live Monitoring Summary

Live Monitoring monitors throughput and usage statistics for physical servers, vNICs, and vHBAs for specific intervals, and displays the statistics in real time.

For physical servers, the following information is displayed:

- Average throughput, which is displayed by interval in the real-time grapher
- Current usage, which is the real-time usage of the entire physical server
- Average, the average throughput for the physical server since the grapher was invoked through Fabric Manager.
- Maximum, the maximum throughput for the physical server since the grapher was invoked through Fabric Manager.

For vNICs and vHBAs, the following information is displayed:

- Ingress bandwidth usage is graphed for any vNIC or vHBA that is deployed on the selected host server. The ingress throughput is tracked in intervals just like the per-server throughput.
- Egress throughput is graphed for any vNIC or vHBA that is deployed on the selected host server. The egress throughput is tracked in intervals just like the per-server throughput.

Displaying Host Server Throughput

Through the Selected Server frame you can see the throughput of an entire selected server. This frame will be blank until you select a server.

The selected server frame contains a real-time grapher for the server’s throughput and historical and calculated statistics.

Note

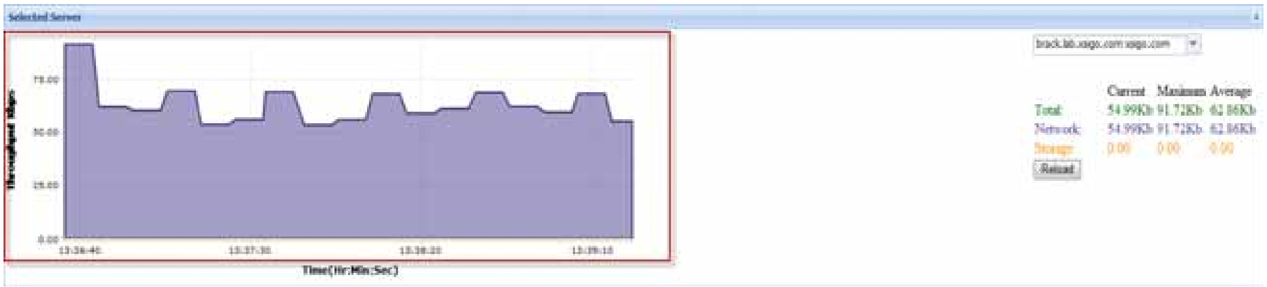
For each server, a ***Reload*** button allows you to flush the current grapher session and start tracking the statistics in a new set of intervals. The ***Reload*** button resets the grapher for the server and any vNICs and vHBAs deployed on it. Even though the ***Reload*** button is in the Server Throughput frame, be aware that it also reloads statistics for virtual I/O on the server.

Real-Time Grapher

The grapher tracks the throughput over an interval and displays the throughput as standard line graph, which consists of an X axis and a Y axis.

- The X axis shows an interval-based time line. By default, each interval is 50 seconds, but this value can be decreased to smaller amounts of time.
- The Y axis shows the throughput in Kbps.

Figure 2 shows the real-time grapher.



	Current	Maximum	Average
Total:	54.99Kb	91.72Kb	62.86Kb
Network:	54.99Kb	91.72Kb	62.86Kb
Storage:	0.00	0.00	0.00

Figure 2 Selected Server Frame of Live Monitoring

The real-time grapher can display the statistics for a non-default interval time by clicking and dragging on the section of the graph that you want to “zoom in.” Figure 3 shows an example of zooming in on a specific statistic you want to display.

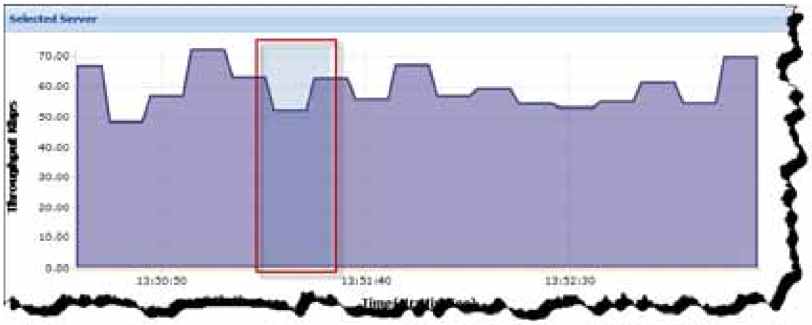


Figure 3 Live Monitoring—Zooming In

In this example, the darker blue box shows the statistics that will be displayed in a smaller interval (less than 50 seconds). This area of statistics was selected by clicking and dragging over the statistics in a top-down, left-to-right motion. Notice that the intervals at this point are 50 seconds, for example from 14:33:20 to 14:34:10.

When the click and drag completes, the selected statistics area is zoomed in, so that a smaller interval is displayed and a more granular focus is given to the statistics, as shown in Figure 4.

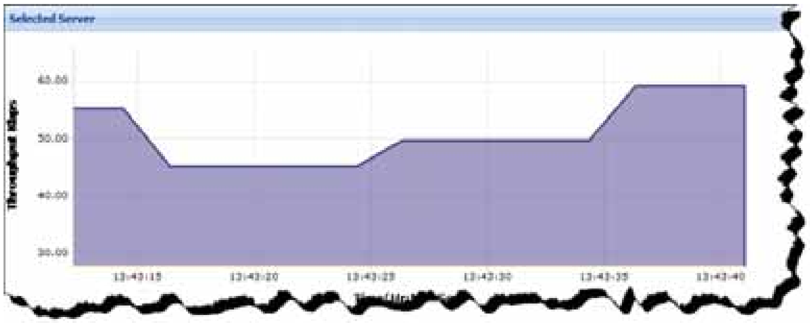
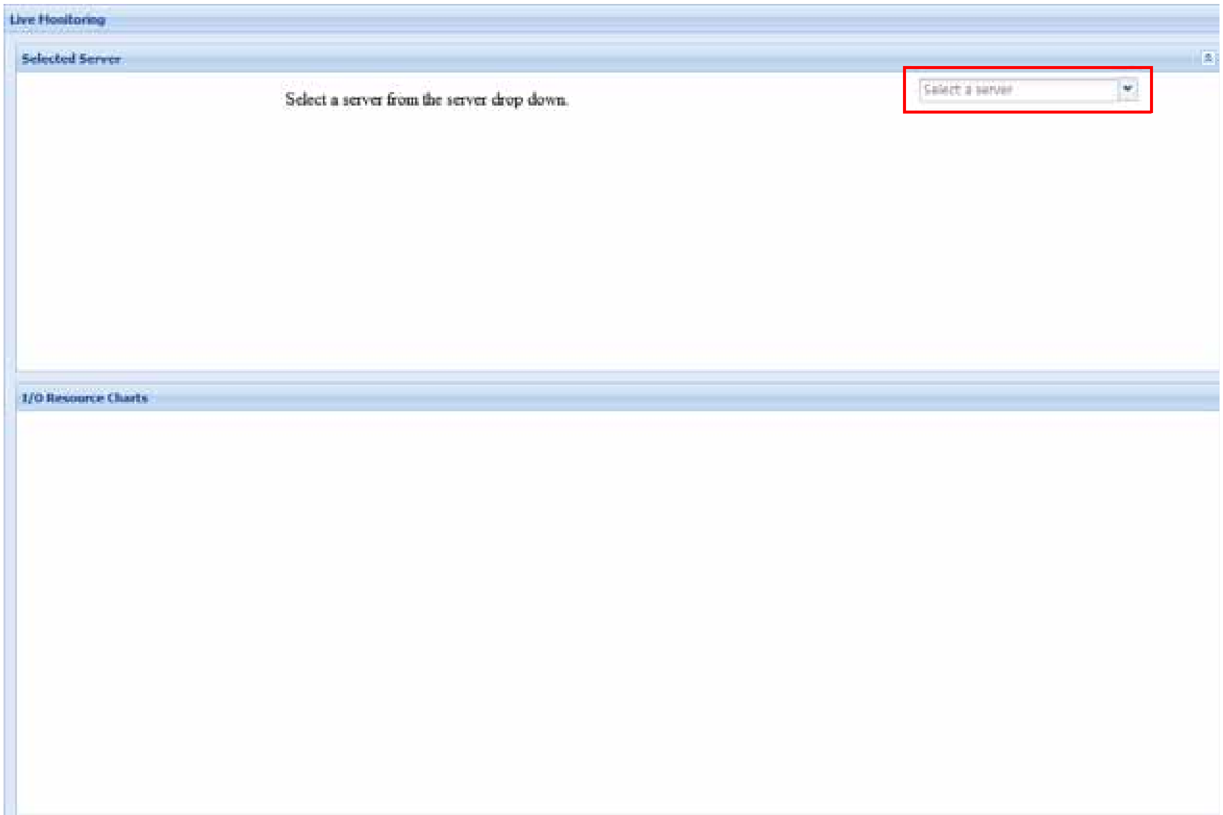


Figure 4 Live Monitoring—Zoomed to a Smaller Interval

To display the Selected Server throughput, follow this procedure:

Step 1 From the Navigation Frame, display Live Monitoring by selecting *Service Manager ->Live Monitoring*. Figure 5 shows the Live Monitoring Summary.

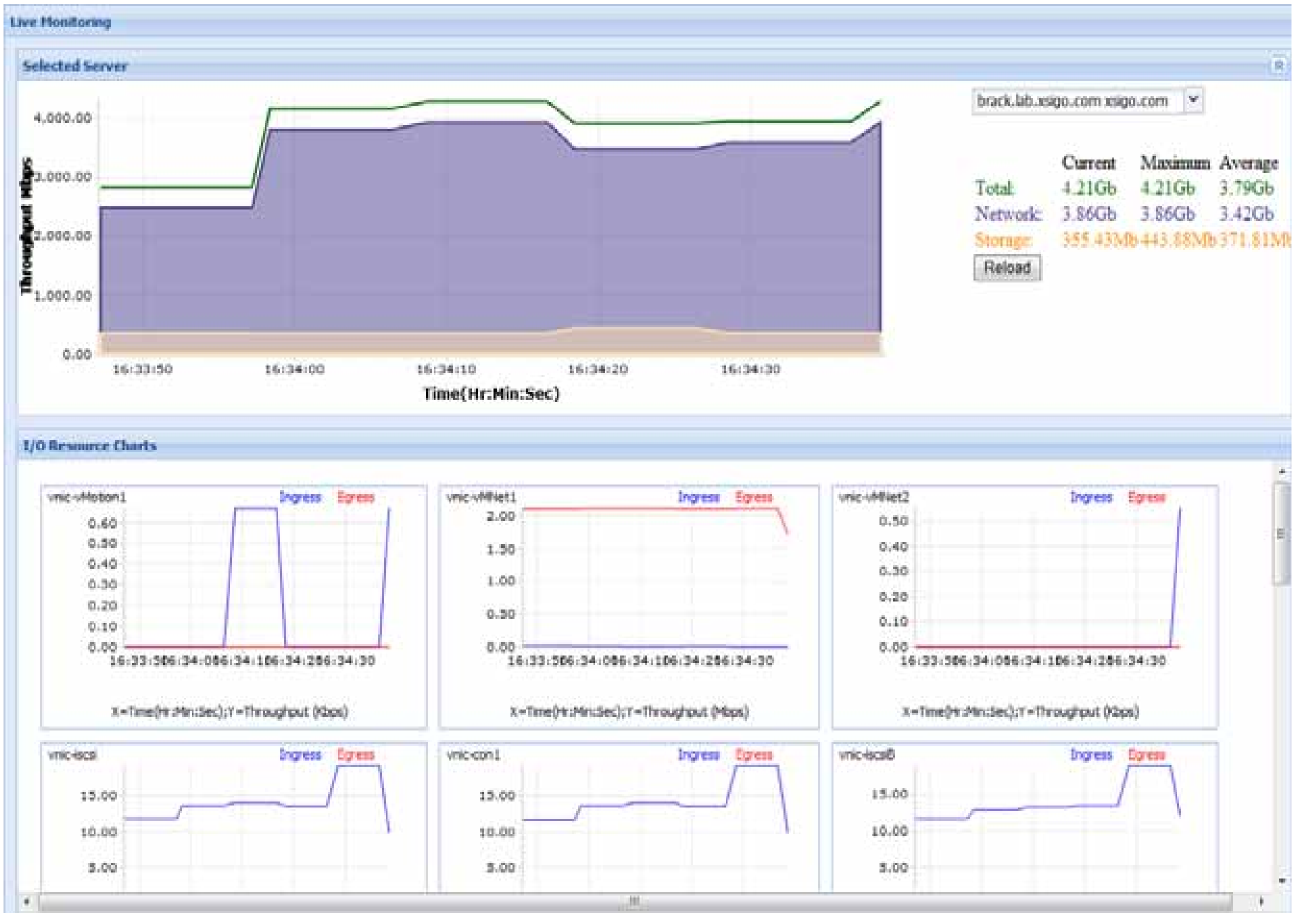


Select a server from the server drop down.

Figure 5 Live Monitoring

Notice that Live Monitoring is blank by default until you select a physical server.

Step 2 From the dropdown menu, select a server for Live Monitoring. After a brief amount of time, the Live Monitoring Summary is displayed.



Live Monitoring

Selected Server

brack.lab.xsigo.com xsigo.com

	Current	Maximum	Average
Total:	4.21Gb	4.21Gb	3.79Gb
Network:	3.86Gb	3.86Gb	3.42Gb
Storage:	355.43Mb	443.88Mb	371.81Mb

Reload

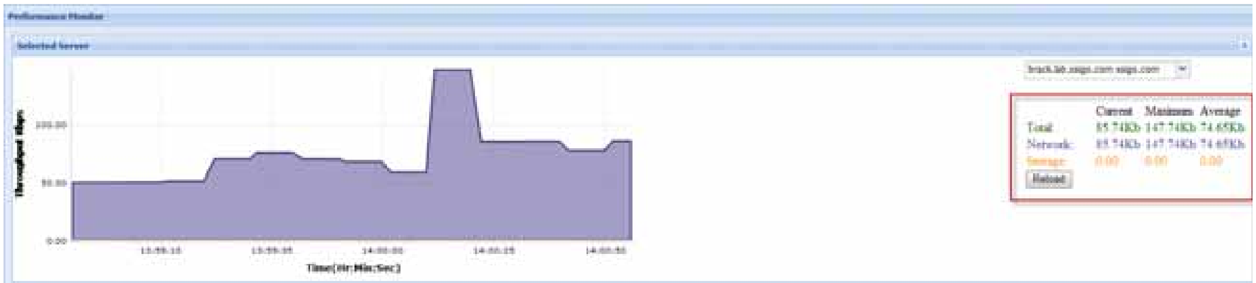
I/O Resource Charts

Figure 6 Live Monitoring

Step 3 As an option, click and drag left-to-right in a downward motion to draw a box over the statistics that you want to zoom in on. You can click and drag right-to-left in an upward motion to zoom out.

Historical and Calculated Statistics

Based on the monitored throughput, Oracle's Xsigo Fabric Manager displays additional information for the selected server in a table on the side of a graph. The additional information is tracked for historical information, unless documented otherwise. Figure 8 shows the table of historical and calculated statistics.



	Current	Maximum	Average
Total	85.74Kb	147.74Kb	74.65Kb
Network:	85.74Kb	147.74Kb	74.65Kb
Storage:	0.00	0.00	0.00

Figure 7 Selected Server Frame — Historical and Calculated Statistics

The following additional information is displayed.

- the aggregate amount of throughput for the current graphing session (Total Current).
- the maximum amount of through for the current graphing session (Total Maximum).
- the average amount of throughput for the current graphing session (Total Average). This statistic is calculated.
- the amount of network throughput for the current graphing session (Network Current).
- the maximum amount of network throughput for the current graphing session (Network Maximum).
- the average amount of network throughput for the current graphing session (Network Average). This statistic is calculated.
- the amount of storage throughput for the current graphing session (Storage Current).
- the maximum amount of storage throughput for the current graphing session (Storage Maximum).
- the average amount of storage throughput for the current graphing session (Storage Average).

Displaying vNIC Throughput

When vNICs are configured and deployed on the host server, Live Monitoring can graph the throughput of each vNIC through the I/O Resource Charts. Each chart is a separate instance of a vNIC that graphs the ingress and egress traffic. Each I/O Resource Chart is a standard line graph consisting of an X axis and a Y axis:

- The X axis shows an interval-based time line. By default, each interval is 50 seconds, but this value can be decreased to smaller amounts of time.
- The Y axis shows the throughput in Kbps.

Each Chart has the ability to track throughput for one or both directions of traffic (ingress only, egress only, or both ingress and egress) depending on what traffic exists on the virtual resource.

Figure 8 shows an example of the I/O Resource Charts for vNICs.

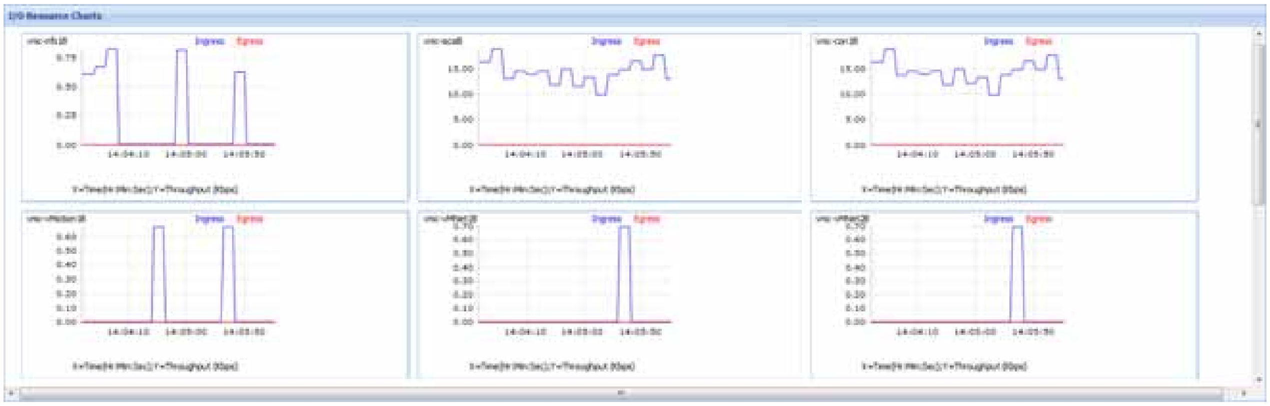
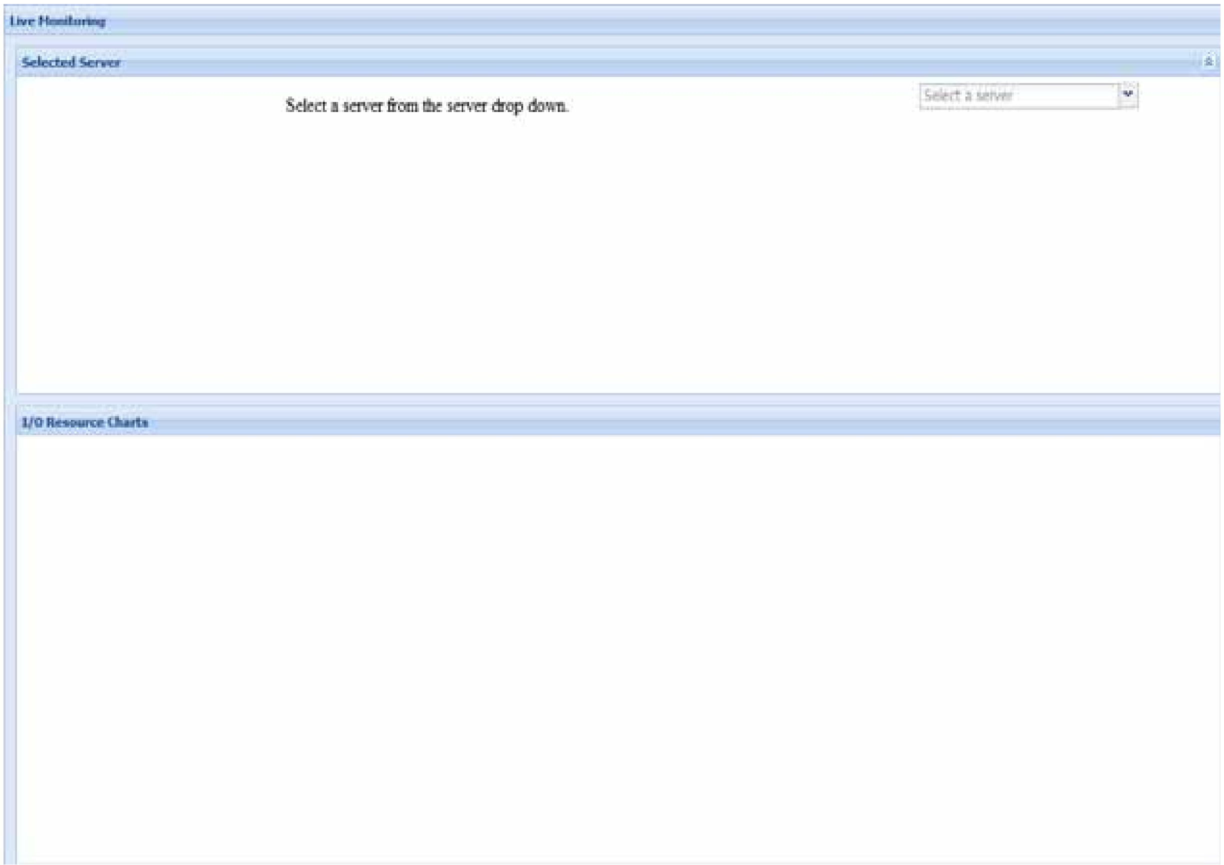


Figure 8 I/O Resource Charts — vNICs

You'll notice that each vNIC has its own chart, which is identified by the vNIC name. Also, each vNIC I/O chart can be zoomed in to show the statistics for a smaller interval. To zoom in, click and drag in a downward motion to create a box over the statistics you want to zoom in on. When you complete the click and drag motion, the interval becomes smaller and the graphed section of statistics becomes larger, as documented in Real-Time Grapher.

The vNIC I/O Resource charts are contained in a separate frame on the Live Monitoring summary. To display the Live Monitoring Summary, follow this procedure:

Step 1 From the Navigation Frame, display Live Monitoring by selecting *Service Manager->Live Monitoring*. Figure 9 shows Live Monitoring.



Live Monitoring

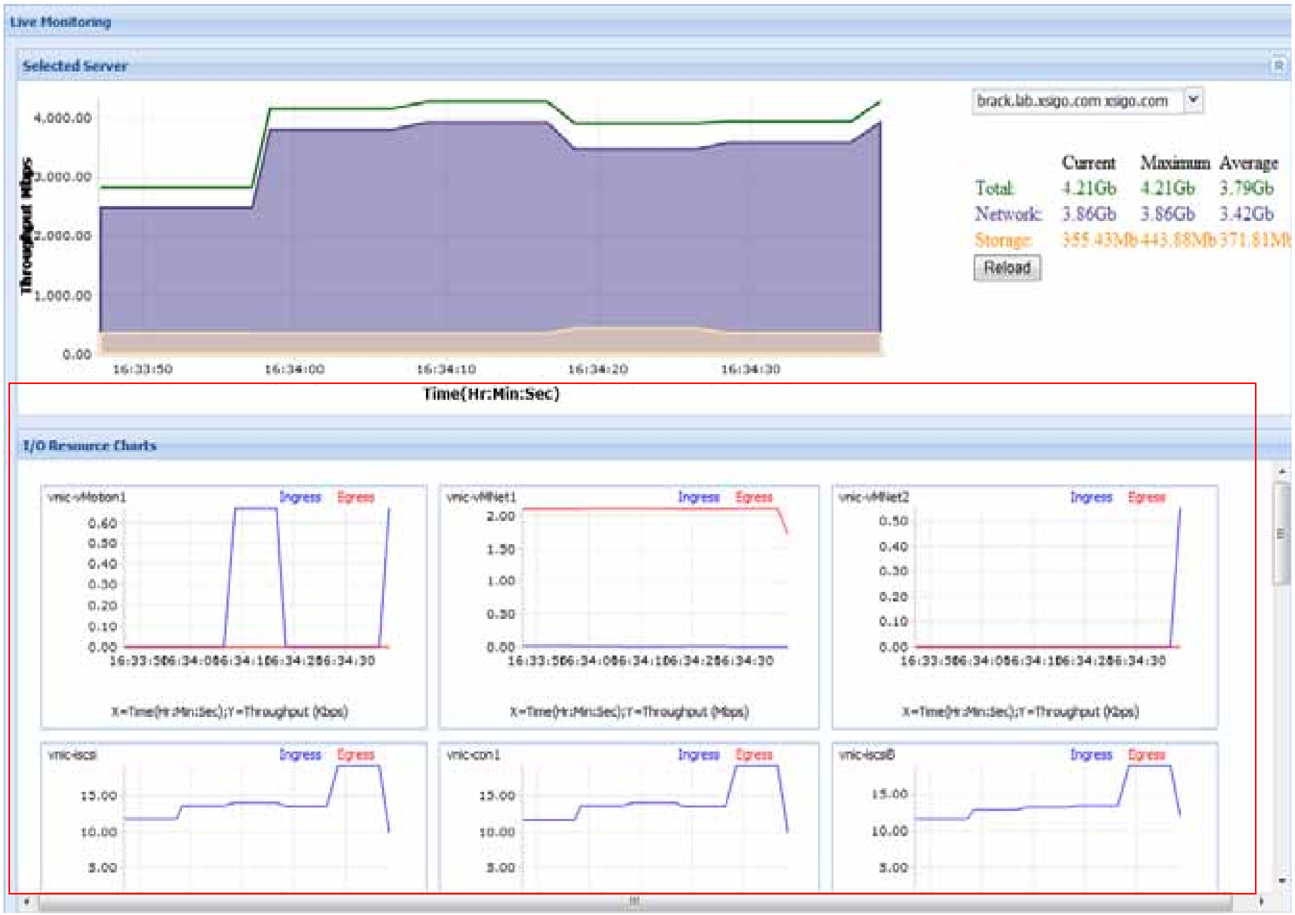
Selected Server

Select a server from the server drop down.

Figure 9 Live Monitoring

Notice that Live Monitoring is blank by default until you select a physical server.

Step 2 From the dropdown menu, select a server for Live Monitoring. After a brief amount of time, the Live Monitoring Summary is displayed. See Figure 10.



brack.lab.xsigo.com xsigo.com

	Current	Maximum	Average
Total:	4.21Gb	4.21Gb	3.79Gb
Network:	3.86Gb	3.86Gb	3.42Gb
Storage:	355.43Mb	443.88Mb	371.81M

Figure 10 Live Monitoring

If enough vNIC are deployed, scroll bars appear on the I/O Resource Charts frame. You might need to scroll the frame to see all the deployed vNICs. Also, if vHBAs are also present, they will be displayed below the vNICs. If you want to see the vHBAs, you might need to scroll the frame to see all the deployed vHBAs.

Step 3 As an option, click and drag left-to-right in a downward motion to draw a box over the vNIC statistics that you want to zoom in on. You can click and drag right-to-left in an upward motion to zoom out.

Displaying vHBA Throughput

When vHBAs are configured and deployed on the host server, Live Monitoring can graph the throughput of each vHBA through the I/O Resource Charts. Each chart is a separate instance of a vHBA that graphs the ingress and egress traffic. Each I/O Resource Chart is a standard line graph consisting of an X axis and a Y axis:

- The X axis shows an interval-based time line. By default, each interval is 50 seconds, but this value can be decreased to smaller amounts of time.
- The Y axis shows the throughput in Kbps.

Each chart has the ability to track throughput for one or both directions of traffic (ingress only, egress only, or both ingress and egress) depending on what traffic exists on the virtual resource.

Figure 11 shows the vHBA I/O Resource Charts.

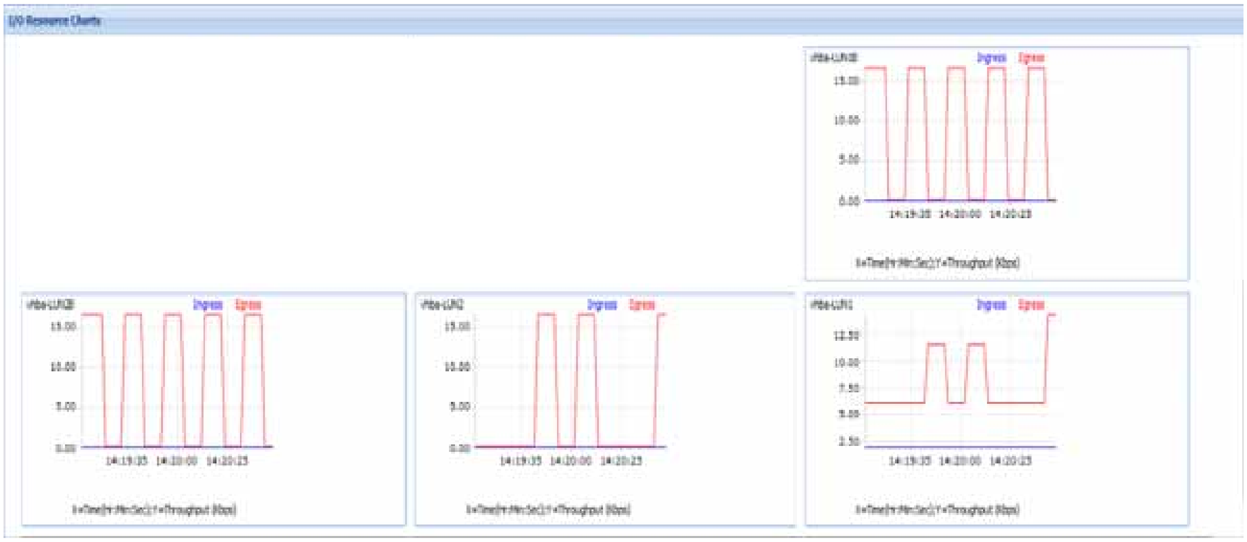
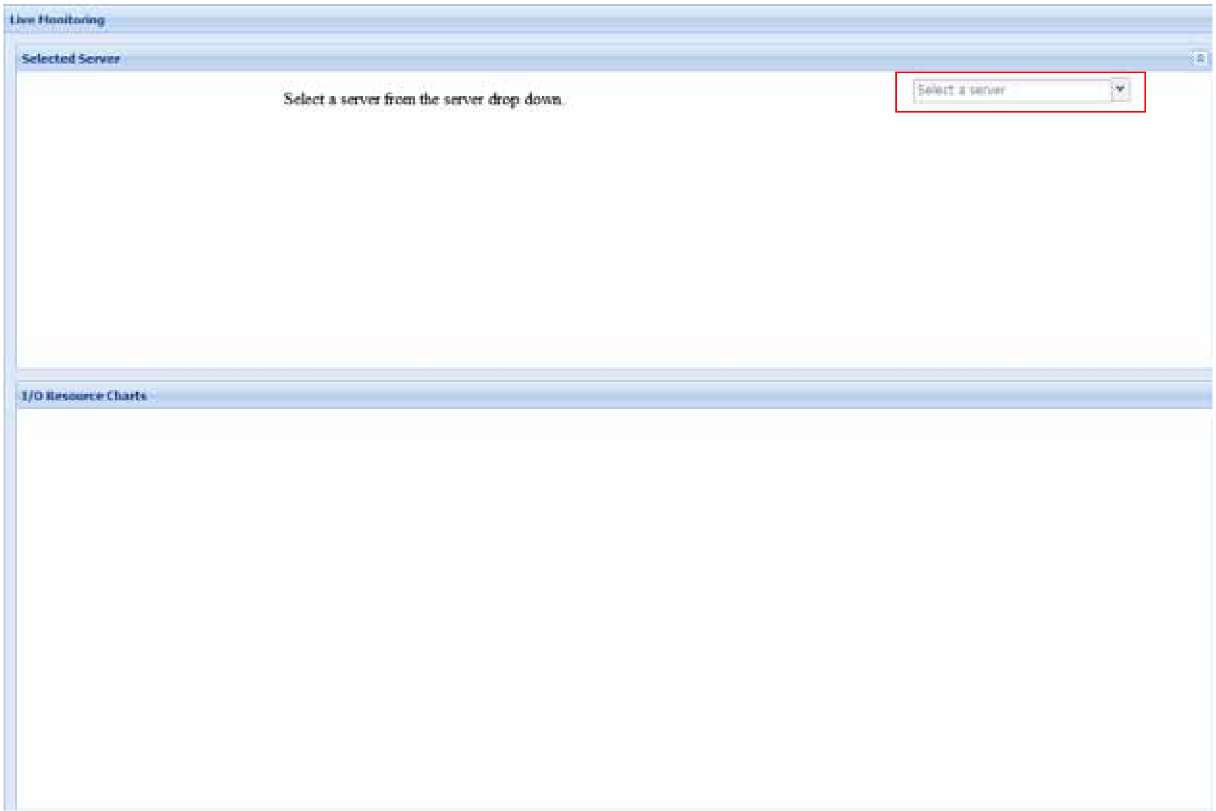


Figure 11 I/O Resource Charts — vHBAs

You’ll notice that each vHBA has its own chart, which is identified be the vHBA name. Also, each vHBA I/O chart can be zoomed in to show the statistics for a smaller interval. To zoom in, click and drag in a downward motion to create a box over the statistics you want to zoom in on. When you complete the click and drag motion, the interval becomes smaller and the graphed section of statistics becomes larger, as documented in Real-Time Grapher.

The vHBA I/O Resource charts are contained in a separate frame on the Live Monitoring summary. To display the Live Monitoring Summary, follow this procedure:

Step 1 From the Navigation Frame, display Live Monitoring by selecting *Service Manager ->Live Monitoring*. Figure 12 shows Live Monitoring.

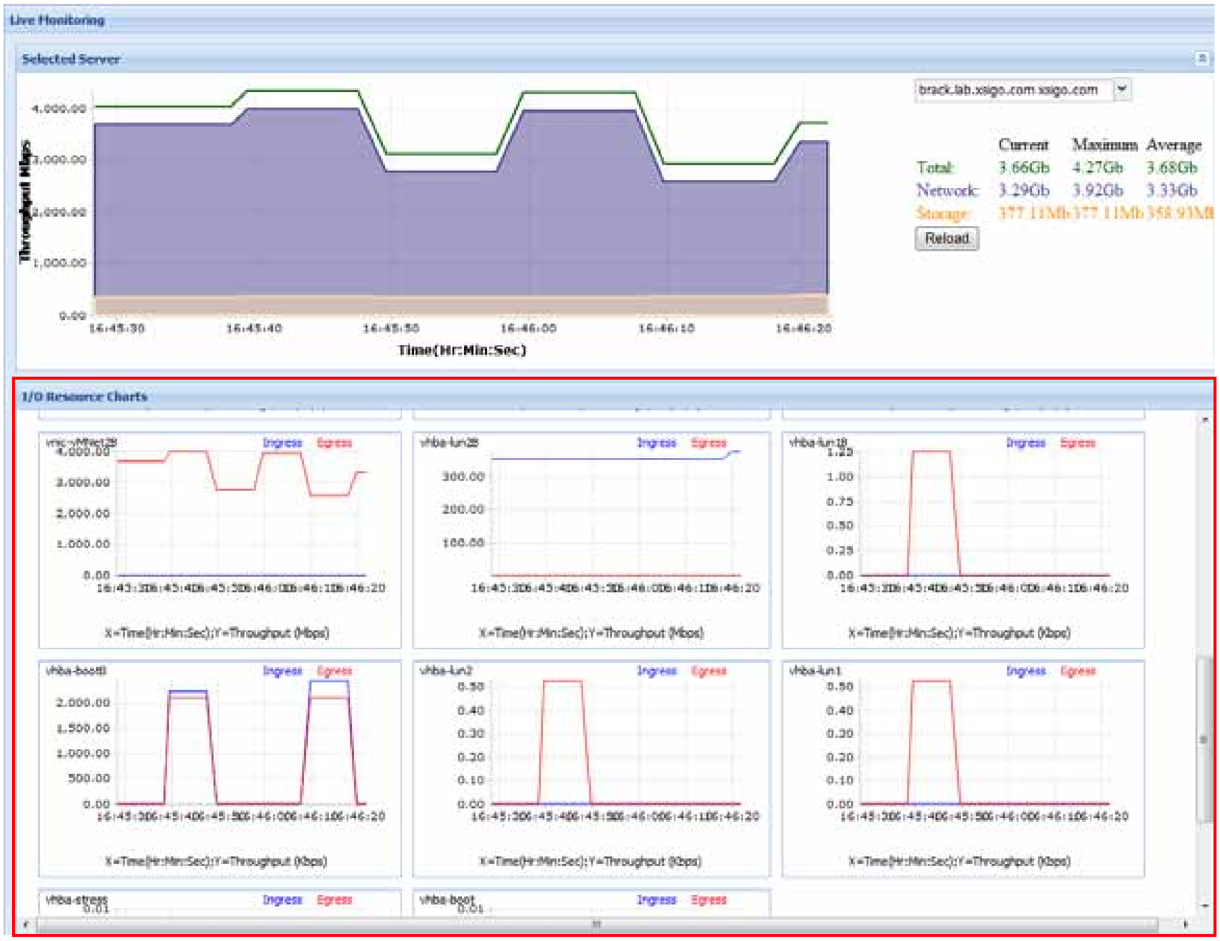


Select a server from the server drop down.

Figure 12 Live Monitoring

Notice that Live Monitoring is blank by default until you select a physical server.

Step 2 From the dropdown menu, select a server for Live Monitoring. After a brief amount of time, the Live Monitoring Summary is displayed. Figure 13 shows the Live Monitoring Summary.



brack.lab.xsigo.com xsigo.com

	Current	Maximum	Average
Total:	3.66Gb	4.27Gb	3.68Gb
Network:	3.29Gb	3.92Gb	3.33Gb
Storage:	377.11Mb	377.11Mb	358.93Mb

Reload

Figure 13 Live Monitoring

If enough vHBAs are deployed, scroll bars appear on the I/O Resource Charts frame. You might need to scroll the frame to see all the deployed vHBAs. Also, if vNICs are also present, they will be displayed above the vHBAs. If you want to see the vNICs, you might need to scroll the frame to see all the deployed vNICs.

Step 3 As an option, click and drag left-to-right in a downward motion to draw a box over the vHBA statistics that you want to zoom in on. You can click and drag right-to-left in an upward motion to zoom out.

Working with the Task Scheduler

This chapter contains the following topics:

Understanding the Task Scheduler

Oracle's Xsigo Fabric Manager Task Scheduler allows you to set times and dates for backing up Fabric Manager Server configurations and Oracle's Xsigo Fabric Director configurations. Backing up a Fabric Manager Server or a Fabric Director can occur either on-demand or on a recurring schedule. Regardless of the schedule type, backups are stored in the following locations on the Fabric Manager Server:

- Linux Fabric Manager Server:
  - — Fabric Manager backups are stored in `/opt/xsigo/xms/xms-backups`
  - — Fabric Director backups are stored in `/opt/xsigo/xms/director-backups`
- Windows Fabric Manager Server:
  - — Fabric Manager backups are stored in `C:\Program Files\xms\xms-backups`
  - — Fabric Director backups are stored in `C:\Program Files\xms\director-backups`

Each backup captures the entire configuration of the Fabric Manager Server or Fabric Director.

