

ExtremeManagement™

Virtualization Configuration using Extreme Fabric Orchestrator

Release 1.2
NN48100-503
Issue 03.01
December 2017

© 2017, Extreme Networks, Inc.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Extreme Networks, Inc. assumes no liability for any errors. Extreme Networks, Inc. reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Extreme Networks shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks' agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Extreme Networks provides a limited warranty on Extreme Networks hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Extreme Networks' standard warranty language, as well as information regarding support for this product while under warranty is available to Extreme Networks customers and other parties through the Extreme Networks Support website: <http://www.extremenetworks.com/support> under the link "Policies" or such successor site as designated by Extreme Networks. Please note that if You acquired the product(s) from an authorized Extreme Networks Channel Partner outside of the United States and Canada, the warranty is provided to You by said Extreme Networks Channel Partner and not by Extreme Networks.

"Hosted Service" means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU

REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND EXTREME NETWORKS INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE ("EXTREME NETWORKS").

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Extreme Networks or an Extreme Networks Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Extreme Networks through electronic means established by Extreme Networks specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Extreme Networks, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Extreme Networks' prior consent and payment of an upgrade fee.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Extreme Networks' website at: <http://www.extremenetworks.com/support/policies/software-licensing> or such successor site as designated by Extreme Networks. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Service Provider

THE FOLLOWING APPLIES TO EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS

AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Extreme Networks product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Security Vulnerabilities

Information about Extreme Networks' security support policies can be found in the Global Technical Assistance Center Knowledgebase at <https://gtacknowledge.extremenetworks.com/>.

Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: <http://documentation.extremenetworks.com>, or such successor site as designated by Extreme Networks.

Contact Extreme Networks Support

See the Extreme Networks Support website: <http://www.extremenetworks.com/support> for product or Hosted Service notices and articles, or to report a problem with your Extreme Networks product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Extreme Networks Support website: <http://www.extremenetworks.com/support/contact/> (or such successor site as designated by Extreme Networks), scroll to the bottom of the page, and select Contact Extreme Networks Support.

Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Extreme Networks, Inc., its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Extreme Networks or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Extreme Networks or the applicable third party.

Extreme Networks is a registered trademark of Extreme Networks, Inc.

All non-Extreme Networks trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

For additional information on Extreme Networks trademarks, please see: <http://www.extremenetworks.com/company/legal/>

Contents

Chapter 1: Preface	8
Purpose.....	8
Training.....	8
Providing Feedback to Us.....	8
Getting Help.....	8
Extreme Networks Documentation.....	9
Subscribing to service notifications.....	10
Chapter 2: New in this document	11
Chapter 3: Virtualization overview	12
VMware vCenter.....	13
Role Based Access Control.....	13
Core Services.....	14
Distributed services.....	14
vCenter plug-ins.....	14
vCenter services interfaces.....	15
vCenter event types.....	15
Use of virtual machines.....	16
One Hop Up Provisioning configuration.....	16
One hop up provisioning prerequisites.....	17
EFO Virtualization user interface.....	18
Topology.....	18
Inventory.....	19
Event Monitor.....	21
Network Profiles.....	22
Rules.....	22
Reports.....	23
Audit logs.....	23
Network Validation.....	23
Device Management.....	24
Chapter 4: Virtualization common icons and procedures	26
EFO Virtualization application icons.....	26
Show or hide columns.....	27
Filter information.....	28
Chapter 5: CDP and LLDP settings configuration	30
Configuring CDP settings on the dvSwitch.....	30
Configuring CDP settings on the vSwitch.....	31
Configuring LLDP settings on the Extreme Networks device.....	31
Configuring LLDP settings on the dvSwitch.....	33
Configuring the location and application type of the ESX server.....	34

Chapter 6: Managing Virtualization..... 35

- vCenter connectivity status..... 35
- Network Discovery procedures..... 35
 - Viewing Virtualization Network Discovery status summary..... 35
 - Viewing Hypervisor Connectivity information..... 36
- Virtualization Inventory procedures..... 36
 - Viewing Inventory information..... 36
 - Viewing Inventory Audit information..... 37
 - Filtering Inventory..... 38
- Event Monitor procedures..... 38
 - Viewing Event Monitor information..... 38
 - Viewing Applied Configurations pane..... 39
 - Viewing Pending/Failed Actions pane..... 39
 - Filtering Event Monitor..... 40
 - Grouping information by fields..... 41
- Network Profiles procedure..... 42
 - Adding a profile..... 43
 - Editing a profile..... 46
 - Deleting a profile..... 46
- Rules management..... 47
 - Adding a rule..... 48
 - Editing a rule..... 49
 - Deleting a rule..... 49
- Reports management..... 50
 - VM topology reports..... 50
 - Applied configurations reports..... 51
 - Pending or Failed actions reports..... 52
 - Generating a report..... 52
 - Exporting data from a report..... 53
 - Exporting a report..... 54
 - Printing a report..... 54
 - Printing a report on the server..... 55
- Audit Logs..... 55
 - Configuring Logging settings..... 56
 - Viewing Audit Logs..... 57
 - Filtering Audit Logs..... 57
- Network Validation procedures..... 58
 - Running Network Validation Report..... 58
 - Filtering Network Validation Report..... 59
- Device Management procedures..... 60
 - Viewing the Device Management status..... 60
 - Managing devices..... 60

Chapter 7: Virtualization backup and restore..... 62

Virtualization database tables	62
Appendix A: Recommendations	64
Rediscoveries and device assignments.....	64
Updating the virtual MAC of a physical adaptor.....	65
Internet browser settings.....	66

Chapter 1: Preface

Purpose

This document provides an overview of the Virtualization application and how to use it to manage your network.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at www.extremenetworks.com/education/.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at internalinfodev@extremenetworks.com

Getting Help

Product purchased from Extreme Networks

If you purchased your product from Extreme Networks, use the following support contact information to get help.

If you require assistance, contact Extreme Networks using one of the following methods:

- [GTAC \(Global Technical Assistance Center\) for Immediate Support](#)
 - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
 - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- [GTAC Knowledge](#) – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- [The Hub](#) – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- [Support Portal](#) – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Product purchased from Avaya

If you purchased your product from Avaya, use the following support contact information to get help.

Go to the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for previous versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

Subscribing to service notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

About this task

You can modify your product selections at any time.

Procedure

1. In an Internet browser, go to <http://www.extremenetworks.com/support/service-notification-form/>.
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.

Chapter 2: New in this document

The following sections detail what is new in *Virtualization Configuration using Extreme Fabric Orchestrator*, NN48100–503. See *Extreme Fabric Orchestrator Release Notes* for a list of supported features.

There are no feature changes in this release.

Chapter 3: Virtualization overview

Virtualization is an application that connects the vCenter server to the system to help the data center administrator configure the network changes that apply to the data center. Before the introduction of Virtualization, server administrators viewed only the virtualized server environment while the network operators viewed only the network topology. Virtualization bridges these two environments to deliver an end-to-end view of the virtualized data center from servers, to virtual machines (VM), to networking devices.

Virtualization provides a link mechanism to the VMware vCenter server to transport data between vCenter and Monitoring application so you can view both the virtual server and network environment. As a result, the server administrator and the network operator are able to work more efficiently together, such as a more effective troubleshooting process, as well as the ability to audit and track the creation, migration and deletion of virtual machines within the data center. The connection strategy between Virtualization and VMware vCenter is part of the server virtualization, a solution that allows you to run multiple virtual machines on a single physical server. This consolidation of servers helps reduce power consumption and cooling costs.

Virtualization connects to the VMware vCenter server and gathers the virtualized server topology (VMs and vSwitches). Virtualization identifies the physical connectivity of each of the ESX servers to the Extreme Networks data switches and the data switch connectivity for the VMs. By stitching this information to the network topology data that is automatically discovered through Monitoring application, you can use Virtualization to view a complete end-to-end virtualized Data Center.

Virtualization is an important component of the Extreme Networks Virtual Enterprise Network Architecture. The Virtual Enterprise Network Architecture is an open, end-to-end virtualization architecture that enables enterprises to build their own private cloud infrastructure. With a private cloud infrastructure, you can improve work efficiency and reduce time-to-service. A unified fabric is formed to establish a resilient infrastructure and maximize use of available bandwidth to simplify provisioning.

You can use Virtualization to automate device provisioning by following VMs as they migrate through the network. As you move VMs from one server to another, you add and delete the appropriate Network Profiles (QoS, ACLs) from the edge devices that are connected to the physical servers. If you require a change in the network configuration, the change occurs automatically in Virtualization, or you can manually request the action before the VM change is implemented. This ensures that the network is configured before you migrate VMs from one server to another, to ensure proper connectivity for the VM traffic.

VMware vCenter

Virtualization connects the VMware vCenter to the Configuration. VMware vCenter is part of the VMware vSphere, a system that manages collections of infrastructure such as storage and networking of a data center. VMware vCenter Server provides important data center services such as access control, performance monitoring and configuration. For more information about VMware vSphere, visit <http://www.vmware.com/support>.

Within a server, you can use the vCenter Server to control the data center, and configure policies to enable management of assignments and resources of virtual machines. After proper configuration, if the network fails, servers are not impacted. Furthermore, VMware vCenter provides the list of MAC addresses through Virtualization; however, information pertaining to the network switch and the slot or port is not delivered through the VMware vCenter.

vCenter gathers resources from ESX/ESXi hosts and sends them to the system administrator. The system administrator can then provision these resources to virtual machines. The following are the vCenter components:

- Role Based Access Control (RBAC)
- Core services
- Distributed services
- Plug-ins
- Various interfaces

Role Based Access Control

You can perform various Role Based Access Control (RBAC) tasks required to manage roles within EFO. You can add or delete a role name, provide group-level authentication functions and element permissions.

Roles management tasks can be performed in **Administration > Roles**.

In EFO, you require appropriate permissions to perform any task. The administrator grants permissions to users by assigning appropriate roles. RBAC supports two types of roles:

- Built-in
- Custom

The user can have read-only or write access permission. Read-only user permission can be overridden with write access to provide both read and write permissions.

Using these roles, you can gain access to various elements with specific permission mappings.

For more information on RBAC and tasks required to manage roles within the EFO, see *Administration using Extreme Fabric Orchestrator*, NN48100–600.

Core Services

Core Services are comprised of a management service for virtual machines. The following table details the Core Services components:

Component	Description
Virtual machine provisioning	Provisions virtual machines and their resources
Host and VM Configuration	Virtual machine and host configuration
Resources and virtual machine inventory management	Organizes virtual machines and resources in the virtual environment and facilitates their management.
Statistics and logging	Logs and reports on the performance and resource of virtual machines, hosts, and clusters.
Alarms and event Management	Tracks and warns of potential resource overuse or event conditions.
Task scheduler	Schedule actions to occur at a given time.
Consolidation	Analyzes the capacity and use of the data center's physical resources.
vApp	A vApp is similar to a virtual machine – it is multi-tiered, but is a separate entity. With vApps, you can perform operations, such as cloning, rebooting and shutting down.