Considerations for Fabric Manager Backups

Fabric Manager Backups can occur in multiple ways. Being aware of these considerations will facilitate your backup and restore operations for Fabric Manager Servers:

- through the Backup Fabric Manager Configuration option on the Maintenance menu (***Maintenance->Backup Fabric Manager Config***), which is represented by the screwdriver icon on the Fabric Manager banner.
- through a Schedule backup (***Schedules->Fabric Manager Backups***)
- through an on-demand backup (***Schedules->Fabric Manager Backups->Execute Now***)

In all cases the same information is backed up, the Fabric Manager Server configuration and all objects that Fabric Manager has under management. However, there are some subtle differences between each method of Fabric Manager backup:

- The difference between ***Maintenance->Backup Fabric Manager Config*** and ***Schedules->Fabric Manager Backups->Execute Now***, is that ***Maintenance->Backup Fabric Manager Config*** requires you to specify a file name whereas ***Schedules->Fabric Manager Backups->Execute Now*** requires a schedule to exist and executes the scheduled backup immediately, not at the scheduled time(s).
- The file names are different depending on which method of backup you choose:
  - — if you perform Fabric Manager backup through ***Maintenance->Backup Fabric Manager Config***, Fabric Manager prompts you for a specific file name, so the file will be named <*name*> plus a date and time stamp— for example, `foobar_2011-04-05_04_01_59_325`
  - — if you perform the Fabric Manager Backup through ***Schedules->Fabric Manager Backups***, Fabric Manager creates its own file name in the format `scheduled_` plus a name, plus a time and date stamp—for example, `scheduled_foobar_2011_04_05_04_01_59_325`
  - — if you perform the backup through ***Schedules->Fabric Manager Backups->Execute Now*** button, Fabric Manager creates its own file name in the format `scheduled_executeNow_` plus a name, plus a time and date stamp—for example, `scheduled_executeNow_foobar_2011_04_05_04_01_59_325`

Regardless of the method you choose for Fabric Manager Server backups, the backup files are stored as XML files and can be restored through ***Maintenance->Restore Fabric Manager Server Config***.

When you need to restore from a specific backup, you will find it helpful to know the different file naming methods listed above so that you will be able to easily restore the specific Fabric Manager Server backup you want.

Take Fabric Manager Backups and Fabric Director Backups at the Same Time

When you need to do a backup of either Fabric Manager or the Fabric Director, it is a best practice to take a backup of both at the same time. The reason for this requirement is objects will not get out of sync, thereby restore operations will occur without problems. Take a backup of all Fabric Directors first, then take the Fabric Manager backups.

When restoring a saved backup, Xsigo requires that you restore both the I.O Director and the Fabric Manager Server at the same time. Restore the Fabric Manager backups first, then restore the Fabric Directors.

Backup and Restore of Fabric Director through Fabric Manager

Fabric Manager supports backup and restore of either the Fabric Manager configuration or the Fabric Director configuration. The backup option for the Fabric Director captures information at a single point in time, and the restore option for the Fabric Director brings back the configuration that was present at the last backup.

Note

The backup and restore options for Fabric Manager affect only the Fabric Manager Server and Fabric Manager configuration. Restoring the Fabric Manager configuration does not bring back the configurations of any Fabric Directors that Fabric Manager is managing. Instead, only the Fabric Manager database is backed up and restored.

Fabric Manager's *backup* option for the Fabric Director operates the same as issuing the **`system export`** command on the Fabric Director. The backup option captures the following information at the time that you initiate the Fabric Director backup through Fabric Manager:

- Hardware inventory of which modules are present in which slots. Any hardware changes made after the backup completes are not written to the last backup, and the changes are not automatically captured. You can always take another backup after the hardware changes are complete, if needed. If you take an additional backup, the previous backup is not deleted. The previous backup is kept along with new one.
- Administrative states of all objects in the Fabric Director. Operational states are not captured in the backup.

Fabric Manager's *restore* option for the Fabric Director operates the same as issuing the **`system import`** command on the Fabric Director. The restore option brings back the hardware inventory and administrative states contained in the last backup.

Some common use cases for Fabric Manager backup and restore of a Fabric Director are:

- Restoring deleted vNICs or vHBAs, but only if no changes have been made to the vNICs. For example, assume you created some vNICs through Fabric Manager and took a Fabric Director backup. If someone else then deletes the vNICs, you can restore the configuration on the Fabric Director to replace the deleted vNICs provided that no other changes have been made to the vNICs. If changes have been made, the vNICs might not be restored correctly.
- Restore a clean Fabric Director configuration. Assume a Fabric Director has been returned to its default configuration—for example, through the **`system clear config`** command. You can then restore the last backed up configuration instead of having to re-create the entire configuration.

Considerations for Fabric Director Backups

Fabric Director backups can occur in multiple ways. Being aware of these considerations will facilitate your backup and restore operations for Fabric Directors:

- through the Backup Fabric Director configuration toolbar button on the Fabric Director Summary (*Fabric Directors->Fabric Directors->**Backup Fabric Director Config*** button)
- through a Schedule backup (***Schedules->Director Backups***)
- through an on-demand backup (***Schedules->Director Backups->Execute Now*** button)

In all cases the same information is backed up. However, there are some subtle differences between each method of Fabric Director backup:

- The difference between *Fabric Directors->Fabric Directors->**Backup Fabric Director Config*** button and *Schedules-> Director Backups->**Execute Now*** button, is that *Fabric Directors->Fabric Directors->**Backup Fabric Director Config*** button requires you to specify a file name whereas ***Schedules->Director Backups ->Execute Now*** button requires a schedule to exist and executes the scheduled backup immediately, not at the scheduled time.
- The file names are different depending on which method of backup you choose:
  - — if you perform a Director backup through *Fabric Directors->Fabric Directors->**Backup Fabric Director Config*** button, Fabric Manager prompts you for a file name, so the file will be named <*director-name*> plus <*file-name*> plus a date and time stamp— for example, `destroyer_backup1_2011-04-05_04_01_59_325`
  - — if you perform a Director backup through ***Schedules->Director Backups***, Fabric Manager creates its own file name in the format <*director-name*>`_scheduled_` plus <*name*>, plus a time and date stamp—for example, `destroyer_scheduled_backup1_2011_04_05_04_01_59_325`
  - — if you perform a Director backup through ***Schedules->Director Backups->Execute Now*** button, Fabric Manager creates its own file name in the format <*director-name*>`_scheduled_executeNow_` plus <*name*>, plus a time and date stamp—for example, `destroyer_scheduled_executeNow_destroyer_2011_04_05_04_01_59_325`

Regardless of the method you choose for Director backups, the backup files are stored as XML files and can be restored through *Xsigo Fabric Directors->Fabric Directors->**Restore Fabric Director Config*** button.

When you need to restore from a specific backup, you will find it helpful to know the different file naming methods listed above so that you will be able to easily restore the specific Director backup you want.

Take Fabric Manager Backups and Fabric Director Backups at the Same Time

When you need to do a backup of either Fabric Manager or the Fabric Director, it is a best practice to take a backup of both at the same time. The reason for this requirement is objects will not get out of sync, thereby restore operations will occur without problems. Take a backup of all Fabric Directors first, then take the Fabric Manager backups.

When restoring a saved backup, Xsigo requires that you restore both the I.O Director and the Fabric Manager Server at the same time. Restore the Fabric Manager backups first, then restore the Fabric Directors.

Director Backup with HA Fabric Directors

When multiple Fabric Directors are deployed, they share a common Ethernet or InfiniBand switching fabric. In a dual-Fabric Director deployment, there is no method of synchronization for backups. As a result, each Fabric Director should be configured with its own Fabric Director backup schedule. Any on-demand backups either through *Fabric Directors*

*->Fabric Directors->****Backup Fabric Director Config*** button or *Schedules->Director Backups->****Execute Now*** button should be manually duplicated across both Fabric Directors to keep their backups in sync.

Scheduled Backups

When you configure the task scheduler, you have the option of running backups either daily, weekly, or monthly:

- daily backups occur every day at time(s) of day that you specify. You can specify more than one scheduled backup time for the same day. For example, it would be a valid configuration to set one daily schedule to run at 6:00 a.m., and also set another schedule that runs at midnight.
- weekly backups occur each week on the day(s) that you specify. You can specify multiple days each week. For example, it would be a valid configuration to set one weekly schedule to run once a week on Monday and another weekly scheduled to run once a week on Friday.
- monthly backups occur each month on the day(s) that you specify at the time(s) of day that you specify. You can specify multiple days each month. For example, it would be a valid configuration to set one monthly schedule to run three different days each month—the 1st, the 14th, and the 28th.

When you configure a schedule, you will set the maximum number of backups that will be kept. The maximum number of backups is a sliding window based on the number that you specify, and only the most recent number of backups is kept. For example, if you specify 5, the first 5 backups are kept. When 6 or more backups occur, the oldest are deleted so that only the newest 5 backups are kept. This sliding windows allows the most recent data to be kept, and also prevents the backups directory from becoming full and consuming an unreasonable amount of disk space.

Scheduled backups complete with silent acknowledgement, so unless an error message is displayed, the scheduled backup has completed successfully. You can, however, check the *Execution History* tab for a timestamp that is close to the time(s) when you started the backup. The presence of the backup in the Execution History verifies that the backup completed successfully.

For information about running scheduled backups, see the appropriate section:

- To backup Fabric Manager Servers based on a recurring schedule, see Creating Fabric Manager Backup Schedules
- To backup Fabric Directors based on a recurring schedule, see Creating Fabric Director Backup Schedules

On-Demand Backups

On-demand backups can be run at any time. When you run them, they complete immediately.

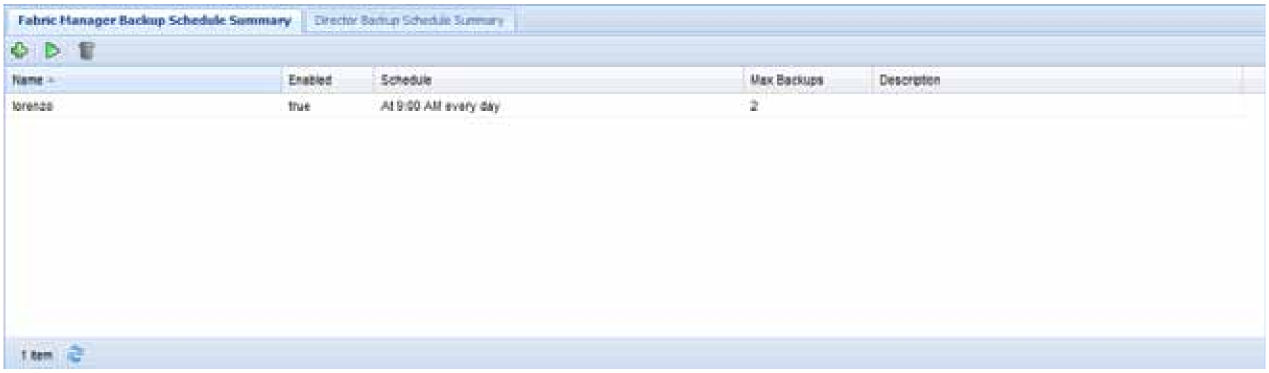
On-demand backups and scheduled backups are not mutually exclusive, so any scheduled backups will run in addition to the on-demand backup. For example, if you have a daily backup set for 4:00 a.m., you can run an on-demand backup at any time, and the scheduled backup still runs at 4:00 a.m. On-demand backups complete with silent acknowledgement, so unless an error message is displayed, the on-demand backup has completed successfully. You can, however, check the *Execution History* tab for a timestamp that is close to the time(s) when you started the backup. The presence of the backup in the Execution History verifies that the backup completed successfully. For information about running an on-demand backup, see the appropriate section:

- To backup up a Fabric Manager Server on-demand, see Running an On-Demand Fabric Manager Backup
- To backup a Fabric Director on-demand, see Running an On-Demand Fabric Director Backup

Displaying Fabric Manager Schedules

Fabric Manager displays the backup schedules for the Fabric Manager Server in the Fabric Manager Backup Schedule Summary, which is a tabbed display. The Fabric Manager Backup Schedule Summary contains a list of all the configured backup schedules, regardless of their operational state (enabled or disabled).

The Fabric Manager Backup Schedule Summary is available through Schedules option on the Navigation Panel. Figure 1 shows an example of the Fabric Manager Backup Schedule Summary tab.


Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary
1 item

Name	Enabled	Schedule	Max Backups	Description
lorenzo	true	At 9:00 AM every day	2	

Figure 1 Fabric Manager Backup Schedule Summary

The Fabric Manager Backup Schedule Summary contains information about configured backup schedules for Fabric Manager Server backup. Table 1 shows the contents of the Fabric Manager Backup Schedule Summary and explains what each field means.

Table 1 Contents of Fabric Manager Backup Schedule Summary

Field...	Means...
Name	The name assigned to the specific Fabric Manager backup schedule.
Enabled	The operational state (either enabled or disabled) for a particular Fabric Manager backup schedule.
Schedule	The specific day(s), time(s), or date(s) on which the backup will run.
Max Backups	The maximum number of backups that are allowed for each particular Fabric Manager Backup Schedule.
Description	An optional alphanumeric string that describes a Fabric Manager Backup Schedule.

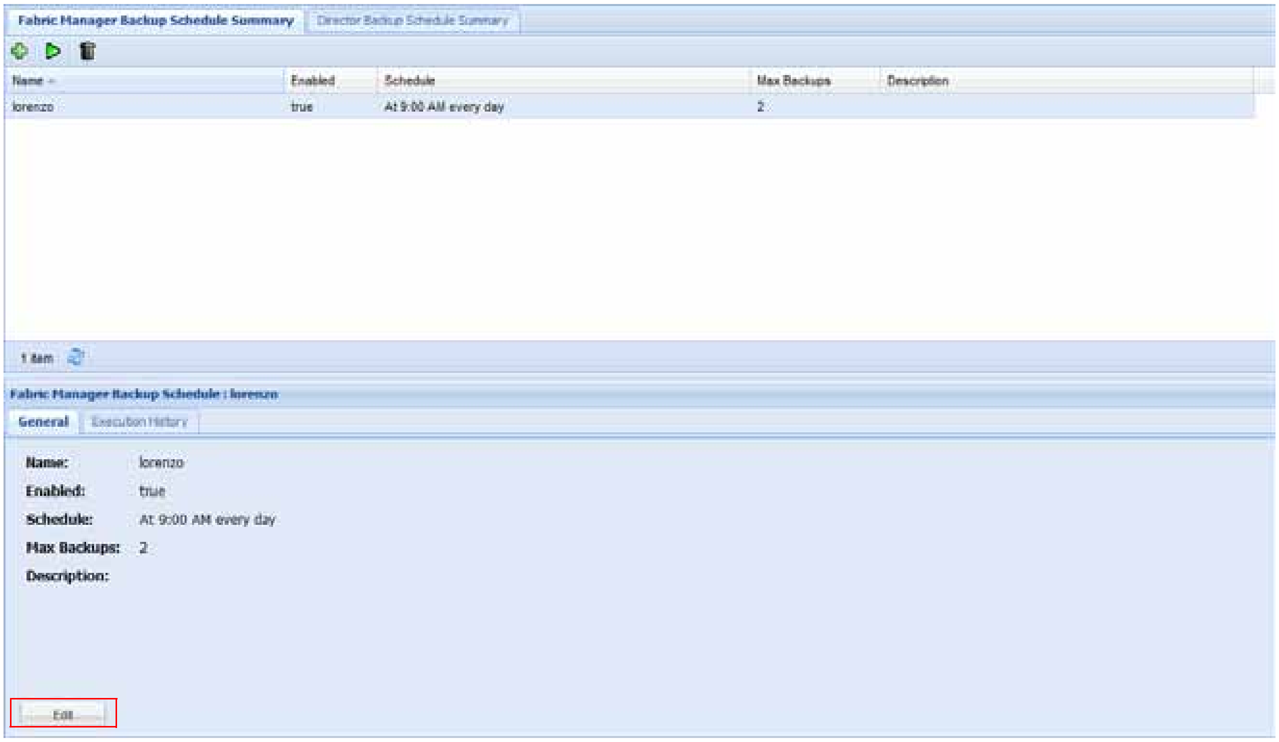
Editing Fabric Manager Backup Schedules

When a backup schedule is created for Fabric Manager, it can be edited at any time. When the edits are completed and the details frame is locked for editing, the new changes take effect based on the new properties. For example, if you had a daily backup schedule set to occur at 7:00 a.m., but decided to set the backup to occur at 3:00 a.m. instead, the new backup will occur at 3:00 a.m. the next morning after you complete edits. Of course, you can always use the on-demand backup feature, to complete an instantaneous backup at any time.

To edit a configured Fabric Manager backup schedule, follow this procedure:

Step 1 Display the Fabric Manager Backup Schedule Summary.

Step 2 In the Fabric Manager Backup Schedule Summary, click the backup schedule that you want to edit. This step populates the Details frame with the properties of the selected backup schedule. Figure 2 shows a sample Details frame.



Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary

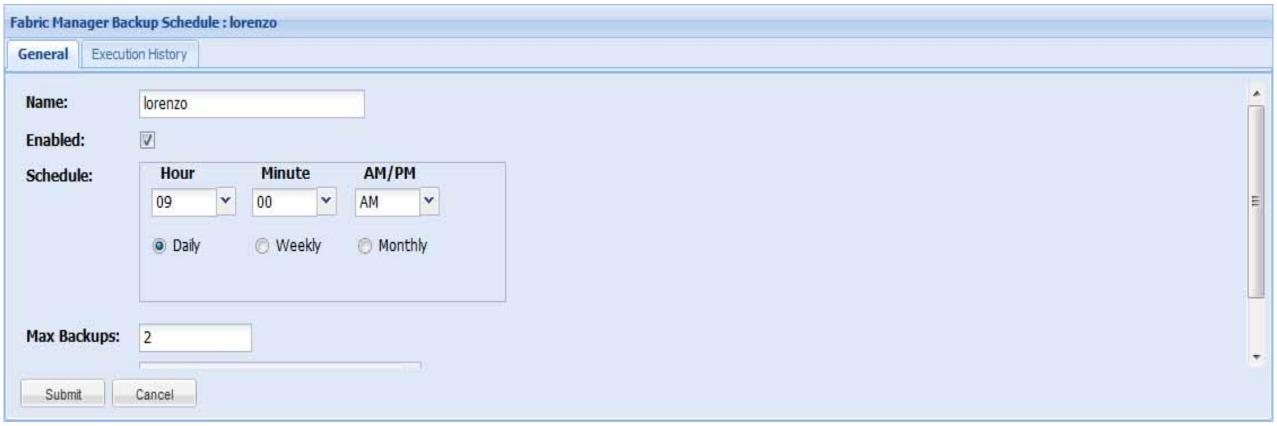
Name	Enabled	Schedule	Max Backups	Description
lorenzo	true	At 9:00 AM every day	2	

1 item
Fabric Manager Backup Schedule : lorenzo
General
Execution History

Name: lorenzo
Enabled: true
Schedule: At 9:00 AM every day
Max Backups: 2
Description:

Figure 2 Fabric Manager Backup Schedules — Details Frame

Step 3 In the Details frame, click the ***Edit*** button to unlock the properties for editing, as shown in Figure 3. This example shows editing a daily backup schedule, but similar properties (name, enable/disable, backup schedule times and dates, maximum number of backups, and description) are editable regardless of whether the backup schedule is daily, weekly, or monthly.



Fabric Manager Backup Schedule : lorenzo

Name:	lorenzo
Enabled:	☑
Schedule:	Hour 09 · Minute 00 · AM/PM AM ● Daily ○ Weekly ○ Monthly
Max Backups:	2

Figure 3 Fabric Manager Backup Schedule Details — Edit General Properties

Step 4 Edit the properties as needed.

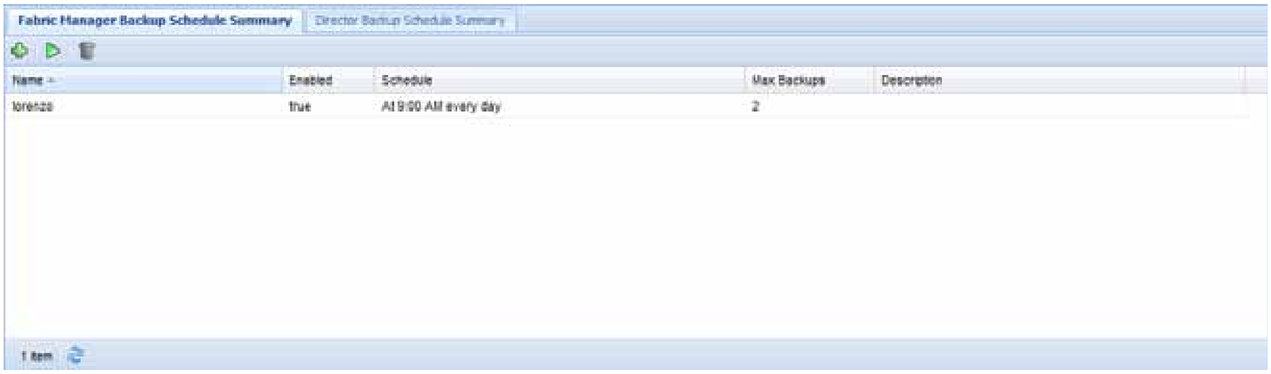
Step 5 When the properties are set correctly, click ***Submit***. The new properties do not take effect unless the ***Submit*** button is clicked.

Renaming Fabric Manager Schedules

Fabric Manager supports renaming a Fabric Manager Schedule, which enables you to change the name without having to completely delete and recreate the entire Fabric Manager Schedule. When the Fabric Manager Schedule is renamed, all other properties for the Fabric Manager Schedule are retained, including the schedule and server(s) affected. As an option, you can also set or change the description for the Fabric Manager Schedule.

You can rename the Fabric Manager Schedule through the Fabric Manager Schedule Details frame. To rename the Fabric Manager Schedule, follow this procedure:

Step 1 On the Navigation Frame, select *Service Manager->Schedules*. Figure 4 shows the Fabric Manager Backup Schedule Summary.



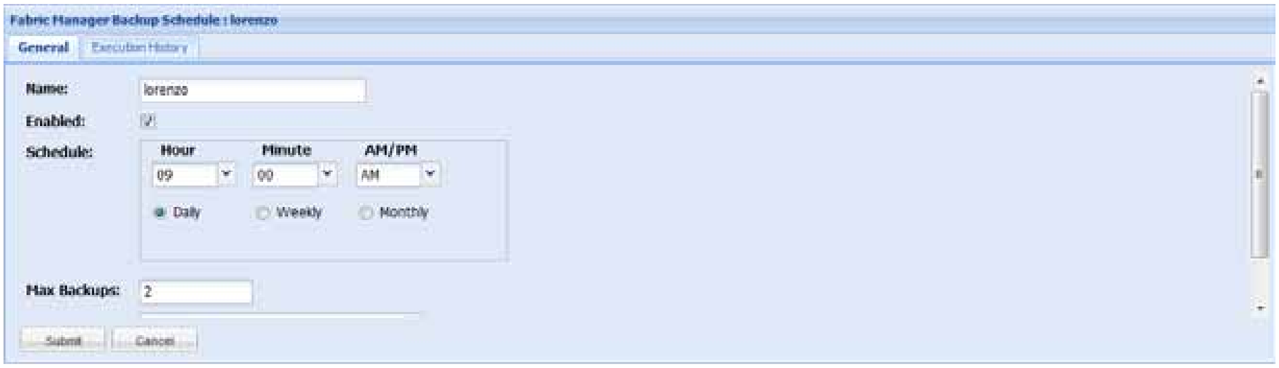
Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary

Name	Enabled	Schedule	Max Backups	Description
lorenzo	true	At 9:00 AM every day	2	

Figure 4 Fabric Manager Backup Schedule Summary

Step 2 Click the backup schedule that you want to rename. This step populates the details frame with its properties.

Step 3 Click the ***Edit*** button to edit the properties of the selected Fabric Manager Schedule, as shown in Figure 5.


Fabric Manager Backup Schedule : lorenzo

Name: lorenzo
Enabled: ☑
Schedule: Hour 09 Minute 00 AM/PM AM
● Daily ○ Weekly ○ Monthly
Max Backups: 2

Figure 5 Fabric Manager Backup Schedule Details — Edit General Properties

Step 4 In the *Name* field, enter the new name for the Fabric Manager Schedule.

Step 5 As an option, you also can set or change the description for the selected Fabric Manager Schedule.

Step 6 When the new name has been specified for the Fabric Manager Schedule, click ***Submit***.

Creating Fabric Manager Backup Schedules

Through Fabric Manager, you can create a set of backup schedules for the Fabric Manager Server(s) in your data center. A Fabric Manager backup schedule sets time(s) and date(s) on which the Fabric Manager Server configuration is copied to a file. Each time the backup runs, the entire configuration is saved, not just the differences from an established baseline.

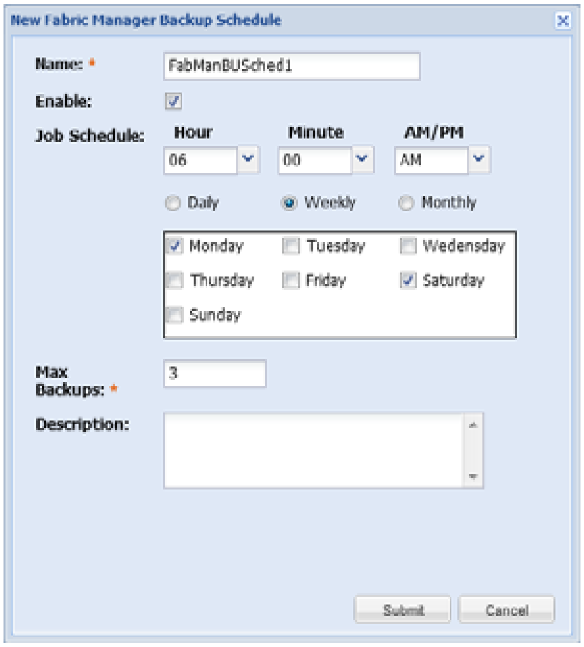
To backup the Fabric Manager Server config, you set a schedule for when the config is backed up and copied to the `xms-backups` directory. The following backup schedules are supported, and you can configure more than one type for the same Fabric Manager Server:

- daily
- weekly
- monthly

To create a Fabric Manager backup schedule, follow this procedure, which uses a weekly backup schedule for illustrative purposes:

Step 1 Display the Fabric Manager Backup Schedule Summary. Figure 1 shows the Fabric Manager Backup Schedule Summary.

Step 2 Click the plus sign to display the New Fabric Manager backup schedule dialog. Figure 6 shows this dialog.



New Fabric Manager Backup Schedule

Name: * FabManBUSched1

Enable: ☑

Job Schedule: Hour 06 Minute 00 AM/PM AM

○ Daily ● Weekly ○ Monthly

☑ Monday □ Tuesday □ Wedensday

□ Thursday □ Friday ☑ Saturday

□ Sunday

Max Backups: * 3

Description:

Figure 6 New Fabric Manager Backup Schedule

Step 3 In the *Name* field, enter an alphanumeric character string that identifies the backup schedule.

Step 4 In the *Enable* checkbox, make sure that the backup schedule is enabled.

Or, as an option, if you want to create the schedule without it being active, you can click to deselect the checkbox. When the checkbox is empty, the backup schedule is disabled.

Step 5 In the *Job Schedule* section, select the hour, minute, and a.m. or p.m. designation for when the backup will run. You must enter additional information if you are creating a weekly or monthly backup schedule:

- For a weekly schedule, you will also need to specify the day(s) on which the backup will run at the specified time(s) (hour, minute, a.m. or p.m.).
- For a monthly schedule, you will also need to select a date(s) of the month on which the backup will run at the specified time(s). The date(s) you select is applied to all months, so be aware of the implications of the date(s) that you select. For example, selecting the 30th of the month is acceptable for months that have 30 or 31 days. However, in February, the backup will not occur on the 30th since that month does not have 30 days. In this example, the backup would not run in February, but would resume in March.

Step 6 In the *Max Backups* field, enter a number from 1 to 99999 that quantifies the maximum number of backups that will occur for the backup schedule that you are creating. When the maximum number of backups is reached, the sliding window keeps only the last X backups. For example, if you have daily backups, and are keeping a maximum of 5, on the sixth day, the first backup is deleted, and the last 5 are kept.

Step 7 As an option, in the *Description* field, enter a description for the backup schedule that you are configuring.

Step 8 When the backup schedule properties are configured, click ***Submit***. The schedule is not created until you click ***Submit***.

Running an On-Demand Fabric Manager Backup

An on-demand Fabric Manager Backup is one that you manually start. On-demand backups can be completed at any time, and they are in addition to any scheduled backups.

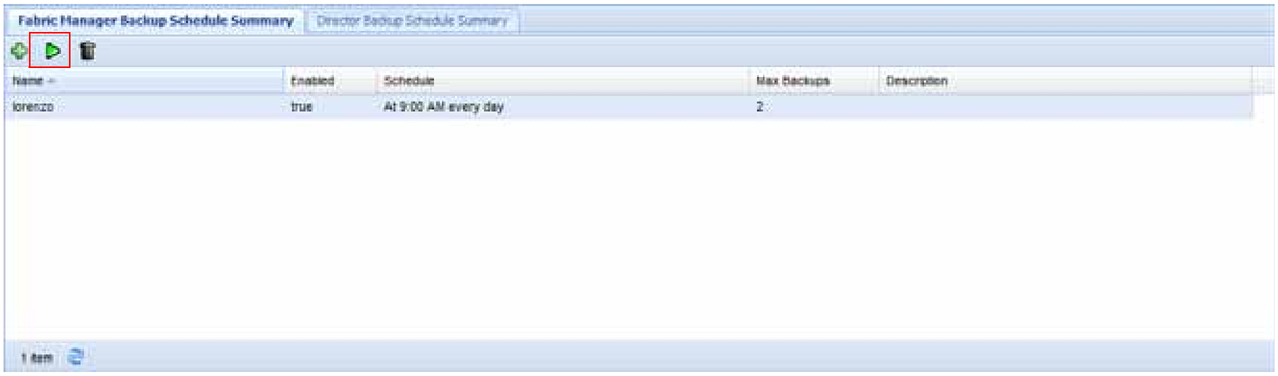
An on-demand backup runs for a configured backup schedule, just not at the scheduled time(s). As a result, a backup schedule must exist for the Fabric Manager Server that you want to backup on an on-demand basis.

You can run an on-demand Fabric Manager backup through the Fabric Manager Backup Schedule Summary tab.

To run an on-demand Fabric Manager backup, follow this procedure:

Step 1 Display the Fabric Manager Backup Schedule Summary.

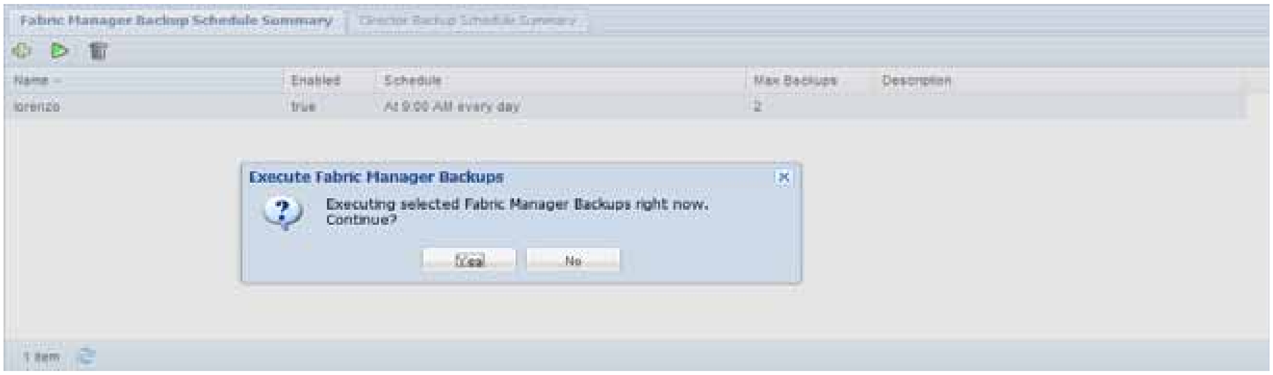
Step 2 Click the backup schedule that you want to run on an on-demand basis. This step activates the ***Execute Now*** button, which is the green arrow on the Fabric Manager Backup Schedule Summary toolbar. See Figure 7.


Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary

Name	Enabled	Schedule	Max Backups	Description
lorenzo	true	At 9:00 AM every day	2	

Figure 7 Fabric Manager Server Backup Schedule Summary — On-Demand Backup

Step 3 Click the ***Execute Now*** button to begin the backup. A confirmation popup dialog is displayed, as shown in Figure 8.


Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary
Execute Fabric Manager Backups
Yes
No
1 item

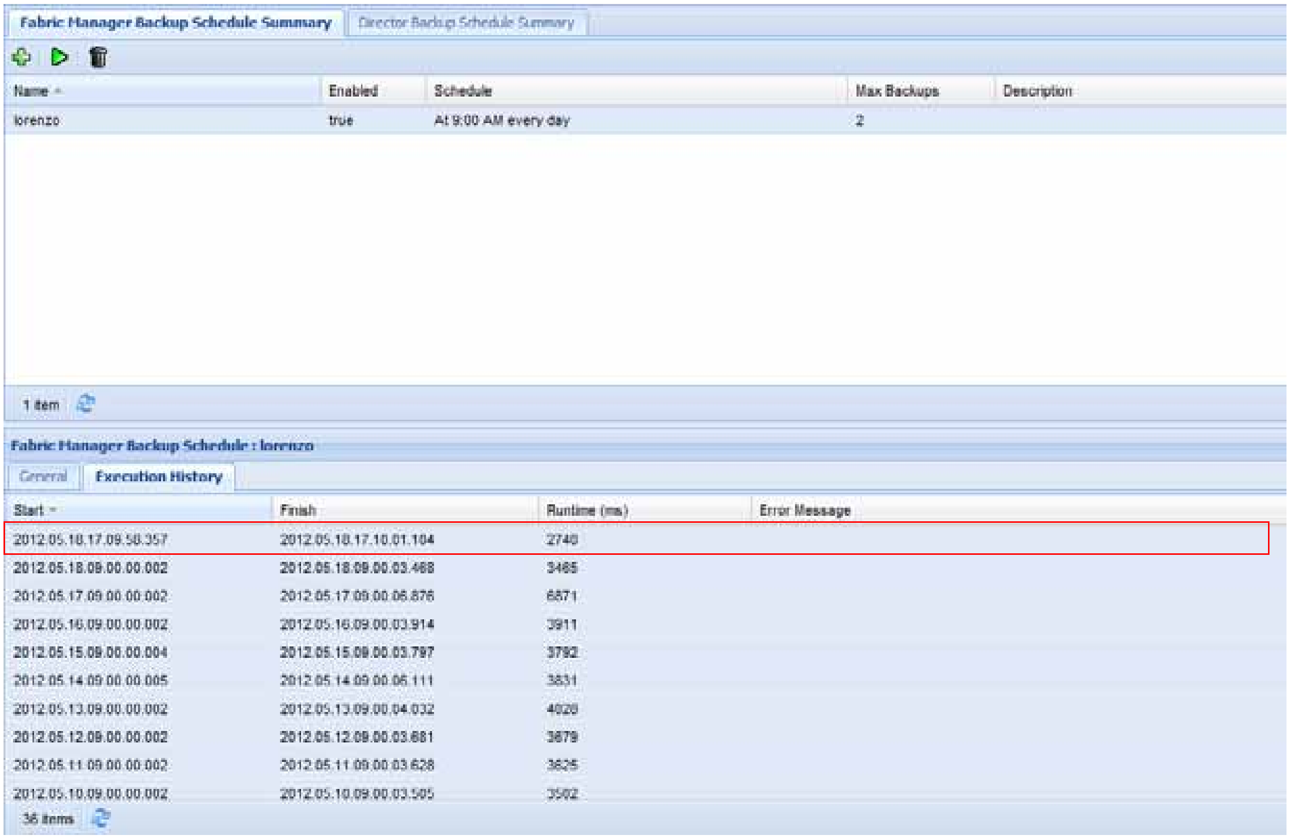
Name	Enabled	Schedule	Max Backups	Description
lorenzo	true	At 9:00 AM every day	2	

Executing selected Fabric Manager Backups right now. Continue?

Figure 8 Execute Fabric Manager Server Backups Confirmation Dialog

Step 4 On the popup dialog, click ***Yes*** to continue. The backup will complete after clicking ***Yes***.

Step 5 Click the *Execution History* tab to verify that the backup completed successfully. The absence of an error message on the *Execution History* tab indicates that the operation completed successfully. See Figure 9.


Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary
1 item
Fabric Manager Backup Schedule : lorenzo
General
Execution History
36 items

Name	Enabled	Schedule	Max Backups	Description
lorenzo	true	At 9:00 AM every day	2	

Start	Finish	Runtime (ms)	Error Message
2012.05.18.17.09.50.357	2012.05.18.17.10.01.104	2740	
2012.05.18.09.00.00.002	2012.05.18.09.00.03.468	3465	
2012.05.17.09.00.00.002	2012.05.17.09.00.06.876	6871	
2012.05.16.09.00.00.002	2012.05.16.09.00.03.914	3911	
2012.05.15.09.00.00.004	2012.05.15.09.00.03.797	3792	
2012.05.14.09.00.00.005	2012.05.14.09.00.06.111	3831	
2012.05.13.09.00.00.002	2012.05.13.09.00.04.032	4028	
2012.05.12.09.00.00.002	2012.05.12.09.00.03.681	3679	
2012.05.11.09.00.00.002	2012.05.11.09.00.03.628	3625	
2012.05.10.09.00.00.002	2012.05.10.09.00.03.505	3502	

Figure 9 Fabric Manager Server Backup Schedule — Execution History

Note

By default, entries in the execution history are listed with the oldest entries at the top. To see the newest entries, you can sort the output. For information about sorting table entries, see Filtering and Sorting Table Displays.