Distributed services

The vCenter Server manages and configures the Distributed services. Distributed services are solutions that enable wider functionality within VMware vSphere. These solutions include VMware DRS, VMware HA, and VMware vMotion.

vCenter plug-ins

Plug-ins are applications that add features and functionality to the vCenter Server. vCenter Server plug-ins include VMware vCenter Converter and VMware Update Manager.

The VMware vCenter Converter allows you to convert physical machines and virtual to ESX/ESXi virtual machines. You can import converted systems into any location in the vCenter Server inventory. The VMware Update Manager allows you to enforce security standards across ESX/ESXi hosts and managed virtual machines.

vCenter services interfaces

vCenter Server contains the following interfaces:

- ESX management — Connects to vCenter agent
- VMware vSphere API — Connects to VMware management clients and third-party solutions.
- Database interface — Connects to Oracle, Microsoft SQL Server, or IBM DB2 to store information, such as virtual machine configurations, host configurations, resources and virtual machine inventory, performance statistics, events, alarms, user permissions, and roles.
- Active Directory interface — Obtains user access control information.

vCenter event types

The vCenter server processes the following types of events, to which Virtualization listens and processes.

The following table describes these events.

Table 1: Virtual Machine Event

VMEvent	Description
VmBeingCreatedEvent	Virtual machine is being created.
VmBeingDeployedEvent	Virtual machine is being deployed from a template.
VmBeingMigratedEvent	Virtual machine is being migrated.
VmBeingHotMigrated	Virtual machine is being hot-migrated.
VmBeingRelocatedEvent	Virtual machine is being relocated.
VmRelocatedEvent	Virtual machine is successfully relocated.
VmCloneEvent	Base event for all clone operations.
VmCloneFailedEvent	The virtual machine clone operation failed.
VmCreatedEvent	Virtual machine is successfully created.
VmDeployedEvent	Virtual machine deployment operation is complete.
VmDeployFailedEvent	The deployment from a template failed.
VmDisconnectedEvent	Virtual machine is disconnected.
VmFailedMigrateEvent	The virtual machine migration failed.
VmMigratedEvent	Virtual machine migration.
VmReconfiguredEvent	Virtual machine is reconfigured.
VmRelocateFailedEvent	The virtual machine relocation failed.

Table continues...

VMEvent	Description
VmRemovedEvent	Virtual machine is removed from the vCenter management.
VmRenamedEvent	Virtual machine is renamed.
VmUpgradeCompleteEvent	Upgrade operation is completed.
VmUpgradingEvent	Virtual hardware on a virtual machine is being upgraded.
DvsCreatedEvent	Distributed virtual switch is created.
DvsDestroyedEvent	Distributed virtual switch is destroyed.
DVPortgroupCreatedEvent	Distributed virtual port group is created.
DVPortgroupDestroyedEvent	Distributed virtual port group is destroyed.
VssCreatedEvent	Virtual standard switch is created.
VssDestroyedEvent	Virtual standard switch is destroyed.
VssPortgroupCreatedEvent	Virtual standard switch port group is created.
VssPortgroupDestroyedEvent	Virtual standard switch port group is destroyed.

Use of virtual machines

Virtualization enables secure end-to-end virtualization of virtual machines, which are commonly used in data centers to reduce costs by lowering cooling, space, and power requirements.

Virtualization automates service provisioning within the data center and oversees the virtual machine lifecycle, including activation, mobility and removal of a virtual machine from the network. You can view applications, servers and devices, either physical or virtual, and follow virtual machine migrations between servers. Furthermore, you can generate reports of these migrations to provide better monitoring regarding moves and network provisioning. As a result, network and server users are better equipped to collaborate.

Virtual machines can promote challenging aspects within a network, such as inconsistent application performance or troubleshooting issues. Virtualization allows the creation of templates and application of rules to overcome these issues. For example, if you want a specific VLAN ID assigned to a particular new device, you can create that type of rule.

One Hop Up Provisioning configuration

Many data networks are virtualized using the Shortest Path Bridging (SPB) technology. Virtualization can help the operator to virtualize the end-to-end network to configure the following:

- VLAN on the edge devices of the SPB Cloud

- VLAN, Traffic Profile/ACL/Bandwidth on the Access ports connected to the virtual world (ESX/ESXi)

The VLAN/Traffic profile on the devices is applied using the preconfigured network profile auto triggered by rules in Virtualization.

You can virtualize the entire end-to-end network using Virtualization to configure the VLAN connectivity using predefined Network Profile and Rules at the edge device connected to ESX, and the distribution or the core device, which forms the edge of the SPB Cloud.

The One Hop Up Provisioning (OHP) feature provisions the shortest path bridging MAC (SPBM) core network devices automatically, in addition to provisioning the edge devices. This feature facilitates the management of edge and core devices.

In order to provision a network device using Virtualization, the device must be managed in Virtualization. A network switch that is connected directly to an ESX server is considered an edge device. By selecting the uplinks from an edge device, the Virtualization operator can specify the core devices to be managed. The core device forms the edge of the SPB cloud, known as the backbone edge bridge (BEB).

One hop up provisioning prerequisites

Virtualization depends on Monitoring for device connectivity details. Enter the credentials for the devices in the credentials UI and the devices will be discovered in the monitoring application. In Virtualization, devices are configured in the device management UI and managed, inventory audit, and hypervisor connectivity are executed on the devices.

The following prerequisites must be met before the One hop up Provisioning (OHP) feature can be configured:

- Configure preferences such as port dissociation for edge and core.
- Complete a discovery in monitoring, and ensure devices connected to the ESXi servers are listed.
- Select the devices of interest in the device management, and save.
- Execute an inventory audit to verify hypervisor connectivity between the ESXi servers and the devices.

Note:

- After the rediscovery of devices in Monitoring, you may need to reselect the devices in the device management.
- The device management disables the selection of neighbor links if the remote device (BEB) is not SPBM supported.

If a VM event occurs, the corresponding events can be seen in Monitor Events. Device details are provided in the Applied Configurations and Pending/Failed Actions panes.

For configuration examples of the OHP feature, see *Administration using Extreme Fabric Orchestrator*, NN48100–600.

EFO Virtualization user interface

The Virtualization user interface has nine tabs:

- Topology — Displays applications, servers, and network devices across both physical and virtual environments. Network displays Topology view by default, if configured.
- Inventory — Displays the end-to-end view of the connectivity between the data center and the network devices. Inventory displays Tabular Inventory view by default, if configured.
- Event Monitor — Displays a list of each transaction that occurs within the vCenter server.
- Network Profiles — Provides the data center and network administrator a configuration interface to define a network profile. A network profile consists of a set of configurations applied to a network switch on a VLAN-id interface basis.
- Rules — Conditions applied to the virtual machine event to determine which of these network profiles apply to which virtual machine event.
- Reports — Displays current and historical data from the data center and the network connectivity, as well as any configuration changes that occurred within the data center.
- Audit Logs — Displays details about configuration changes made to devices, as well as major operations, and details about the inventory audit and the hypervisor connectivity.
- Device Management — Provides a configuration interface to manage network devices.
- Network Validation — Displays a report showing the inconsistencies in the physical network based on the Network Profiles attached to the VM network.

Topology

Use the Topology to view the end-to-end network topology including applications, servers, and network devices across both physical and virtual environments. The Topology feature performs a discovery of the devices in your network, and creates a topology map showing the discovered devices and the connections between them. By default, the Topology view displays when Virtualization is launched for the first time.

You can use the Topology view to perform the following:

- display a logical topology map of your network, such as Hosts server and the virtual machines
- view link data and device connections
- view network information, such as Distributed Switch, PortGroups with VLAN, and MAC address for virtual machines and the association with the Port Groups
- search on Host, VM, and physical device
- view events based on Host and VM

- perform Network Discovery

Hover over a device or edge link to display information, such as Device IP, NIC, and connected ports.

The following figure shows an example of the Topology view.

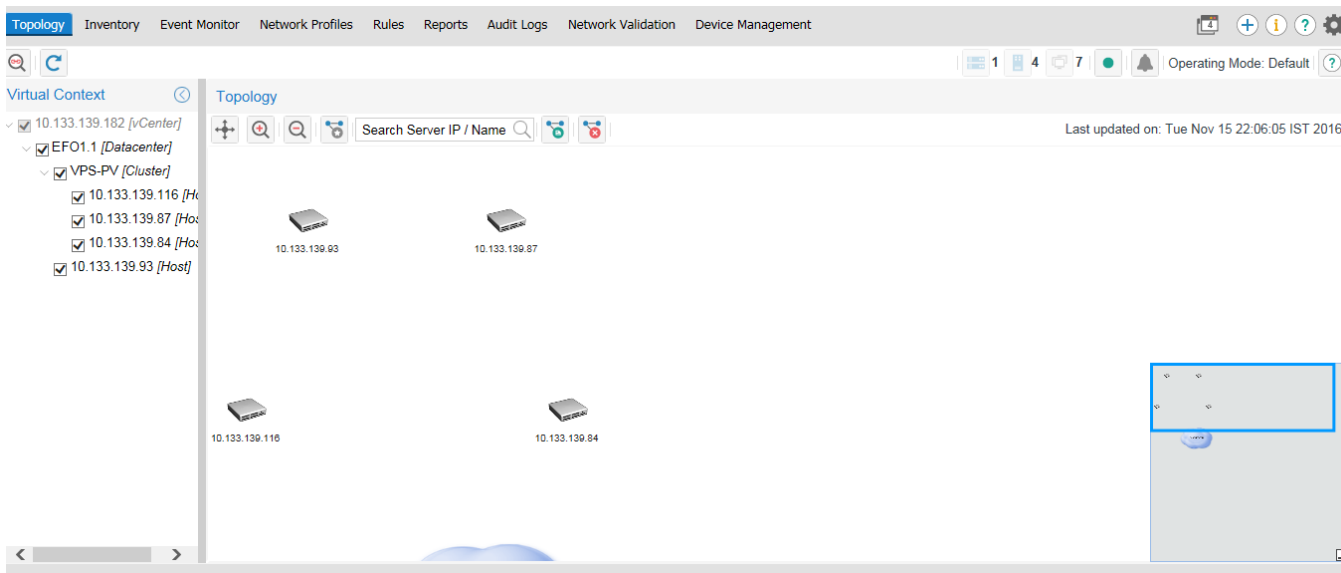


Figure 1: Virtualization Topology view

You can track the VM network and provisioning changes, which help to monitor and troubleshoot the network.

You can also view and monitor different stages of a VM life cycle, including create, migrate, edit, and delete, as well as the following items:

- Virtual machine inventory from the data center
- Configuration changes made to devices
- VMware vCenter triggers that were not applied

Inventory

Inventory displays an inventory of virtual machines that are managed within Virtualization and the data switch connectivity for the virtualized server topology. If a virtual machine is part of the managed devices, the details of this virtual machine display in the Inventory pane. Inventory displays the end-to-end view of the connectivity between the data center and the network devices. The information displayed in the panes is read-only, and contains the ESX/ESXi server information along with the virtual machines, the MAC addresses and the associated network switches.

Inventory provides Hypervisor Inventory and Virtual Machines views.

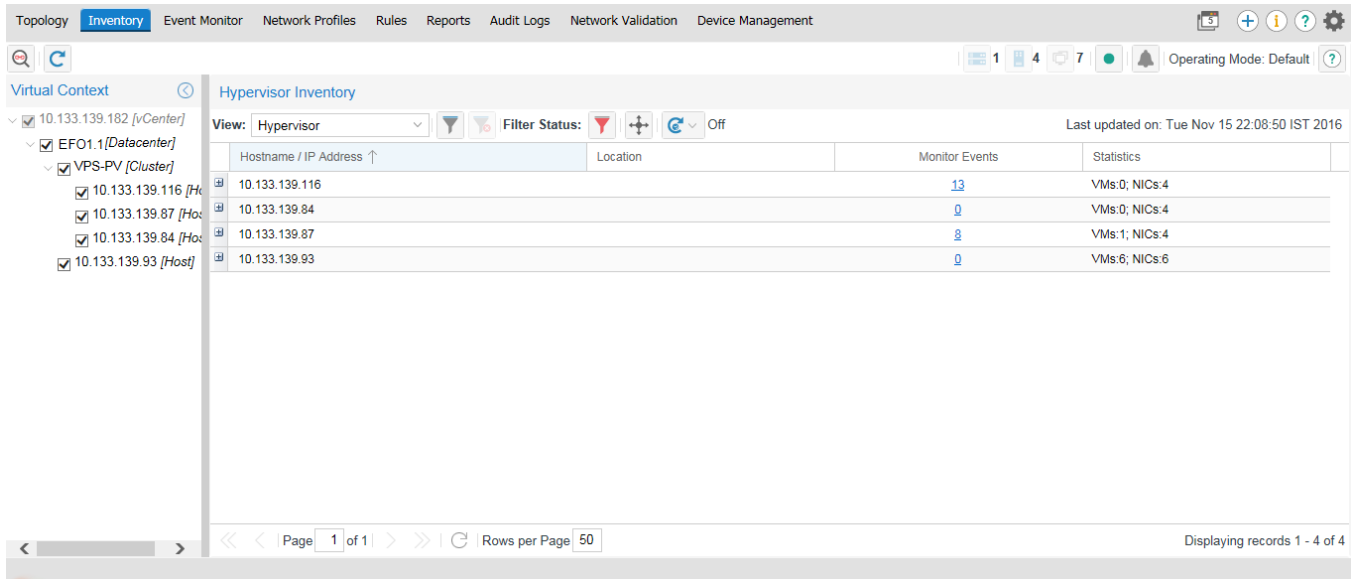


Figure 2: Hypervisor Inventory

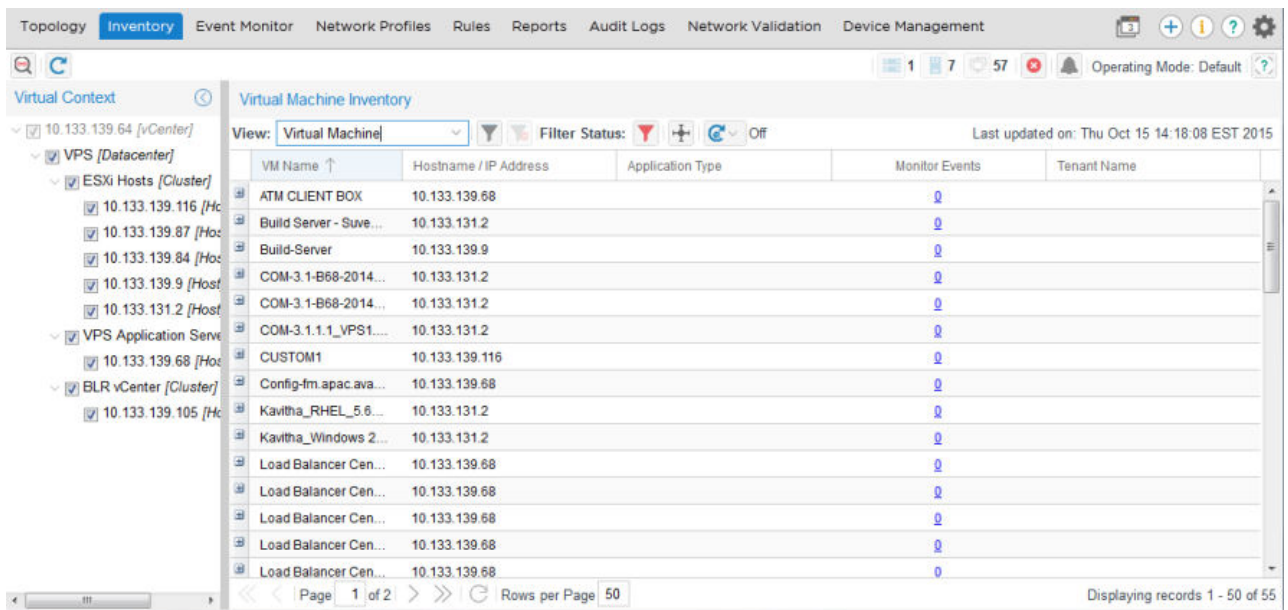


Figure 3: Virtual Machine Inventory

You can configure the Hypervisor Inventory and Virtual Machines panes to automatically refresh at different intervals. You can choose one of the following options to configure an automatic refresh:

- off—default value, disables the refresh timer
- 30 secs—refresh every 30 seconds
- 1 min—refresh every 1 minute
- 5 min—refresh every 5 minutes

- 10 min—refresh every 10 minutes

Inventory displays Tabular Inventory view of the network when the Network View Setting is configured to Tabular Inventory in Preferences. For more information about changing the Inventory display to Tabular Inventory, see *Administration using Extreme Fabric Orchestrator*, NN48100–600.

You can use the filter to view the devices that are linked to the ESX Server or a VM. In the Filter drop-down, a filtering option can be used to show only the devices linked to the VM(s). The search can be further refined by entering a search string in the Filter box.

Event Monitor

Event Monitor displays a list of each transaction that occurs within the vCenter server. After you create a virtual machine, it is sent through the network from vCenter to Virtualization. The monitor displays the attributes of this creation, if the addition of the virtual machine was either successful or partially successful, and if the creation failed or is in a pending state.

When you select a row within Event Monitor, the corresponding information appears in Applied Configuration pane and Pending/Failed Actions pane. Click Refresh to refresh the Event Monitor pane.

The screenshot shows the Event Monitor interface with a table of transactions and two side panels. The table has columns for Event Type, Event Name, VM Name, Action, Status, VLA, Rule, Network Profile, and Timestamp. The Status column shows 'Information' for topology changes and 'Success' for VM-related actions. The side panels show 'Applied Configurations' and 'Pending/Failed Actions' with columns for Action, Parameters, Status, and Message.

Event Type	Event Name	VM Name	Action	Status	VLA	Rule	Network Profile	Timestamp
TopologyCh...	DvsDest...	N/A	N/A	Information				Thu C
TopologyCh...	DvsCre...	N/A	N/A	Information				Thu C
TopologyCh...	DVPortg...	N/A	N/A	Information				Thu C
TopologyCh...	DVPortg...	N/A	N/A	Information				Thu C
TopologyCh...	vSwitch...	N/A	N/A	Information				Thu C
TopologyCh...	Vswitch...	N/A	N/A	Information				Thu C
TopologyCh...	vSwitch...	N/A	N/A	Information				Thu C
VMEdit-401...	VmReco...	test01	Auto	Success	502	test502	test502	Thu C
VMEdit-401...	VmReco...	test1	N/A	Information				Thu C
VMEdit-401...	VmReco...	test1	Auto	Success	502	test502	test502	Thu C
VMMigrate [...]	VmRelo...	test1	Auto	Success	502	test502	test502	Thu C
VMMigrate [...]	VmRelo...	test1	Auto	Success	503	test503	test503	Thu C
VMMigrate [...]	VmBein...	test1	Auto	Success	502	test502	test502	Thu C
VMMigrate [...]	VmBein...	test1	Auto	Success	503	test503	test503	Thu C
VMMigrate [...]	VmRelo...	test1	Auto	Success	502	test502	test502	Thu C
VMMigrate [...]	VmBein...	test1	Auto	Success	502	test502	test502	Thu C
VMMigrate [...]	VmRelo...	test1	Auto	Success	503	test503	test503	Thu C

Figure 4: Event Monitor

You can use the configuration option to automatically refresh the Event Monitor pane at different intervals. The timer defaults to the off position, or you can choose one of the following options to configure an automatic refresh:

- off—default value, disables the refresh timer

- 15 secs—refresh every 15 seconds
- 30 secs—refresh every 30 seconds
- 1 min—refresh every 1 minute
- 5 min—refresh every 5 minutes
- 10 min—refresh every 10 minutes

Network Profiles

Network configuration is simplified by providing a template called network profile for defining configuration parameters and which are used across the device types. Because Virtualization responds to lifecycle changes of VMs in the datacenter, network profiles can be used to define device configurations to be performed.

Use the network profiles to define the VLAN and port configurations that are applied to a switch port. A network profile provides a view of the VLAN, bandwidth, metering, access control and QoS configuration and ensures that the trunk is correctly configured to support the VM traffic. After you define and save a set of configurations, if a change occurs on the datacenter, the network profile is applied to the corresponding data switch in the network to support this change.

Service ID [i-SID] and Service name are added into the Network Profiles.

Network profiles can be applied to different devices, such as 45xx, 55xx, and 86xx.

Rules

Rules are conditions to which network profiles are applied. Network profiles are applied to switch ports based on preconfigured rules. As a result the rule binding service is dependent on the network profile service. Virtualization provides a rule infrastructure to determine which network profiles are applied to which virtual machine. You can define rules based on the location of the ESX server, the application server type of the virtual machine, and the VLAN ID of the port groups to which a virtual machine is connected.

A rule may have simple or complex criteria, and is executed for a virtual machine event only if the event matches a single rule. You can configure rules to occur automatically or manually. Automatic rules imply that if an exact rule match is found for a virtual machine event, then the configuration defined in the related network profile is applied on the device. Manual rules imply that, if a rule is matched for a virtual machine event, the configuration defined in the associated network profile is not automatically applied to the network devices and you can apply the rule manually. For more information about network profiles, see [Network Profiles](#) on page 22.