Enabling or Disabling Fabric Manager Backup Schedules

Fabric Manager Backup Schedules are in either of the following states:

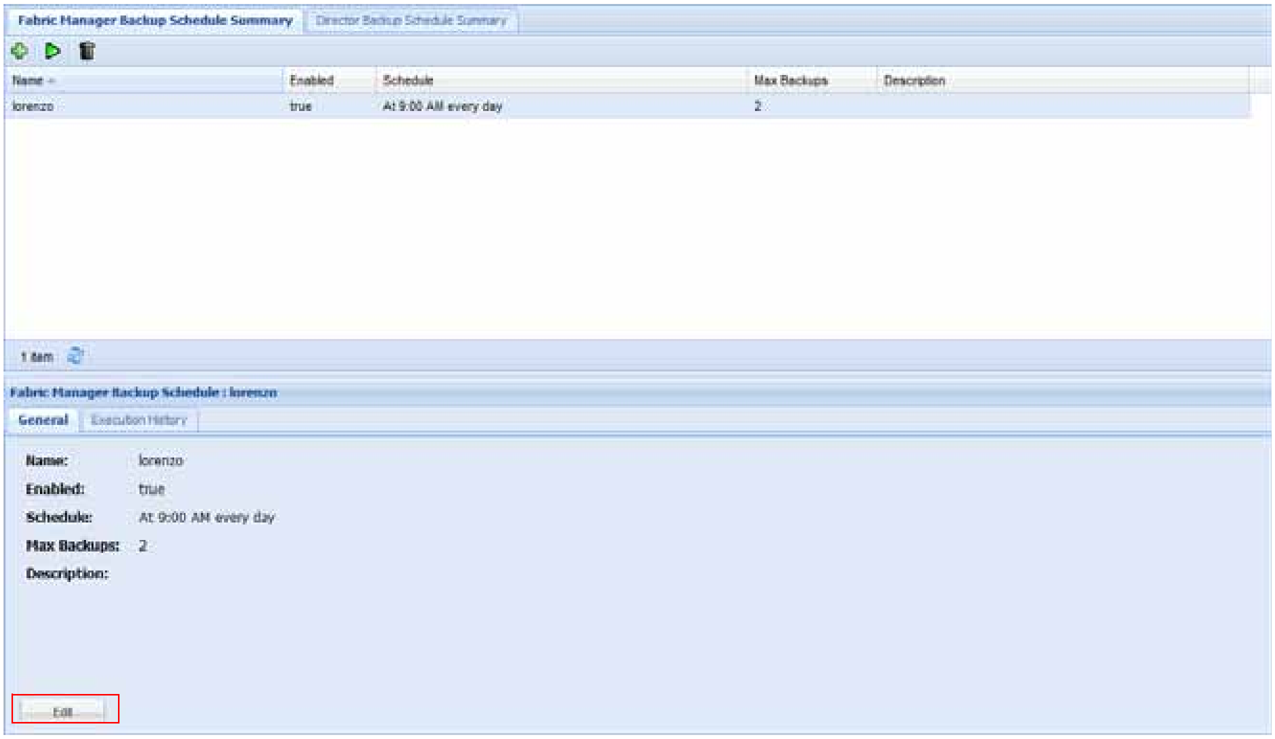
- Enabled, in which the scheduled backup will run at its designated date(s) and time(s) until the maximum number of backups has occurred.
- Disabled, in which the scheduled backup will not run until explicitly re-enabled. Even if a scheduled backup is disabled, you still can run an on-demand backup as needed.

By default, when you create a Fabric Manager Backup Schedule, it is enabled. However, you can manually disable a Fabric Manager Backup schedule, or re-enable a disabled Backup Scheduled. If you will be enabling or disabled Fabric Manager Backup Schedules, you must do so individually. Fabric Manager does not currently support a “disable all” or “enable all” option for Fabric Manager Server Backup Schedules.

You can enable or disable individual Fabric Manager backup Schedules by editing a currently configured Fabric Manager Backup Schedule:

Step 1 Display the Fabric Manager Backup Schedule Summary.

Step 2 In the Fabric Manager Backup Schedule Summary, click the backup schedule that you want to edit. This step populates the Details frame with the properties of the selected backup schedule. Figure 10 shows a sample Details frame.



Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary

Name	Enabled	Schedule	Max Backups	Description
lorenzo	true	At 9:00 AM every day	2	

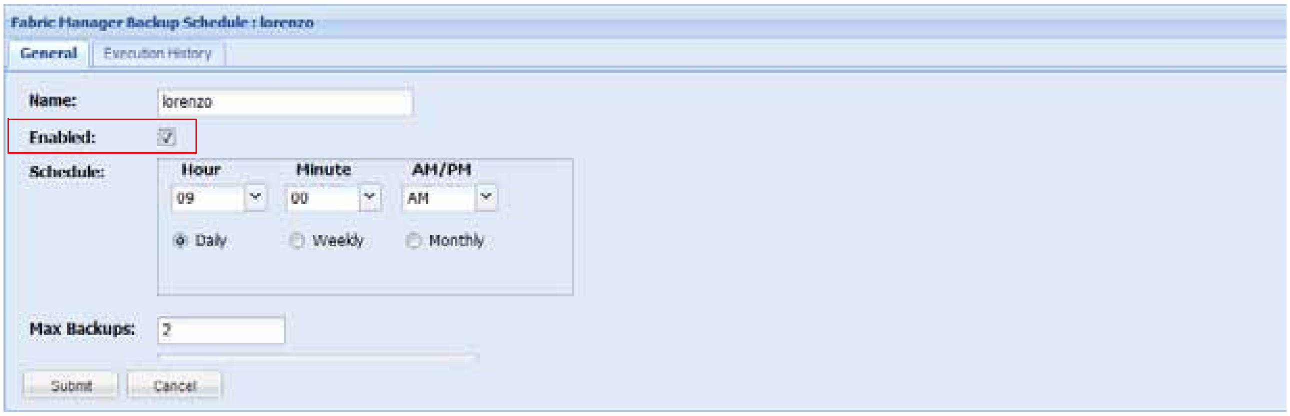
Fabric Manager Backup Schedule : lorenzo

General
Execution History

Name: lorenzo
Enabled: true
Schedule: At 9:00 AM every day
Max Backups: 2
Description:

Figure 10 Fabric Manager Backup Schedules — Details Frame

Step 3 In the Details frame, click the ***Edit*** button to unlock the properties for editing, as shown in Figure 11. This example shows editing a daily backup schedule, but similar properties (name, enable/disable, backup schedule times and dates, maximum number of backups, and description) are editable regardless of whether the backup schedule is daily, weekly, or monthly.



Fabric Manager Backup Schedule : lorenzo

Name: lorenzo
Enabled: ☑
Schedule: Hour 09 Minute 00 AM/PM AM
● Daily ○ Weekly ○ Monthly
Max Backups: 2

Figure 11 Fabric Manager Backup Schedule Details — Edit General Properties

Step 4 Click the *Enabled* checkbox to set the appropriate state for the backup schedule:

- Enabled state occurs when the *Enabled* checkbox contains a check mark. This checkbox is a toggle, so each click alternates between Enabled and Disabled.
- Disabled state occurs when the *Enabled* checkbox does not contain a check mark. This checkbox is a toggle, so each click alternates between Enabled and Disabled.

Step 5 When the appropriate properties have been edited, click ***Submit*** to save the changes.

Creating Fabric Director Backup Schedules

Through Fabric Manager, you can create a set of backup schedules for the Fabric Director(s) in your data center. A Fabric Director backup schedule sets a time(s) and date(s) on which the Fabric Director configuration is copied to a file. Each time the backup runs, the entire configuration is saved, not just the differences from an established baseline.

Also, you can keep a specific number of backups by setting the maximum number of backups to keep. This maximum number is a sliding window, so that only the last *X* number of backups is kept. For example, if you are doing weekly backups, and set a maximum of 12 backups, on the 13th week that backup is deleted and only the last 12 are kept.

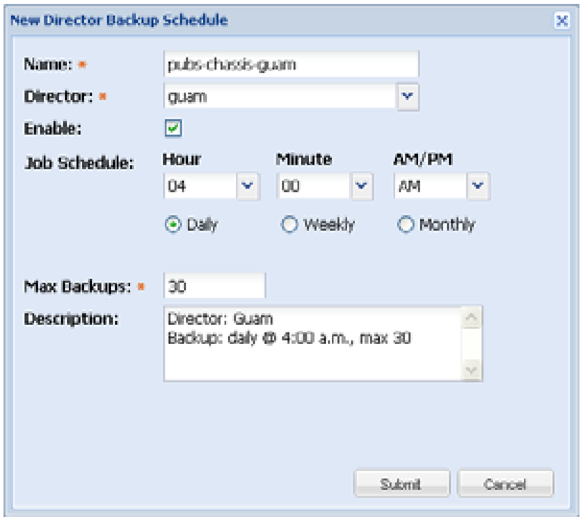
To backup the Fabric Director config, you set a schedule for when the config is backed up and copied to the `director-backups` directory. The following backup schedules are supported, and you can configure more than one type for the same Fabric Director:

- daily
- weekly
- monthly

To create a Fabric Director backup schedule, follow this procedure, which uses a weekly backup schedule for illustrative purposes:

Step 1 Display the Director Schedule Summary. Figure 1 shows the Fabric Director Schedule Summary.

Step 2 Click the plus sign to displayed the New Director Backup Schedule dialog. Figure 12 shows this dialog.



New Director Backup Schedule

Name: * pubs-chassis-guam

Director: * guam

Enable: ☑

Job Schedule: Hour 04 Minute 00 AM/PM AM

● Daily ○ Weekly ○ Monthly

Max Backups: * 30

Description: Director: Guam
Backup: daily @ 4:00 a.m., max 30

Figure 12 New Director Backup Schedule — Create Schedule

Step 3 In the *Name* field, enter an alphanumeric character string that identifies the backup schedule.

Step 4 From the *Director* dropdown menu, select the Fabric Director for which you will be creating the backup schedule. If the Fabric Director is not displayed, it has not yet been discovered by Fabric Manager.

Step 5 In the *Enable* checkbox, make sure that the backup schedule is enabled.

Or, as an option, if you want to create the schedule without it being active, you can click to deselect the checkbox. When the checkbox is empty, the backup schedule is disabled.

Step 6 In the *Job Schedule* section, select the hour, minute, and a.m. or p.m. designation for when the backup will run. You must enter additional information if you are creating a weekly or monthly backup schedule:

- For a weekly schedule, you will also need to specify the day(s) on which the backup will run at the specified time(s) (hour, minute, a.m. or p.m.).
- For a monthly schedule, you will also need to select a date(s) of the month on which the backup will run at the specified time(s). The date(s) you select is applied to all months, so be aware of the implications of the date(s) that you select. For example, selecting the 30th of the month is acceptable in months that have 30 or 31 days. However, in February, the backup will not occur on the 30th since that month does not have 30 days. In this example, the backup would not run in February, but would resume in March.

Step 7 In the *Max Backups* field, enter a number from 1 to 99999 that quantifies the maximum number of backups that will occur for the backup schedule that you are creating. The maximum backups number you enter sets the size of the sliding window, so that only the last X number of backups is kept. For example, if you are doing daily backups, and have set a maximum of 5, on the sixth day that backup is deleted so that only the most recent 5 backups are kept.

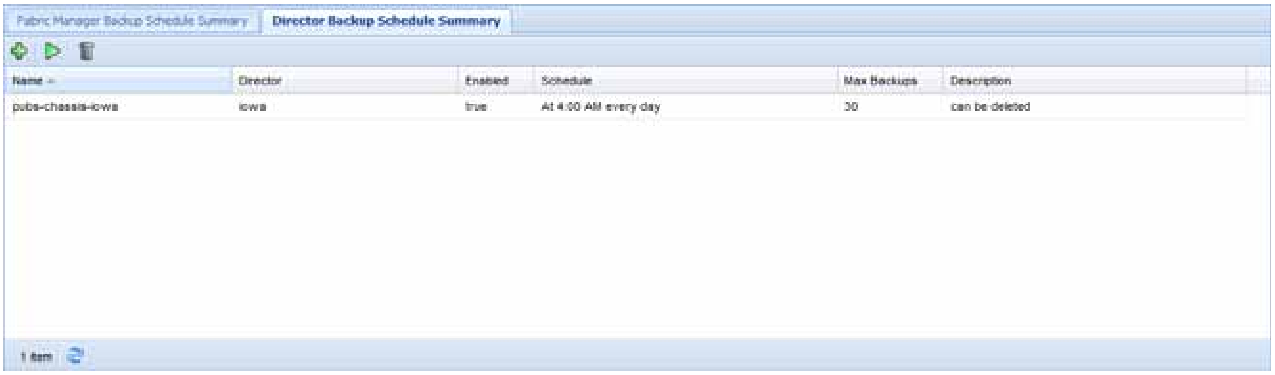
Step 8 As an option, in the *Description* field, enter a description for the backup schedule that you are configuring.

Step 9 When the backup schedule properties are configured, click ***Submit***. The schedule is not created until you click ***Submit***.

Displaying Fabric Director Backup Schedules

Fabric Manager displays the backup schedules for the Fabric Director in the Fabric Director Schedule Summary, which is a tabbed display. The Director Schedule Summary contains a list of all the configured backup schedules, regardless of their operational state (enabled or disabled).

The Director Schedule Summary is available through Schedules option on the Navigation Panel. Figure 13 shows an example of the Director Schedule Summary tab.



Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary

Name	Director	Enabled	Schedule	Max Backups	Description
pubs-chassis-iowa	iowa	true	At 4:00 AM every day	30	can be deleted

Figure 13 Director Backup Schedule Summary

The Director Schedule Summary contains information about configured backup schedules for Fabric Directors. Table 2 shows the contents of the Director Backup Schedule Summary and explains what each field means.

Table 2 Contents of Director Backup Schedule Summary

Field...	Means...
Name	The name assigned to the specific Director Backup schedule.
Director	The name of the Fabric Director that will be backed up.
Enabled	The operational state (either enabled or disabled) for a particular Director Backup schedule.
Schedule	The specific day(s), time(s), or date(s) on which the backup will run.
Max Backups	The maximum number of backups that are allowed for each particular Director Backup Schedule.
Description	An optional alphanumeric string that describes a Director Backup Schedule.

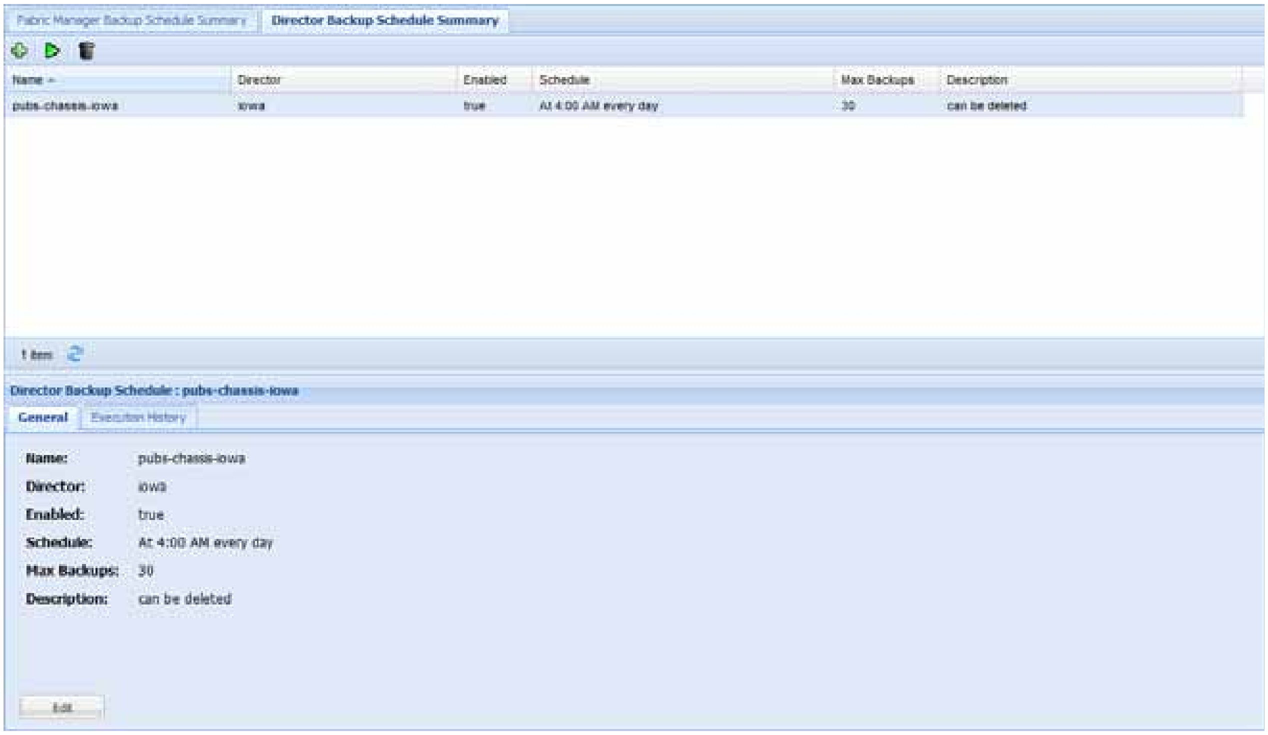
Editing Director Backup Schedules

When a backup schedule is created for a Fabric Director, it can be edited at any time. When the edits are completed and the details frame is locked for editing, the new changes take effect based on the new properties. For example, if you had a daily backup schedule set to occur at 7:00 a.m., but decided to set the backup to occur at 3:00 a.m. instead, the new backup will occur at 3:00 a.m. the next morning after you complete edits. Of course, you can always use the on-demand backup feature, to complete an instantaneous backup at any time.

To edit a configured Director Backup schedule, follow this procedure:

Step 1 Display the Director Backup Schedule Summary.

Step 2 In the Director Backup Schedule Summary, click the backup schedule that you want to edit. This step populates the Details frame with the properties of the selected backup schedule. Figure 14 shows a sample Details frame.



Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary

Name	Director	Enabled	Schedule	Max Backups	Description
pubs-chassis-iowa	iowa	true	At 4:00 AM every day	30	can be deleted

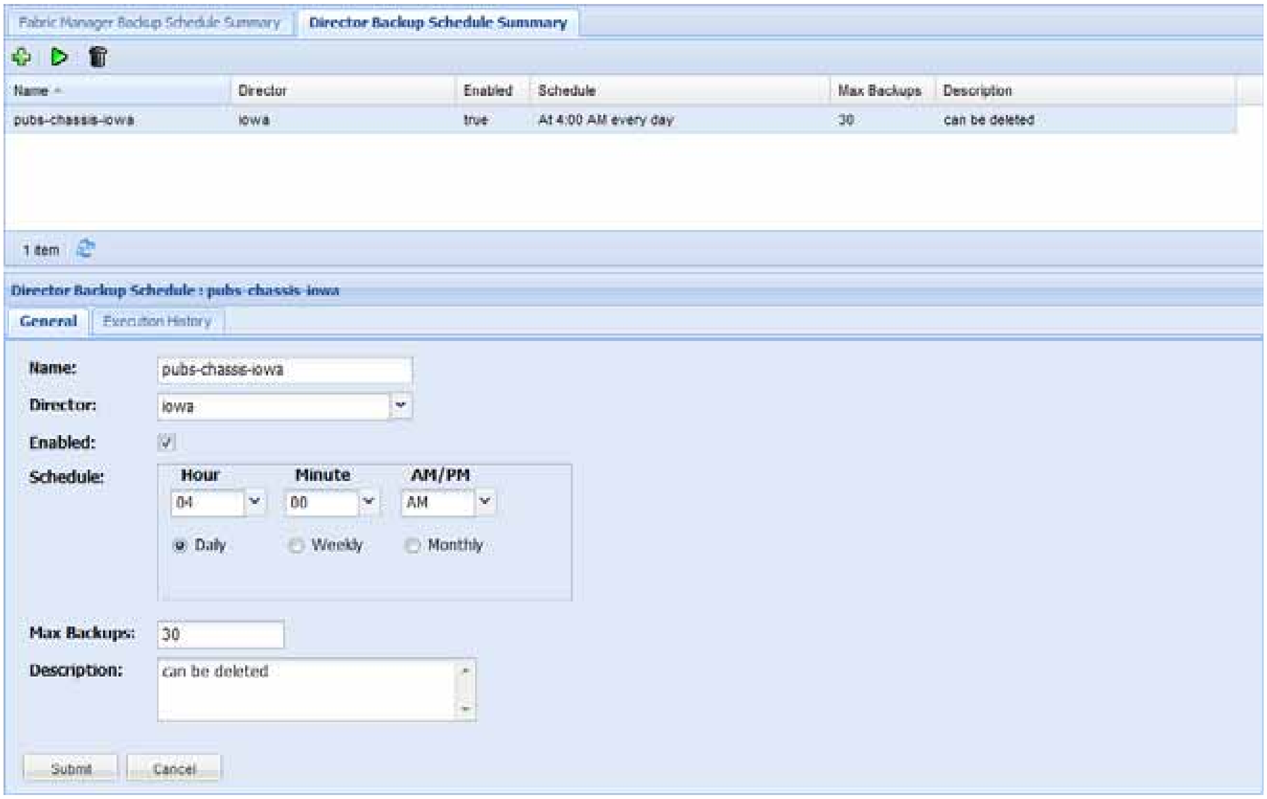
Director Backup Schedule : pubs-chassis-iowa

General
Execution History

Name: pubs-chassis-iowa
Director: iowa
Enabled: true
Schedule: At 4:00 AM every day
Max Backups: 30
Description: can be deleted

Figure 14 Director Backup Schedules — Details Frame

Step 3 In the Details frame, click the ***Edit*** button to unlock the properties for editing, as shown in Figure 15. This example shows editing a daily backup schedule, but similar properties (name, enable/disable, backup schedule times and dates, maximum number of backups, and description) are editable regardless of whether the backup schedule is daily, weekly, or monthly.



Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary

Name	Director	Enabled	Schedule	Max Backups	Description
pubs-chassis-iowa	iowa	true	At 4:00 AM every day	30	can be deleted

1 item

Director Backup Schedule : pubs-chassis-iowa

General
Execution History

Name: pubs-chasse-iowa

Director: iowa

Enabled: ☑

Schedule: Hour 04 Minute 00 AM/PM AM

● Daily ○ Weekly ○ Monthly

Max Backups: 30

Description: can be deleted

Figure 15 Director Backup Schedule Details — Edit General Properties

Step 4 Edit the properties as needed.

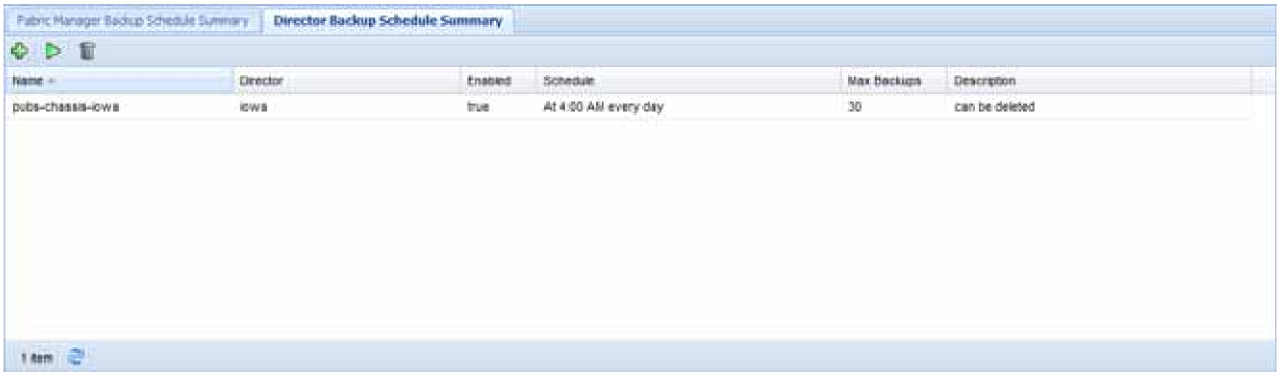
Step 5 When the properties are set correctly, click ***Submit***. The new properties do not take effect unless the ***Submit*** button is clicked.

Renaming Director Backup Schedules

Fabric Manager supports renaming a Director Backup Schedule, which enables you to change the name without having to completely delete and recreate the entire Director Backup Schedule. When the Director Backup Schedule is renamed, all other properties for the Director Backup Schedule are retained, including the schedule and Director(s) affected. As an option, you can also set or change the description for the Director Backup Schedule.

You can rename the Director Backup Schedule through the Director Backup Schedule Details frame. To rename the Director Backup Schedule, follow this procedure:

Step 1 On the Navigation Frame, select *Service Manager->Schedules*. Figure 16 shows the Director Backup Schedule Summary.

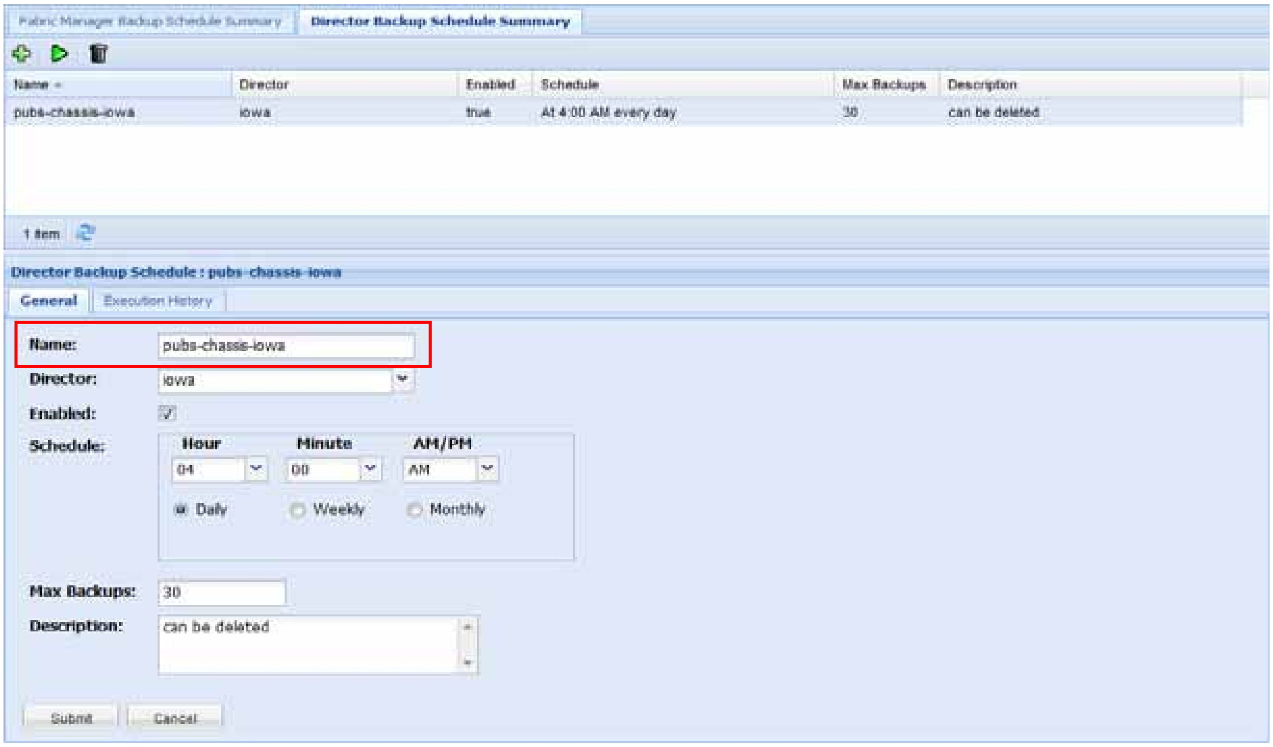

Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary

Name	Director	Enabled	Schedule	Max Backups	Description
pubs-chassis-iowa	iowa	true	At 4:00 AM every day	30	can be deleted

Figure 16 Director Backup Schedule Summary

Step 2 Select a Director Backup Schedule to populate the details frame with its properties.

Step 3 Click the ***Edit*** button to edit the properties of the selected Director Backup Schedule, as shown in Figure 17.


Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary

Name	Director	Enabled	Schedule	Max Backups	Description
pubs-chassis-iowa	iowa	true	At 4:00 AM every day	30	can be deleted

1 item
Director Backup Schedule : pubs-chassis-iowa
General
Execution History

Name: pubs-chassis-iowa

Director: iowa

Enabled: ☑

Schedule: Hour 04 Minute 00 AM/PM AM

● Daily ○ Weekly ○ Monthly

Max Backups: 30

Description: can be deleted

Figure 17 Director Backup Schedule Details — Edit General Properties

Step 4 In the *Name* field, enter the new name for the Director Backup Schedule.

Step 5 As an option, you also can set or change the description for the selected Director Backup Schedule.

Step 6 When the new name has been specified for the Director Backup Schedule, click ***Submit***.

Running an On-Demand Fabric Director Backup

An on-demand Director Backup is one that you manually start. On-demand backups can be completed at any time, and they are in addition to any scheduled backups.

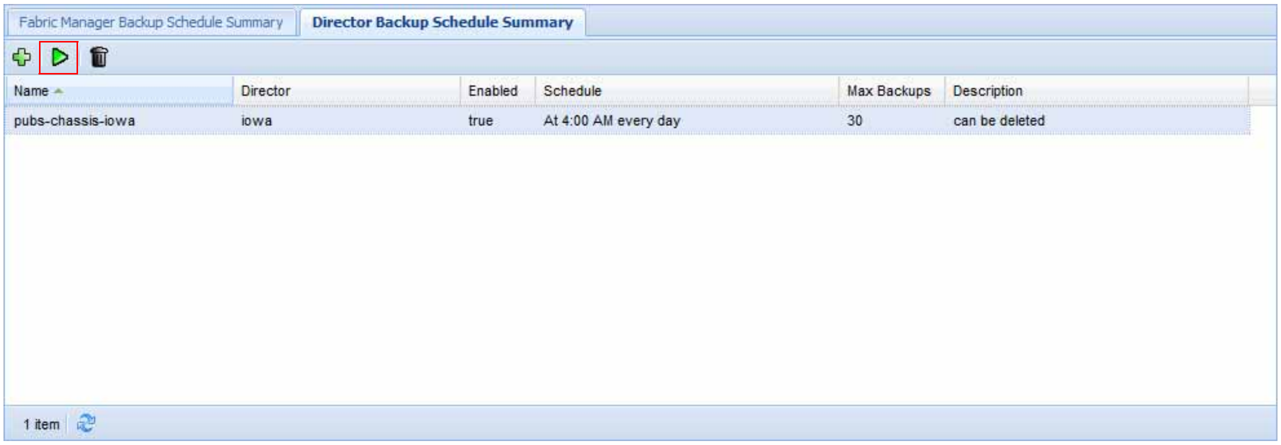
An on-demand backup runs for a configured backup schedule, just not at the scheduled time(s). As a result, a backup schedule must exist for the Director that you want to backup on an on-demand basis.

You can run an on-demand Director backup through the Director Backup Schedule Summary tab.

To run an on-demand Director backup, follow this procedure:

Step 1 Display the Director Backup Schedule Summary.

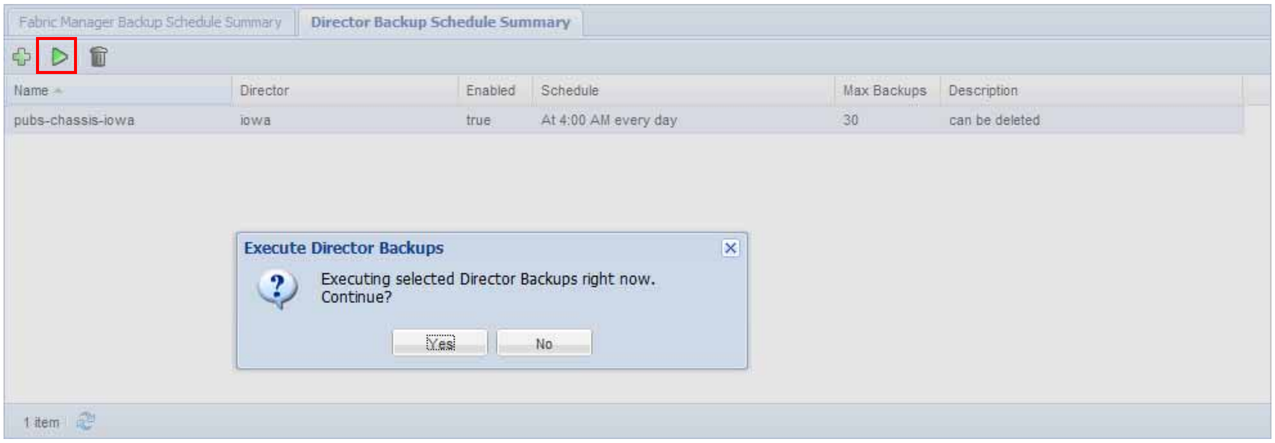
Step 2 Select the backup schedule that you want to run on an on-demand basis. This step activates the ***Execute Now*** button, which is the green arrow on the Director Backup Schedule Summary toolbar. See Figure 18.


Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary
1 item

Name	Director	Enabled	Schedule	Max Backups	Description
pubs-chassis-iowa	iowa	true	At 4:00 AM every day	30	can be deleted

Figure 18 Director Backup Schedule Summary — On-Demand Backup

Step 3 Click the ***Execute Now*** button to begin the backup. A confirmation popup dialog is displayed, as shown in Figure 19.


Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary

Name	Director	Enabled	Schedule	Max Backups	Description
pubs-chassis-iowa	iowa	true	At 4:00 AM every day	30	can be deleted

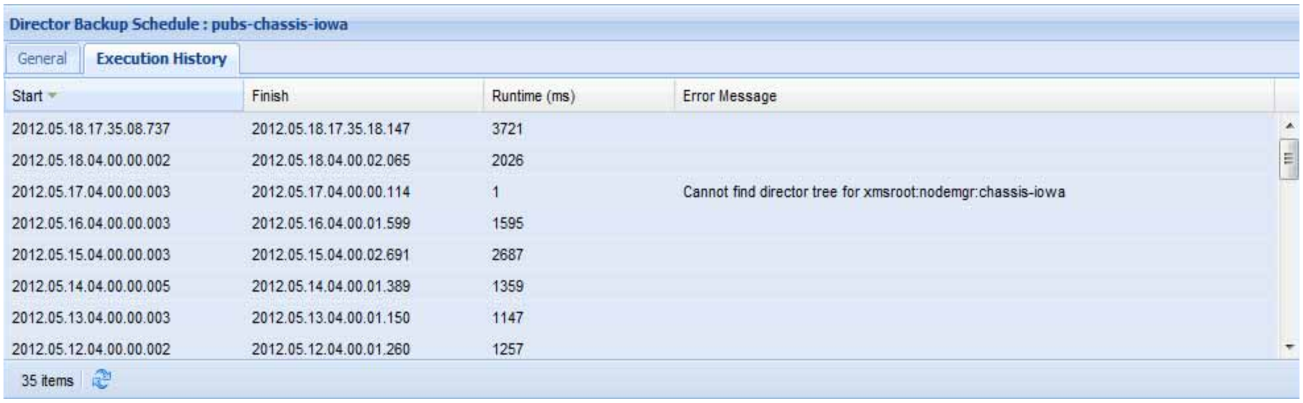
Execute Director Backups

Executing selected Director Backups right now.
Continue?

Figure 19 Execute Director Backups Confirmation Dialog

Step 4 On the popup dialog, click ***Yes*** to continue. The backup will complete after clicking ***Yes***.

Step 5 Click the *Execution History* tab to verify that the backup completed successfully. The absence of an error message on the *Execution History* tab indicates that the operation completed successfully. See Figure 20.


Director Backup Schedule : pubs-chassis-iowa

Start	Finish	Runtime (ms)	Error Message
2012.05.18.17.35.08.737	2012.05.18.17.35.18.147	3721	
2012.05.18.04.00.00.002	2012.05.18.04.00.02.065	2026	
2012.05.17.04.00.00.003	2012.05.17.04.00.00.114	1	Cannot find director tree for xmsroot:nodemgr:chassis-iowa
2012.05.16.04.00.00.003	2012.05.16.04.00.01.599	1595	
2012.05.15.04.00.00.003	2012.05.15.04.00.02.691	2687	
2012.05.14.04.00.00.005	2012.05.14.04.00.01.389	1359	
2012.05.13.04.00.00.003	2012.05.13.04.00.01.150	1147	
2012.05.12.04.00.00.002	2012.05.12.04.00.01.260	1257	

Figure 20 Director Backup Schedule — Execution History

Note

By default, entries in the execution history are listed with the oldest entries at the top. To see the newest entries, you can sort the output. For information about sorting table entries, see Filtering and Sorting Table Displays.

Enabling or Disabling Fabric Director Backup Schedules

Fabric Director backup schedules are in either of the following states:

- Enabled, in which the scheduled backup will run at its designated date(s) and time(s) until the maximum number of backups has occurred.
- Disabled, in which the schedule backup will not run until explicitly re-enabled.

By default, when you create a Director Backup Schedule, it is enabled. However, you can manually disable a Director Backup schedule, or re-enable a disabled Backup Scheduled. If you will be enabling or disabled Director Backup Schedules, you must do so individually. Oracle's Xsigo Fabric Manager does not currently support a disable all or enable all option for Oracle's Xsigo Fabric Director Server Backup Schedules.

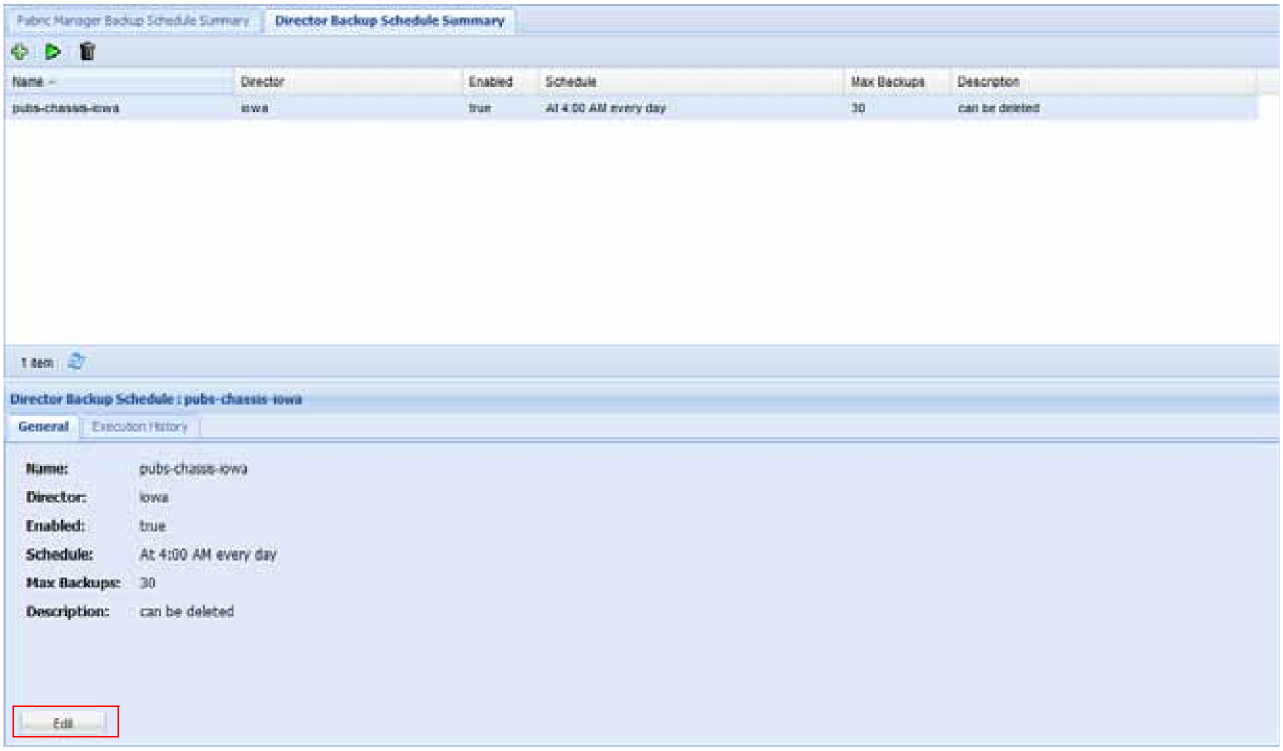
Note

Even if a backup schedule is disabled, you still can run an on-demand backup as needed.