Reports

You can generate reports to view the current and historical data of the end-to-end data center and network connectivity, as well as the configurations performed on the network devices in response to the changes in the data center. You can generate the following types of reports:

- VM topology — Shows the connectivity of the VMs, the ESX server that the VMs are hosted on, the Vswitch/ Dvswitch to which the VMs are connected, as well as the network devices providing the link for these VMs.
- Applied configurations — Shows the configurations applied to the network devices. You can generate this type of report to include only a specific time period.
- Pending/Failed actions — Shows the network device actions that are pending or failed. Details about the result of the actions are displayed. You can generate this type of report to include only a specific time period.

After you generate a report, you can print or export the given report in different formats, such as Excel, Postscript, PDF, Word and PowerPoint.

Audit logs

Use the audit logs to view the operations you performed within Virtualization. Audit logs display the virtual machine events processed and the configurations that were made on the network devices. The audit logs detail changes that occurred to events, when these changes happened, and the status of the event processing. You can apply filter options to the audit logs to search for information by fields.

You can configure the audit log settings by clicking the Preferences icon on the quick toolbar. In the Preferences section, you can set boundaries in regards to file size and the level at which debug logs and audit logs appear. You can also enable audit log purge and configure the audit log retention time.

Network Validation

Network Validation generates a report showing the inconsistencies in the physical network based on the Network Profiles attached to the VM network.

You can generate the Network Validation report for various types of inconsistencies in the network. Following are the types of inconsistencies:

- VLANs unavailable on the Edge device and one hop device for the existing VMs in the vCenter
- Unused VLANs on the Edge device and one hop device

- VLANs available on the SPBm capable device for the existing VMs in the vCenter, but I-SID not configured on the VLAN
- VLANs available on the device, but required ports not associated to the VLAN

VM Name	Host Name	NIC Name	Virtual Swi...	Network La...	PG VlanId	Device IP	State	Error Msg
VM Name: -- (2 Reports)								
--	--	--	--	--	--	10.133.139...	Unused	Following vLans[800] configured by VPS are not used on the Vi
--	--	--	--	--	--	10.133.139...	Unused	Following vLans[202, 203, 503, 501, 502] configured by VPS ar
VM Name: MTB (16 Reports)								
MTB	10.133.139...	vmnic3	vSwitch2	VPG_555	555	10.133.139...	Unavailable	Ports [1/9, 1/20, 1/8, 1/23, 1/22] not associated to the vlan : 55
MTB	10.133.139...	vmnic3	vSwitch2	VPG_555	555	10.133.139...	Unavailable	Ports[1/8] not associated to the vlan : 555
MTB	10.133.139...	vmnic3	vSwitch2	VPG_555	555	10.133.139...	Unavailable	Ports[1/20] not associated to the vlan : 555
MTB	10.133.139...	vmnic3	vSwitch2	VPG_555	555	10.133.139...	Unavailable	Ports[1/9] not associated to the vlan : 555
MTB	10.133.139...	vmnic3	vSwitch2	VPG_666	666	10.133.139...	Unavailable	Ports [1/9, 1/20, 1/8, 1/23, 1/22] not associated to the vlan : 66
MTB	10.133.139...	vmnic3	vSwitch2	VPG_666	666	10.133.139...	Unavailable	Ports[1/8] not associated to the vlan : 666
MTB	10.133.139...	vmnic3	vSwitch2	VPG_666	666	10.133.139...	Unavailable	Ports[1/20] not associated to the vlan : 666
MTB	10.133.139...	vmnic3	vSwitch2	VPG_666	666	10.133.139...	Unavailable	Ports[1/9] not associated to the vlan : 666
MTB	10.133.139...	vmnic2	vSwitch2	VPG_555	555	10.133.139...	Unavailable	Ports [1/9, 1/20, 1/8, 1/23, 1/22] not associated to the vlan : 55
MTB	10.133.139...	vmnic2	vSwitch2	VPG_555	555	10.133.139...	Unavailable	Ports[1/8] not associated to the vlan : 555
MTB	10.133.139...	vmnic2	vSwitch2	VPG_555	555	10.133.139...	Unavailable	Ports[1/20] not associated to the vlan : 555
MTB	10.133.139...	vmnic2	vSwitch2	VPG_555	555	10.133.139...	Unavailable	Ports[1/9] not associated to the vlan : 555

Figure 5: Network Validation

Device Management

You can use the Device Management tab to view the managed devices in Monitoring and view the status of the managed devices within Virtualization. You can view the number of devices and the corresponding data relating to the type of switch, the slot number, when the device was last updated, and if the device is managed or unmanaged.

*** Note:**

Virtualization depends on Monitoring for device connectivity details. Enter the credentials for the devices in the credentials UI and the devices will be discovered in the monitoring application. In Virtualization, devices are configured in the device management UI and managed, inventory audit, and hypervisor connectivity are executed on the devices. Once all the devices are discovered in Monitoring, these devices are managed but the links between them are not managed in the Device Management.

Device Management enable you to perform the following actions:

- Manage or unmanage edge and core devices.
- Manage or unmanage stack units of a stackable device in the Stack Units tab.

- Specify uplinks for the edge device (which is connected to ESX/ESXi server) in the Neighbor tab. If the selected link is part of an MLT/SMLT, the UI automatically selects other links of the MLT/SMLT.
- Select an uplink for the edge device for Virtualization to automatically manage the core devices (BEB), which are connected to the edge device.
- Validate links between the edge and the core device (BEB).
- Filter by Device IP or Device type.
- View the Used license count.

*** Note:**

- After devices are rediscovered in Monitoring, devices may need to be reselected in Device Management.
- The device manager disables the selection of neighbor links if the remote device (BEB) is not SPBm supported.
- Refresh reloads the entire device information. Unsaved data is lost.

*** Note:**

The Virtualization application recaptures all related device inventories and topologies when a device is changed from the managed state to the unmanaged state. Extreme Networks recommends that you minimize such state changes.

Chapter 4: Virtualization common icons and procedures

The following icons and procedures are common to many activities.

EFO Virtualization application icons

The following table details the Virtualization application icons.


























	Online Help
	Device Management
	Network Discovery status information
	Distributed Switch Info
	Clear Highlights
	Save topology
	Clear Saved topology
	The number of data centers discovered by Virtualization
	The number of ESX/ESXi hosts discovered by Virtualization
	The number of VMs discovered by Virtualization
	Indicates Virtualization is connected to the vCenter Server
	Indicates Virtualization is disconnected from the vCenter Server
	Indicates notifications present.
	Indicates no notifications present.

Table continues...

 Off	Refresh timer
	Refresh the visible pane
	Filter option
	Clear Filter option
	Add
	Edit
	Copy an existing network profile
	Delete
Filter Status: 	Filter applied
	No filter applied
	This option is available only in Event Monitor tab. If the action is in manual mode in the Event Monitor tab, you can click this option to manually mark the action as complete.

Show or hide columns

In the Virtualization application, you can show or hide columns to better manage the overall quantity of information. This functionality is available in Event Monitor, Network Profiles, Rules, and Audit Log. In addition, you can sort the columns in ascending or descending order and filter the results.

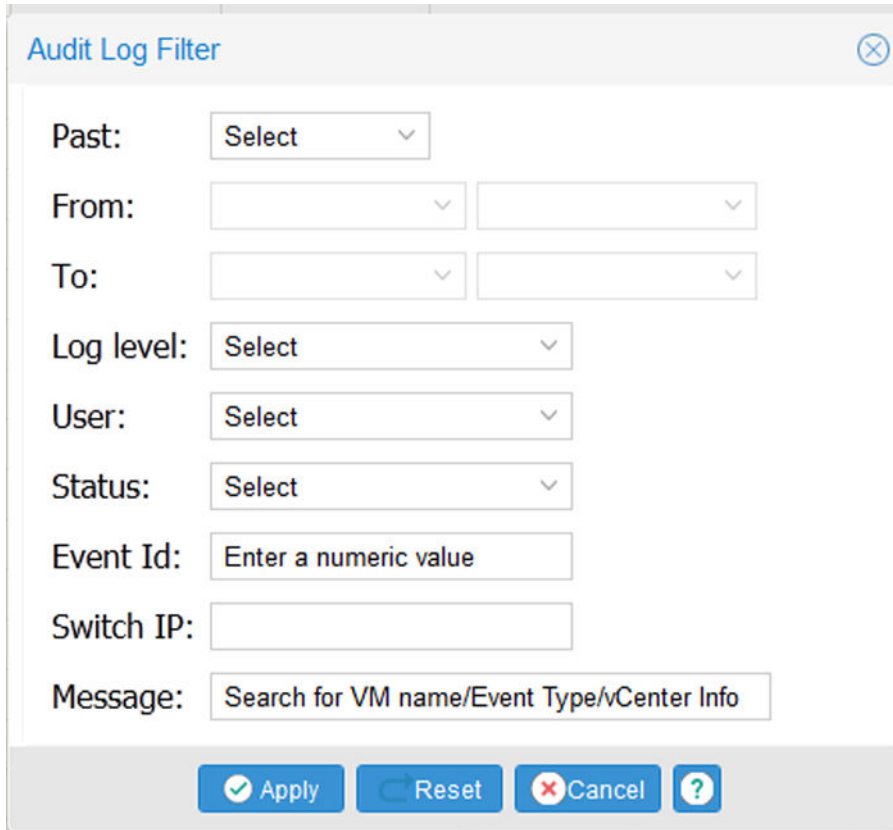
Date/Time ↓	Log L...	User	Status	Event ID	Switch IP	Message
2015-10-15 17:20:44	Sum...	admin	SUCCE.			Next Audit Log purge sc
2015-10-15 17:20:44	Sum...	admin	SUCCE.			Next monitor purge sche
2015-10-15 17:15:01	Error	admin	FAILURE			led to establish conn
2015-10-15 17:14:56	Error	admin	FAILURE			led to establish conn
2015-10-15 17:14:31	Error	admin	FAILURE			led to establish conn
2015-10-15 17:14:01	Error	admin	FAILURE			led to establish conn
2015-10-15 17:13:56	Error	admin	FAILURE			led to establish conn
2015-10-15 17:13:31	Error	admin	FAILURE			led to establish conn
2015-10-15 17:13:01	Error	admin	FAILURE			led to establish conn
2015-10-15 17:12:56	Error	admin	FAILURE			led to establish conn
2015-10-15 17:12:31	Error	admin	FAILURE			Failed to establish conn
2015-10-15 17:12:01	Error	admin	FAILURE			Failed to establish conn
2015-10-15 17:11:56	Error	admin	FAILURE			Failed to establish conn

Figure 6: Show or hide columns

Filter information

Filters can be applied to sort and filter the information that displays. You can select conditions so that only certain information displays.

You can filter information in Inventory, Event Monitor, and Audit Log.



The image shows a dialog box titled "Audit Log Filter" with a close button (X) in the top right corner. The dialog contains several filter criteria:

- Past:** A dropdown menu with "Select" and a downward arrow.
- From:** Two adjacent dropdown menus.
- To:** Two adjacent dropdown menus.
- Log level:** A dropdown menu with "Select" and a downward arrow.
- User:** A dropdown menu with "Select" and a downward arrow.
- Status:** A dropdown menu with "Select" and a downward arrow.
- Event Id:** A text input field with the placeholder text "Enter a numeric value".
- Switch IP:** A text input field.
- Message:** A text input field with the placeholder text "Search for VM name/Event Type/vCenter Info".