You can enable or disable individual Director Backup Schedules by editing a currently configured Director Backup Schedule:

Step 1 Display the Director Backup Schedule Summary.

Step 2 In the Director Backup Schedule Summary, click the backup schedule that you want to edit. This step populates the Details frame with the properties of the selected backup schedule. Figure 21 shows a sample Details frame.



Fabric Manager Backup Schedule Summary
Director Backup Schedule Summary

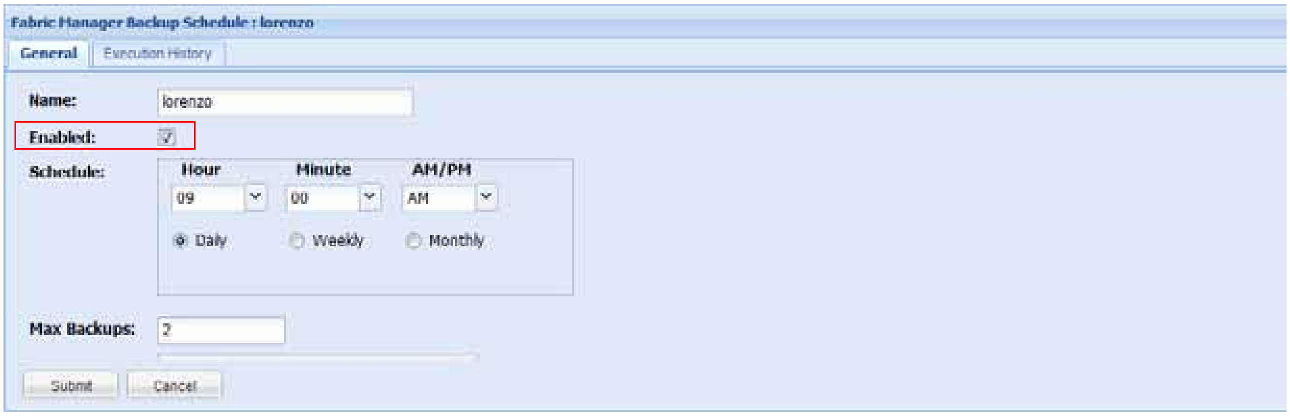
Name	Director	Enabled	Schedule	Max Backups	Description
pubs-chassis-iowa	iowa	true	At 4:00 AM every day	30	can be deleted

1 item
Director Backup Schedule : pubs-chassis-iowa
General
Execution History

Name: pubs-chassis-iowa
Director: iowa
Enabled: true
Schedule: At 4:00 AM every day
Max Backups: 30
Description: can be deleted

Figure 21 Director Backup Schedules — Details Frame

Step 3 In the Details frame, click the ***Edit*** button to unlock the properties for editing, as shown in Figure 22. This example shows editing a daily backup schedule, but similar properties (name, enable/disable, backup schedule times and dates, maximum number of backups, and description) are editable regardless of whether the backup schedule is daily, weekly, or monthly.



Name: lorenzo
Enabled: ☑
Schedule: Hour 09 Minute 00 AM/PM AM
● Daily ○ Weekly ○ Monthly
Max Backups: 2

Figure 22 Director Backup Schedule Details — Edit General Properties

Step 4 Click the *Enabled* checkbox to set the appropriate state for the backup schedule:

- *Enabled* state occurs when the *Enabled* checkbox contains a check mark. This checkbox is a toggle, so each click alternates between Enabled and Disabled.
- *Disabled* state occurs when the *Enabled* checkbox does not contain a check mark. This checkbox is a toggle.

Working with LUN Masks

This chapter documents the following topics:

- Understanding LUN Masks
- Creating LUN Masks
- Displaying LUN Masks
- Adding LUNs to an Existing LUN Mask
- Removing LUNs from the LUN Mask

Understanding LUN Masks

LUN Masks enable you to zone out specific LUNs or storage targets from servers or initiators. With LUN Masks, you can keep security in the storage network by keeping LUNs that contain sensitive data in a private, restricted section of the Fibre Channel network.

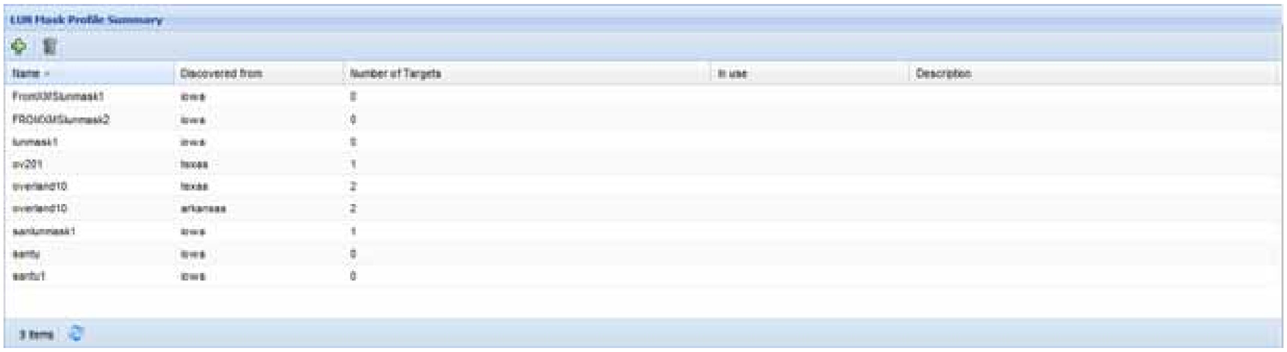
Through Oracle's Xsigo Fabric Manager, LUN Masks are created and applied to vHBAs to determine which hosts can see which storage resources. A LUN Mask must be associated with a vHBA to control whether or not the LUNs are reported. If you create a LUN Mask, but do not associate it with one or more vHBAs, all hosts will be able to see all storage resources.

Creating LUN Masks

LUN Masks are created through the LUN Mask Summary, and must be created before they can be assigned to a vHBA. The LUN Mask will be assigned to individual vHBAs, not the Storage Cloud that provides vHBA terminations.

To create a LUN Mask, follow this procedure:

Step 1 Select *Storage Cloud Manager->LUN Mask Profiles* to display the LUN Mask Summary. Figure 1 shows this dialog.



LUN Mask Profile Summary

Name	Discovered from	Number of Targets	In use	Description
FromXMSlunmask1	iowa	0		
FROMXMSlunmask2	iowa	0		
lunmask1	iowa	0		
ov201	texas	1		
overland10	texas	2		
overland10	arkansas	2		
sanlunmask1	iowa	1		
santu	iowa	0		
santu1	iowa	0		

9 items

Figure 1 LUN Mask Profile Summary

You can add a new LUN Mask by clicking the plus sign (+), and you can delete one or more LUN Masks by selecting them in the LUN Mask Profile Summary, then clicking the garbage can icon.

Step 2 Click the plus sign to display the Create LUN Mask Profile Dialog. Figure 2 shows this dialog.

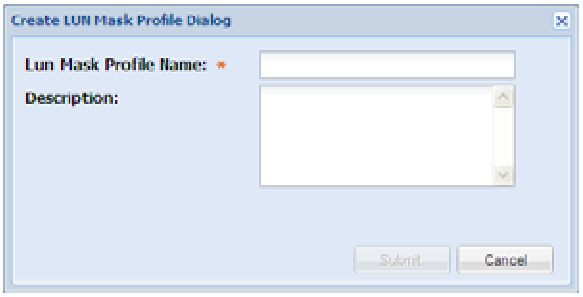


Figure 2 Create LUN Mask Profile

Step 3 In the *LUN Mask Profile Name* field, enter an alphanumeric string that names the LUN Mask Profile that you are creating.

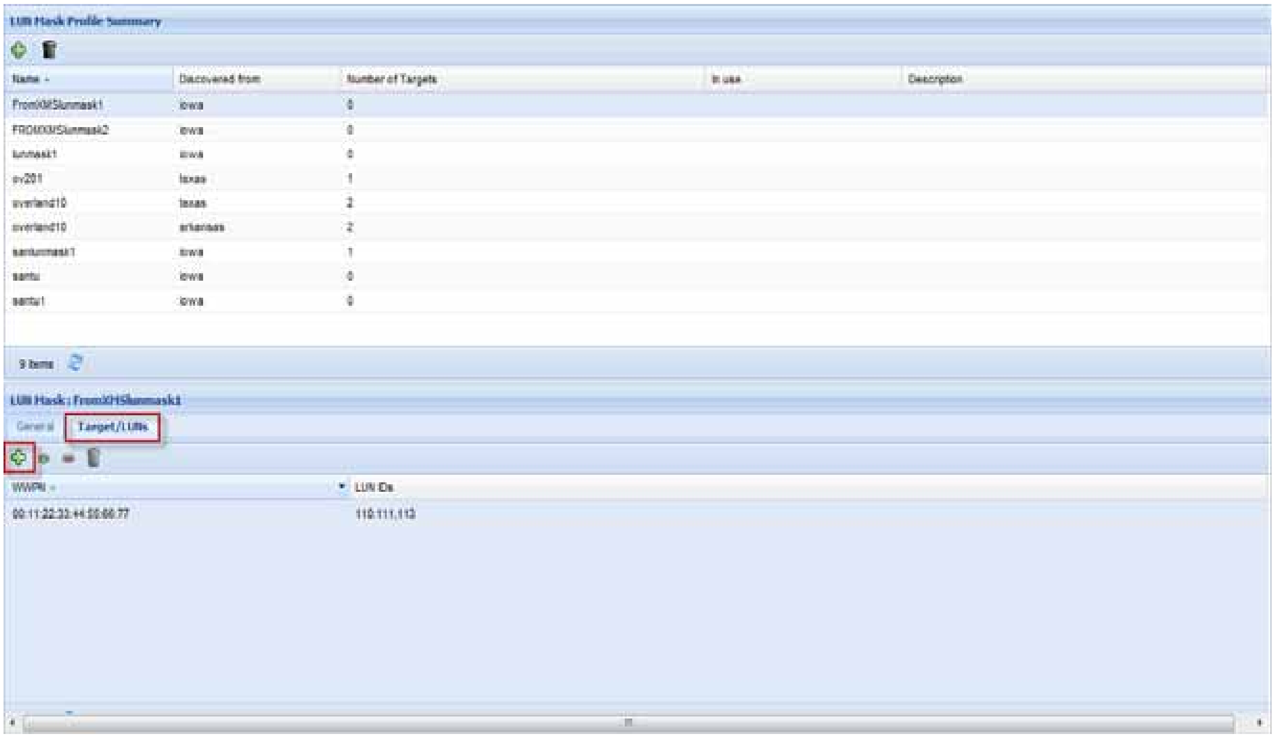
Step 4 As an option, in the *Description* field, enter an alphanumeric string that describes the LUN Mask Profile that you are creating.

Step 5 Click ***Submit*** to create the LUN Mask Profile.

Note

At this point, the LUN Mask Profile exists, but it is an empty profile. You will need to populate the empty LUN Mask with individual records that determine the WWN and LUN IDs to which the LUN Mask will be applied.

Step 6 When the LUN Mask Profile has been created, select it in the LUN Mask Profile Summary. By selecting it, the LUN Mask Profile is displayed in the LUN Mask Profile Details frame, as shown in Figure 3.



LUN Mask Profile Summary

Name	Discovered from	Number of Targets	In use	Description
FromXMSlunmask1	iowa	0		
FROMXMSlunmask2	iowa	0		
lunmask1	iowa	0		
ov201	texas	1		
overland10	texas	2		
overland10	arkansas	2		
santumask1	iowa	1		
santu	iowa	0		
santu1	iowa	0		

9 items

LUN Mask : FromXMSlunmask1

WWPN	LUN IDs
00:11:22:33:44:55:66:77	110,111,113

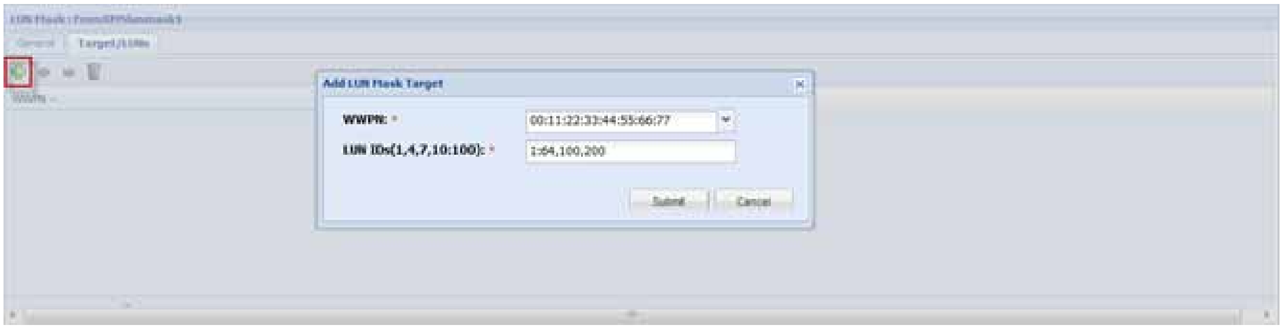
Figure 3 LUN Mask Profile — Targets and LUNs

You can add target WWPN and LUN information for a storage resource by clicking the plus sign, and you can delete one or more WWPN and LUN entries by selecting the entry in on the *Target/LUNs* tab, then clicking the garbage can icon.

By default, when the selected LUN Mask is displayed in the details frame, the *General* tab is displayed.

Step 7 Click the *Target/LUNs* tab as shown in Figure 3.

Step 8 On the *Target/LUNs* tab, click the plus sign to display the Add LUN Mask Target dialog. Figure 4 shows this dialog.



Add LUN Mask Target

WWPN: * 00:11:22:33:44:55:66:77

LUN IDs(1,4,7,10:100): * 1:64,100,200

Figure 4 LUN Mask Profile — Add LUN Mask Target

Step 9 In the *WWPN* field, enter the world-wide port number for the storage resource you want added to the LUN Mask Profile.

Step 10 In the *LUN IDs* field, enter the LUN number(s) for the storage resource you want added to the LUN Mask Profile. Multiple LUN numbers can be specified as either a comma-separated list, or a range of LUNs can be specified by using a colon (:) as a separator.

Step 11 Click ***Submit*** to configure the target and LUN(s) in the selected LUN Mask Profile.

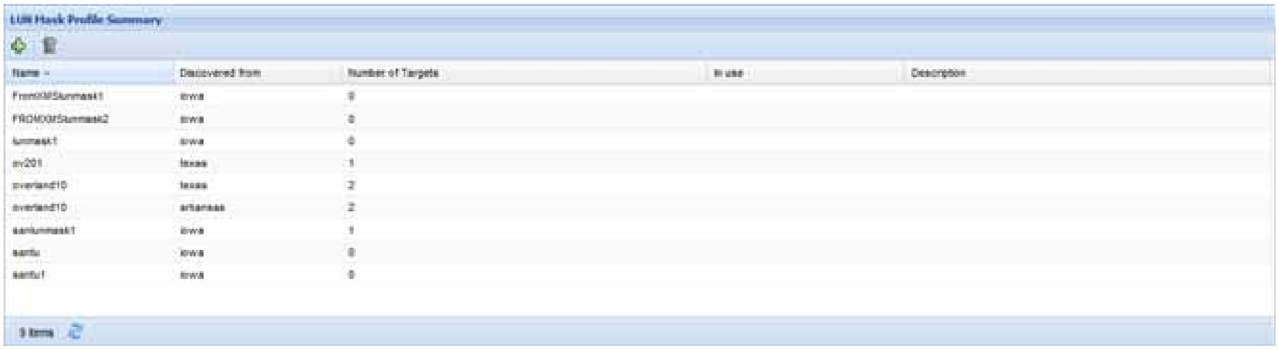
Step 12 Check the *Target/LUNs* tab to verify that the correct WWPN and LUN entry was added to the selected LUN Mask Profile. You can also check the LUN Mask Profile Summary to verify that the “Number of Targets” column has incremented (or decremented if you are deleting one or more entries) by the number of entries you are adding or deleting.

Displaying LUN Masks

When LUN Mask Profiles are configured, you can display them through the LUN Mask Profiles Summary, which is a table of all LUN Mask Profiles configured in Fabric Manager. Additional, detailed information about individual LUN Mask Profiles and their contents is available in the LUN Mask Profiles Details frame below the LUN Mask Profile Summary.

Displaying LUN Mask Profile Summary

The LUN Mask Profile Summary contains all configured LUN Mask Profiles in Oracle’s Xsigo Fabric Manager regardless of whether they are assigned to a Storage Cloud. Figure 5 shows the LUN Mask Profile summary.



LUN Mask Profile Summary

Name	Discovered from	Number of Targets	In use	Description
FromXMSlunmask1	iowa	0		
FROMXMSlunmask2	iowa	0		
lunmask1	iowa	0		
ov201	texas	1		
overland10	texas	2		
overland10	arkansas	2		
sanlunmask1	iowa	1		
santu	iowa	0		
santu1	iowa	0		

9 items

Figure 5 LUN Mask Profile Summary

Table 1 shows the contents of the LUN Mask Profile Summary and explains what each field means.

Table 1 Contents of the LUN Mask Summary

Field	Indicates
Name	The name of each configured LUN Mask Profile.
Discovered From	The name of the Oracle Xsigo Fabric Director that discovered storage target in the LUN Mask Profile.
Number of Targets	The number of storage targets contained in each LUN Mask.
In Use	The state of the LUN Mask with regard to whether or not it is used by an I/O Profile that is deployed to a host server. If no value is displayed, the LUN Mask is configured but not actually in use on a server.
Description	The description string (if any) that was applied to the LUN Mask Profile. If this field is blank, either no description string was specified when the LUN Mask Profile was created, or the LUN Mask Profile was originally created with a description string, but the LUN Mask Profile was later edited and the description string was removed.

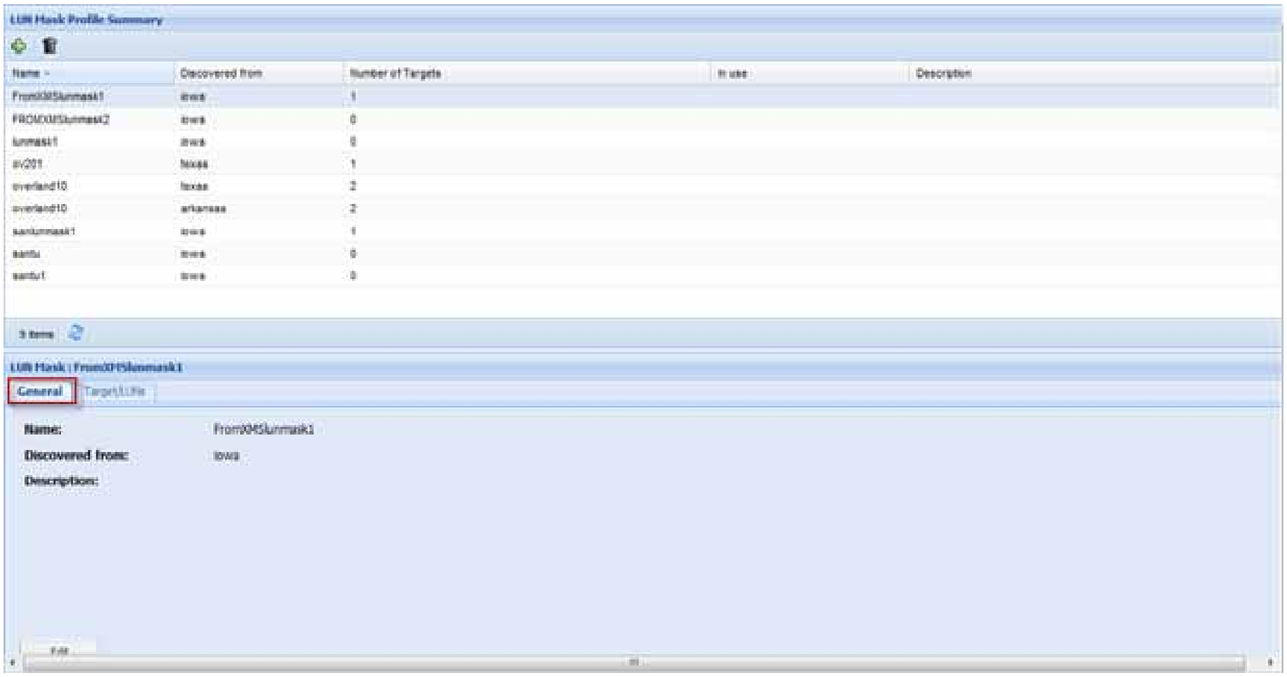
Displaying LUN Mask Profile Details

The LUN Mask Profile Details frame is a section of the work panel that is located below the LUN Mask Profile Summary. This frame is a list of fields for a selected LUN Mask Profile.

The LUN Mask Profile Details frame enables you to display additional, detailed information for a single LUN Mask Profile and contains an ***Edit*** button, which unlocks editable parts of the details frame so that you can set or change information elements of the details frame.

To use the LUN Mask Profile Details frame, you must first select a configured LUN Mask Profile from the LUN Mask Profile Summary. By selecting a LUN Mask Profile from the summary, you provide an element that will be the focus of the LUN Mask Profile Details frame.

Figure 6 shows the LUN Mask Profile Details frame. Notice that the details frame is contextual, so that it displays detailed information for the item selected in the LUN Mask Profile Summary.



LUN Mask Profile Summary

Name	Discovered from	Number of Targets	In use	Description
FromXMSlunmask1	iowa	1		
FROMXMSlunmask2	iowa	0		
lunmask1	iowa	0		
sv201	texas	1		
overland10	texas	2		
overland10	arkansas	2		
sanlunmask1	iowa	1		
santu	iowa	0		
santu1	iowa	0		

9 items

LUN Mask : FromXMSlunmask1

Name: FromXMSlunmask1
Discovered from: iowa
Description:

Figure 6 LUN Mask Profile Details

Adding LUNs to an Existing LUN Mask

Through the LUN Mask Details frame, you can add one or more LUNs to the an existing LUN Mask as needed. When LUNs are added to the target mask, they will be masked as needed.

Note

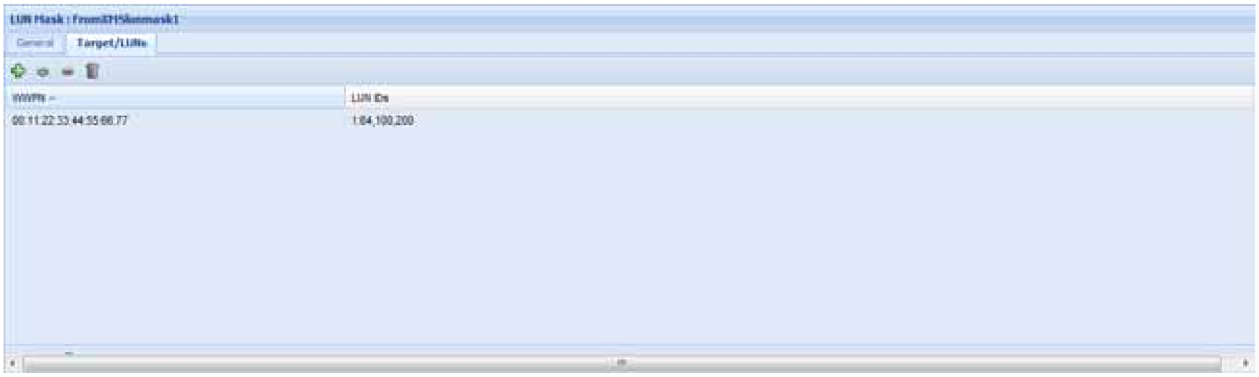
Adding LUNs to a LUN Mask might require a rescan of the vHBA, which is supported through a toolbar button (the satellite dish) on the *vHBAs* tab of the Physical Server details page.

To add LUNs to a specified target, follow this procedure:

Step 1 Display the LUN Mask Summary.

Step 2 Select a LUN Mask from the summary to highlight it. This step populates the LUN Mask Details frame with additional details for the selected LUN Mask.

Step 3 Click the *Target/LUNs* tab, as shown in Figure 7.



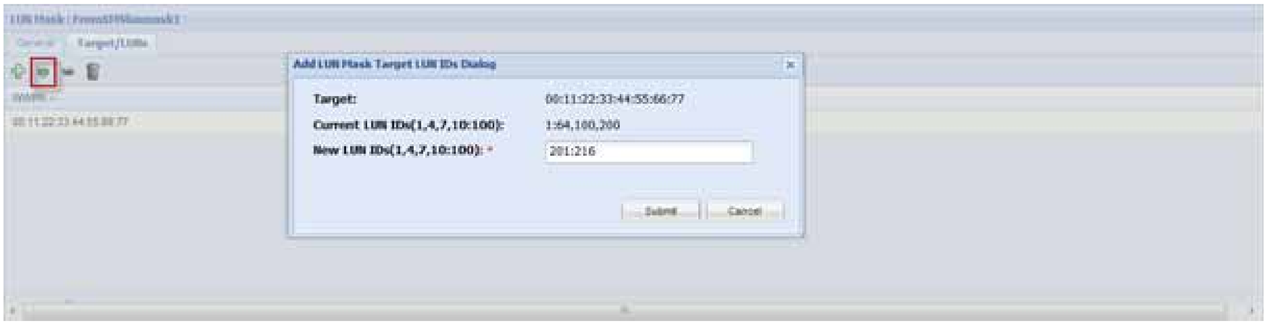
LUN Mask : FromEHPSlunmask1

WWPN	LUN IDs
00:11:22:33:44:55:66:77	1:64,100,200

Figure 7 LUN Mask Detail — Target/LUNs Tab

Step 4 On the *Target/LUNs* tab, click the WWPN for which you want to add more LUNs to the LUN Mask. This step activates the ***Add LUNs to Target*** button.

Step 5 Click the ***Add LUN IDs to the Selected Target*** button to display the Add LUN Mask Target LUN IDs dialog as shown in Figure 8.



Add LUN Mask Target LUN IDs Dialog

Target: 00:11:22:33:44:55:66:77

Current LUN IDs(1,4,7,10:100): 1:64,100,200

New LUN IDs(1,4,7,10:100): * 201:216

Figure 8 LUN Mask Details — Add LUN IDs to LUN Mask

Step 6 In the *New LUN IDs* field, enter the LUN ID(s) that you want to add to the existing LUN Mask. Any LUNs already configured in the LUN Mask are kept, and the LUNs you specified are added to the mask. A single LUN can be added, or multiple LUNs can be added by specifying a comma-separated list, or a hyphenated range of LUNs.

Step 7 When the LUN(s) are specified, click ***Submit*** to update the LUNs in the LUN Mask.

Removing LUNs from the LUN Mask

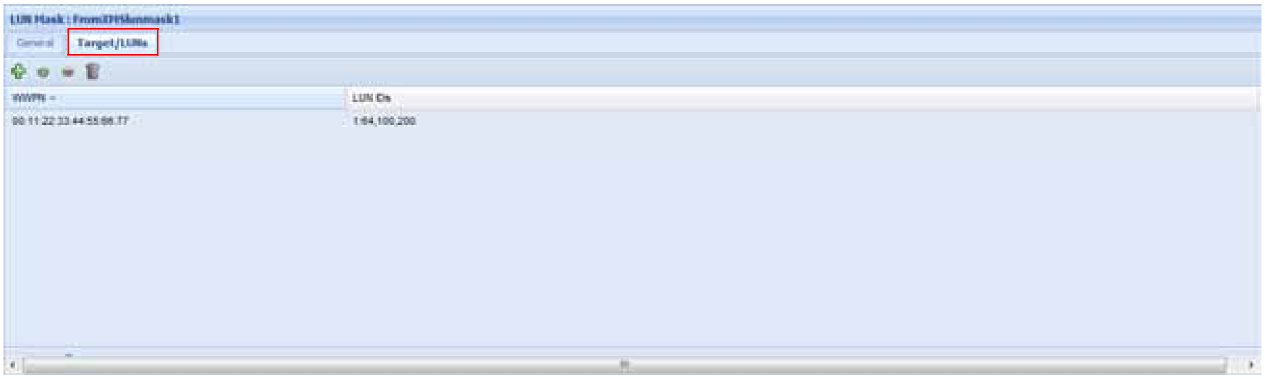
Through the LUN Mask Details frame, you can remove one or more LUNs from an existing LUN Mask as needed. When LUNs are removed from the target mask, they will no longer be masked. Removing LUNs from a LUN Mask might require a rescan of the vHBA. If the LUNs are removed, but are still being masked, you can attempt to rescan the vHBA from the Physical Server details frame (*Server Resource Manager->Physical Server* details frame->*vHBAs* tab ->***Prescan/Rescan for Fibre Channel***).

To remove LUNs from an existing LUN Mask, follow this procedure:

Step 1 Display the LUN Mask Summary.

Step 2 Select a LUN Mask from the summary to highlight it. This step populates the LUN Mask Details frame with additional details for the selected LUN Mask.

Step 3 Click the *Target/LUNs* tab, as shown in Figure 9.



WWPN	LUN IDs
00:11:22:33:44:55:66:77	1,64,100,200

Figure 9 LUN Mask Detail — Target/LUNs Tab

Step 4 On the *Target/LUNs* tab, click the WWPN for which you want to add more LUNs to the LUN Mask. This step activates the ***Add LUNs to Target*** button.

Step 5 Click the ***Remove LUNs IDs from Selected Target*** button to display the ***Add LUN Mask Target LUN IDs*** dialog as shown in figure Figure 10.

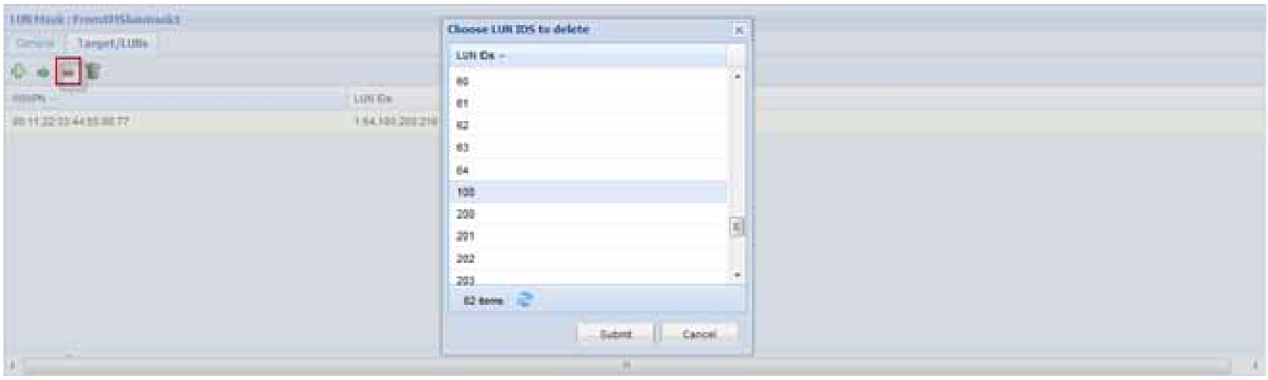


Figure 10 LUN Mask Detail — Delete LUN IDs from LUN Mask

Step 6 From the Choose LUN IDs to Delete dialog, click as many LUNs as you want to delete from the LUN Mask.

Step 7 Click ***Submit*** to remove the LUNs from the LUN Mask.

Working with SAN QoS

This chapter documents the following topics:

Understanding SAN QoS

A SAN QoS Profile allows you to place bandwidth usage parameters on a Storage Cloud so that specific amounts of traffic are allowed, or specific amounts of the throughput is available. SAN QoS is enforced by a shaper profile, which attempts to guarantee bandwidth by controlling traffic through delaying and queuing frames that exceed the Committed Information Rate (CIR) value you set. When you configure a SAN QoS Profile on a Storage Cloud or vHBA, you are assigning shaping parameters to the read and write data that affect the host server that uses that Storage Cloud.

The SAN QoS Profile uses Committed Information Rate (CIR) to guarantee bandwidth.

You can assign one SAN QoS Profile to a Storage Cloud or vHBA, and you can assign the same SAN QoS Profile to multiple, different Storage Clouds or vHBAs. For more information about SAN QoS on a Storage Cloud as opposed a vHBA, see QoS Assignment at Cloud Level and vHBA Level.

Pre-defined SAN QoS profiles are supplied by Xsigo in different bandwidth configurations to facilitate QoS use on Storage Cloud(s) or vHBAs.

Understanding Default SAN QoS Profiles

Oracle's Xsigo Fabric Manager contains default SAN QoS Profiles, which are pre-configured for efficient bandwidth availability and resource usage. You can apply the default SAN QoS profiles directly to a Storage Cloud or a vHBA.

Default SAN QoS Profiles are pre-configured in Fabric Manager for application to Storage Clouds or vHBAs. Fabric Manager supports the following default SAN QoS Profiles:

- 50M_125M (50 Mbps CIR and 125 Mbps PIR)
- 125M_250m (125 Mbps CIR and 250 Mbps PIR)
- 250M_500M (250 Mbps CIR and 500 Mbps PIR)
- 500M_1G (500 Mbps CIR and 1 Gbps PIR)
- 1G_2G (1 Gbps CIR and 2 Gbps PIR)
- 2G_4G (2 Gbps CIR and 4 Gbps PIR)
- 4G_8G (4 Gbps CIR and 8 Gbps PIR)

When you are binding a SAN QoS Profile to a Storage Cloud, you can select a default QoS Profile from the list of all available QoS Profiles for that particular module.

Displaying SAN QoS Profiles

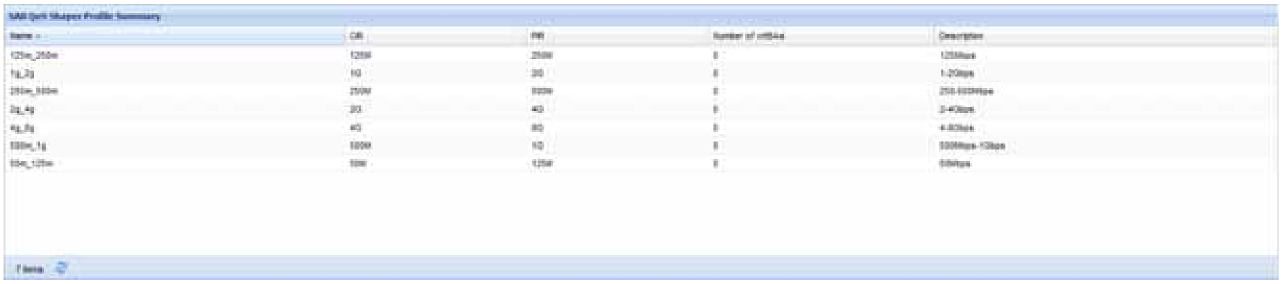
When SAN QoS Profiles are assigned, you can display them through the SAN QoS Summary, which is a table of all SAN QoS Profiles configured in Fabric Manager. Additional, detailed information about individual SAN QoS Profiles is available in the SAN QoS Profile Details frame below the SAN QoS Profile Summary.

Displaying the SAN QoS Summary

The SAN QoS Summary contains all configured SAN QoS Profiles in Oracle's Xsigo Fabric Manager regardless of whether they are assigned to a Storage Cloud or a vHBA.

To display the SAN QoS Summary, follow this procedure:

Step 1 Display the SAN QoS Summary by selecting *Storage Cloud Manager->SAN QoS*. Figure 1 shows the SAN QoS Summary.



SAN QoS Shaper Profile Summary

Name	CIR	PIR	Number of vHBAs	Description
125m_250m	125M	250M	0	125Mbps
1g_2g	1G	2G	0	1-2Gbps
250m_500m	250M	500M	0	250-500Mbps
2g_4g	2G	4G	0	2-4Gbps
4g_8g	4G	8G	0	4-8Gbps
500m_1g	500M	1G	0	500Mbps-1Gbps
50m_125m	50M	125M	0	50Mbps

7 items

Figure 1 SAN QoS Summary

Table 1 shows the contents of the SAN QoS Summary and explains what each field means.

Table 1 Contents of the SAN QoS Summary

Field	Indicates
Name	The name of each configured SAN QoS Profile.
CIR	The committed information rate, which is the amount of guaranteed bandwidth for constant traffic.
PIR	The peak information rate, which is the maximum amount of total bandwidth that can be consumed by traffic.
Number of vHBAs	The total number of vHBAs that each SAN QoS Profile is attached to.
Description	The description string (if any) that was applied to the SAN QoS Profile. If this field is blank, either no description string was specified when the SAN QoS Profile was created, or the SAN QoS Profile was originally created with a description string, but the SAN QoS Profile was later edited and the description string was removed.