At the bottom of the dialog, there are four buttons: "Apply" (with a checkmark icon), "Reset" (with a circular arrow icon), "Cancel" (with a red X icon), and a help button (with a question mark icon).

Figure 7: Audit Log filter

Chapter 5: CDP and LLDP settings configuration

This chapter provides concepts and procedures to configure CDP and LLDP settings on .

Configuring CDP settings on the dvSwitch

Before you begin

Ensure that you have the administrative privileges to access the VM Network in vSphere Client.

About this task

Configure the Cisco Discovery Protocol (CDP) settings on dvSwitch to ensure proper connectivity between the ESX server and the ERS Devices.

Important:

You must configure the CDP settings both on the dvSwitch and on the vSwitch. For more information, see [Configuring CDP settings on the vSwitch](#) on page 31.

Procedure

1. Launch the vSphere Client.
2. In the **Inventory** tab, click **Networking**.
3. In the left pane, right-click the dvSwitch to configure, and then select **Edit settings**.
The dvSwitch Settings window displays.
4. In the Properties tab, select **Advanced**.
5. In the Advanced section, under Discovery Protocol, configure the **Status** as **Enabled** and the **Type** as **Cisco Discovery Protocol**.
6. In the **Operation** drop-down box, select either **Advertise** or **Both**.
7. Click **OK**.

Configuring CDP settings on the vSwitch

Before you begin

Ensure that you have the administrative privileges to access the VM Network in vSphere Client.

About this task

Configure the Cisco Discovery Protocol (CDP) settings on the vSwitch to ensure proper connectivity between the ESX server and the ERS Devices. You can change these settings using the ESX server.

! Important:

You must configure the CDP settings both on the dvSwitch and on the vSwitch. For more information, see [Configuring CDP settings on the dvSwitch](#) on page 30.

Procedure

1. Log in as **Root**.
2. To get the current CDP setting, type the following command: `esxcfg-vswitch -b <vSwitchName>`, where <vSwitchName> is the name of the vSwitch through which you configured VM traffic to flow.

The result of the command displays `listen`, `advertise`, or `both`, depending on the configuration.

3. To change the mode to both or advertise, type one of the following commands: `esxcfg-vswitch -B both <vSwitchName>`, or `esxcfg-vswitch -B advertise <vSwitchName>`.

Configuring LLDP settings on the Extreme Networks device

Configure LLDP on the Extreme Networks device to send the following information to allow Virtualization to discover the network:

- Chassis ID (enabled by default)
- Port ID (enabled by default)
- Management Address (must be manually enabled)
- Port Description (must be manually enabled)

* Note:

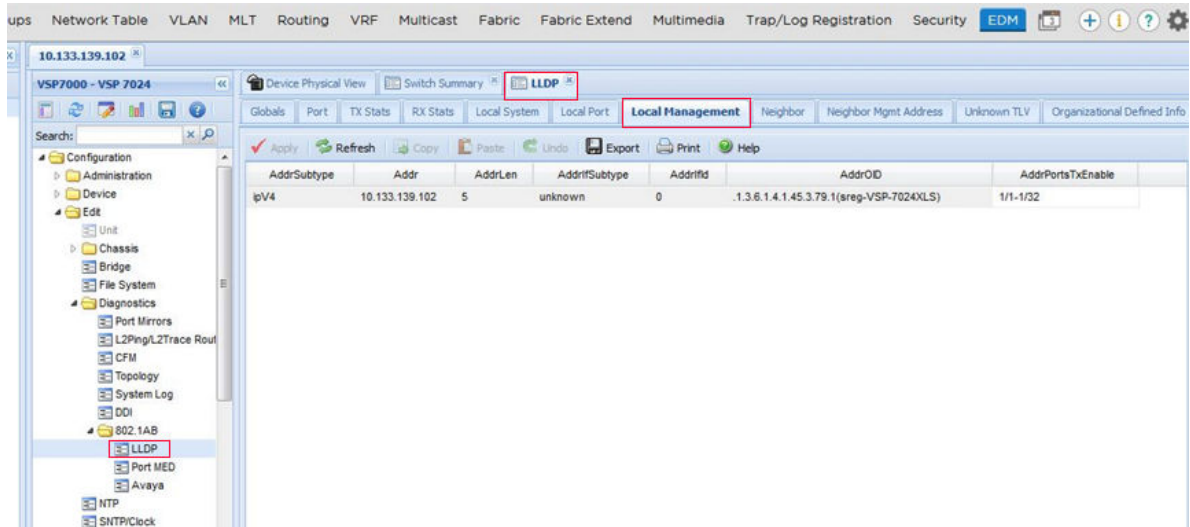
The following Extreme Networks devices support LLDP:

- ERS 45xx / ERS 48xx

- ERS 5xxx
- VSP 7000

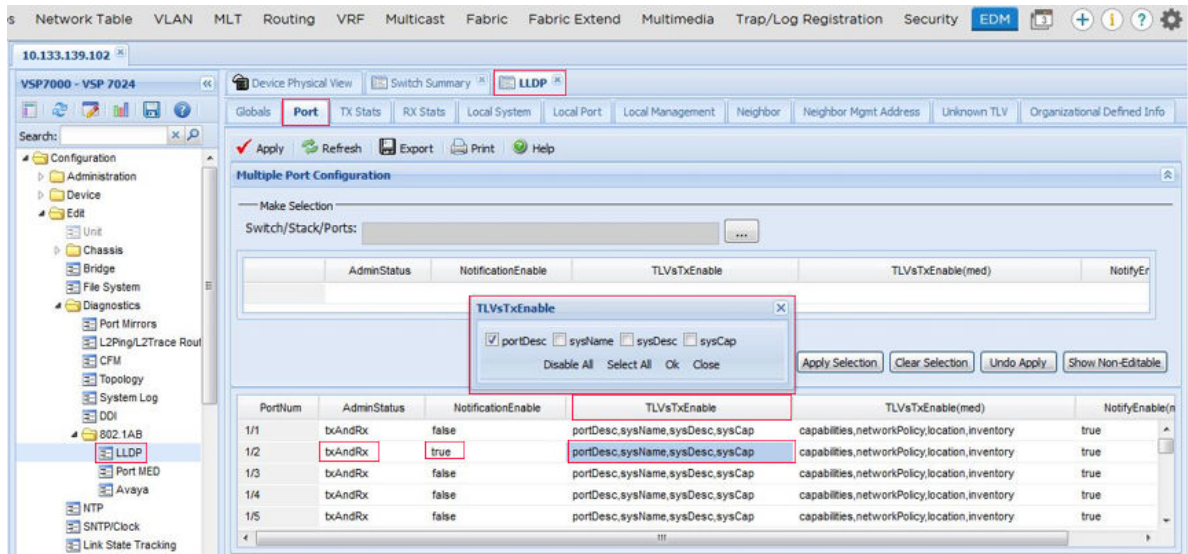
Procedure

1. Enable the Management Address to be published for specific ports:



- a. Launch EDM for the device on which LLDP is to be enabled.
- b. On the Left Pane, navigate to **Configuration > Edit > Diagnostics > 802.1AB**.
- c. Click **LLDP**.
- d. On the right pane, click **Local Management**.
- e. Select the ports to which ESX is connected and click **Apply**.

2. Enable the device to send Port Description information for specific ports.



- Launch EDM for the device on which LLDP is to be enabled.
- On the Left Pane, navigate to **Configuration > Edit > Diagnostics > 802.1AB**.
- Click **LLDP**.
- On the right pane, click **Port**.
- In the bottom pane, for the port that is connected to ESX, configure **TLVs TxEnable** as **PortDesc**, **NotificationEnable** as **true** and **AdminStatus** as **txAndRx**.
- Click **Apply**.

Configuring LLDP settings on the dvSwitch

Before you begin

Ensure that you have the administrative privileges to access the VM Network in vSphere Client.

About this task

Configure the Link Layer Discovery Protocol (LLDP) settings on dvSwitch to ensure proper connectivity between the ESX server and the Extreme Networks devices.

! Important:

You must configure the LLDP settings on the dvSwitch and on the Extreme Networks device. For more information, see [Configuring LLDP settings on the Extreme device](#) on page 31.

Procedure

1. Launch the vSphere Client.

2. In the **Inventory** tab, click **Networking**.
3. In the left pane, right-click the dvSwitch to configure, and then select **Edit Settings**.
The dvSwitch Settings window displays.
4. In the Properties tab, click **Advanced**.
5. In the Advanced section, ensure that LLDP **Status** is enabled.
6. In the **Type** drop-down box, select **Link Layer Discovery Protocol**.
7. In the **Operation** drop-down box, select either **Listen** or **Both** (Listen and Advertise).
8. Click **OK**.

Configuring the location and application type of the ESX server

Before you begin

Ensure that you have the administrative privileges to access the VM Network in vSphere Client.

About this task

Configure the Location and the ApplicationType of the ESX server to ensure proper functionality of the ESX server within Virtualization.

Procedure

1. Launch the vSphere Client.
2. In the **Inventory** tab, click **Clusters**.
3. In the left pane, select the ESX server to configure.
4. In the **Summary** tab, under **Annotations**, click **Edit**.
The Edit Annotations window displays.
5. Click **Add**.
The Add Custom Attribute window displays.
6. In the Add Custom Attribute window, enter the values for the **Name**, **Value**, and **Type** fields.
7. Click **OK** to close the Add Custom Attribute window.
8. Click **OK**.

Chapter 6: Managing Virtualization

The following sections provide the procedures for configuring and managing Virtualization.

vCenter connectivity status

The vCenter connectivity status displays the current vCenter server connectivity status and provides an option to reconnect to the vCenter server. The status of the vCenter connection is indicated by a red icon (disconnected) or green icon (connected) in the status bar information area. A dialog box displays with a description of the connection status of the vCentre.

The notification icon is highlighted in the status bar during vSwitch and dvSwitch create and remove operations.

Click **Reconnect** to reconnect to the vCenter server.

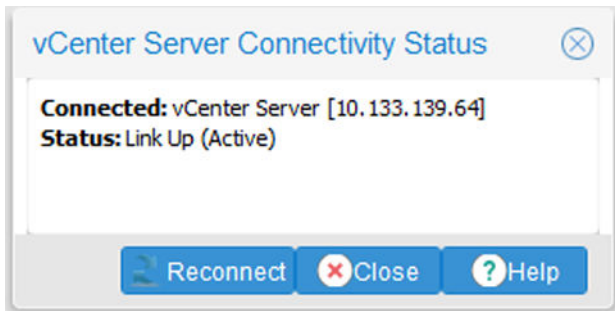


Figure 8: vCenter connectivity status dialog box

Network Discovery procedures

This section provides the Network Discovery procedures.