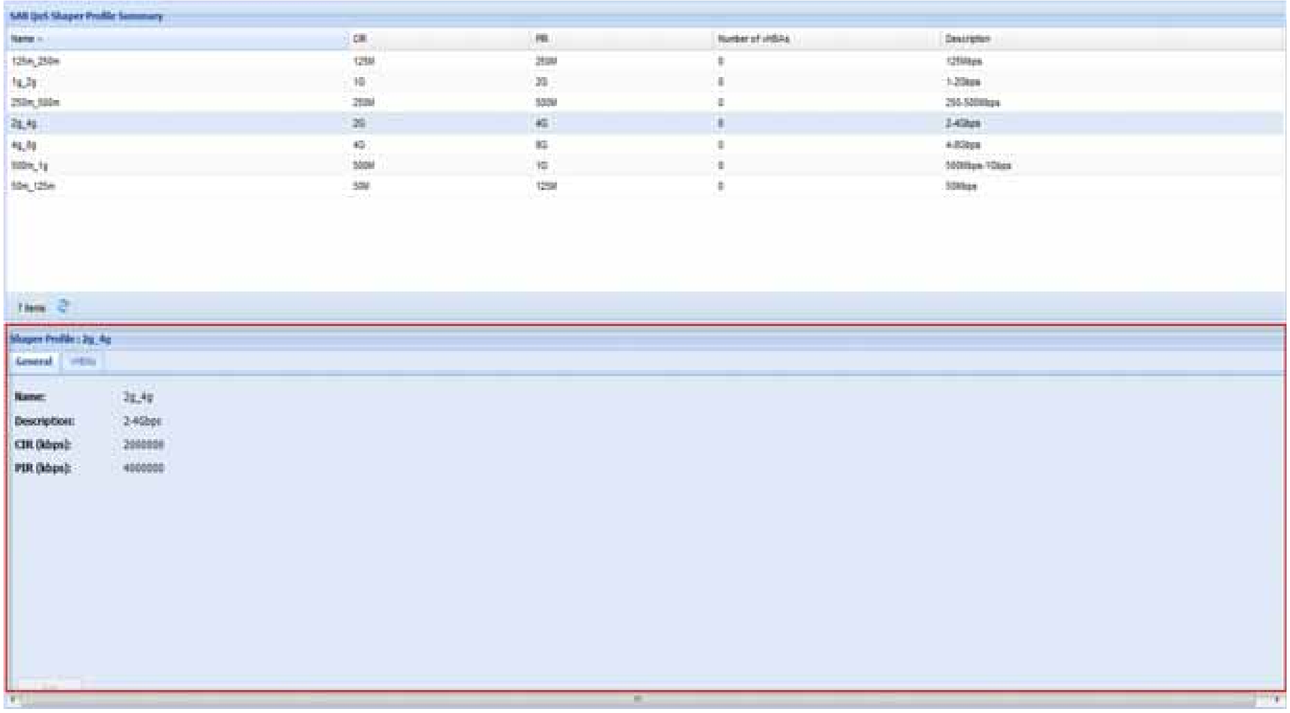
Displaying the SAN QoS Details

The SAN QoS Profile Details frame is a section of the work panel that is located below the SAN QoS Profile Summary. This frame is a list of fields for a selected SAN QoS Profile that shows the CIR that shapes bandwidth usage on the vHBA.

The SAN QoS Profile Details frame enables you to display additional, detailed information for a single SAN QoS Profile and contains an ***Edit*** button, which unlocks editable parts of the details frame so that you can set or change information elements of the details frame.

To use the SAN QoS Profile Details frame, you must first select a configured SAN QoS Profile from the SAN QoS Profile Summary. By selecting a SAN QoS Profile from the summary, you set the focus of the SAN QoS Profile Details frame. When the SAN QoS Profile is selected in the summary, you will see its details displayed in the Details frame.

Figure 2 shows the SAN QoS Profile Details frame. Notice that the details frame is contextual, so that it displays detailed information for the item selected in the Storage Cloud Summary.



SAN QoS Shaper Profile Summary

Name	CIR	PIR	Number of vHBAs	Description
125m_250m	125M	250M	0	125Mbps
1g_2g	1G	2G	0	1-2Gbps
250m_500m	250M	500M	0	250-500Mbps
2g_4g	2G	4G	0	2-4Gbps
4g_8g	4G	8G	0	4-8Gbps
500m_1g	500M	1G	0	500Mbps-1Gbps
50m_125m	50M	125M	0	50Mbps

7 items

Shaper Profile : 2g_4g

Name: 2g_4g

Description: 2-4Gbps

CIR (kbps): 2000000

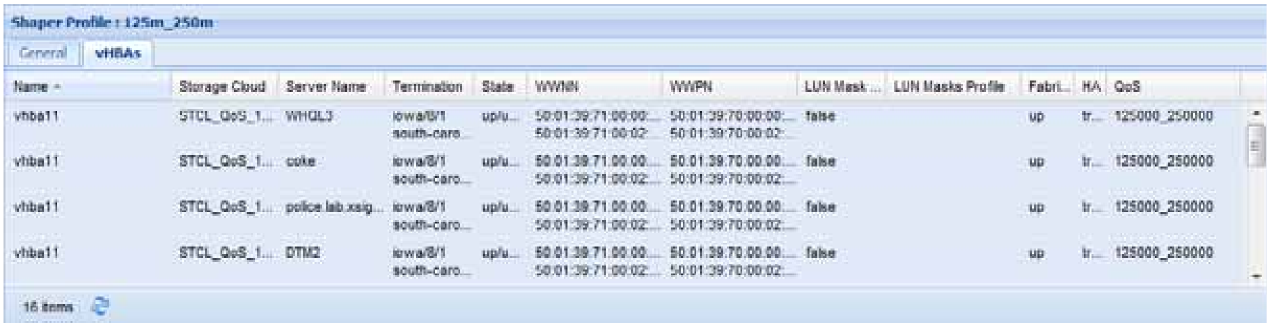
PIR (kbps): 4000000

Figure 2 SAN QoS Profile Details Frame

Displaying the vHBAs Associated with a SAN QoS Profile

The *vHBAs* tab displays a summary of all the vHBAs that are currently associated with the selected SAN QoS Profile. If the Number of vHBAs field on the SAN QoS Shaper Profile Summary shows a non-zero value, you can use the *vHBAs* tab to display information about which vHBAs are using the selected SAN QoS Profile.

Figure 3 shows an example of the vHBAs associated with a SAN QoS Profile.



Shaper Profile : 125m_250m

Name	Storage Cloud	Server Name	Termination	State	WWNN	WWPN	LUN Mask ...	LUN Masks Profile	Fabri...	HA	QoS
vhba11	STCL_QoS_1...	WHQL3	iowa/8/1 south-caro...	up/u...	50:01:39:71:00:00:... 50:01:39:71:00:02:...	50:01:39:70:00:00:... 50:01:39:70:00:02:...	false		up	tr...	125000_250000
vhba11	STCL_QoS_1...	coke	iowa/8/1 south-caro...	up/u...	50:01:39:71:00:00:... 50:01:39:71:00:02:...	50:01:39:70:00:00:... 50:01:39:70:00:02:...	false		up	tr...	125000_250000
vhba11	STCL_QoS_1...	police.lab.xsig...	iowa/8/1 south-caro...	up/u...	50:01:39:71:00:00:... 50:01:39:71:00:02:...	50:01:39:70:00:00:... 50:01:39:70:00:02:...	false		up	tr...	125000_250000
vhba11	STCL_QoS_1...	DTM2	iowa/8/1 south-caro...	up/u...	50:01:39:71:00:00:... 50:01:39:71:00:02:...	50:01:39:70:00:00:... 50:01:39:70:00:02:...	false		up	tr...	125000_250000

16 items

Figure 3 SAN QoS Details — *vHBAs* Tab

Working with Domains

This chapter contains the following topics:

Understanding Resource Domains

Oracle's Xsigo Fabric Director, Oracle's Xsigo Fabric Manager Server, physical servers, and Network and Storage Clouds reside in domains, which are logical groupings of resources in the network. Typically, domains are arranged by a functional group, such as a business unit or department, but domains can be created with virtually any theme—a lab domain, a production domain, a domain of top-quality hardware, a domain of mid-quality hardware, a domain of services or applications, and so on.

Fabric Manager enables you to create the individual domains within your network by carving out the resources required and grouping them into a needed domain. Be aware that domain boundaries are strictly enforced, so the Fabric Manager Server and the Fabric Directors it is managing must be in the same domain.

Domain Resources and Unmanaging a Fabric Director

When domains are created, they can be configured with specific resources—for example, Fabric Directors, users, clouds, and I/O Modules. If a domain contains specific resources (including a Fabric Director), and that Fabric Director is unmanaged and remanaged, the individual resources (including the Fabric Director) are not automatically put back into the respective domain(s). In this situation, the resources that were assigned to a domain(s) are put into the default domain.

The individual domain(s) still exist but will not be populated with the resources present before the unmanage operation. This behavior occurs by design to add speed and flexibility in reassigning resources in real time. By clearing the resources from their previous domain, they can be quickly reassigned to new domains as needed. Be aware that if you intend the same resources to be put back into the domain(s) that contained them before the Fabric Director was unmanaged, you must manually re-assign the resources to the correct domains.

Understanding the Default Domain

By default, all resources discovered and managed by Fabric Manager reside in the default domain, which exists without any need to configure it. However, when you create additional domains, you are pulling resources out of the default domain and adding them to the specific domain that you are creating.

The process of configuring a domain is available only to the administrator-level (i.e., root) Fabric Manager user. The domain admin user (which is used to manage individual domains) cannot create individual domains. The act of creating a domain must be done through the root or admin user of the default domain. When you log in to Fabric Manager as root, the *Security Manager->Resource Domains* option is available of the Navigation Panel. Use this option to create individual domains that will be later managed by the admin users. When the domain is created, individual resources are added to it to allow for virtual connectivity to hosts—for example, a domain might contain one or more Fabric Manager Server(s), Fabric Directors, FC and GE Switches, and hosts. When that domain and resources are created by the administrator-level (root) user, the admin user for each domain can be created to manage that domain and its subset of the overall resources.

Default Domain Users

In the default domain, users that have administrator role can create, update, or remove non-default domains. These users can also add Fabric Directors and I/O Modules to the non-default domains, as well as delete them from the non-default domains.

In a standard usage model the administrator-level user (root) is a site administrator, and the non-default administrator (domain admin) is the administrator of individual domains. For example, think of a data center that sells rack space and services to other companies. The default domain administrator (site administrator), has access and control of the Fabric

Directors and creates the individual domains for each paying company. Within the domain for each company, perhaps a few I/O Modules are available for end-to-connectivity. The I/O Modules are put into the company’s domain by the default domain administrator, and from that point the configuration of a company’s domain occurs through the non-default domain administrator for that domain.

Configuring Non-Default Domains

Non-default domains allow you to create logical partitions in order to subdivide physical environments from a configuration and management perspective. For example, you could create a sub-domain for finance, engineering, customer support, and so on. Within each of these non-default domains you can then assign host servers, Fabric Directors or I/O modules, Network Clouds, and Storage Clouds as needed to provide the connections required for each domain.

Individual non-default domains can be created by individual domain admins (admin users, not the root user). After the individual non-default domains are created by root, the individual domain admin users can then administer their domain(s). Individual non-default domains enable the Fabric Director and Fabric Manager to create individual logical partitions of resources that can be assigned and used as needed.

The following resources are available in non-default domains:

- Host servers. When the host servers are added to a non-default domain, they are available to the domain admins for that domain. The servers are not available to other users or admins from other domains.
- Fabric Directors or I/O Modules (but not both) which provide termination points for Xsigo virtual I/O. The Xsigo RBAC model supports configuring the required roles for domain administrators and users. The Fabric Directors or I/O Modules that are added to a non-default domain are not available to other users or admins from other domains. Of the users for a non-default domain, only the domain admin has rights to manage the Fabric Directors or I/O Modules.

  Fabric Directors or I/O modules that are managed by Fabric Manager, but not part of a user’s domain, cannot be managed.

  I/O Modules can be added into (or deleted from) a non-default domain as needed by the domain admin. Other functionality for I/O Modules are available to the appropriate users in that domain. For example, users with network role can administer the Network Cloud and Gigabit Ethernet I/O Modules and ports, but not Storage Clouds, SAN resources or features, or Fibre Channel cards.

  Fabric Directors and I/O Modules can be assigned to only one domain at a time, and they cannot be shared across domain boundaries.
- Network and Storage clouds. Clouds can be added to the domain by the administrator of the default domain or, the domain administrator of the sub-domain. Functionality for other features are available to the appropriate users in that domain. For example, users with the storage role can administer the Storage Cloud, Fibre Channel cards and ports, and SAN resources and features. However, they cannot administer the Network Cloud or any of its associated resources or features.

  Network and Storage Clouds can contain only the resources that are assigned to the domain, and these resources can exist in only one domain at a time including the default domain. The resources in a domain cannot be shared across multiple domains, however, a Network or Storage Cloud can be used by multiple domains.

Users can be configured in multiple domains, but a user can be logged in to only one domain at a time. For example, assume user Joe belong to the engineering and customer support domains. Joe can log in to engineering and make changes as needed. Joe can also log in to customer-support and make changes as needed, but he must first log out of engineering.

Non-Default Domain Users

Non-default domain users are those uses that can access a particular domain in the Fabric Manager management framework, but not the default domain. The most powerful user of a non-default domain is the administrator, which in a typical usage model is the domain admin. The domain administrator takes the elements that are provided to the domain by the default domain administrator (the site administrator), then uses the elements to create the required connectivity for the domain.

Users in a non-default domain have some additional rights, but also some restrictions.

Users with Administrator Role

A user with the administrator role in a non-default domain can do the following within the respective domain:

- view and make changes on all the Fabric Directors and I/O Modules in the domain.
- create, update, or delete a Network Cloud that has I/O modules that are assigned to the domain. However, Network or Storage Clouds that are shared by multiple domains cannot be modified.
- view all user role mappings in the domain.
- Add or remove any I/O Module from a Fabric Director in the domain.

The administrator of a non-default domain cannot do the following:

- Discover a new Fabric Director
- Remove a Fabric Director from a domain
- Use any options on the Fabric Manager maintenance menu. As a result, all the Maintenance menu items will be greyed out.

Users with Network Role

A user with the network role in a non-default domain can do the following within the respective domain:

- create, update, or delete a Network Cloud that has I/O modules that are assigned to the domain. However, Network that are shared by multiple domains cannot be modified.
- View the I/O Module summary for the domain. This page is relevant to the current domain only, so only those Gigabit Ethernet modules that are added to the domain will be viewable.
- Make changes to the Gigabit Ethernet modules in the domain.

A user with network role in a non-default domain can view only the Fabric Director Summary of all Fabric Directors in the domain. A list of all Fabric Directors in all domains is not accessible to the non-domain user with the Network role.

Users with Storage Role

A user with storage role in a non-default domain can do the following within the respective domain:

- create, update, or delete a Storage Cloud that has I/O modules that are assigned to the domain. However, Storage Clouds that are shared by multiple domains cannot be modified.
- View the I/O Module summary for the domain. This page is relevant to the current domain only, so only those Fibre Channel modules that are added to the domain will be viewable.
- Make changes to the Fibre Channel modules in the domain.

A user with storage role in a non-default domain can view only the Fabric Director Summary of all Fabric Directors in the domain. A list of all Fabric Directors in all domains is not accessible to the non-domain user with the Storage role.

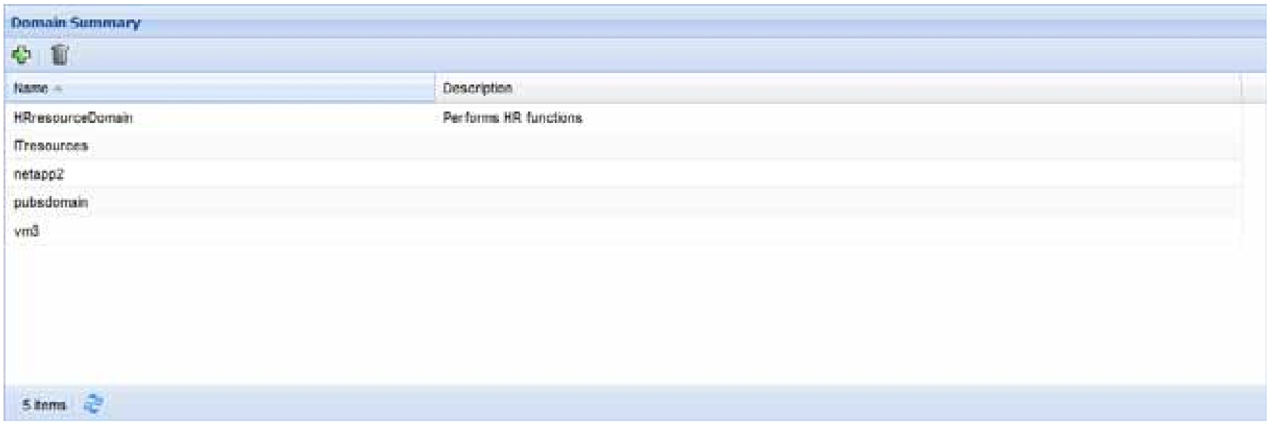
Displaying Domain Information

Domain information is available through the Domain Summary, which is a list of individual domains that are configured. The Domain Summary shows a different amount of domains depending on whether you are logged in as root or standard admin:

- as root, all configured domains are displayed (including the default domain)
- as admin, the domain(s) are displayed only if that admin user has rights to them. With this model, you can keep domain information completely separate from admin users who are not supposed to see other domains. For example, you might not want the admin for the Engineering domain seeing or having access to the Finance domain.

To display the Domain Summary, follow this procedure:

Step 1 On the Navigation panel, select *Security Manager->Resource Domains* to display the Domain Summary. This option will be available only if you are logged in with an administrator account. Figure 1 shows the Domain Summary.



Domain Summary

Name	Description
HRresourceDomain	Performs HR functions
ITresources	
netapp2	
pubsdomain	
vm3	

5 items

Figure 1 Domain Summary

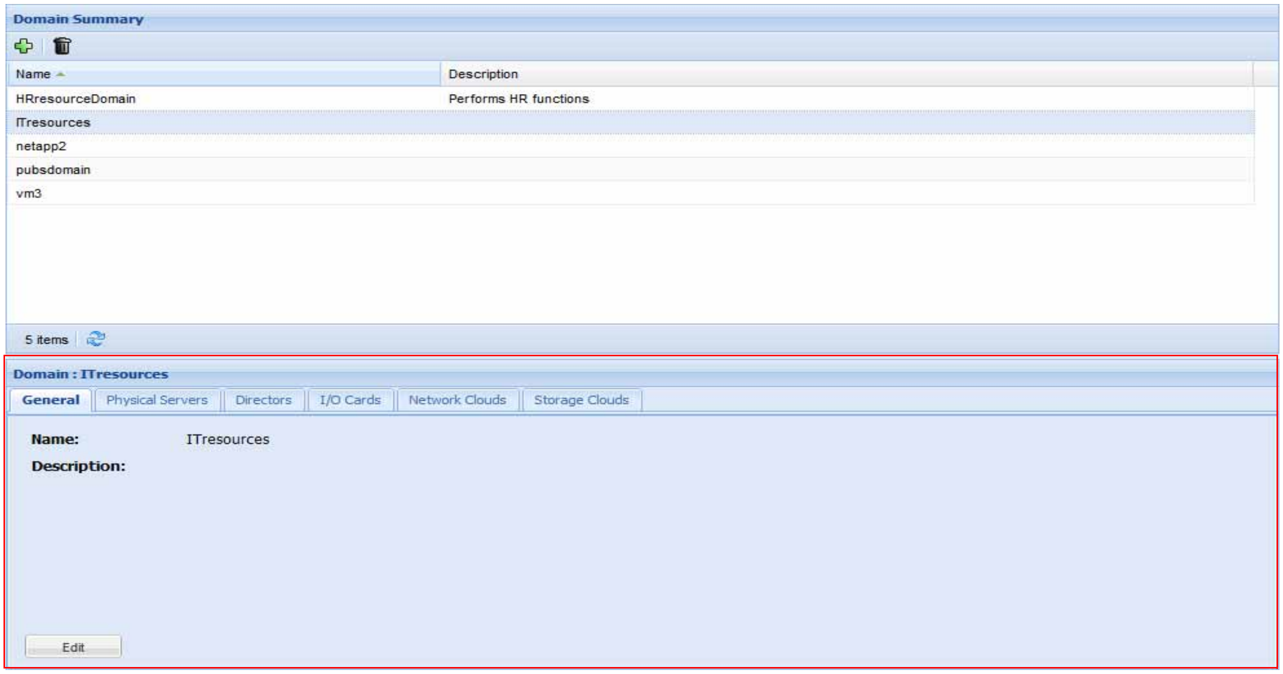
Notice that the Domain Summary contains toolbar controls to add a new domain (+) and delete an existing domain.

Displaying Detailed Information for Domains

Additional information is available for the configured domains through the Domain Details frame.

Step 1 On the Navigation panel, select *Security Manager->Resource Domains* to display the Domain Summary. This option will be available only if you are logged in with an administrator account.

Step 2 On the Domain Summary, select a configured domain to populate the Domain Details frame with information about the selected domain. Figure 2 shows the Domain Details Frame.



Name	Description
HRresourceDomain	Performs HR functions
ITresources	
netapp2	
pubsdomain	
vm3	

5 items

Domain : ITresources

Name: ITresources

Description:

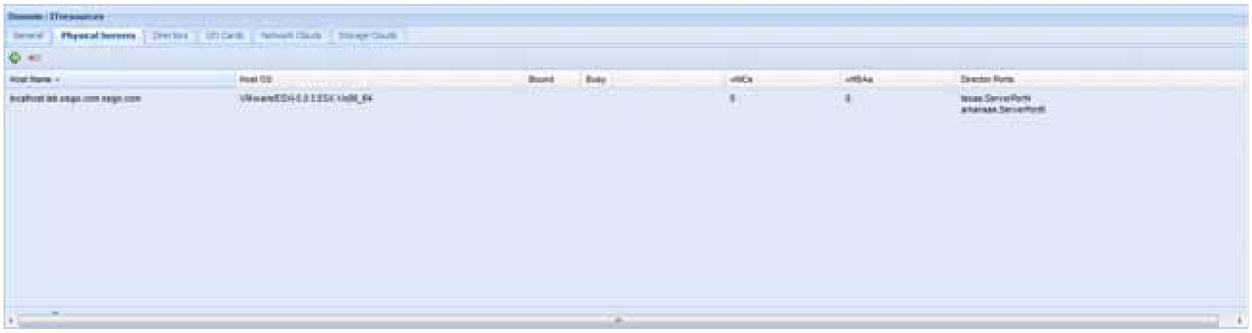
Figure 2 Domain Summary

Notice that the Domain Summary contains toolbar controls to add a new domain (+) and delete an existing domain. When domains are added, the resources for the new domain are removed from the default domain. When domains are deleted, any resources in them are returned to the default domain.

By default, the *General* tab is displayed in the details frame. The general information contains the name of the domain and any optional description. You can edit the description in the details frame by clicking the ***Edit*** button.

Displaying the Servers in a Domain

You can display information about the physical servers in a specific domain through the ***Physical Servers*** tab. By clicking this tab, you display a list of physical servers that are in the domain. Through the ***Physical Servers*** tab, you can add more physical servers to the domain, or delete selected servers from the domain. It is possible to have an empty domain (one with no servers) by deleting all servers in the domain. In this case, the domain remains configured as a software entity that contains no servers. Figure 3 shows a sample of the ***Physical Servers*** tab.



Domain : ITresources

Host Name	Host OS	Bound	Busy	vNICs	vHBAs	Director Ports
localhost.lab.xsigo.com.xsigo.com	VMware/ESXi-5.0.1ESX-4x86_64			8	0	texas.ServerPort4 arkansas.ServerPort8

Figure 3 Domain Details — Physical Servers

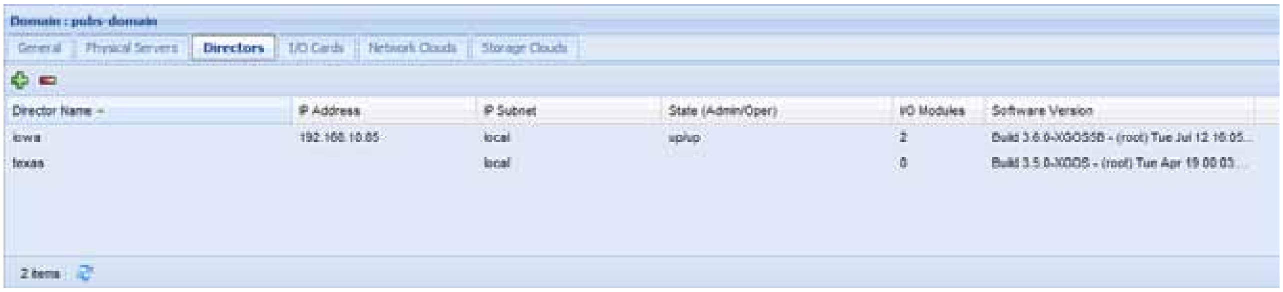
Table 1 shows the fields on the ***Physical Servers*** tab and explains what each field means.

Table 1 Contents of the Physical Servers Tab

Field Name	Means
Host Name	The name of the physical server(s) in the domain.
Host OS	The version (or build) string for the operating system currently running on the physical server.
Bound	The state of whether or not the server is bound to an I/O Template. If the server is bound, this field contains a check mark. If the server is not bound, the field is empty.
Busy	An indicator of whether or not the server is currently busy processing a configuration or management task (for example, busy binding to or unbinding from an I/O Profile).
vNICs	Shows the total number of vNICs configured on the server. These vNICs can be in any state, not just the operational vNICs.
vHBAs	Shows the total number of vHBAs configured on the server. These vHBAs can be in any state, not just the operational vHBAs.
Director Ports	Shows the individual high-speed interconnect ports on the Fabric Director on which the server is connected.

Displaying the Fabric Directors in a Domain

You can display information about the Fabric Directors in a specific domain through the *Directors* tab. By clicking this tab, you display a list of all the Fabric Directors that are partitioned into a non-default domain. Through this tab, you can add more Fabric Directors to, or delete them from, a specific domain. It is possible to have an empty domain (one with no Fabric Directors) by deleting all Fabric Directors in the domain. In this case, the domain remains configured as a software entity. Fabric Directors can be in only one domain at a time. If you delete one or more Fabric Directors, they return to the default domain, where they can then be reassigned to another non-default domain. Figure 4 shows a sample of the *Directors* tab.



Director Name ▾	IP Address	IP Subnet	State (Admin/Oper)	I/O Modules	Software Version
iowa	192.168.10.85	local	up/up	2	Build 3.6.0-XGOS5B - (root) Tue Jul 12 16:05...
texas		local		0	Build 3.5.0-XGOS - (root) Tue Apr 19 00:03...

2 items

Figure 4 Domain Details — Fabric Directors

It is possible that this dialog is empty depending on the type of termination you use for the domain. Each domain needs some kind of termination point for the virtual I/O within it. The virtual I/O can be terminated in either of the following ways:

- Terminated on a Fabric Director. In this case, one or more entire Fabric Directors are added to the domain. All I/O Modules in the Fabric Director are then added to the domain, and virtual I/O connections can be terminated on any of the ports on any of the cards in any of the Fabric Directors. This option might be preferable depending on the domain that you are configuring. For example, if the domain you are configuring is large or mission critical, you might need an entire Fabric Director's worth of I/O modules to connect the servers in the domain.
- Terminated on an I/O Module. In this case, one or more I/O modules are added to the domain. Only the I/O Modules that you explicitly add will be contained in the domain. This option might be preferable depending on the domain that you are configuring. For example, if the domain you are configuring is small or not mission critical, you might need only a few I/O modules in the domain (instead of an entire Fabric Director) to connect the servers in the domain.

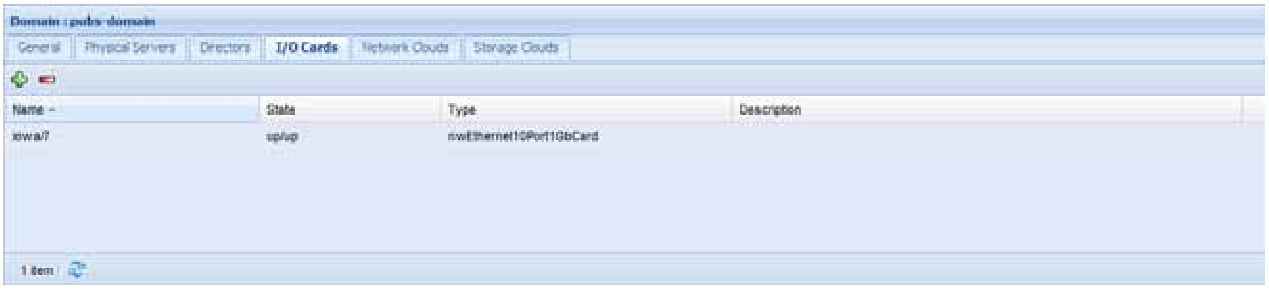
These options are mutually exclusive, so either Fabric Directors are added to the domain, or I/O cards are added to the domain, but not both. If Fabric Directors are added to the domain, the *Directors* tab will contain information when you add one or more Fabric Directors to the domain. If I/O Modules are added to the domain, or if no Fabric Directors have been added to the domain yet, this tab will be empty.

Table 2 Contents of the Directors Tab

Field Name	Means
Director Name	The name of the Fabric Director in the domain
IP Address	The IP address of the Fabric Director.
IP Subnet	The subnet on which the Fabric Director is currently configured.
State (Admin/Oper)	The administrative and operational states of the Fabric Director.
I/O Modules	The total number of I/O Modules available on each Fabric Director in the domain.
Software Version	The version of Oracle's XgOS software that is currently installed and running on the Fabric Director.

Displaying the I/O Cards in a Domain

You can display information about the I/O cards in a specific domain through the *I/O Cards* tab. By clicking this tab, you display a list of all the I/O cards that are partitioned into a non-default domain. Through this tab, you can add more I/O cards to, or delete them from, a specific domain. It is possible to have an empty domain (one with no I/O cards) by deleting all I/O cards in the domain. In this case, the domain remains configured as a software entity. I/O cards can be in only one domain at a time. If you delete one or more I/O cards, they return to the default domain, where they can then be reassigned to another non-default domain. Figure 5 shows a sample of the *I/O Cards* tab.



Domain : pubs-domain

Name	State	Type	Description
iowa/7	up/up	nwEthernet10Port1GbCard	

1 item

Figure 5 Domain Details — I/O Cards

It is possible that this dialog is empty depending on the type of termination you use for the domain. Each domain needs some kind of termination point for the virtual I/O within it. The virtual I/O can be terminated in either of the following ways:

- Terminated on a Fabric Director. In this case, one or more entire Fabric Directors are added to the domain. All I/O Modules in the Fabric Director are then added to the domain, and virtual I/O connections can be terminated on any of the ports on any of the cards in any of the Fabric Directors. This option might be preferable depending on the domain that you are configuring. For example, if the domain you are configuring is large or mission critical, you might need an entire Fabric Director’s worth of I/O modules to connect the servers in the domain.
- Terminated on an I/O Module. In this case, one or more I/O Modules are added to the domain. Only the I/O Modules that you explicitly add will be contained in the domain. This option might be preferable depending on the domain that you are configuring. For example, if the domain you are configuring is small or not mission critical, you might need only a few I/O modules in the domain (instead of an entire Fabric Director) to connect the servers in the domain.

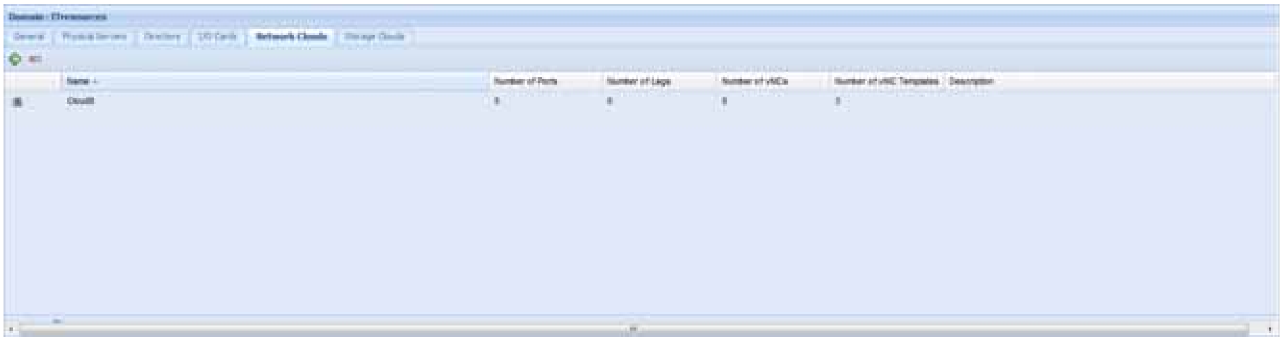
These options are mutually exclusive, so either Fabric Directors are added to the domain, or I/O cards are added to the domain, but not both. If Fabric Directors are added to the domain, the *Directors* tab will contain information when you add one or more Fabric Directors to the domain. If no I/O Modules are added to the domain, or if no Fabric Directors have been added to the domain yet, this tab will be empty.

Table 3 Contents of the I/O Cards Tab

Field Name	Means
Name	The name of the I/O Card that is assigned to the current domain. The name is a `slot/port` notation for a standard I/O card, or `slot.port` notation for a LAG on the I/O card.
State	The administrative and operational state of the I/O card
Type	The type string for the I/O card. In this example, the I/O card is a 10-Port 1 Gbps card, as indicated by the string `nwGbEthernet10Port1GbCard`.
Description	The optional description string (if any) that is assigned to each Network Cloud in the domain.

Displaying the Network Clouds in a Domain

You can display information about the Network Clouds in a specific domain through the *Network Clouds* tab. By clicking this tab, you display a list of Network Clouds that are in the domain. Through the *Network Clouds* tab, you can add more Network Clouds to the domain, or delete selected Network Clouds from the domain. It is possible to have an empty domain (one with no network clouds) by deleting all Network Clouds in the domain. In this case, the domain remains configured as a software entity that contains no Network Clouds. Figure 6 shows a sample of the *Network Clouds* tab.



Name	Number of Ports	Number of Lags	Number of vNICs	Number of vNIC Templates	Description
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	

Figure 6 Domain Details — Network Clouds

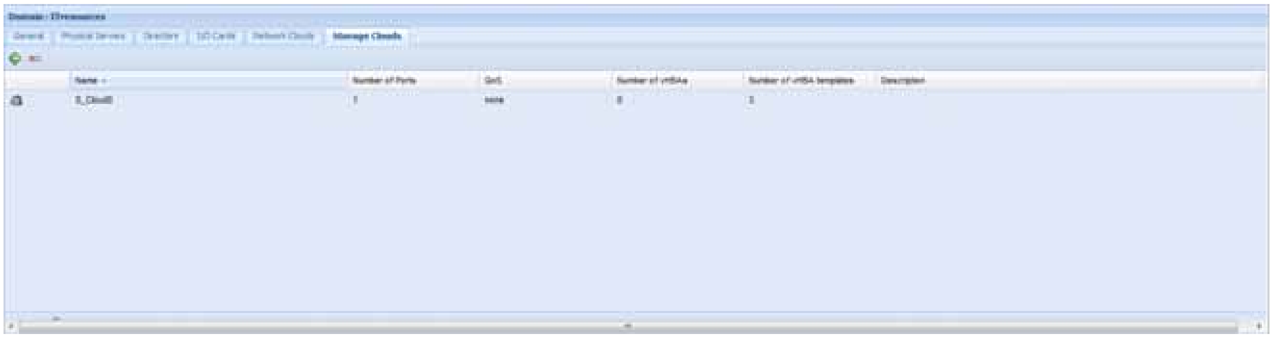
Table 4 shows the contents of the Network Clouds tab and explains what each field means.

Table 4 Contents of the Network Clouds Tab

Field Name	Means
Name	The name of the Network Cloud(s) in the domain.
Number of Ports	The total number of Ethernet ports in each Network Cloud, not the total number of ports in the domain.
Number of LAGs	The total number of Ethernet link aggregation groups (if any) configured in the domain. This number displayed in this column shows both static and dynamic (LACP) LAGs.
Number of vNICs	The total number of vNICs connected to the Network Cloud.
Number of vNIC Templates	The total number of I/O Templates containing vNICs that are used by the I/O Profile connected to the Network Cloud.
Description	The optional description string (if any) that is assigned to each Network Cloud in the domain.

Displaying the Storage Clouds in a Domain

You can display information about the Storage Clouds in a specific domain through the *Storage Clouds* tab. By clicking this tab, you display a list of Storage Clouds that are in the domain. Through the *Storage Clouds* tab, you can add more Storage Clouds to the domain, or delete selected Storage Clouds from the domain. It is possible to have an empty domain (one with no Storage Clouds) by deleting all Storage Clouds in the domain. In this case, the domain remains configured as a software entity that contains no Storage Clouds. Figure 7 shows a sample of the *Storage Clouds* tab.



Name	Number of Ports	QoS	Number of vHBAs	Number of vHBA templates	Description
S_Cloud0	1	none	0	1	

Figure 7 Domain Details — Storage Clouds

Table 5 shows the contents of the Storage Clouds tab and explains what each field means.

Table 5 Contents of the Storage Clouds Tab

Field Name	Means
Name	The name of the Storage Cloud(s) in the domain.
Number of Ports	The total number of Fibre Channel ports in each Storage Cloud, not the total number of ports in the domain.
QoS	The name of the SAN QoS profile (if any) that is applied to each Storage Cloud in the domain.
Number of vHBAs	The total number of vHBAs configured in the Storage Cloud.
Number of vHBA Templates	The total number of I/O Templates containing vHBAs that are used by the I/O Profile connected to the Storage Cloud.
Description	The optional description string (if any) that is assigned to each Storage Cloud in the domain.

Creating a Domain

When you are creating a domain, you are carving out a set of resources from the overall default domain. The Domain will include Ethernet ports, Fibre Channel ports, and physical servers that will be required in the domain. Domains are created by using the Create Domain Wizard, which will guide you through the steps of identifying which Network Clouds, Storage Clouds, and physical servers will be used to create the domain. When you run the wizard, the following objects must be available to be selectable in the wizard:

- Network Cloud(s) for the domain. The Network Cloud consists of one or more termination GE ports. The port cannot be assigned to another cloud.
- Storage Clouds for the domain. The Storage Cloud consists of one or more termination FC ports. The port cannot be assigned to another cloud.
- Physical hosts, which must be connected to a Fabric Director which Fabric Manager is managing. The host(s) cannot already be deployed (connected to a Network or Storage Cloud).

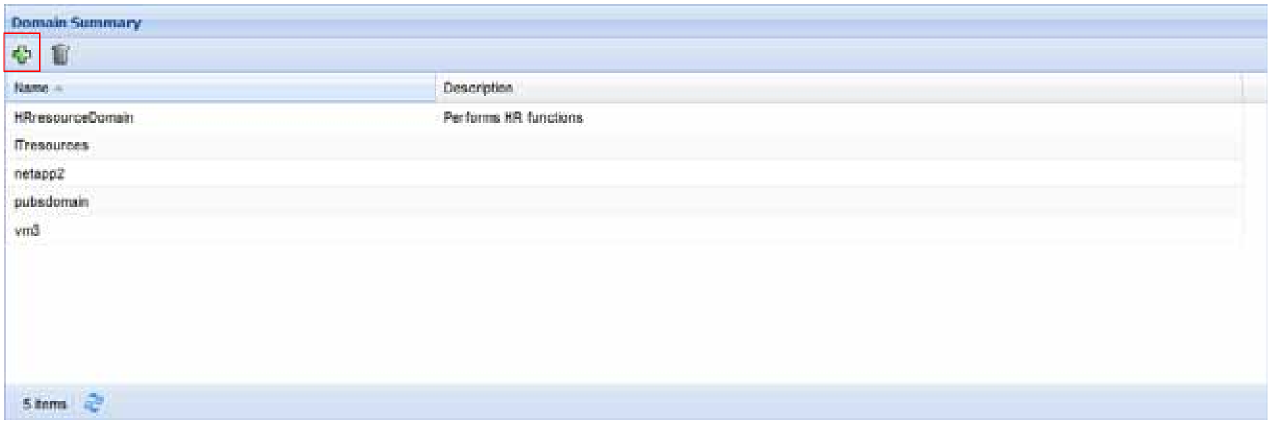
When you create a domain, you must be logged in as a root-level administrator account so that you can carve out the resources from the default domain. After the domain is configured, you can log back in with a domain admin account for that domain, and continue to configure and manage that individual domain. When you are logged in to the domain as a domain admin, the *Security Manager->Resource Domains* is no longer available, and no other domains are accessible.