Viewing Virtualization Network Discovery status summary

When you start EFO Virtualization, an automatic inventory audit is performed followed by a hypervisor connectivity operation.

About this task

Perform the following procedure view a summary of the Virtualization Network Discovery status.

Procedure

1. From the EFO menu bar, select **Virtualization > Topology** or **Virtualization > Inventory**.
2. Click the **Network Discovery** icon on the Virtualization dashboard.
The Virtualization Network Discovery Status window displays.
3. Click **Refresh** to manually refresh the screen.
4. Click **Close**.

Viewing Hypervisor Connectivity information

After the Network Discovery is complete, you can view the entire network connectivity of the virtual machines in the data center. Hypervisor connectivity is automatically performed every 24 hours by default to ensure that any changes in the network setup are captured. You can reschedule the hypervisor connectivity schedule interval using the Preferences icon on the Extreme Fabric Orchestrator (EFO) quick toolbar. For more information on configuring Virtualization preferences, see *Administration using Extreme Fabric Orchestrator*, NN48100–600.

About this task

Perform the following procedure view the Virtualization Hypervisor Connectivity information.

Procedure

1. From the EFO menu bar, select **Virtualization > Topology** or **Virtualization > Inventory**.
2. Click the **Network Discovery** icon to display a summary of the Virtualization Network Discovery Status.
The Virtualization Network Discovery Status window displays.
3. Click **Details** in the **Hypervisor Connectivity** section of the **Summary** tab.

Virtualization Inventory procedures

This section provides the Virtualization Inventory procedures.

Viewing Inventory information

About this task

Perform the following steps to view the Virtualization Inventory information.

Procedure

1. From the EFO menu bar, select **Virtualization > Inventory**.
2. Select **Hypervisor** or **Virtual Machine** from the **View** drop-down menu.

Field descriptions

Field	Description
Hypervisor Inventory	
Hostname/IP Address	IP Address of the host server.
Location	Location of the server. Provided as an attribute on the ESX/ESXi server.
Monitor Events	Opens the Event Monitor tab.
Statistics	Number of Virtual Machines (VM) and Network Interface Cards (NIC).
Virtual Machine	
VM Name	Name of the Virtual Machine.
Hostname/IP Address	Name/IP Address of the Host server.
Application Type	Application server type of virtual machine. Provided as custom attribute in the VM by the user.
Monitor Events	Number of events being monitored.
Tenant Name	Name of the Tenant.

Viewing Inventory Audit information

Inventory audit captures the topology of the datacenter. The Inventory audit information ensures that Virtualization captures important information, such as all data centers, clusters, ESX servers, virtual machines, and related Vswitches/Dvswitches, PortGroups. Each time you start the Virtualization application, an inventory audit is automatically performed to capture this information and keep Virtualization updated. vCenter server details and credentials are found in the Virtualization Preferences Global tab on the menu bar.

About this task

Perform the following procedure view the Virtualization Inventory Audit information.

Procedure

1. From the EFO menu bar, select **Virtualization > Topology** or **Virtualization > Inventory**.
2. Click **Network Discovery** icon to display a summary of the Virtualization Network Discovery Status.
The Virtualization Network Discovery Status window displays.
3. Click **Details** in the **Inventory Audit** section of the **Summary** tab.

Filtering Inventory

Virtualization Inventory provides a filter option to search for information by fields. The filter can be based on a single field or combination of multiple fields.

About this task

Perform the following procedure to filter the Virtualization Inventory information.

Procedure

1. From the EFO menu bar, select **Virtualization > Inventory**.
2. Select **Hypervisor** or **Virtual Machine** from the **View** drop-down menu to view the Virtualization Inventory information.
3. Click the **Show Filter** icon.
4. Enter the filter options in the filter window.
5. Click **Apply**.
6. **(Optional)** Click the **Clear Filter** icon to clear the applied filters.

Event Monitor procedures

This section provides the Event Monitor procedures.

Viewing Event Monitor information

Event Monitor displays a list of each transaction that occurs within the vCenter server. After you create a virtual machine, it is sent through the network from vCenter to Virtualization. The monitor displays the attributes of this creation, if the addition of the virtual machine was either successful or partially successful, and if the creation failed or is in a pending state.

About this task

Perform the following steps to view the Virtualization Event Monitor information.

Procedure

1. From the EFO menu bar, select **Virtualization > Event Monitor**.
The Event Monitor window displays.
2. **(Optional)** Click the **Refresh** icon to refresh the view.

Event Monitor field descriptions

Field	Description
Event Type	The event type from the vCenter.
Event Name	The event name from the vCenter.
VM Name	The name of the virtual machine.
Action	Insert a description of this field.Type of action that occurred within the vCenter in EFO Virtualization. If the result of the Action is Auto, then the status is automatically delivered. If an Action is in a Manual mode, the event is either in a pending, partial success, or failed state.
Status	Displays the status of the given event, which can be either success, pending, or failed.
VLAN ID	Number of the VLAN.
Rule	Displays the rule associated to the event.
Network Profile	The associated network profile of the event.
Timestamp	Date and time at which the event occurred.

Viewing Applied Configurations pane

The Applied Configurations pane displays a list of successful configuration changes on the various devices. You can view these configuration changes by selecting a specific event from the Event Monitor pane. If the event configuration is successful, the given event from the Monitor Events pane is populated in the Applied Configurations pane.

The following table describes the content of the Applied Configurations pane.

Field	Description
Action	The name of the operation that was performed on the device.
Switch IP	IP address of the switch.
Parameter	Associated parameter.
Message	Displays the details of the configuration changes.
Timestamp	The date and time at which the configuration occurred on the switch.

Viewing Pending/Failed Actions pane

The Pending/Failed Actions pane displays a list of pending or failed configurations on the devices. If an action is pending or failed, an explanation appears in the message column. The status of an action is pending if there is no rule matching the VM event or if the matching rule is manual. If the pending action is a result of irrelevant or missing information, you can review the data and manually confirm the status if required.

*** Note:**

If the action of the event in the Event Monitor pane is in Manual mode and the status of the action in the Pending/Failed Actions pane is pending, you can mark the action as manually completed.

The following table describes the content of the Pending/Failed Actions pane.

Field	Description
Action	The type of action that is either pending or failed.
Switch IP	IP address of the switch.
Parameter	The associated parameter.
Status	Indicates if the action is pending, partial success, or failed.
Message	Displays the reason for which the action is either pending or failed.
Timestamp	The date at which the action occurred.

Filtering Event Monitor

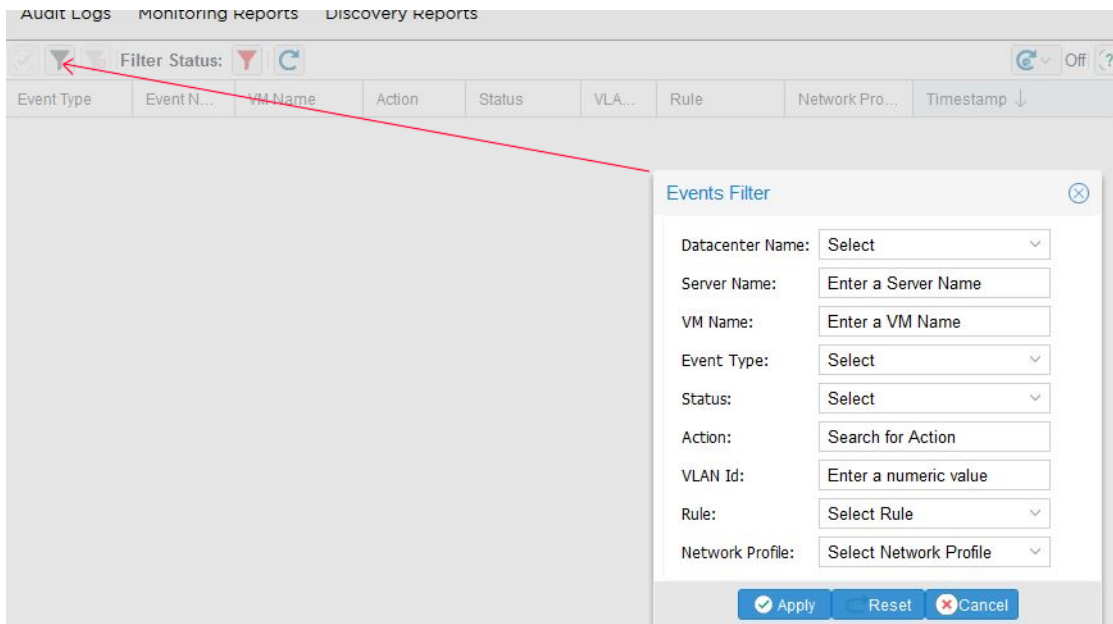
About this task

Perform the following steps to apply the Filter option to the VM events that have occurred on a particular ESX/ESXi server.

Procedure

1. From the EFO menu bar, select **Virtualization > Event Monitor**.
The Event Monitor window displays.
2. Click **Filter**.
The Events Filter window displays.
3. Select the options to filter.
4. Click **Apply**.

Example



Click **Clear Filter** to clear the applied filters and restore all the records in the table.

Grouping information by fields

Related information can be viewed in adjoining rows.

* Note:

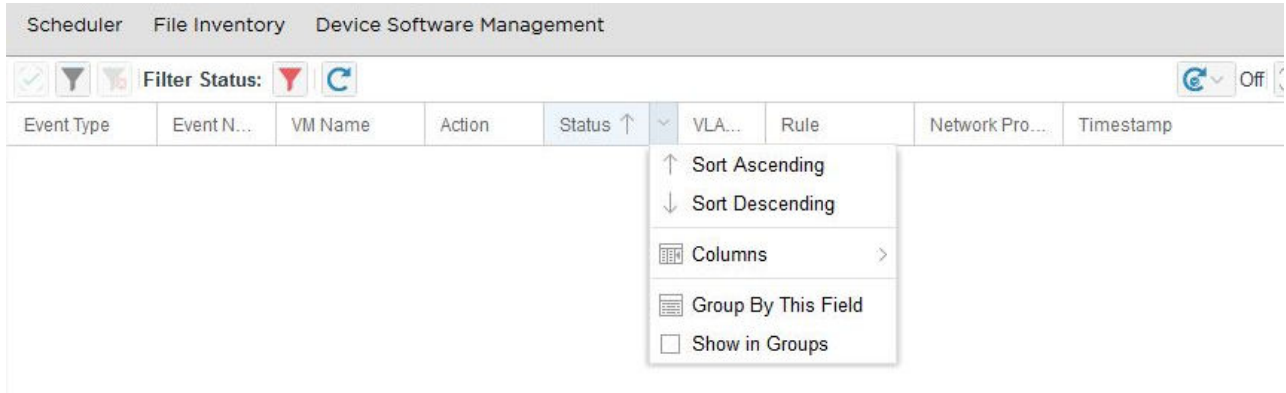
You can group information by fields for Event Monitor only.