In typical deployments, creating a domain takes the following steps:

- Adding Physical Servers to a Domain
- Adding either Fabric Directors or I/O Modules to a domain, but not both
- Adding Network Connectivity to a Domain.
- Add Storage Connectivity to a Domain

To create a domain, follow this procedure:

Step 1 On the Navigation panel, select *Security Manager->Resource Domains* to display the Domain Summary. This option will be available only if you are logged in with an administrator account. Figure 8 shows the Domain Summary.



Domain Summary

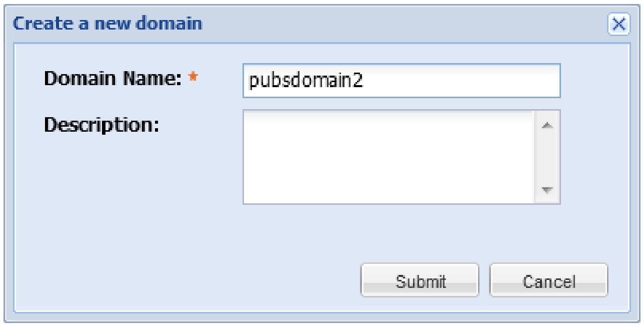
Name	Description
HRresourceDomain	Performs HR functions
ITresources	
netapp2	
pubsdomain	
vm3	

5 items

Figure 8 Domain Summary

Notice that the Domain Summary contains toolbar controls to add a new domain and delete an existing domain. When domains are added, the resources for the new domain are removed from the default domain. When domains are deleted, any resources in them are returned to the default domain.

Step 2 On the Domain Summary, click the plus sign (+) to start the Create Domain Wizard, and displays the Define a Domain page of the wizard. Figure 9 shows this dialog.



Create a new domain

Domain Name: * pubsdomain2

Description:

Figure 9 Create Domain — Define a Domain

Step 3 In the *Name* field, enter the name for the domain that you are creating.

Step 4 As an option, you can enter an alphanumeric character string that describes the domain that you are creating.

Step 5 Click ***Submit*** to create the domain. When you click ***Submit***, the domain is created as an empty container to which you will add the required components to provide virtual connectivity to the host(s).

Adding Fabric Directors to a Domain

When you have a domain created, you need to populate it with the network entities that the domain needs. One of these network entities is the termination port for virtual I/O. You have an option for specifying the termination points for the domain:

— Fabric Directors. If you add Fabric Directors to the domain, all I/O Modules in the Fabric Director are placed into the domain and available for connections.

— I/O Modules. If you add I/O Modules to the domain, only the I/O Modules you select are added. This option provides you with an additional level of granularity. For example, if the domain is relatively small, you might not want to use an entire Fabric Director's worth of I/O modules. In this case, you can use only a few of the modules for the domain, and reserve the other I/O Modules for other uses or other domains.

The choice of adding Fabric Directors or I/O Modules is a mutually exclusive one. You can add either, but not both. You will need to determine which option suits the domain.

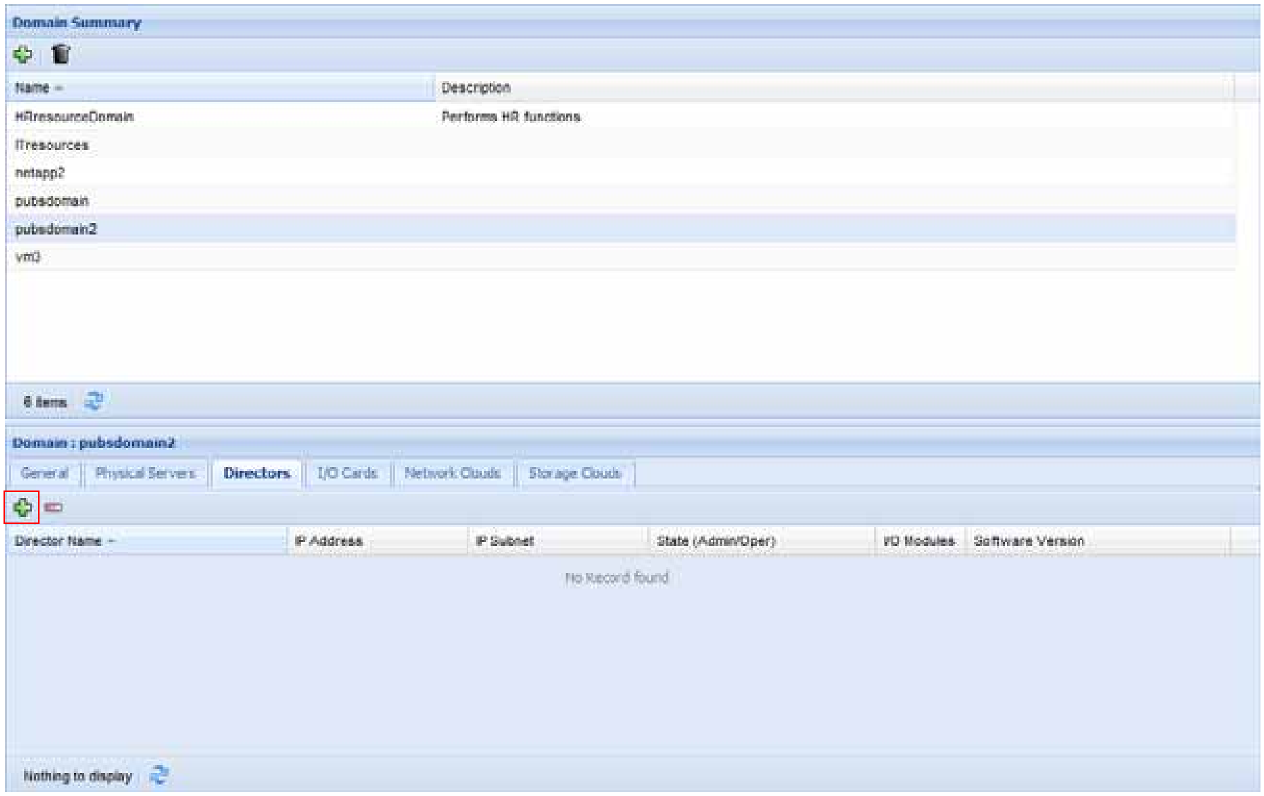
- If you will add Fabric Directors to the domain, complete the procedure in this section.
- If you will be adding I/O modules to the domain, skip the procedure in this section, and Adding I/O Modules to a Domain.

You can add Fabric Directors to the domain thorough the *Directors* tab on the Domain Details page.

To add a Fabric Director to a domain, follow this procedure:

Step 1 On the Domain Summary, click the domain to which you want to add a Fabric Director. This step populates the Domain Details frame with the selected domain.

Step 2 On the Domain Details frame, click the *Directors* tab as shown in Figure 10.



Domain Summary

Name	Description
HRresourceDomain	Performs HR functions
ITresources	
netapp2	
pubsdomain	
pubsdomain2	
vm3	

6 items

Domain : pubsdomain2

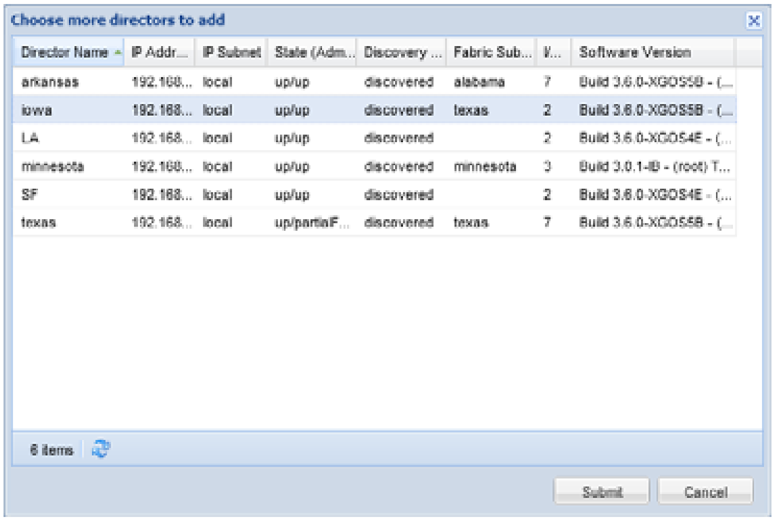
Director Name	IP Address	IP Subnet	State (Admin/Oper)	I/O Modules	Software Version

No Record found

Nothing to display

Figure 10 Domain Details — Directors Tab

Step 3 On the Details frame, click the plus sign (+) to add Fabric Directors to the domain. See Figure 11.



Choose more directors to add

Director Name	IP Addr...	IP Subnet	State (Adm...	Discovery ...	Fabric Sub...	I/...	Software Version
arkansas	192.168...	local	up/up	discovered	alabama	7	Build 3.6.0-XGOS5B - (...
iowa	192.168...	local	up/up	discovered	texas	2	Build 3.6.0-XGOS5B - (...
LA	192.168...	local	up/up	discovered		2	Build 3.6.0-XGOS4E - (...
minnesota	192.168...	local	up/up	discovered	minnesota	3	Build 3.0.1-IB - (root) T...
SF	192.168...	local	up/up	discovered		2	Build 3.6.0-XGOS4E - (...
texas	192.168...	local	up/partialF...	discovered	texas	7	Build 3.6.0-XGOS5B - (...

6 items

Figure 11 Selecting Fabric Directors for the Domain

Step 4 On the dialog, click the Fabric Director(s) you want to add to the domain. For an HA deployment, you will select two Fabric Directors. You can use standard key sequences to select multiple servers. For example, on a Windows Fabric Manager client, ***CTRL*** + click selects multiple Fabric Directors, ***Shift*** + click selects all Fabric Directors.

Step 5 Click ***Submit*** to add the selected Fabric Directors to the domain.

Step 6 Proceed to the next section.

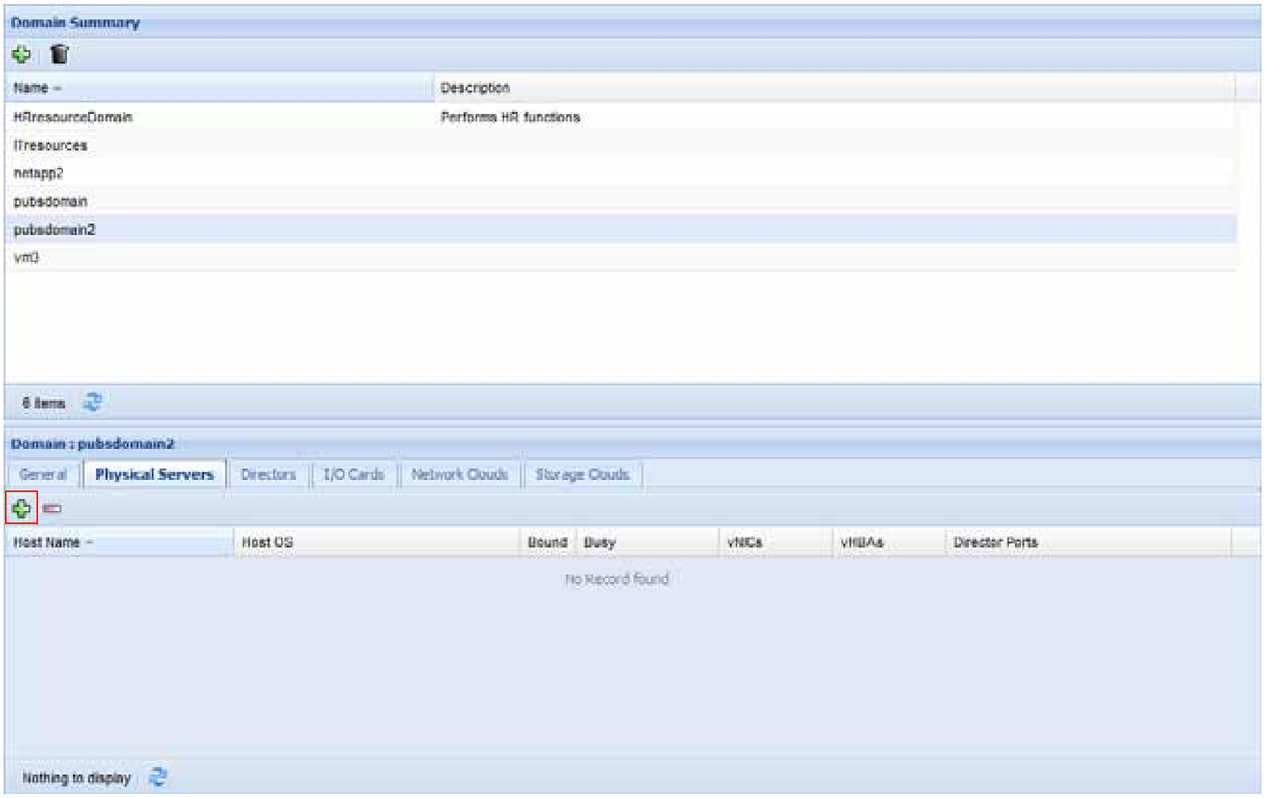
Adding Physical Servers to a Domain

When you have a domain created, you need to populate it with the network entities that the domain needs. One of these network entities is the physical host server(s). You can add physical servers to the domain thorough the Physical servers tab on the Domain Details page.

To add servers to the domain, follow this procedure:

Step 1 On the Domain Summary, click the domain in which you want the server configured. This step populates the Domain Details frame with the selected domain.

Step 2 On the Domain Details frame, click the *Physical Servers* tab as shown in Figure 12.



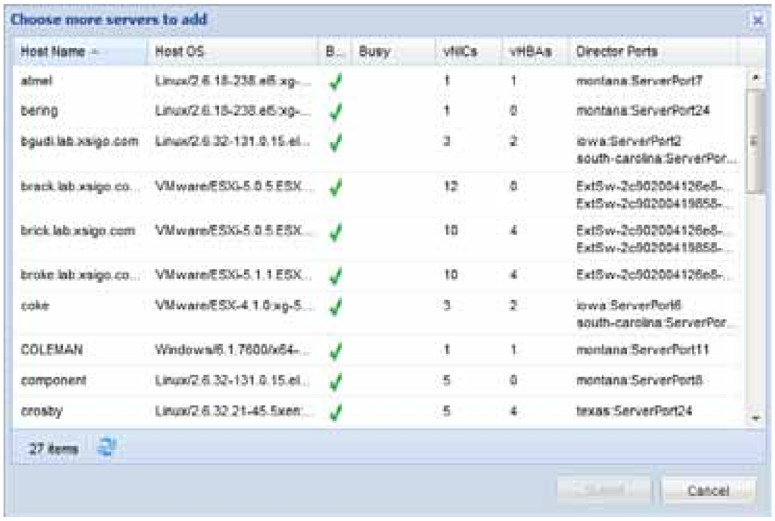
Name	Description
HRresourceDomain	Performs HR functions
ITresources	
netapp2	
pubsdomain	
pubsdomain2	
vm0	

Host Name	Host OS	Bound	Busy	vNICs	vHBAs	Director Ports

No Record found

Figure 12 Domain Details — Physical Servers Tab

Step 3 On the Physical servers tab, click the plus sign (+) to start the add server dialog. See Figure 13.



Choose more servers to add

Host Name	Host OS	B...	Busy	vNICs	vHBAs	Director Ports
almel	Linux/2.6.18-238.el5.xg-...	✓		1	1	montana:ServerPort7
bering	Linux/2.6.18-238.el5.xg-...	✓		1	0	montana:ServerPort24
bgudi.lab.xsigo.com	Linux/2.6.32-131.0.15.el...	✓		3	2	iowa:ServerPort2 south-carolina:ServerPor...
brack.lab.xsigo.co...	VMware/ESXi-5.0.5.ESX...	✓		12	0	ExtSw-2c902004126e8-... ExtSw-2c90200419858-...
brick.lab.xsigo.com	VMware/ESXi-5.0.5.ESX...	✓		10	4	ExtSw-2c902004126e8-... ExtSw-2c90200419858-...
broke.lab.xsigo.co...	VMware/ESXi-5.1.1.ESX...	✓		10	4	ExtSw-2c902004126e8-...
coke	VMware/ESX-4.1.0.xg-5...	✓		3	2	iowa:ServerPort6 south-carolina:ServerPor...
COLEMAN	Windows/6.1.7600/x64-...	✓		1	1	montana:ServerPort11
component	Linux/2.6.32-131.0.15.el...	✓		5	0	montana:ServerPort8
crosby	Linux/2.6.32.21-45.5xen...	✓		5	4	texas:ServerPort24

27 items

Figure 13 Selecting the Physical Servers for the Domain

Step 4 Select the server(s) that you want to add to the domain. You can use standard key sequences to select multiple servers—for example, on a Windows Fabric Manager client, ***CTRL*** + click or ***Shift*** + click.

Step 5 When the servers have been specified, click ***Submit*** to add them to the domain.

Step 6 Proceed to the next section.

Adding I/O Modules to a Domain

When you have a domain created, you need to populate it with the network entities that the domain needs. One of these network entities is the termination port for virtual I/O. You have an option for specifying the termination points for the domain:

— Fabric Directors. If you add Fabric Directors to the domain, all I/O Modules in the Fabric Director are placed into the domain and available for connections.

— I/O Modules. If you add I/O Modules to the domain, only the I/O Modules you select are added. This option provides you with an additional level of granularity. For example, if the domain is relatively small, you might not want to use an entire Fabric Director’s worth of I/O modules. In this case, you can use only a few of the modules for the domain, and reserve the other I/O Modules for other uses or other domains.

The choice of adding Fabric Directors or I/O Modules is a mutually exclusive one. You can add either, but not both. You will need to determine which option suits the domain.

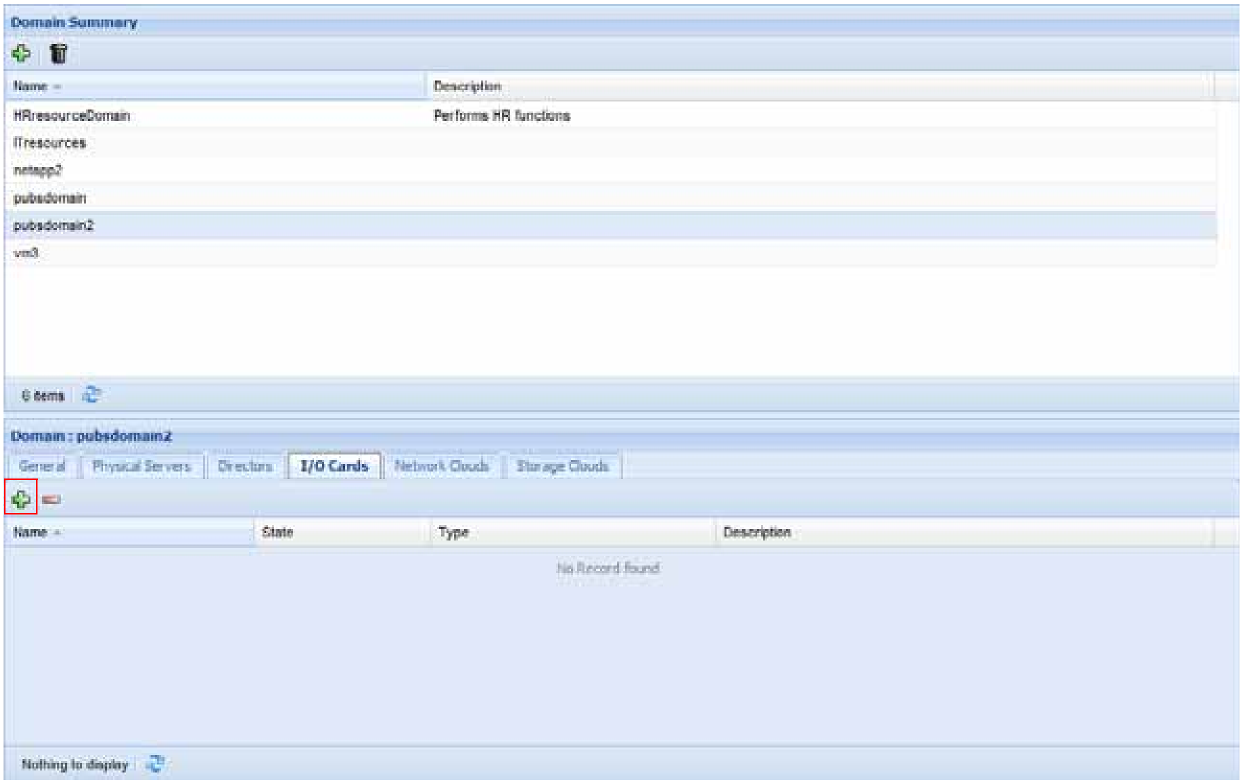
- If you will add Oracle’s Xsigo Fabric Directors to the domain, skip the procedure in this section, and proceed to Adding Fabric Directors to a Domain.
- If you will be adding I/O modules to the domain, complete the procedure in this section.

You can add I/O modules to the domain thorough the *I/O Cards* tab on the Domain Details page.

To add an I/O module to a domain, follow this procedure:

Step 1 On the Domain Summary, click the domain to which you want to add an I/O module. This step populates the Domain Details frame with the selected domain.

Step 2 Click the *I/O Cards* tab as shown in Figure 14.

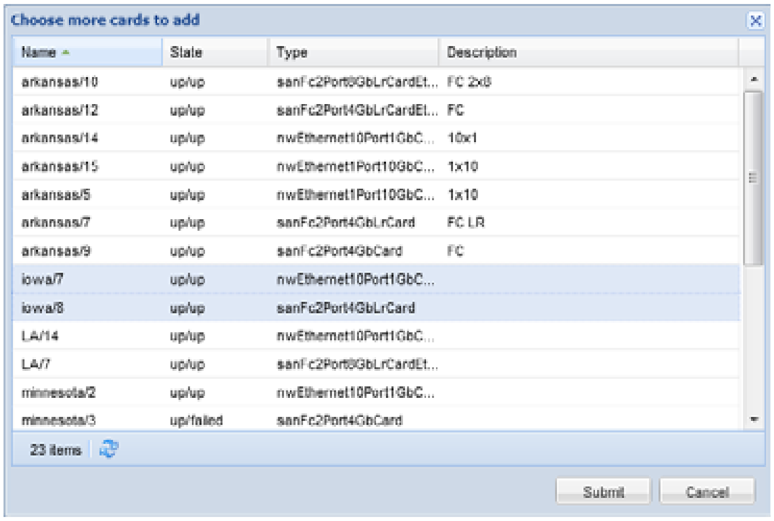


Name	Description
HRresourceDomain	Performs HR functions
ITresources	
netapp2	
pubsdomain	
pubsdomain2	
vm3	

Name	State	Type	Description
No Record found			

Figure 14 Domain Details — I/O Cards Tab

Step 3 Click the plus sign (+) to display a dialog through which you can add one or more I/O Modules to the domain.



Choose more cards to add

Name	State	Type	Description
arkansas/10	up/up	sanFc2Port8GbLrCardEt...	FC 2x8
arkansas/12	up/up	sanFc2Port4GbLrCardEt...	FC
arkansas/14	up/up	nwEthernet10Port1GbC...	10x1
arkansas/15	up/up	nwEthernet1Port10GbC...	1x10
arkansas/5	up/up	nwEthernet1Port10GbC...	1x10
arkansas/7	up/up	sanFc2Port4GbLrCard	FC LR
arkansas/9	up/up	sanFc2Port4GbCard	FC
iowa/7	up/up	nwEthernet10Port1GbC...	
iowa/8	up/up	sanFc2Port4GbLrCard	
LA/14	up/up	nwEthernet10Port1GbC...	
LA/7	up/up	sanFc2Port8GbLrCardEt...	
minnesota/2	up/up	nwEthernet10Port1GbC...	
minnesota/3	up/failed	sanFc2Port4GbCard	

23 items

Figure 15 Selecting the I/O Cards for the Domain

Step 4 On the dialog select one or more I/O Modules to add them to the domain. For an HA deployment, you will select two I/O cards of the same type. You can use standard key sequences to select multiple I/O cards. For example, on a Windows Fabric Manager client, ***CTRL*** + click selects multiple I/O cards, ***Shift*** + click selects all I/O cards.

Step 5 Click ***Submit*** to add the selected I/O cards to the domain.

Step 6 Proceed to the next section.

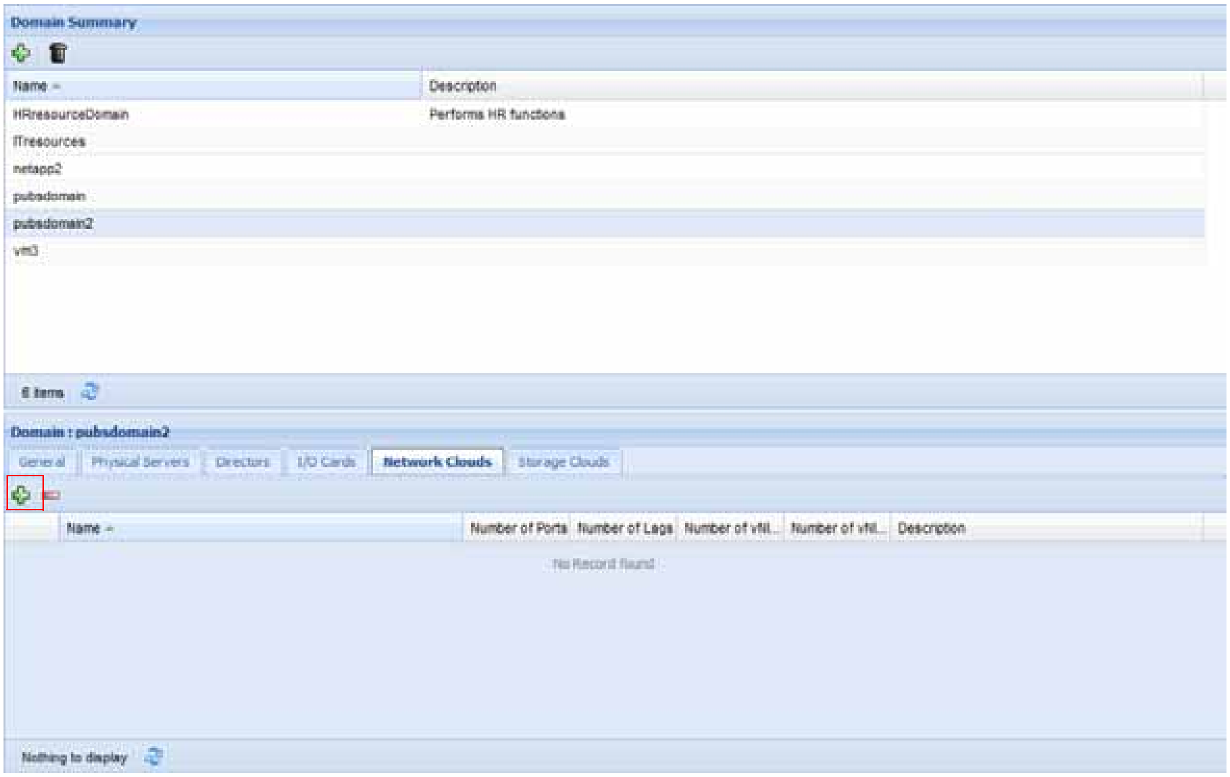
Adding Network Connectivity to a Domain

When you have a domain created, you need to populate it with the network entities that the domain needs. One of these network entities is a Network Cloud, which provides connectivity to network resources. You can add Network Clouds to the domain thorough the *Network Clouds* tab on the Domain Details page.

To add a Network Cloud to the domain, follow this procedure:

Step 1 On the Domain Summary, click the domain to which you want to add a Network Cloud. This step populates the Domain Details frame with the selected domain.

Step 2 On the details frame, click the *Network Clouds* tab as shown in Figure 16.



Domain Summary

Name	Description
HRresourceDomain	Performs HR functions
ITresources	
netapp2	
pubsdomain	
pubsdomain2	
vm3	

6 items

Domain : pubsdomain2

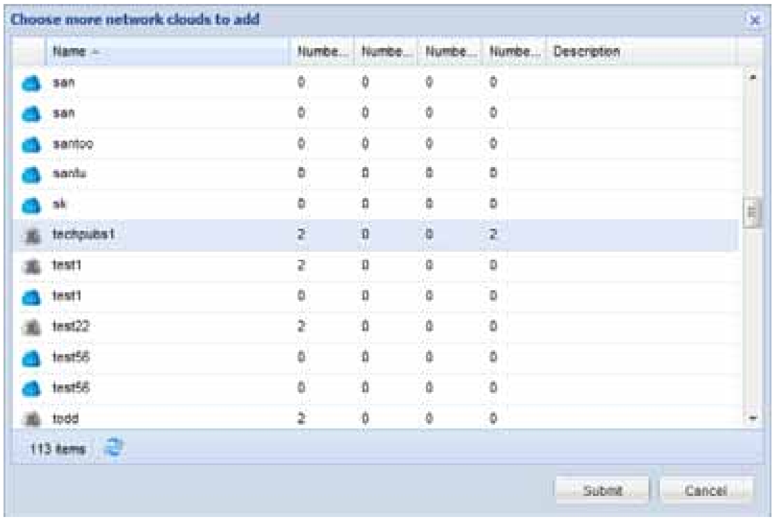
Name	Number of Ports	Number of Lags	Number of vNI...	Number of vNI...	Description

No Record found

Nothing to display

Figure 16 Domain Details — Network Clouds Tab

Step 3 Click the plus sign (+) to display a dialog that adds the Network Cloud. See Figure 17.



Choose more network clouds to add

Name	Numbe...	Numbe...	Numbe...	Numbe...	Description
san	0	0	0	0	
san	0	0	0	0	
santoo	0	0	0	0	
santu	0	0	0	0	
sk	0	0	0	0	
techpubs1	2	0	0	2	
test1	2	0	0	0	
test1	0	0	0	0	
test22	2	0	0	0	
test56	0	0	0	0	
test56	0	0	0	0	
todd	2	0	0	0	

113 items

Figure 17 Selecting the Network Clouds for the Domain

Step 4 On the dialog, select the Network Cloud that you want to add to the domain. For an HA deployment, you will select two I/O cards of the same type. You can use standard key sequences to select multiple I/O cards. For example, on a Windows Fabric Manager client, ***CTRL*** + click selects multiple I/O cards, ***Shift*** + click selects all I/O cards.

Step 5 Click ***Submit*** to add the Network Cloud to the domain.

Step 6 Proceed to the next section.

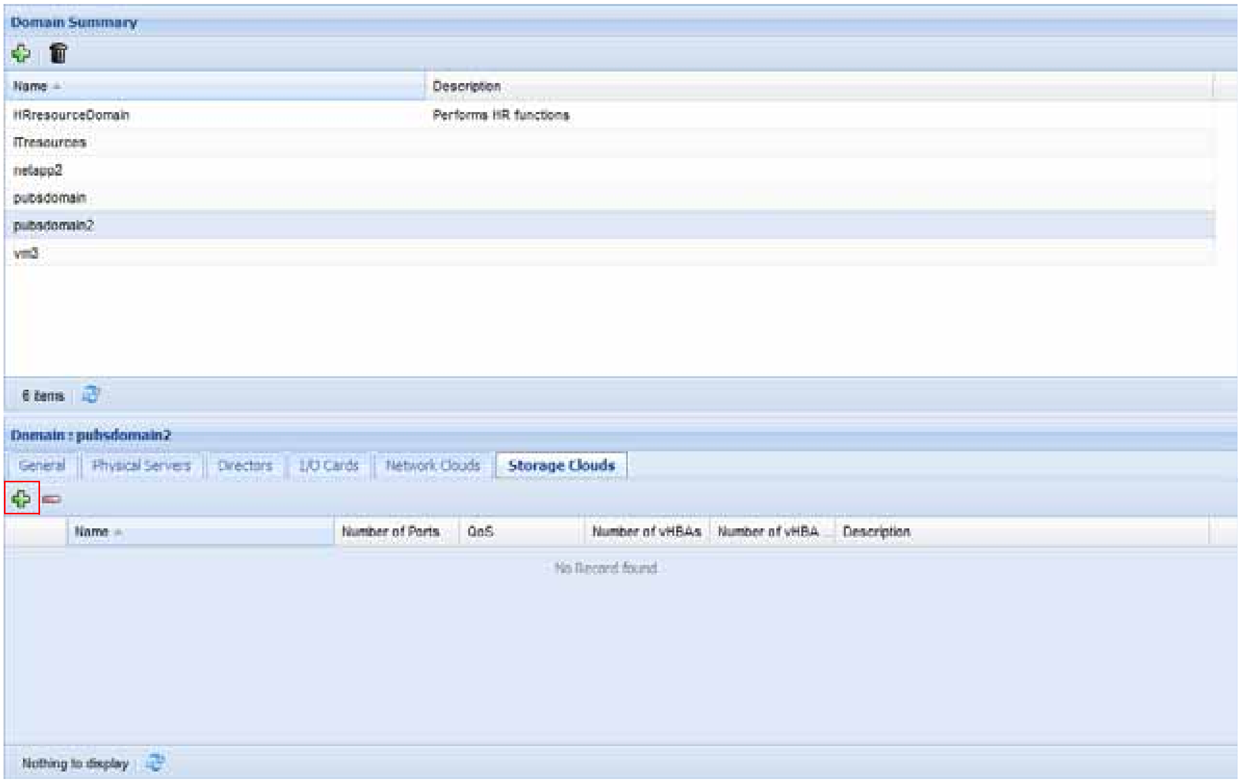
Add Storage Connectivity to a Domain

When you have a domain created, you need to populate it with the SAN entities that the domain needs. One of these storage entities is a Storage Cloud, which provides connectivity to storage resources. You can add Storage Clouds to the domain thorough the *Storage Clouds* tab on the Domain Details page.

To add a Storage Cloud to the domain, follow this procedure:

Step 1 On the Domain Summary, click the domain to which you want to add a Storage Cloud. This step populates the Domain Details frame with the selected domain.

Step 2 On the details frame, click the *Storage Clouds* tab as shown in Figure 18.



Domain Summary

Name	Description
HRresourceDomain	Performs HR functions
ITresources	
netapp2	
pubsdomain	
pubsdomain2	
vm3	

6 items

Domain : pubsdomain2

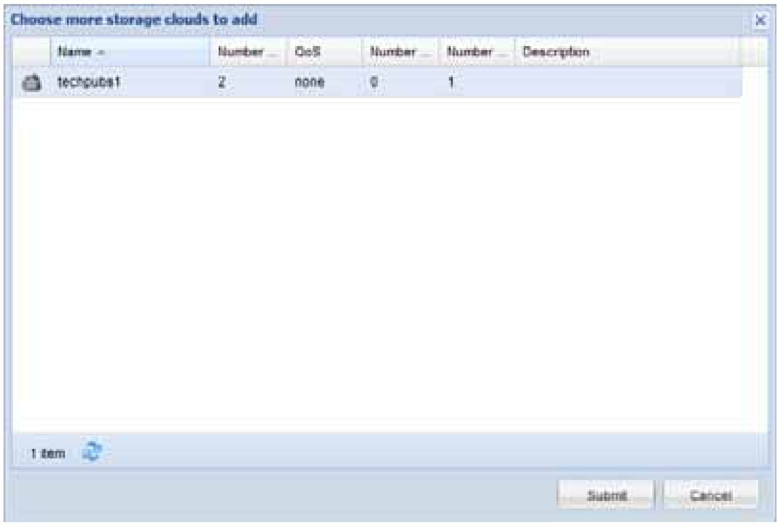
Name	Number of Ports	QoS	Number of vHBAs	Number of vHBA ...	Description

No Record found

Nothing to display

Figure 18 Domain Details — Storage Clouds Tab

Step 3 Click the plus sign (+) to display a dialog through which you can add one or more I/O Modules to the domain.



Choose more storage clouds to add

Name	Number ...	QoS	Number ...	Number ...	Description
techpubs1	2	none	0	1	

1 item

Figure 19 Selecting the Storage Clouds for the Domain

Step 4 On the dialog, select the Storage Cloud that you want to add to the domain. For an HA deployment, you will select two I/O cards of the same type. You can use standard key sequences to select multiple I/O cards. For example, on a Windows Oracle Xsigo Fabric Manager client, ***CTRL*** + click selects multiple I/O cards, ***Shift*** + click selects all I/O cards.

Step 5 Click ***Submit*** to add the Storage Cloud to the domain.

Working with User Roles

This chapter contains the following topics:

Understanding the Xsigo Identity Management System

Oracle’s Xsigo Fabric Director has a robust system of user management called the Identity Management System (IMS). The IMS has an internal system (called the internal IMS) and also has an external system called the external IMS:

- Internal IMS, is the Fabric Director’s assignment of a user to a role group. The role group has permissions associated with it that determine what system object the user can use when logged in and a member of that role. This assignment of a user to a role is called internal because the mapping of user-to-role as well as the authorization and authentication of that user occurs on the Fabric Director. For information about the internal IMS, see Using the Internal IMS.
- External IMS is the assignment of a user to a role group also. The authorization and authentication aspects of logging in through that user occur off of the Fabric Director and Oracle’s Xsigo Fabric Manager Server. Authentication and authorization occur typically on an external device—for example, through a RADIUS server—that is connected to the Fabric Manager Server through a Fabric Director.

Using the Internal IMS

The Fabric Director’s internal IMS consists of user accounts and roles. Users and roles are interrelated:

- User accounts enable login and access to the Fabric Manager system and the Fabric Director. User accounts are created on the Fabric Director and the Fabric Manager Server to grant people access to the chassis.
- The role that a user belongs to determines which objects the user can modify. When a user is logged in and becomes a member of a particular role, the user gets only the permissions that are granted to that role.

When a user account is created, it is assigned to a role. The role determines the permissions that the user has in Fabric Manager.

Understanding Local Users

Each Fabric Director supports local users which are user accounts on each Fabric Director. Local user accounts are local because they are independent accounts that exist on individual Fabric Directors.

Typically, a local user account is mapped into a role group. That role group provides the permissions for what objects the user can and cannot write to. When a user account is assigned to a role, the conditions are created for what actions the user can perform, and what objects the user can configure, change, or manage. For information about roles, see Understanding Roles.

It is possible to create a local user without assigning the user to a specific role group. In this case, the user is assigned to the “operator” role group by default. The operator role group is the most restrictive. It provides read-only access.

All users have a role group—either a role group that is explicitly assigned to the user, or the operator role group that is assigned by default.