Procedure

1. Select the desired field.
2. Click **Group By This Field** in the list.

Example

The following figure shows the fields grouped in rows.



To ungroup the fields, clear the **Show in Groups** selection.

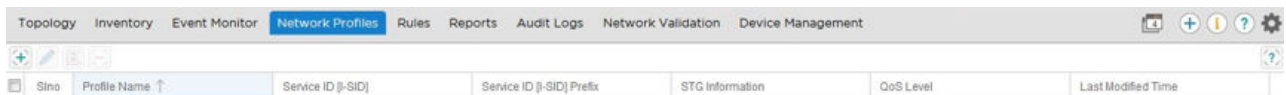
Network Profiles procedure

This section provides the Network Profiles procedures.

Network configuration is simplified by providing a template called network profile for defining configuration parameters and which are used across the device types. Because Virtualization responds to lifecycle changes of VMs in the datacenter, network profiles can be used to define device configurations to be performed.

Use the network profiles to define the VLAN and port configurations that are applied to a switch port. A network profile provides a view of the VLAN, bandwidth, metering, access control and QoS configuration and ensures that the trunk is correctly configured to support the VM traffic. After you define and save a set of configurations, if a change occurs on the datacenter, the network profile is applied to the corresponding data switch in the network to support this change.

The following image shows the Network Profiles table.



The following table details the attributes for the profiling table.

Attribute	Description	Range	Default value
Sno	Serial number	Numeric	—
Profile Name	Name of the profile	Mandatory field. Maximum 13 characters	—

Table continues...

Attribute	Description	Range	Default value
Service ID [I-SID]	Service ID of the profile	Contains between 1 and 1677214 characters	—
Service ID [I-SID] Prefix	Service ID prefix of the profile	—	—
STG Information	The Spanning Tree Group information	Mandatory field. Numeric between 1 and 64	1
QoS Level	Number of the QoS	Mandatory field. Numeric between 0 and 7	0
Last Modified Time	Date and time at which the profile was last updated	—	—

Adding a profile

About this task

You must add a profile to properly commission Virtualization. You can use profiles to create a definition that you want to send to the server.

Procedure

1. From the EFO menu bar, select **Virtualization > Network Profiles**.

- Click the **+** sign on the **Network Profiles** tab. The **Add Profile** window displays.

- Type the information in the applicable fields. Ensure the mandatory fields are complete, such as **Profile name**, **VLAN ID**, and **STG Id**. You can also choose to select the **Configure different setting for the Edge and Core Device** check box.

*** Note:**

After you add a new profile, you cannot edit the Profile name, VLAN ID, and the STG ID. Determine whether frames in this VLAN should be assigned a high switching priority by selecting High Priority (1K).

+ Tip:

The **Traffic Profile/ACL Configuration** section is optional. Use this section to configure a device port to allow or drop traffic that meets the specified criteria. For example, Ethernet Routing Switches (ERS) 45xx, 55xx, and 56xx are stackable devices, whereas ERS 86xx and 88xx are modular devices. If you add a network profile without configuring the Traffic Profile/ACL, only the VLAN configuration is applied to the network device.

4. Click **Save**.

The following table describes the values for adding a profile.

Value	Variable
Profile Name	Name of the profile. Mandatory field.
VLAN Configuration	
Configure different setting for the Edge and Core Device	Configures different setting for the Edge and Core Device when check box is selected.
STG ID	The Spanning Tree Group ID.
Edge And Core ID	Specifies different STG IDs for edge and core devices when provisioning the physical network for a VM event.
QoS Level	Selects a Qos level from the available options. The default value is 0.
High Priority (1K)	A flag to note whether frames in this VLAN should be assigned a high switching priority.
Configure L2VSN with Switched UNI	Configures L2VSN with Switched UNI when check box is selected.
Service ID [I-SID]	I-SID used to provision a Service (L2 VSN Service) on an UNI either as CVLAN or a Switched mode.
Service ID Type [I-SID]	Use the Service ID [I-SID] provided by the user in the network profile to configure the actual I-SID.
Traffic Profile/ACL Configuration (Stackable Type)	
Protocol	Protocol is the ipv4 protocol number [0..255]; 1(icmp-ipv4), 2(igmp), 6(tcp), 17(udp), 46(rsvp), 58(icmp-ipv6).
Action Drop	Action to be Performed, Drop or Pass.
Action Set Precedence	The precedence for the Classifier Filter Set.
Committed Rate (kbps)	Committed rate is integer value [0..10230000] in multiples of 64 or 1000.
Traffic Profile/ACL Configuration (Modular Type)	
Priority	Priority for ACE.
Ace Mode	Mode of ACE.
Peak Rate (kbps)	Peak Rate in kb/s [1000-10000000].

Table continues...

Value	Variable
tcpSrcPort	Comma separated list of ports: {0..65535} in ascending order.
udpSrcPort	Comma separated list of ports: {0..65535} in ascending order.
tcpDstPort	Comma separated list of Port: {0..65535} in ascending order or {echo, ftpdata, ftpcontrol, ssh, telnet, dns, http, bgp, hdot323}.
udpDstPort	Comma separated list of Port: {0..65535} in ascending order or {echo, dns, bootpServer, bootpClient, tftp, rip, rtp, rtcp}. This content is case sensitive.

Editing a profile

About this task

You can edit an existing profile from the Network Profile service. Perform the following procedure to edit a profile.

 **Note:**

Extreme Networks recommends that you do not edit a profile that already applies to a device. You can still edit the selected profile; however, a warning message appears stating that you are editing an already applied profile.

Procedure

1. From the EFO menu bar, select **Virtualization > Network Profiles**.
2. Select the profile you want to edit.

 **Note:**

You cannot edit the Profile Name, STG ID, VLAN ID and Service ID [I-SID] of an already existing profile.

3. On the Profiles tab, click the **Edit an existing network profile** icon.
The **Edit Profile** window appears.
4. Edit the content you want to change in each appropriate field.
5. Click **Save**.

Deleting a profile

About this task

You can use the delete option in the Network Profile service if you no longer need a specific profile. Perform the following procedure to delete a profile from the list of existing profiles.

*** Note:**

You cannot delete a profile if a rule or a device is associated with the profile or if this is the last profile having a particular VLAN Id and there is any VLAN I-SID VId entry with the same VLAN Id. If you try to delete the profile, an error message appears and the deletion fails.

Procedure

1. From the EFO menu bar, select **Virtualization > Network Profiles**.
2. Select the profile you want to delete.
3. On the **Profiles** tab, click the **Delete an existing network profile** icon.
4. In the **Delete Profile** window, click **Yes**.

Rules management

You can simplify configurations by using rules. Rules are conditions that apply to network profiles to determine which of these network profiles apply to which virtual machine (VM) event. When a VM is migrated, Virtualization receives that VM event from the vCenter server and supports the migration by sending the configuration to the data center switch. You can apply a maximum of five criteria for each rule you create, with each of the criteria being based on the following three options:

- Location—The value of the custom field, Location of the ESX/ESXi host on which the VM is hosted or being migrated to.
- VM Application Type—The application server type of the virtual machine.
- Port Group (VLAN ID)—The VLAN ID of the port groups to which a virtual machine is connected.
- Port Group (Name)—The name of the port group to which a virtual machine is connected.

A rule is either configured as automatic or manual. In the case of an automatic rule, if a match is found for a virtual machine event, then the configuration defined in the related network profile is applied on the device of the physical network. As for a manual rule, the configuration defined in the associated network profile is not automatically applied to the network devices, in which case you can use the Dashboard to manually mark the configuration as completed by the operator.

Virtualization cannot choose between more than one applicable rule.

*** Note:**

Extreme Networks recommends that you configure rules during the Virtualization setup process to enable proper functionality.

The following figure shows the Rules table:

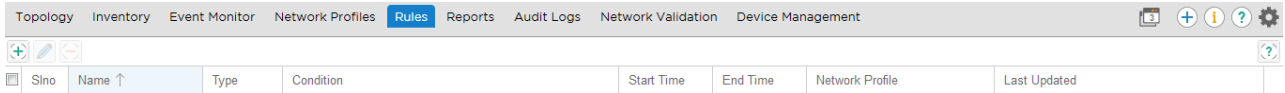


Figure 9: Rules table

The following table lists the details of the tabs in the Rules table.

Field	Description
Sno	The row number of the rule.
Name	The name of the rule.
Type	The type of rule, either manual or auto. If manual is applied, the action is only in a proposed state. If auto is applied, the configurations are applied to the appropriate switch.
Condition	The condition attributed to the rule.
Start Time	Start time of the interval when this rule can be applied.
End Time	End time of the interval when this rule can be applied.
Network Profile	Name of the network profile.
Last Updated	The date and time at which the rule was last updated.

Adding a rule

About this task

You can add a rule to apply specific conditions to a VM event to select the network profile which is applied to the data switch. After you add a rule, each rule that applies to a specific network profile is populated in the Monitor pane where you can view and monitor the status of those events.

Perform the following procedure to add a rule.

Procedure

1. From the EFO menu bar, select **Virtualization > Rules**.
2. Click the **+** sign on the **Rules** tab. The **Add Rule** window displays.
3. In the **Name** field, type the name of the rule.
4. In the Network Profile drop-down box, select a network profile for the given rule.
5. **(Optional)** Select **Automatic** to automatically configure the rule of the selected network profile.
6. In the **Effective Time** area, type the start time and end time at which you want to begin and end the given rule.
7. In the **Condition Criteria** section, select the conditions to apply to the given rule.
8. Click **Save**, and then click **Close**.

Variable	Description
Name	Name of the rule.
Network Profile	Select the appropriate network profile for the given rule.
Automatic	Enables automatic configuration of the rule. If you disable the Automatic option, the rule is set to manual. If you want the rule set to manual, you can review the information before you apply the configuration in the Pending/Failed Actions pane.
Start Time	The time at which the rule begins to apply.
End Time	The time at which the rule ends.
Condition criteria	Use this section to apply conditions to the given rule. Select the appropriate criteria from the available drop-down boxes. You can add a maximum of five conditions.

Editing a rule

About this task

Perform the following procedure to edit a rule.

Procedure

1. From the EFO menu bar, select **Virtualization > Rules**.
2. Select the rule you want to edit.
3. On the **Rule** tab, click the **Edit** button.

The **Edit Rule** window appears.

4. Edit the content you want to change in each field.
5. Click **Save**.

Deleting a rule

About this task

You can delete a rule that you no longer require within Virtualization. Perform the following procedure to delete an existing rule.

Procedure

1. From the EFO menu bar, select **Virtualization > Rules**.
2. Select the rule you want to delete.

3. On the Rules tab, click the **Delete** button.
The **Delete Rules** window appears.
4. Click **Yes** in the **Delete Rules** window.

Reports management

This section provides information about the various reports you can generate.

Reports management tasks can be performed in **Virtualization > Reports**. If you want to generate a report to include only a specific time period, you can define that time period by configuring the criteria in the reports table.