Understanding Roles

Roles are software constructions that are associated with one or more user accounts. The roles set the amount of control that a user has within the Fabric Manager and Fabric Director system. Roles typically are created based on the division of system administration tasks in the data center. For example, some common roles are:

- network, for managing IP network and routing connectivity.
- storage, for managing storage capacity, configuration, and connectivity.

Fabric Manager supports a set of default roles. Each group has permissions on different hardware, software, and network components. Table 1 shows the roles with which a user can be associated.

Table 1 Roles

Role	Privileges for...
operator	read access to Fabric Director features
network	vNIC configuration and management, Network QoS
storage	vHBA configuration and management, SAN QoS
server	compute resource configuration and management
administrator	full admin responsibilities
no access	Nothing. Users with this role cannot use Fabric Manager and cannot display any information in it.

Note

A special case exists for any user that is assigned to the administrator role. In such a case, when the user logs in, Fabric Manager maps that individual user account to the root account (admin/admin), which grants the user all permissions on the Fabric Director.

Defining a User in Fabric Manager

Fabric Manager users are defined on each Fabric Manager server. For proper access, each Fabric Manager user account must also exist in the OS of the server where Fabric Manager is loaded.

When you create a Fabric Manager user account, you will define the user account name (which should be the same as the OS level user account) and specify a role. You do not need to specify a different password for the Fabric Manager user account because the user's network (domain) password is used.

Users will use the Fabric Manager user account and their network/domain password on the Fabric Manager login page. After successfully logging in, the current user name is displayed at the right side of the banner. Figure 1 shows an example of the current user name displayed on the Fabric Manager Dashboard. In this figure, the logged in user is highlighted with a red box.

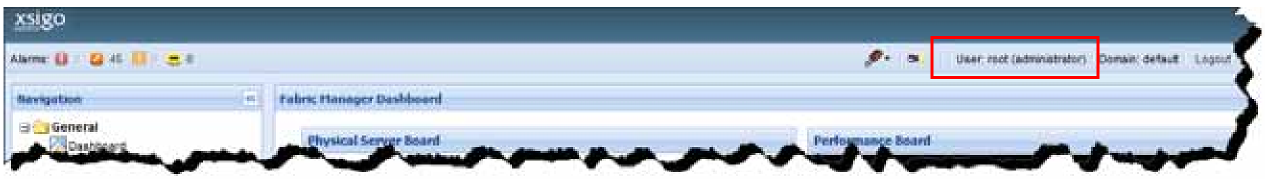


Figure 1 Fabric Manager Welcome Page Displaying Currently Logged-In User

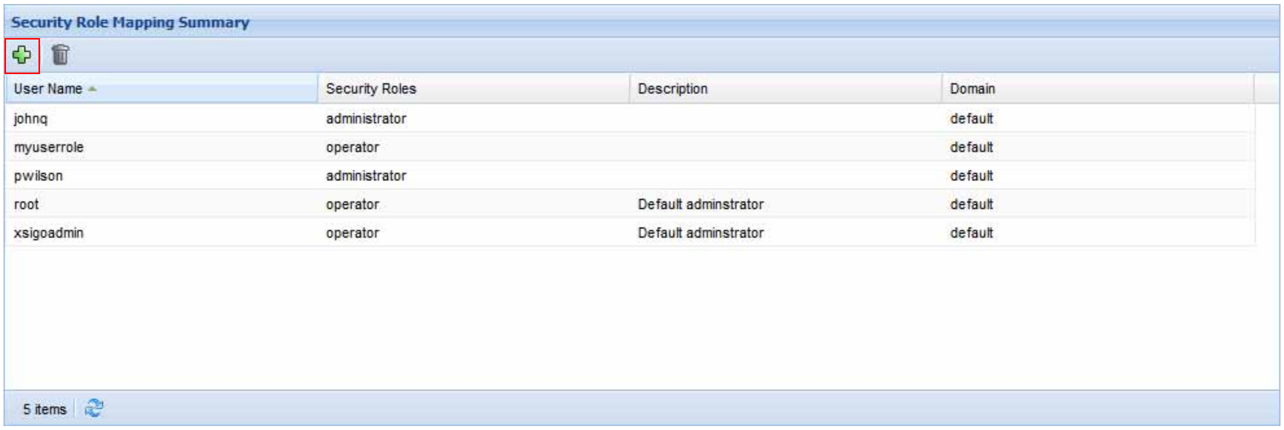
This section documents how to create a global user account at the Fabric Manager level. For information about how to create a local user on a Fabric Director, see Defining a Local User on the Fabric Director.

Be aware of the following considerations:

- The Fabric Manager user must also exist as a user at the OS level of the Fabric Manager Server. If the user does not exist in the Linux OS of a Linux Fabric Manager Server, or in the Windows OS of a Windows Fabric Manager Server, that OS user must be created now. The OS level user account must exist to allow for authentication and log in to Fabric Manager. After authentication, the OS level user account is not used. At that point, Fabric Manager user accounts are used, and they are what enforce role-based access (RBAC) privileges.
- If a specific Fabric Manager role is not configured for a Fabric Manager user, after logging in, that user is assigned to the "operator" role by default, which is the most restrictive role available.

To define a user at the Fabric Manager level, follow this procedure:

Step 1 From the navigation panel, select *Security Manager->User Roles*. This step displays the Security Role Mapping Summary. Figure 2 shows this table.



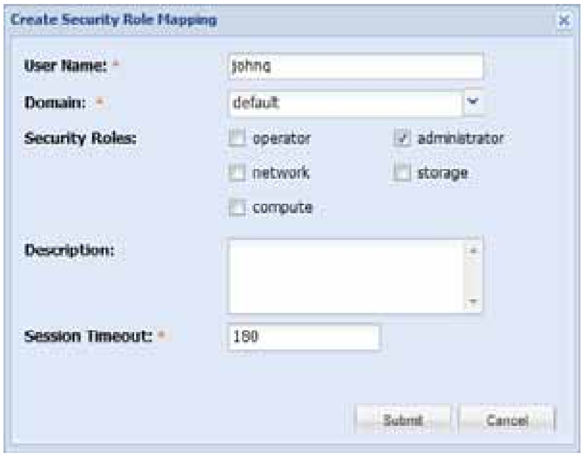
Security Role Mapping Summary

User Name	Security Roles	Description	Domain
johnq	administrator		default
myuserrole	operator		default
pwilson	administrator		default
root	operator	Default adminstrator	default
xsigoadmin	operator	Default adminstrator	default

5 items

Figure 2 User Summary Page — User List

Step 2 Click ***New...*** to display the Create Security Role Mapping dialog. Figure 3 shows this page.



User Name: * johng

Domain: * default

Security Roles: □ operator ☑ administrator □ network □ storage □ compute

Description:

Session Timeout: * 180

Figure 3 Create Security Role Mapping Dialog

Step 3 In the *User Name* field, enter a string from 1 to 128 characters in length that names the user account that you are creating.

Step 4 From the *Domain* dropdown menu, select a specific domain in which this user and role will be created. By default, all users and their roles are created in the default domain unless a custom domain is selected.

Step 5 From the *Security Roles* list, click the checkbox for the role that you want to assign to the user that you are creating. If no user is specified, the operator role is assigned.

Step 6 As an option, in the *Description* field, you can enter a string that describes the user account that you are creating.

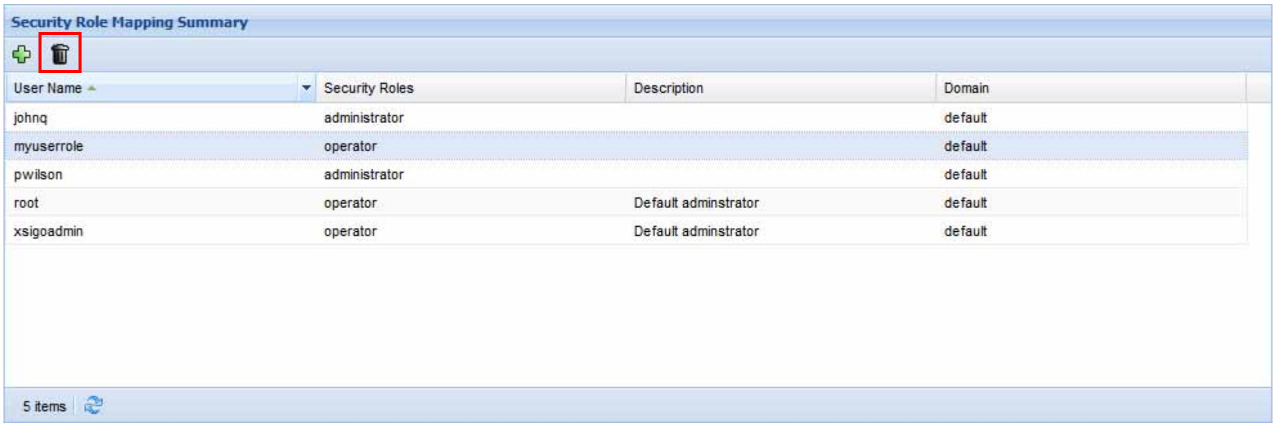
Step 7 When all information on the Create Security Role Mapping dialog is correct, click ***Finish*** to close the dialog and complete creating a user and its roles.

Deleting a User from Fabric Manager

Any global user configured in Fabric Manager can be deleted through the User List. When a Fabric Manager user is deleted, that user account can no longer pass authentication at the Fabric Manager server. As a result, that user can no longer use Fabric Manager to manage the Fabric Director. However, if a local user account is still configured on the Fabric Director (not the Fabric Manager server), that user can manage the Fabric Director through the CLI.

You can delete a Fabric Manager user account through the User List summary page. To delete a Fabric Manager user, follow this procedure:

Step 1 From the navigation panel, select *General->User Management*. This step displays the User List summary page. Figure 4 shows the User List.



Security Role Mapping Summary

User Name	Security Roles	Description	Domain
johnq	administrator		default
myuserrole	operator		default
pwilson	administrator		default
root	operator	Default adminstrator	default
xsigoadmin	operator	Default adminstrator	default

5 items

Figure 4 User Summary Page — User List

Step 2 On the Security Role Mapping Summary, click the name of the user(s) that you want to delete. This step activates the garbage can icon.

Step 3 When the user(s) are highlighted, click the garbage can icon to delete the selected user(s). When you click the garbage can icon, a confirmation page is displayed to have you verify that you really do want to delete the users.

Step 4 Click ***Yes*** to delete the specified users. Or, you can also select ***No*** to abort the deletion of the selected users.

Note

Remember that this Fabric Manager user can no longer log in and manage Fabric Directors through Fabric Manager when the account is deleted. However, if there is a local account on a specific Fabric Director, that user can still log in to that chassis CLI through Oracle's XgOS. You will need to remove that local account on any Fabric Director if you do not want the deleted user to have any access to Fabric Directors at all.

Defining a Local User on the Fabric Director

After creating the user at the Fabric Manager level, you should also create the local user account on each Fabric Director where you want the account available. You do not need to create the local user accounts on all Fabric Directors, just on the Fabric Directors that the user will need to access. The local user account is pushed to the Fabric Director. When a local user account is created, it exists on the Fabric Director and can be used for chassis access through Oracle's XgOS CLI.

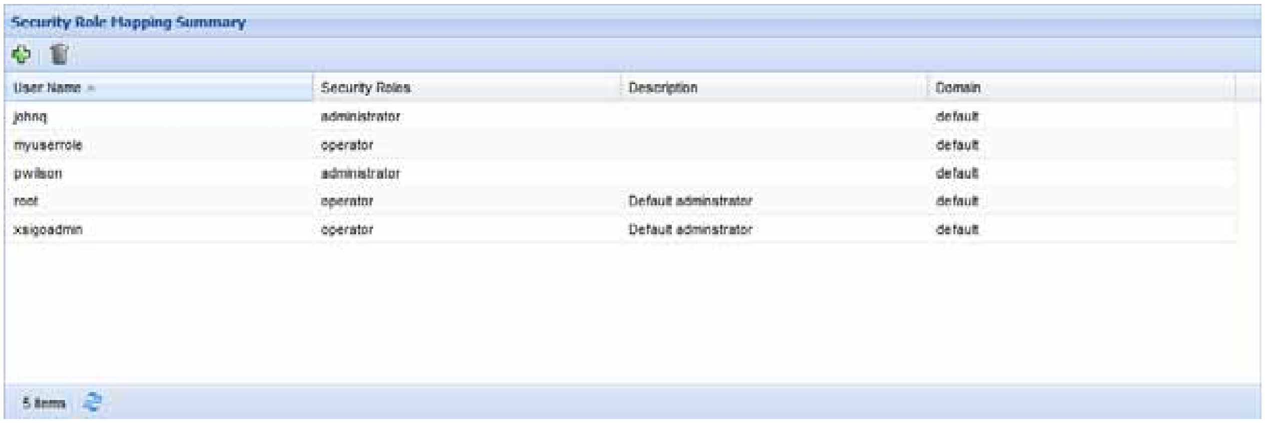
Defining an local user occurs on each individual Fabric Director. For information about creating a local user, see Understanding Local Users.

Renaming a Fabric Manager User

Fabric Manager supports renaming a Fabric Manager user, which enables you to change the name without having to completely delete and recreate the Fabric Manager user. When the Fabric Manager user is renamed, all other properties for the Fabric Manager user are retained, including the domain and security roles associated with the user. As an option, you can also set or change the description for the Fabric Manager user.

You can rename the Fabric Manager user through the Fabric Manager User Details frame. To rename the Fabric Manager user, follow this procedure:

Step 1 On the Navigation Frame, select *Security Manager->User Roles*. Figure 5 shows the Fabric Manager User summary.



Security Role Mapping Summary

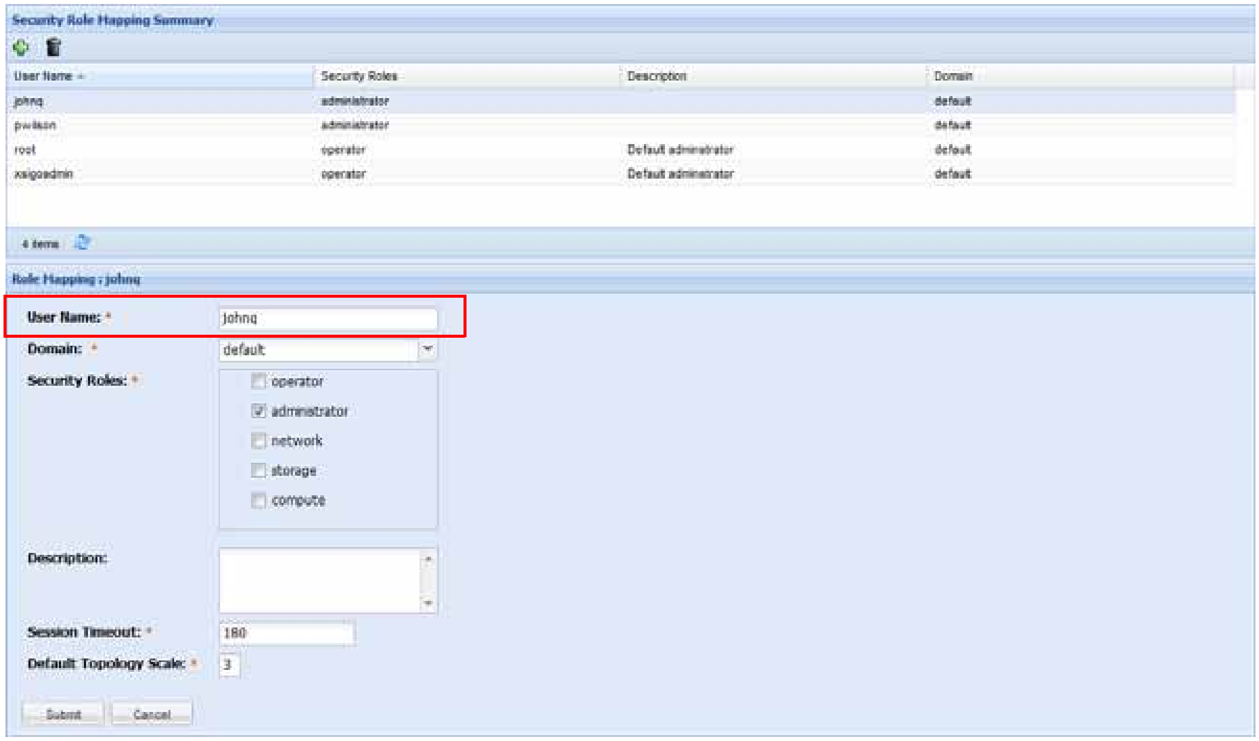
User Name	Security Roles	Description	Domain
johnq	administrator		default
myuserrole	operator		default
pwilson	administrator		default
root	operator	Default administrator	default
xsigoadmin	operator	Default administrator	default

5 items

Figure 5 Fabric Manager User Summary

Step 2 Select a Fabric Manager user to populate the details frame with its properties.

Step 3 Click the ***Edit*** button to edit the properties of the selected Fabric Manager user, as shown in Figure 6.



Security Role Mapping Summary

User Name	Security Roles	Description	Domain
johnq	administrator		default
pwilson	administrator		default
root	operator	Default administrator	default
xsigoadmin	operator	Default administrator	default

4 items

Role Mapping : johnq

User Name: *	johnq
Domain: *	default
Security Roles: *	□ operator ☑ administrator □ network □ storage □ compute
Description:	
Session Timeout: *	180
Default Topology Scale: *	3

Figure 6 Security Role Mapping Details — Editing Details to Rename Fabric Manager User

Step 4 In the *User Name* field, enter the new name for the Fabric Manager user.

Step 5 As an option, from the *Domain* dropdown menu, you can select or change the role for the Fabric Manager user.

Step 6 As an option, you also can set or change the roles for the selected Fabric Manager user.

Step 7 As an option, you also can set or change the description for the selected Fabric Manager user.

Step 8 When the new name has been specified for the Fabric Manager user, click ***Submit***.

Changing the Role Assigned to a User Account

After a user account has been created, you can change the role that is assigned to the account. When you change the role assigned to the account, it is possible to affect the priviliges assigned to the user. For example, if the user was part of the compute role, that user had the ability to affect Server Profiles. However, if you change that user account from the compute group to the operator group, that user no longer has the ability to affect Server Profiles. In this example, the user would be able to only view information (read-only) because of being configured in the new role.

Each user account can be assigned to only one role. So if the same person needs access to multiple aspects of the Fabric Director, you can either assign that person to a powerful role (such as server or administrators) or create two different user accounts that provide specific areas of control. For example, if you do not want to give user “timmy” the administrator role, but you want “timmy” to be able to control vNICs and vHBAs, you could create two user accounts:

- one account called “timmy_nic” and assign that user account to the network role.
- the other account called “timmy_hba” and assign that user account to the storage role.

Depending on which user account is used for logging in, the appropriate amount of control can be assigned without giving super user priviliges.

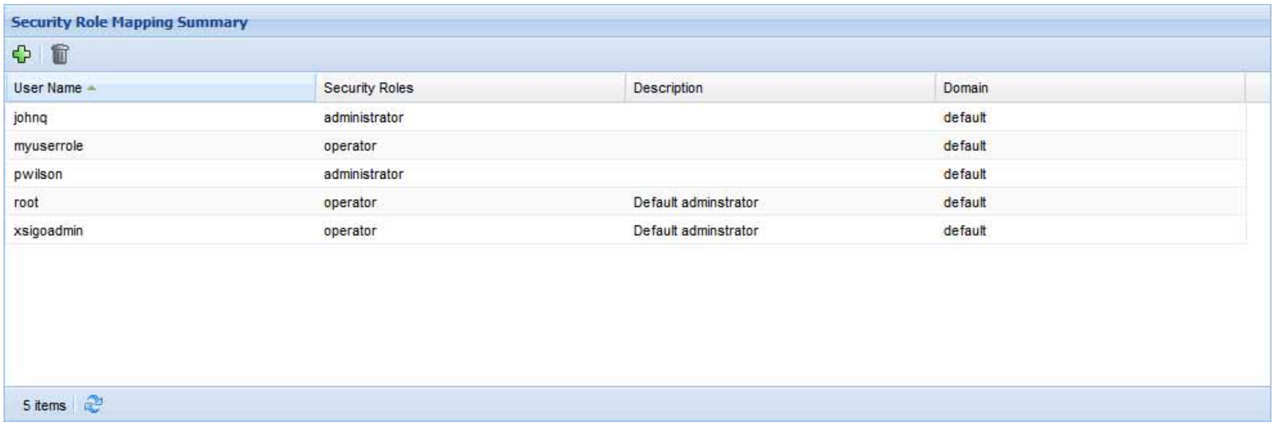
A role (and the privileges associated with it) are applied to the session for a user account whenever that user account logs in.

- If you change the role assigned to a user account, the new role (and its associated privileges) are applied the next time that user account logs in.
- If you change the role for an account that is currently logged in, the old role (and the associated privileges) remains in effect until that user account logs out of the current Fabric Manager session. For example, if two user accounts with administrator role are currently logged in, and you set the other user account’s role to something other than “administrator” that other account will still have “administrator” role (and its privileges) as long as it remains logged in. When the other account logs out, the new non-administrator role is applied whenever the other account logs in again.

You can change the role assigned to an existing user account through the User Details page for that user account.

To change the role assigned to a user account, follow this procedure:

Step 1 From the navigation panel, select *Service Manager->User Roles* to display the Security Role Mapping Summary. Figure 7 shows this table.



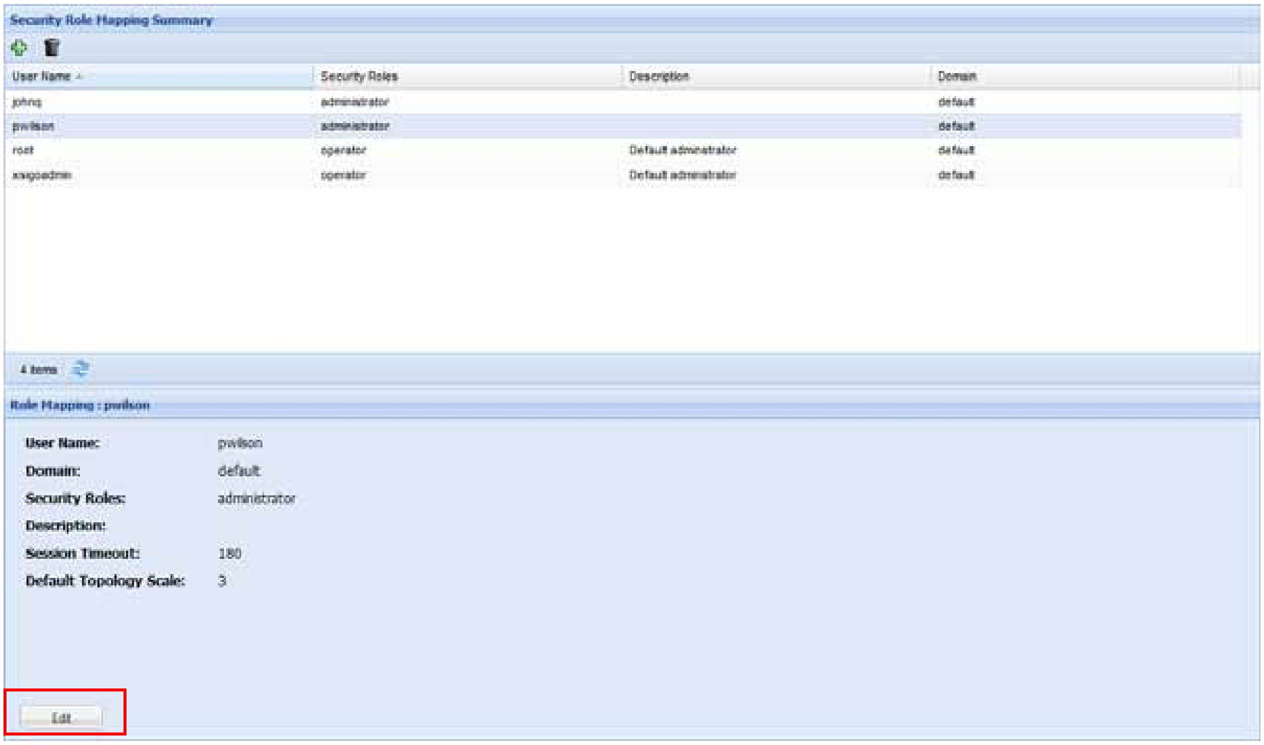
Security Role Mapping Summary

User Name	Security Roles	Description	Domain
johnq	administrator		default
myuserrole	operator		default
pwilson	administrator		default
root	operator	Default adminstrator	default
xsigoadmin	operator	Default adminstrator	default

5 items

Figure 7 Security Role Mapping Summary

Step 2 On the Security Role Mapping Summary, select the user account for which you want to change the security role. This step activates the Security Role Mapping Details frame and populates it with the details for the selected user. Figure 8 shows this page.



Security Role Mapping Summary

User Name	Security Roles	Description	Domain
johnq	administrator		default
pwilson	administrator		default
root	operator	Default adminstrator	default
xsigoadmin	operator	Default adminstrator	default

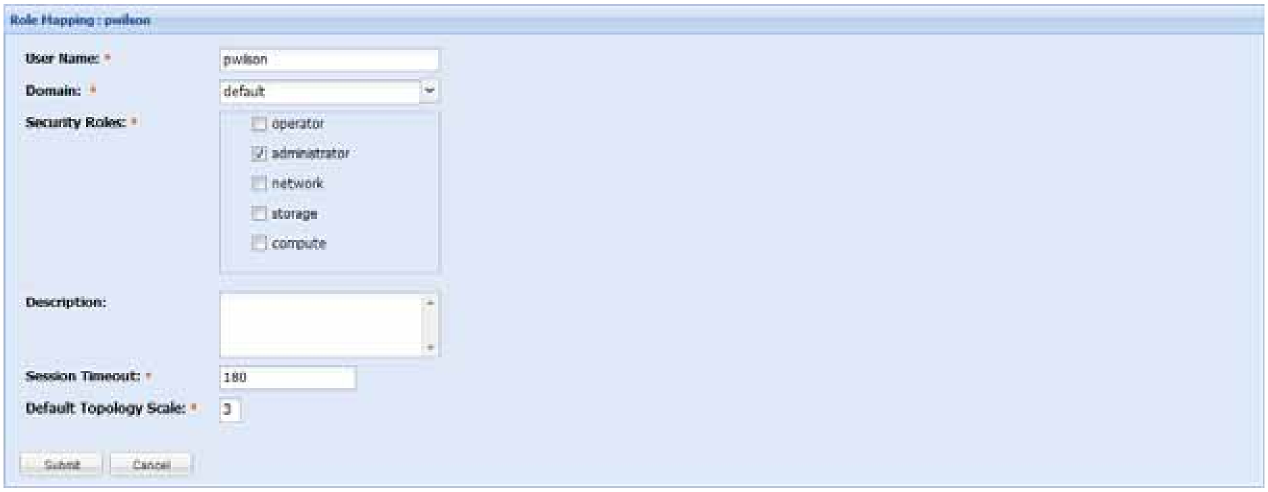
4 items

Role Mapping : pwilson

User Name:	pwilson
Domain:	default
Security Roles:	administrator
Description:	
Session Timeout:	180
Default Topology Scale:	3

Figure 8 Role Mapping Details Frame

Step 3 Click ***Edit...*** to unlock the editable fields in the Role Mapping Details frame, as shown in Figure 9.



Role Mapping : pwilson

User Name: *	pwilson
Domain: *	default
Security Roles: *	□ operator ☑ administrator □ network □ storage □ compute
Description:	
Session Timeout: *	180
Default Topology Scale: *	3

Figure 9 Security Role Mapping Details Frame — Editable

Step 4 As an option, in the *User Name* field, you can change the name of the Fabric Manager user for which roles will be set or changed.

Step 5 As an option, in the *Domain* dropdown menu, you can change the domain in which the user account exists.

Step 6 As an option, in the *Security Roles* list, you can change the security role assigned to the user account by clicking the checkbox next to the new role that you want to assign. A user can have only one role assigned to it.

Step 7 As an option, in the *Description* field, you can enter an alphanumeric character string that describes the user account that you are editing.

Step 8 When the user and its role information is correct, click ***Submit*** complete editing the user account and close the Role Mapping Details Frame. When you click ***Submit***, a confirmation dialog is displayed that requires to you confirm that you do actually want to make changes to the user account.

Step 9 On the confirmation dialog, click ***Yes*** to make the changes to the user account, or ***No*** to abort editing the user account without making any changes.

Mapping Users in External Groups Into Fabric Manager

Fabric Manager has enhanced group mapping functionality that enables you to specify a mapping between a user's group and either a role defined in Fabric Manager or a domain, or both. With this feature, the user's group is defined on an external Identity Management System (IMS) such as AD or LDAP, and when that user logs into the group, that group is mapped to a Fabric Manager role (if desired), or a specific domain in Fabric Manager (if desired) or both. As a result of the group mapping to role or domain (or both), the user then gets either the corresponding role, or access to only the resources in the mapped domain, or both the corresponding role and resources in the mapped domain.

Groups are identified by a regular expression that is matched against the list of groups to which a user belongs. (Regular expressions are parts of strings that represent a pattern for the overall larger string, and they can contain wildcards for the substitution of the rest of the overall string. For example, `app.*` is a regular expression for "applications".) When a match is found, the role (or domain) is set for that user to that specified in the mapping.

Note

The regular expression must match the whole group name not part of it. For example, `abc` would not match for the group `abcd`. However, `abc.*` would match the group name.

With the Group Mapping feature, you can specify a mapping of a group name to a Fabric Manager role, or group name to domain so that a user does not have to add special groups just for Fabric Manager.

The Group Mapping feature can be used instead of creating Fabric Manager users and roles and domains. However, if the user is configured through a Group Mapping and a Fabric Manager local user, priority is given to the Fabric Manager user and its associated roles or domains.

Consider the following example. Assume a user belongs to the following groups:

```
admins, administrators, adminguys, customerA
```

The group mapping can be created to allow a user to log in as admin in a domain called `customer_a`:

Table 2 Group Mapping to Role or Domain

Group	Role/Domain
admin.*	Role: administrator
CustomerA	Domain: customer_a

In this example, the same user would be able to login as a member of any admin.* group and receive the "administrator" role in Fabric Manager, and if the same user is able to login to the `CustomerA` group, then that user would also have access to the resources that belong to the `customer_a` domain.

A mapping can be created for both a role and a domain. In such a case, the two options are additive, so the user would log into any admin group and receive the administrator role for only the domain `customer_a`. If the user is part of a different group that receives a different role, or the group is mapped to a different domain, then different conditions could apply.

Group Role mapping is accessible through the Security Manager on the navigation frame. See the following sections:

- Mapping an External IMS Group to a Fabric Manager Role
- Mapping a Group to a Domain

Mapping an External IMS Group to a Fabric Manager Role

The Group Mapping feature has a separate tab for mapping external IMS groups (for example, AD groups) to Fabric Manager roles. On the Group Mapping summary, the *Group Role Mapping Summary* tab supports linking one or more groups in an external IMS to one or more specific Fabric Manager roles. When multiple roles are set for a mapping, the users that are in the affected group are mapped into the corresponding roles. For example, assume the group `Xsigo_Server_Storage_Admins` is created on an AD server. This group is then mapped to the Server and Storage roles in the Fabric Manager RBAC roles. This mapping is supported, and in this case, users in the `Xsigo_Server_Storage_Admins` group will now have multiple roles.

To support enhanced security, the `no-access role` can be used. This role is a special case that allows no access to Fabric Manager, not even read-only access. With the no-access role, you can block certain groups from even seeing any of the information within Fabric Manager. For strictest security, Xsigo recommends putting the domain users of Fabric Manager and Fabric Directors into their respective groups, and putting everyone else into the no-access group.

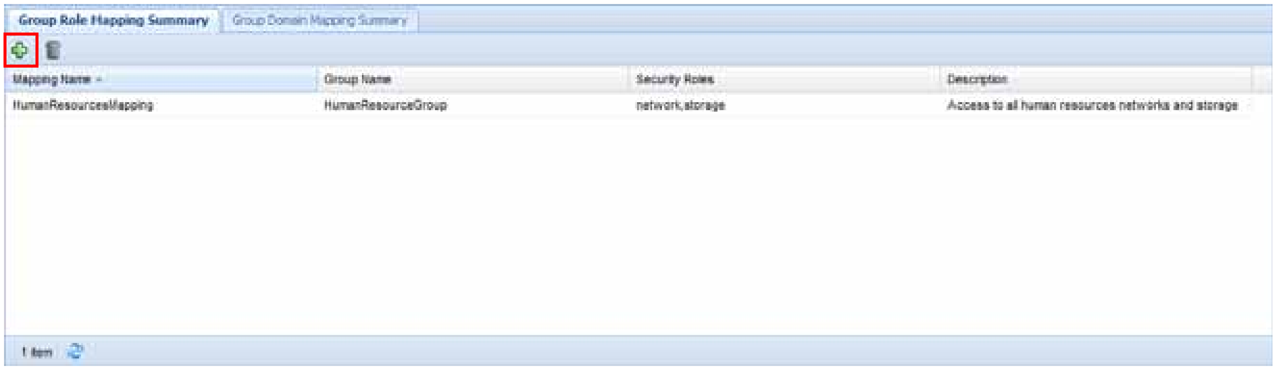
Note

When mapping external IMS groups, be aware that currently you cannot have an administrator, network, storage, or compute role in a non-default domain. If these roles are used in a non-default domain, users will be logged in as operator (read-only). In the default domain, administrator, network, storage, and compute roles can be assigned and function predictably.

To map an external IMS group to a Fabric Manager role, follow this procedure:

Step 1 On the navigation frame, select *Security Manager->Group Mapping* to display the group mapping summary. By default, the *Group Role Mapping Summary* tab should be displayed, as shown in Figure 10.

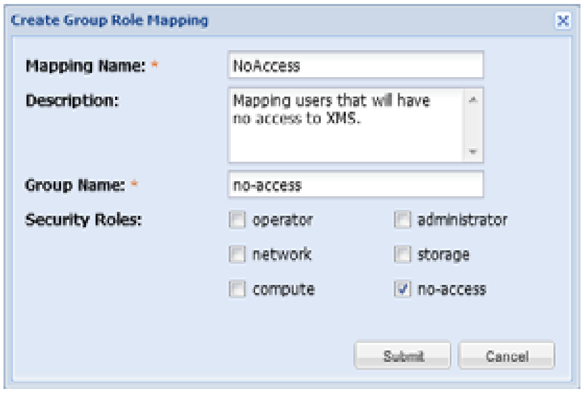
If the *Group Role Mapping Summary* tab is not displayed, click it now.



Mapping Name ⌄	Group Name	Security Roles	Description
HumanResourcesMapping	HumanResourceGroup	network,storage	Access to all human resources networks and storage

Figure 10 Group Mapping — Role Summary

Step 2 On the Group Role Summary tab, click the plus sign (+) to display the Create Group Role Mapping dialog. Figure 11 shows this dialog.



Create Group Role Mapping

Mapping Name: * NoAccess

Description: Mapping users that will have no access to XMS.

Group Name: * no-access

Security Roles: □ operator □ administrator □ network □ storage □ compute ☑ no-access

Figure 11 Group Mapping — Create Role Mapping for Group

Step 3 In the *Mapping Name* field, enter the name of the mapping that you are creating for the external IMS group.

Step 4 As an option, in the *Description* field, enter an alphanumeric character string that describes the mapping that you are creating.

Step 5 In the *Group Name* field, enter the name of the external IMS group that you are mapping to a Fabric Manager role. Enter the group name exactly as it appears on the external IMS (for example, exactly as it appears on the AD server) or in the form of a regular expression.

Step 6 From the *Security Roles* checkboxes, select the Fabric Manager role that you want the External IMS group mapped to. This step determines the exact privileges that will be granted to any user in the mapped group. Table 1 shows the Fabric Manager roles and provides a brief description of what each role controls.

Note

For `Network`, `Storage`, and `Compute` roles, you can assign some or all of these roles to the same group. For `Administrator` and `Operator` roles, these roles are mutually exclusive with each other, and all other roles. You can assign either `Administrator` or `Operator` to the same group.

Step 7 When the mapping name, external group name and Fabric Manager roles have been specified, click ***Submit*** to create the mapping. When the mapping is successfully created, any user that logs in to the specified group will receive the correct role in Fabric Manager.

Mapping a Group to a Domain

The Group Mapping feature has a separate tab for mapping external IMS groups (for example, AD groups) to Fabric Manager domains. On the Group Mapping summary, the *Group Domain Mapping Summary* tab supports linking one or more groups in an external IMS to one or more specific Fabric Manager domains.

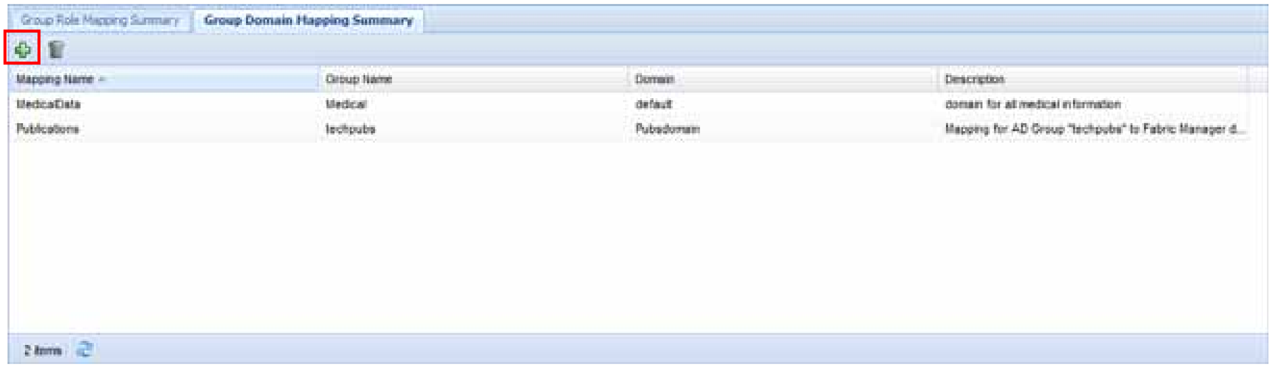
Note

Fabric Manager has a default domain, which encompasses all resources discovered and managed by Fabric Manager. The default domain always exists even if specific domains exist. If you will be mapping an external IMS group to a specific Fabric Manager domain, that specific domain must already exist to be a selectable option. If you need to create a specific domain, see Working with Domains.

To map an external IMS group to a specific domain in Fabric Manager follow this procedure:

Step 1 From the navigation frame, select *Security Manager->Group Mapping*. By default, the Group Role Mapping Summary is displayed.

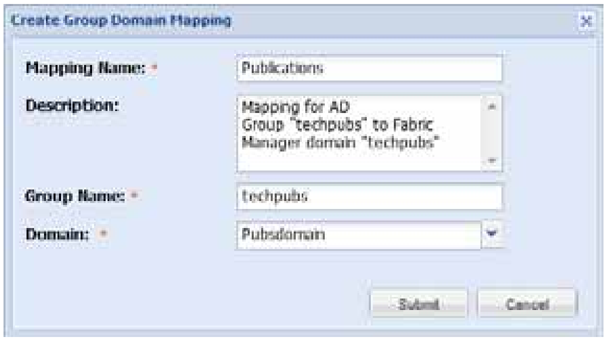
Step 2 Click the *Group Domain Mapping Summary* tab to display the Group Domain Mapping Summary, as shown in Figure 12.



Mapping Name	Group Name	Domain	Description
MedicalData	Medical	default	domain for all medical information
Publications	techpubs	Pubsdomain	Mapping for AD Group "techpubs" to Fabric Manager d...

Figure 12 Group Mapping — Domain Mapping Summary

Step 3 On the Group Domain Mapping Summary, click the plus sign (+) to display the Create Role Domain Mapping dialog. Figure 13 shows this dialog.


Create Group Domain Mapping

Mapping Name: * Publications

Description: Mapping for AD Group "techpubs" to Fabric Manager domain "techpubs"

Group Name: * techpubs

Domain: * Pubsdomain

Figure 13 Group Mapping — Create Role Mapping for Domain

Step 4 In the *Mapping Name* field, enter the name of the mapping that you are creating for the external IMS group.

Step 5 As an option, in the *Description* field, enter an alphanumeric character string that describes the mapping that you are creating.

Step 6 In the *Group Name* field, enter the name of the external IMS group that you are mapping to a Fabric Manager role. Enter the group name exactly as it appears on the external IMS (for example, exactly as it appears on the AD server) or in the form of a regular expression.

Step 7 From the *Domain* dropdown menu, select the domain to which users in the external IMS group will be mapped. The domain must be configured for it to be a selectable option. If the domain you want is not listed, it does not exist in Fabric Manager and must be created. See Working with Domains.

Step 8 When the mapping name, external group name, and Fabric Manager domain have been specified, click ***Submit*** to create the mapping. When the mapping is successfully created, any user that logs in to the specified group will be granted access to only the resources available in the specified domain.

Configuring Fabric Manager to Authenticate Users Against AD

This section documents how to configure Fabric Manager so that it authenticates users against AD. When this procedure is complete, users in the AD domain will be able to log in to Fabric Manager and use the RBAC user role you assign to them through Fabric Manager. If you will be using LDAP/AD for authentication in a Windows domain, install the Fabric Manager software on a Windows server that is a member of that domain as mentioned in Installing Fabric Manager on a Windows Server.

Note

A separate procedure exists if you want users to be able to log in to the Fabric Director itself. You can use Fabric Manager to configure this method of access—for example, allowing AD to authenticate users that `ssh` into Oracle's Xsigo Fabric Director. For more information, see Displaying Active Directory Properties and Configuring AD Properties for Fabric Manager.

To configure authentication of Fabric Manager users against AD LDAP users, the procedure occurs on both the AD server and on in Fabric Manager.

Set Up the AD Server

Users and groups need to exist on the AD server.

- If they do not exist, you will need to configure the users and group(s) for Fabric Manager that you want AD LDAP to authenticate. Then, you will need to add the users to their respective group(s). This section documents creating the users and groups on the AD server. For illustrative purposes, this procedure uses `user0` and `XsigoAdmin` as the user and group that will be accessing Fabric Manager and using AD authentication to do so. If your users and groups do not already exist, perform the procedure in this section.
- If they already exist, you can use a regular expression when mapping the existing group to a Fabric Manager user role. For information about regular expressions and mapping the role groups, see Mapping Users in External Groups Into Fabric Manager. When you are familiar with using regular expressions in the group role mapping, proceed to Set Up the Group In Fabric Manager and Assign Roles. You do not need to perform the procedure in this section if the users and groups already exist.

To configure the users and groups on the AD server, follow this procedure:

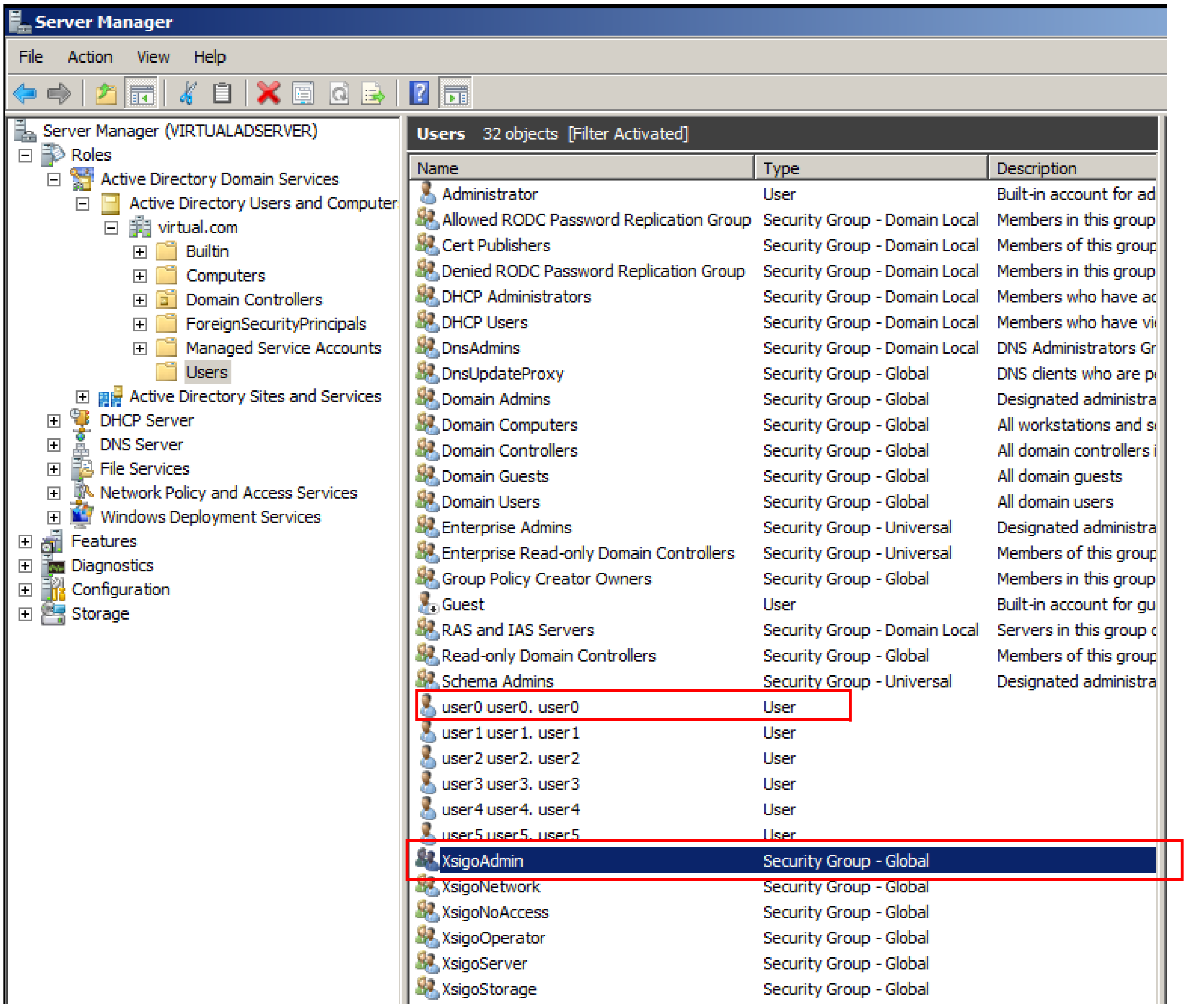
Note

The following procedure provides general guidelines. If you need additional help with creating AD groups and users, see the documentation that accompanied your AD server.

Step 1 Log in to the AD server as a domain administrator.

Step 2 Using AD Server Manager (or whichever method you choose), create the group for Fabric Manager that will need authentication through AD.

Step 3 Using AD Server Manager (or whichever method you choose), create the users in the group that will be authenticated when accessing Fabric Manager. See Figure 14.


Server Manager
File
Action
View
Help
Server Manager (VIRTUALADSERVER)
Roles
Active Directory Domain Services
Active Directory Users and Computer
virtual.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Active Directory Sites and Services
DHCP Server
DNS Server
File Services
Network Policy and Access Services
Windows Deployment Services
Features
Diagnostics
Configuration
Storage

Users 32 objects [Filter Activated]

Name	Type	Description
Administrator	User	Built-in account for ad
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group
Cert Publishers	Security Group - Domain Local	Members of this group
Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group
DHCP Administrators	Security Group - Domain Local	Members who have ac
DHCP Users	Security Group - Domain Local	Members who have vi
DnsAdmins	Security Group - Domain Local	DNS Administrators Gr
DnsUpdateProxy	Security Group - Global	DNS clients who are p
Domain Admins	Security Group - Global	Designated administra
Domain Computers	Security Group - Global	All workstations and s
Domain Controllers	Security Group - Global	All domain controllers i
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Universal	Designated administra
Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group
Group Policy Creator Owners	Security Group - Global	Members in this group
Guest	User	Built-in account for gu
RAS and IAS Servers	Security Group - Domain Local	Servers in this group c
Read-only Domain Controllers	Security Group - Global	Members of this group
Schema Admins	Security Group - Universal	Designated administra
user0 user0. user0	User	
user1 user1. user1	User	
user2 user2. user2	User	
user3 user3. user3	User	
user4 user4. user4	User	
user5 user5. user5	User	
XsigoAdmin	Security Group - Global	
XsigoNetwork	Security Group - Global	
XsigoNoAccess	Security Group - Global	
XsigoOperator	Security Group - Global	
XsigoServer	Security Group - Global	
XsigoStorage	Security Group - Global	

Figure 14 Create User(s) and Group(s) on the AD Server

In this example, `user0` is a member of the `XsigoAdmin` group.

Step 4 Repeat this procedure as needed to create additional AD groups and users.

When the AD groups and users are completely configured, you need to map the group(s) into one or more Fabric Manager RBAC role groups. Proceed to Set Up the Group In Fabric Manager and Assign Roles.

Set Up the Group In Fabric Manager and Assign Roles

When you set up Fabric Manager, you will map the existing AD group(s) into Fabric Manager and assign one or more user roles to those group(s). Any users that log in through the group (`XsigoAdmin` in this example) will get the role assigned to the group.

To map the AD group into Fabric Manager and assign roles, follow this procedure:

Step 1 Verify that the server where Fabric Manager software is (or will be) installed is a member of the AD domain. (For example, if the AD domain covers `companyA.com`, make sure that the Windows Fabric Manager Server is a member of a fully qualified domain name for `companyA.com`., such as `xmsserver.companyA.com`

> Note
>
> The Fabric Manager Server and the AD server(s) must all be in the same domain. If any of this equipment is in a different domain, authentication will not complete successfully.

Step 2 Log in to Fabric Manager with a Fabric Manager local administrator account (not the AD domain account).

Step 3 Click the *Maintenance* icon, which looks like a screwdriver on the banner. Figure 15 shows this option.

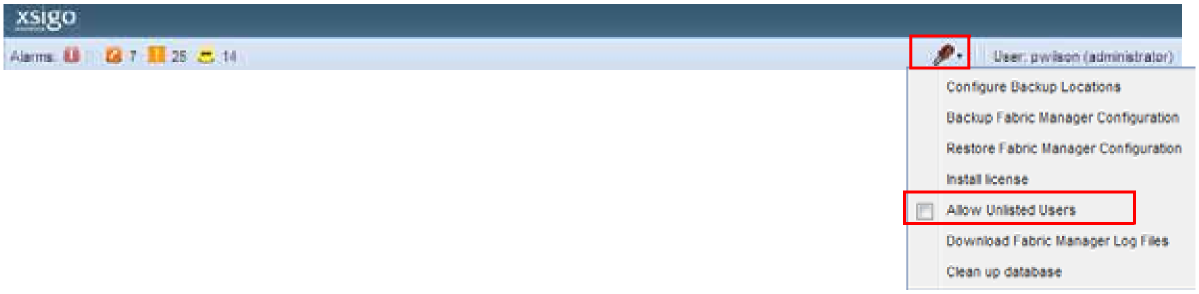
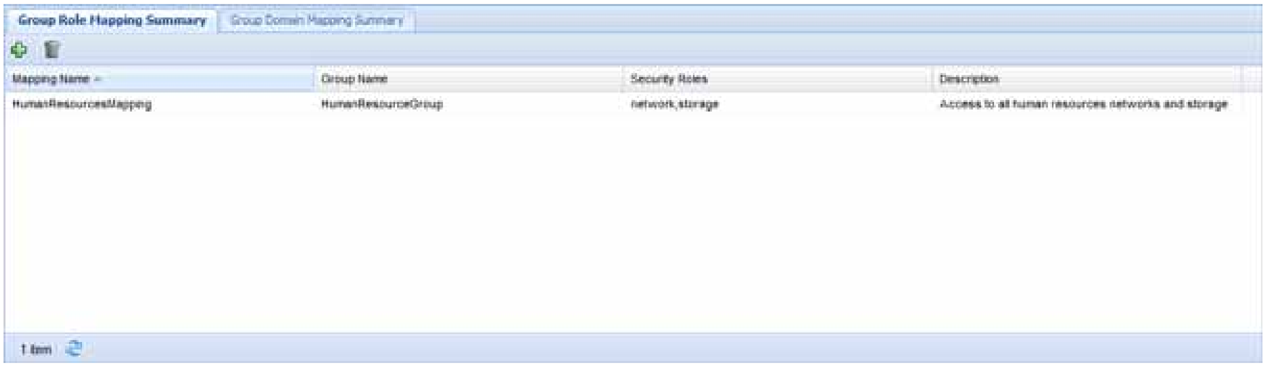

xsigo
Alarms: 0 7 25 14
User: pwilson (administrator)
Configure Backup Locations
Backup Fabric Manager Configuration
Restore Fabric Manager Configuration
Install license
□ Allow Unlisted Users
Download Fabric Manager Log Files
Clean up database

Figure 15 Allowing Unlisted Users Access to Fabric Manager

Step 4 Click the check box to allow or prevent unlisted users access to Fabric Manager. This option allows users not specifically configured in Fabric Manager (for example, users configured on an AD server) to be allowed access to Fabric Manager.

> Note
>
> For more information about the Allowed Unlisted User options, see Allowing or Preventing Unlisted Users Access to Fabric Manager.

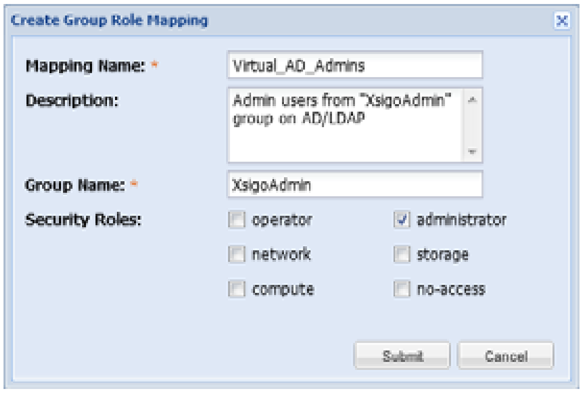
Step 5 Select *Security Manager->Group Mapping* to display the Group Role Mapping Summary tab as shown in Figure 16.



Mapping Name	Group Name	Security Roles	Description
HumanResourcesMapping	HumanResourceGroup	network,storage	Access to all human resources networks and storage

Figure 16 Group Mapping Summary

Step 6 On the Group Role Mapping Summary, click the plus sign (+) to display the Create New Group Role Mapping dialog as shown in Figure 17.



Mapping Name: * Virtual_AD_Admins

Description: Admin users from "XsigoAdmin" group on AD/LDAP

Group Name: * XsigoAdmin

Security Roles: □ operator ☑ administrator □ network □ storage □ compute □ no-access

Figure 17 Creating Group Role Mapping for the AD Group on the AD Server

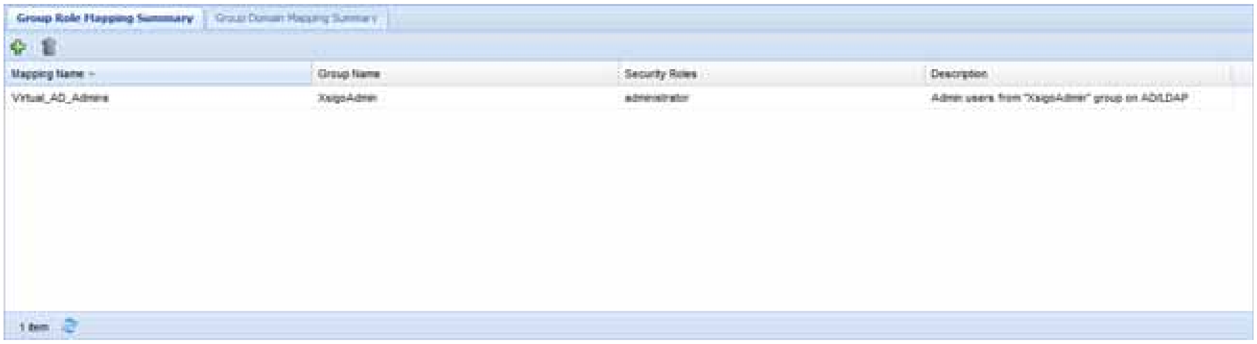
Step 7 In the *Mapping Name* field, enter an alphanumeric character string that names or describes the group role mapping that you are configuring.

Step 8 As an alternative, in the *Description* field, you can enter a string that describes the mapping from the AD group to the Fabric Manager role.

Step 9 In the *Group Name* field, enter the name of AD Group you configured on the AD server (`XsigoAdmin` in this example). The group name must be an exact match between the AD server and this field. This field supports regular expressions. (For more information about regular expressions in a group role mapping, see Mapping Users in External Groups Into Fabric Manager.)

Step 10 From the *Security Roles* checkboxes, click the appropriate role(s) that you are granting to the user(s) that are members of the AD group named in the *Group Name* field. In this example, any user (such as `user0`) from the `XsigoAdmin` group that logs in to Fabric Manager will be granted administrator privileges in Fabric Manager after AD authentication occurs successfully.

Step 11 Click ***Submit*** and verify that the role group mapping was created correctly. See Figure 18. Make sure that the AD group displayed in the *Group Name* field correctly represents the AD group configured on the AD server.



Mapping Name	Group Name	Security Roles	Description
Virtual_AD_Admins	XsigoAdmin	administrator	Admin users from "XsigoAdmin" group on AD/LDAP

Figure 18 Group Role Mapping for AD Group

Step 12 On the Fabric Manager banner, click ***Logout*** as shown in Figure 19.

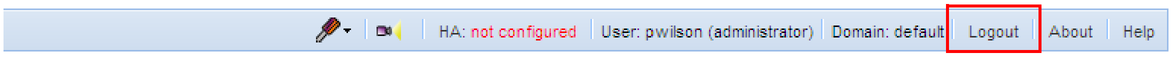

HA: not configured | User: pwilson (administrator) | Domain: default

Figure 19 Log Out of Fabric Manager

Step 13 Log in to Fabric Manager as one of the users from the AD group you just mapped into Fabric Manager, as shown in Figure 20. In this example, the user `user0` is logging in to Fabric Manager.

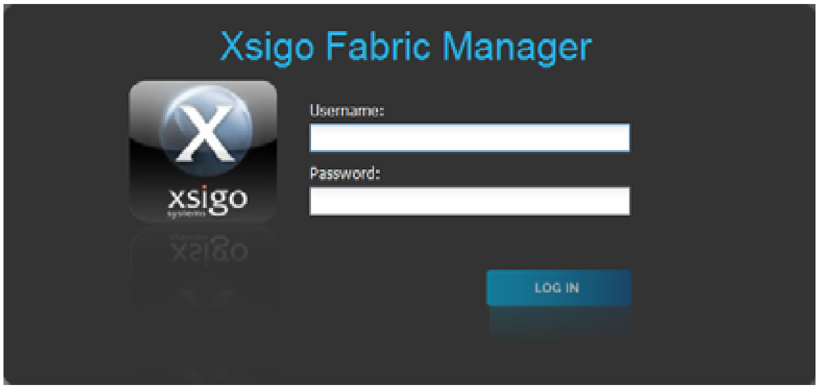


Figure 20 Log In to Fabric Manager as a User from the AD Group

Step 14 Check the Fabric Manager banner for the currently logged in user, which should be the user from the AD group that you just used to log in to Oracle's Xsigo Fabric Manager. Also, make sure that the correct user role is assigned to the user. See Figure 21.

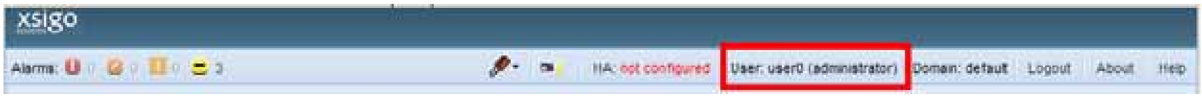
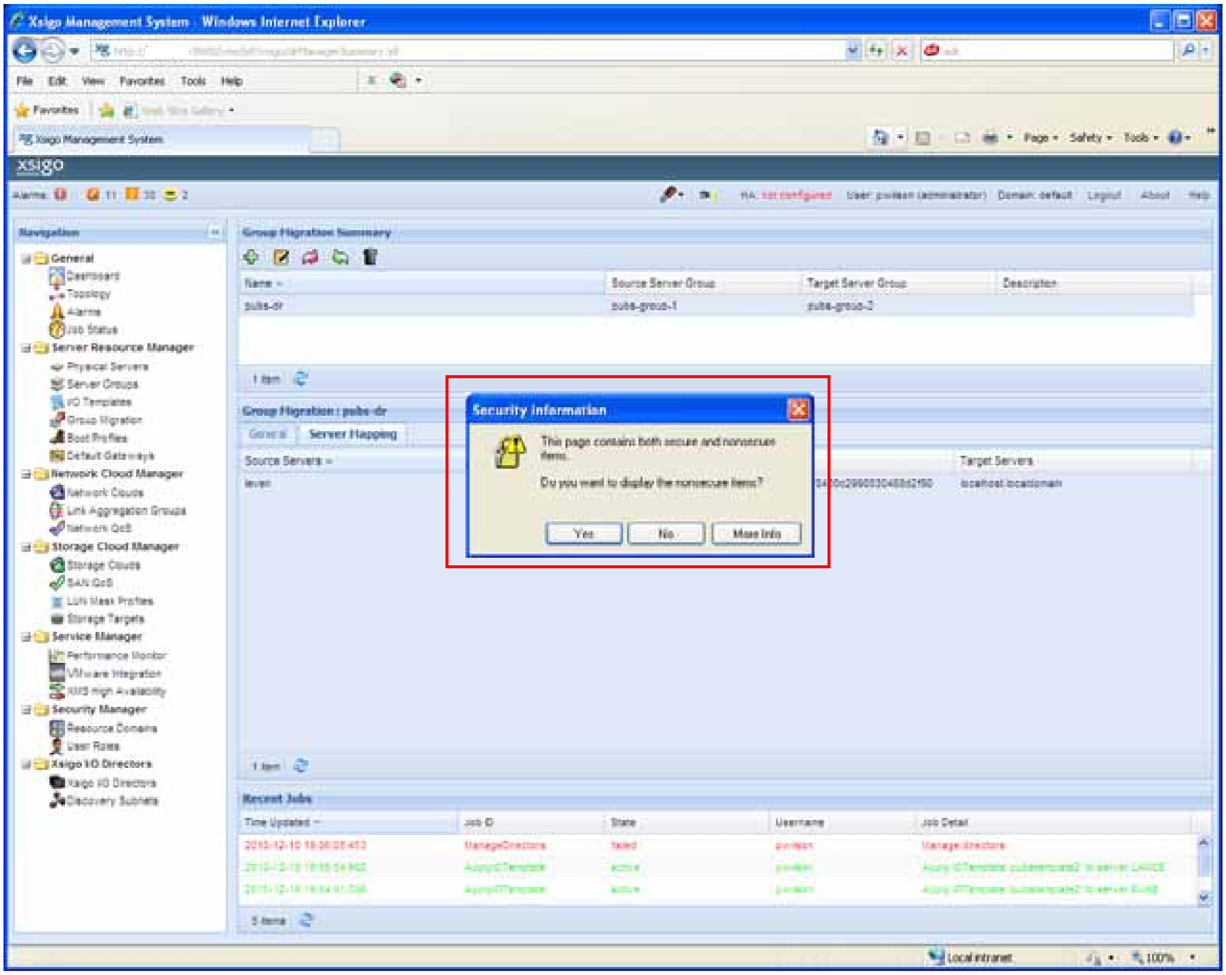


Figure 21 Banner Showing User from AD Group Logged In

Step 15 Repeat this procedure as needed to create additional mappings for additional AD groups.

When using Oracle’s Xsigo Fabric Manager with Internet Explorer, you might see the Security Information pop-up dialog whenever a new Fabric Manager page is displayed. The pop-up informs you about secure and non-secure content on the page, and requires you to choose whether the non-secure items are displayed. Figure 1 shows an example of this popup, which primarily has occurred in an IE 7.0 browser.



This page contains both secure and nonsecure items.

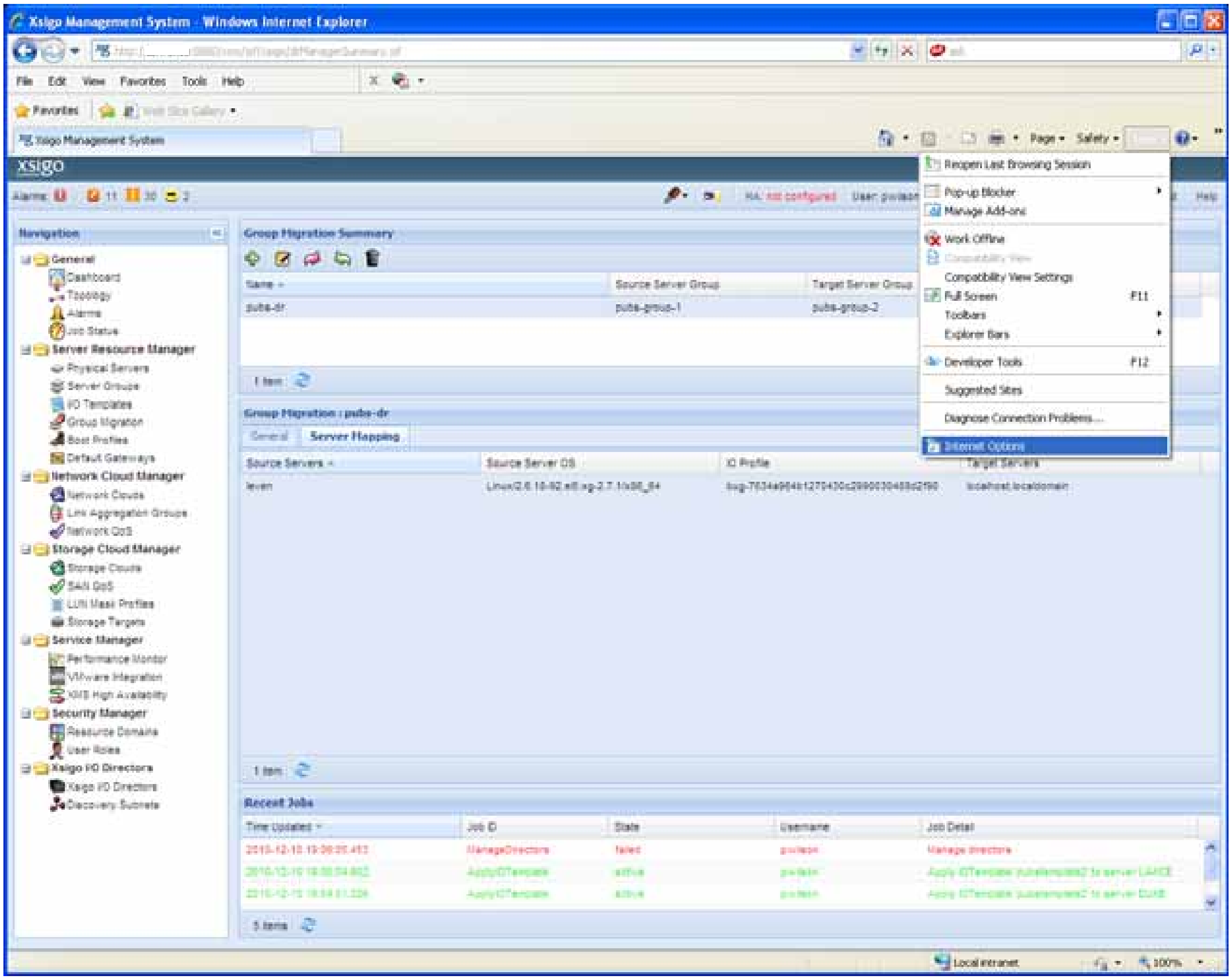
Do you want to display the nonsecure items?

Figure 1 Internet Explorer Security Information Prompt

The recurring Security Information pop-up can be inconvenient when you are using Fabric Manager with IE to configure and manage Xsigo virtual I/O. You can change a setting within IE and stop the prompt from being displayed.

To stop the Security Information prompt from being displayed, follow this procedure:

Step 1 Select *Tools->Internet Options* as shown in Figure 2.



Name	Source Server Group	Target Server Group
pubs-dr	pubs-group-1	pubs-group-2

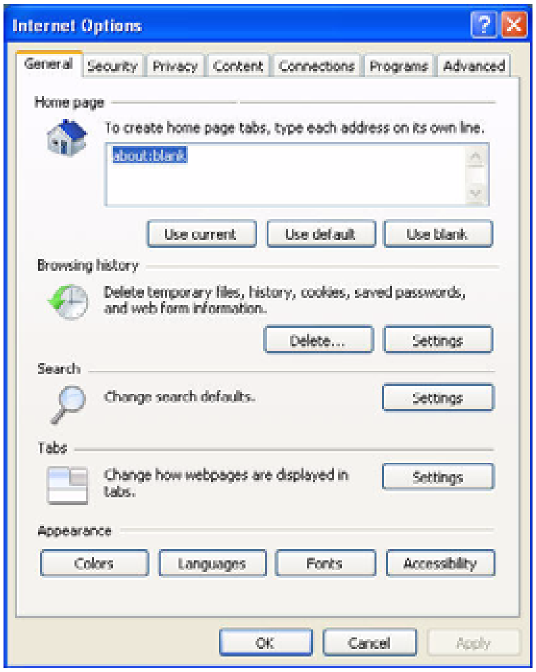
Source Servers	Source Server OS	IO Profile	Target Servers
leven	Linux/2.6.18-92.el5.xg-2.7.1/x86_64	[illegible]	localhost.localdomain

Figure 2 Tools Menu — Internet Options

Note

Figure 2 shows the default browser layout for Internet 7.0. Because IE browser layout can be customized, the *Tools* menu might appear in a different location if you have set a custom format. However, regardless of the IE browser format, the *Tools* menu should always be present.

When you select Internet Options, the Internet Options page is displayed as shown in Figure 3.



To create home page tabs, type each address on its own line.

about:blank

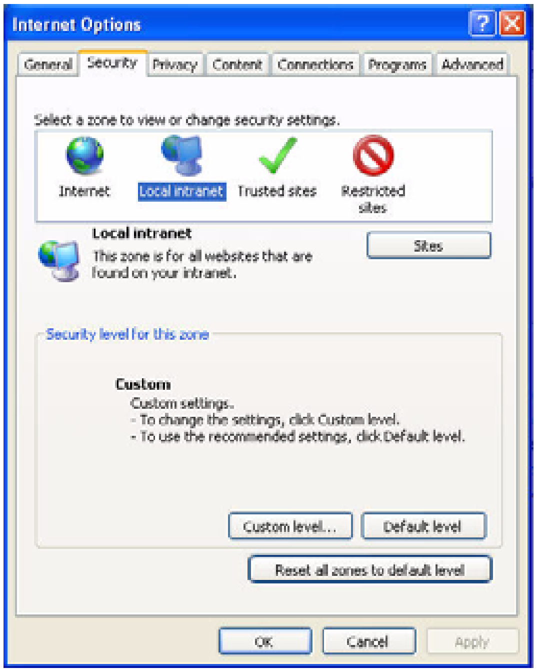
Delete temporary files, history, cookies, saved passwords, and web form information.

Change search defaults.

Change how webpages are displayed in tabs.

Figure 3 Internet Explorer — Internet Options Dialog

Step 2 Click the *Security* tab as shown in Figure 4.



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

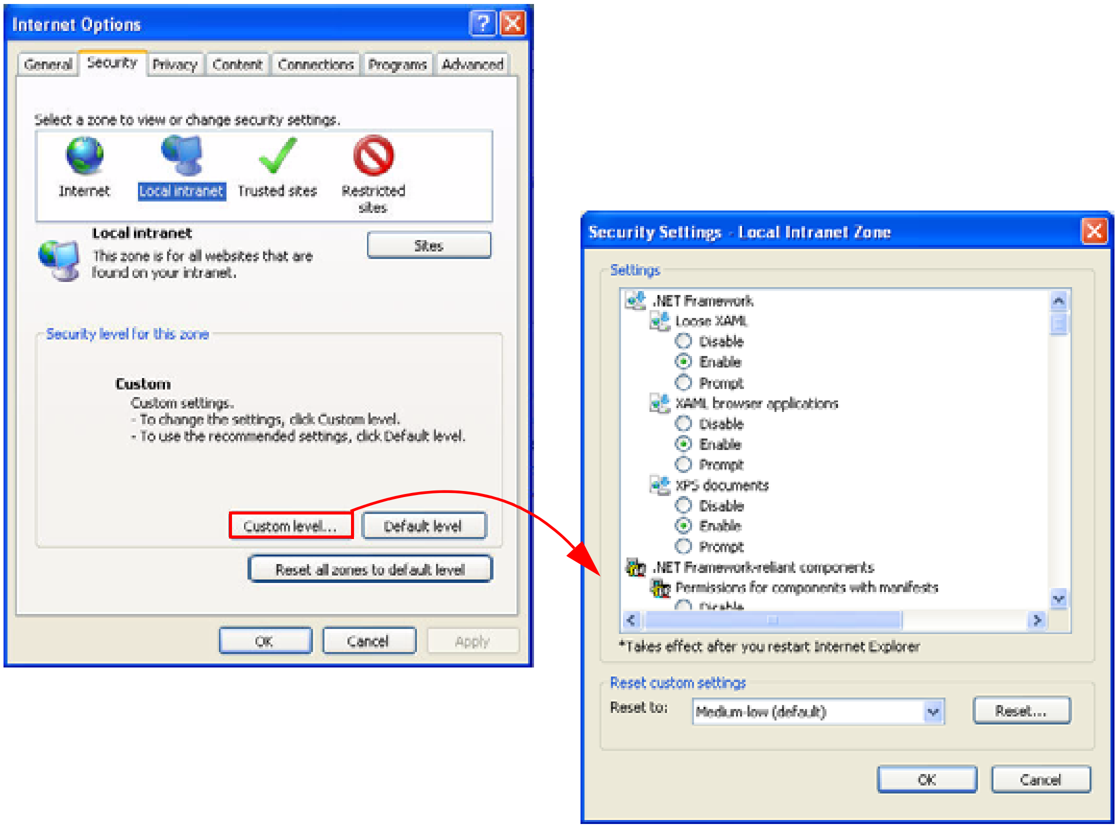
Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

Figure 4 Internet Explorer Internet Options Dialog — Security Tab

Step 3 In the “Select a zone to view or change security settings” section, click one of the four zones displayed to select it. Because your Fabric Manager Client and Oracle’s Xsigo Fabric Manager Server might span multiple zones, you should disable the Security Information pop-up in all zones. You will need to do so for each zone individually.

Step 4 Click ***Custom Level...*** to display the Security Settings dialog as shown in Figure 5.



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

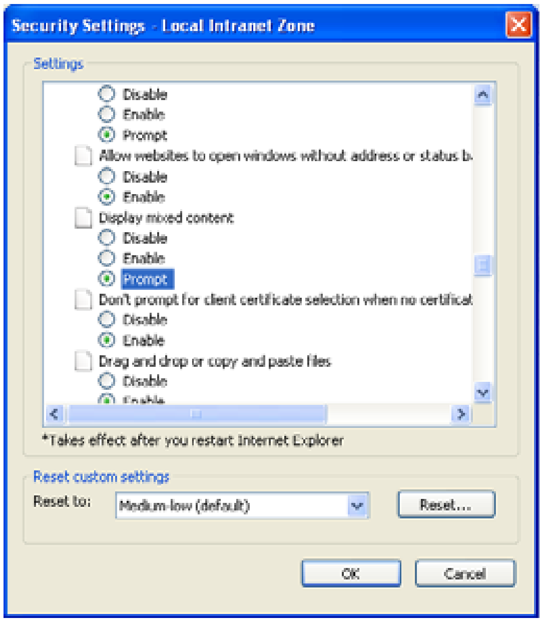
.NET Framework
Loose XAML
○ Disable
● Enable
○ Prompt
XAML browser applications
○ Disable
● Enable
○ Prompt
XPS documents
○ Disable
● Enable
○ Prompt
.NET Framework-reliant components
Permissions for components with manifests
○ Disable

*Takes effect after you restart Internet Explorer

Reset to: Medium-low (default)

Figure 5 Internet Explorer Security Settings Dialog

Step 5 Scroll down until you find a setting called *Display mixed content* in the “Miscellaneous” section which is near the bottom of the list. Figure 6 shows this setting.



Security Settings - Local Intranet Zone

Settings

○ Disable
○ Enable
● Prompt
Allow websites to open windows without address or status b
○ Disable
● Enable
Display mixed content
○ Disable
○ Enable
● Prompt
Don't prompt for client certificate selection when no certificat
○ Disable
● Enable
Drag and drop or copy and paste files
○ Disable
● Enable

*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-low (default)

Figure 6 Security Settings Dialog — Display Mixed Content

Note

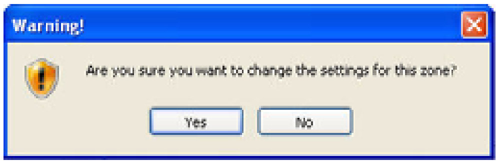
[Figure 6] shows the default state (“Prompt”) for the *Display mixed content* setting. This setting can be changed to control whether the Security Information pop-up is displayed.

Step 6 From the *Display mixed content* setting, select “Enable” to allow the display of secure and non-secure information in the browser.

Step 7 Click ***OK*** to accept “Enabled.”

Step 8 Repeat Step 3 on page 518 through Step 7 on page 519 for all zones to disable the Security Information pop-up for each zone individually.

Step 9 When the *Display mixed content* setting is set to “Enabled” for all zones, click ***Apply*** on the Security Options page. A warning dialog is displayed as shown in Figure 7.



Warning!

Are you sure you want to change the settings for this zone?

Figure 7 Warning! Pop-up — Changing Settings

Step 10 Click ***Yes*** to confirm the state change and close the *Warning!* pop-up.

Step 11 Click ***OK*** on any remaining dialogs to close them.