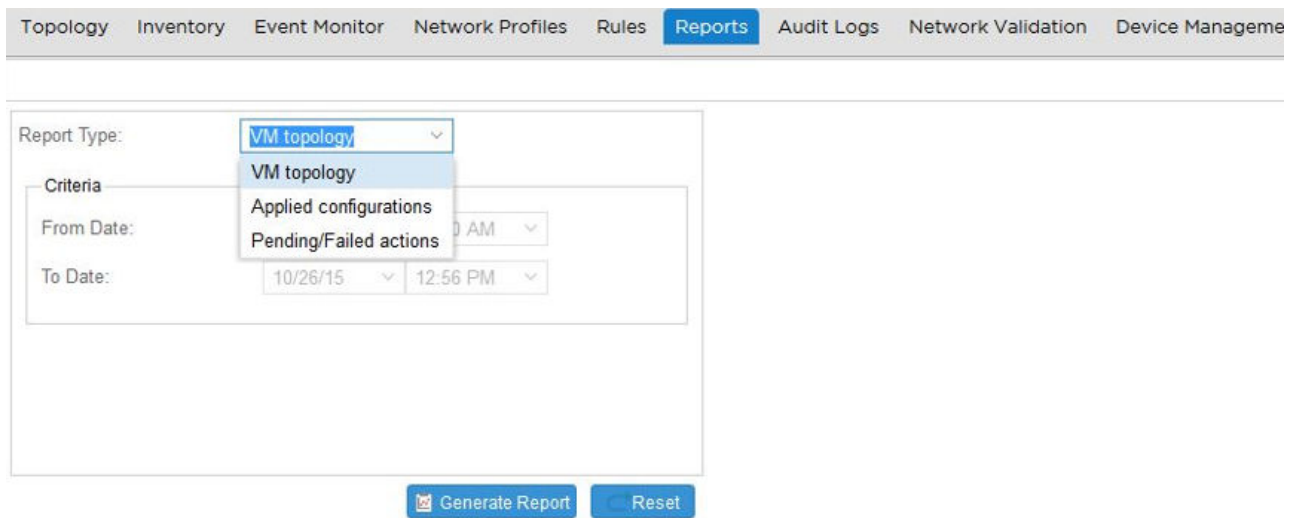


Figure 10: Reports view

VM topology reports

The VM topology report allows you to view the end-to-end topology information of the virtual machines.

The VM topology report displays the following information from the device inventory.

Field	Description
Data Center	Name of the data center applied to the report.
Server	Name of the server.
Location	Location of the server.

Table continues...

Field	Description
VM	Name of the virtual machine.
VM Application Type	The type of virtual machine that is used in the report.
Switch (v/dv)	The name of the virtual switch or the distributed virtual switch.
Type	The discovery protocol type, for example, CDP or LLDP, on the virtual switch.
Status	The discovery protocol status, for example, enabled or disable.
Operation	The discovery protocol operation can be BOTH or LISTEN.
Port Group (v/dv)	The name of the virtual port group or the distributed virtual port group.
Port Group VLAN ID	The number of the port group or the VLAN.
VM Adaptor	The network adaptor of the VM.
Uplink (v/dv)	The name of uplink ports of the virtual switch or the distributed virtual switch.
Physical Adaptor	The name of the physical adaptor.
Switch IP	The IP address of the switch to which the VM/ESX/ ESXi is connected.
Slot/Port	The slot or port info of the switch.

Applied configurations reports

The Applied configurations report provides information about successfully applied configurations on the physical network, or devices, for VM events during a specific period.

The Applied configurations report displays the following information from the device inventory.

Field	Description
Sl.No.	Switch slot number.
Event	The name of the event used in the report.
VM	The name of the virtual machine.
VLAN ID	The number of the VLAN
Action	The type of action that applied to the network.
Rule	The rule that applied to the network profile.
Network Profile	The network profile associated with the rule.
Status	The status of the event. Status can be success, pending, or failed.
Timestamp	The date and time when the event occurred.

Pending or Failed actions reports

The Pending/Failed actions report provides information about the pending or failed actions on the network. You can also view the actions that failed when you try to match a network profile.

The Pending/Failed actions report displays the following information from the device inventory.

Field	Description
Sl.No.	Switch slot number.
Event	The name of the event used in the report.
VM	The name of the virtual machine.
VLAN ID	The number of the VLAN
Action	The type of action that applied to the network.
Rule	The rule that applied to the network profile.
Network Profile	The network profile associated with the rule.
Status	The status of the event. Status can be pending, or failed.
Timestamp	The date and time when the pending or failed report occurred.

Generating a report

About this task

You can generate a report to view data that stems from configurations and topology that occurs within Virtualization. Complete the following procedure to generate one of the following types of reports.

- VM topology
- Applied configurations
- Pending/Failed actions

Procedure

1. From the EFO menu bar, select **Virtualization > Reports**.
2. In the **Reports** tab, in the **Report Type** field, select the type of report you want to generate.
3. In the **Criteria** section, enter the appropriate time frame for which you want to view the specific data.

 **Note:**

This step does not apply to the VM topology report.

4. Click **Generate Report**.

Exporting data from a report

About this task

You can export data from a report to your computer for reference. Perform the following procedure to export data from a report.

Procedure

1. From the EFO menu bar, select **Virtualization > Reports**.
2. On the **Reports** tab, in the **Report Type** field, select the type of report you want to view.
3. In the **Criteria** section, enter the appropriate time frame for which you want to view the specific data.
4. Click **Generate Report**.
5. Click the **Export Data** icon on the **Report**.
The Export Data window appears.
6. In the **Available result sets** field, select the appropriate option for the selected report.
7. In the **Available Columns** area, select the type of columns that you want to export from the given report, and then click the **Add all/Add** icon to import the selected columns in the **Selected Columns** area.
8. In the **Export format** field, select the format in which you want to view the data.
9. Select the **Output** encoding.
10. In the **Separator** field, select the type of separator you want to use.
11. Select either **Export column's data type** or **Export column as locale neutral**.
12. Click **OK**.

Variable	Value
Available result sets	The list of available viewable options
Available columns	The list of columns that are available to view
Selected columns	The list of columns that contain the data that you select to export
Export format	The format in which you want to view the exported data. The format defaults to .csv.
Output encoding	<ul style="list-style-type: none"> • UTF-8: • Other (If blank, use the local encoding)
Separator	The type of separator you want to use to export the data.

Exporting a report

About this task

You can export report to your computer for reference. Perform the following procedure to export a report.

Procedure

1. From the EFO menu bar, select **Virtualization > Reports**.
2. On the **Reports** tab, in the **Report Type** field, select the type of report you want to view.
3. In the **Criteria** section, enter the appropriate time frame for which you want to view the specific data.
4. Click **Generate Report**.
5. Click the **Export Report** icon on the **Report**.
The Export Report window appears.
6. In the **Export format** drop-down list, select the format type to export the report.
7. Select the desired page option for exporting.
8. Click **OK**.

Printing a report

Before you begin

You must generate a report or access an existing report. For more information about generating a report, see [Generating a report](#) on page 52.

About this task

After you generate a report, you can print the report to store a hard copy of the data. Perform the following procedure to print a report.

Procedure

1. Click the **Print** icon on the **Report**.
The **Print Report** window appears.
2. Select the **Print Format,HTML** or **PDF**.
3. Select the desired page option for printing.
4. Click **OK**.

Printing a report on the server

Before you begin

You must generate a report or access an existing report. For more information about generating a report, see [Generating a report](#) on page 52.

About this task

After you generate a report, you can print the report to the server for future reference. Perform the following procedure to print a report to the server.

Procedure

1. Click the **Print report on the server** icon on the **Report**.
The **Print report on the server** window appears.
2. Select the appropriate values for printing.
3. Click **OK**.

Audit Logs

All of the managers including Topology and Discovery send log messages to audit and debug logs. You can use **Virtualization > Audit Logs** to view details about configuration changes that occurred within Virtualization, such as the inventory audit or port scan, as well as the status of these operations, and the processing of these events.

EFO Virtualization debug logs are located at `<COM_HOME>\vps\log\vps_debug.log`. You can access the audit log preferences through the Preferences icon on the EFO menu bar.

You can generate Virtualization audit logs with the help of the logging service in Configuration. A refresh icon is available in the Audit Log tab to view the most recent audit logs within Virtualization. To differentiate Configuration from Virtualization, Virtualization audit logs are preceded by Virtualization.

The following figure shows an example of Audit Logs.

Topology Inventory Event Monitor Network Profiles Rules Reports Audit Logs Network Validation Device Management						
Filter: None						
Date/Time ↓	Log Level	User	Status	Event ID	Switch IP	Message
2015-10-26 00:00:00	Summary	admin	SUCCESS			License Check Complete, Current License Validity : true
2015-10-26 00:00:00	Summary	admin	SUCCESS			License Check Complete, Current License Validity : true
2015-10-26 00:00:00	Summary	admin	SUCCESS			License Check Complete, Current License Validity : true
2015-10-25 00:00:00	Summary	admin	SUCCESS			License Check Complete, Current License Validity : true
2015-10-25 00:00:00	Summary	admin	SUCCESS			License Check Complete, Current License Validity : true
2015-10-25 00:00:00	Summary	admin	SUCCESS			License Check Complete, Current License Validity : true
2015-10-24 00:00:00	Summary	admin	SUCCESS			License Check Complete, Current License Validity : true

Figure 11: Audit Logs view

Configuring Logging settings

You can configure settings for Audit Log Configuration and Debug Log Configuration. Click the preferences icon from the quick access toolbar to open the **Preferences** page.

Configuring Audit Log

About this task

Perform the following steps to configure Audit Log settings.

Procedure

1. On the Preferences page, click **Virtualization** from the left navigation pane.
The Preferences page displays the **Virtualization** on the right side of the page.
2. Click the **Logging** tab.
The Logging pane is displayed.
3. In the Audit Log Configuration section, configure the following settings:
 - In **Level** field, select **On** or **Off** from the drop-down list.
 - Select or clear **Enable Purge** check box, to enable or disable purge.
 - In **Retention Time in Days [15–120]** field, specify the number of records in days you want to purge. The default value is 60.
4. Click **Apply**.

Configuring Debug Log

About this task

Perform the following steps to configure Debug Log settings.

Procedure

1. On the **Preferences** page, click **Virtualization** from the left navigation pane.
The Preferences page displays the **Virtualization** on the right side of the page.

2. Click the **Logging** tab.

The Logging pane is displayed.

3. In the Debug Log Configuration section, configure the following settings:
 - In **File Size** field, enter the maximum file size. The default value is 10 MB.
 - In **Level** field, select **Off**, **Error**, **Warn**, **Info**, or **Debug** log level from the list.
The default is `Info`.
 - In **No. of Files [1–10]** configure the number of log files. The default value is 3.
4. Click **Apply**.

Viewing Audit Logs

Perform the following procedure to view and refresh the audit logs.

Procedure

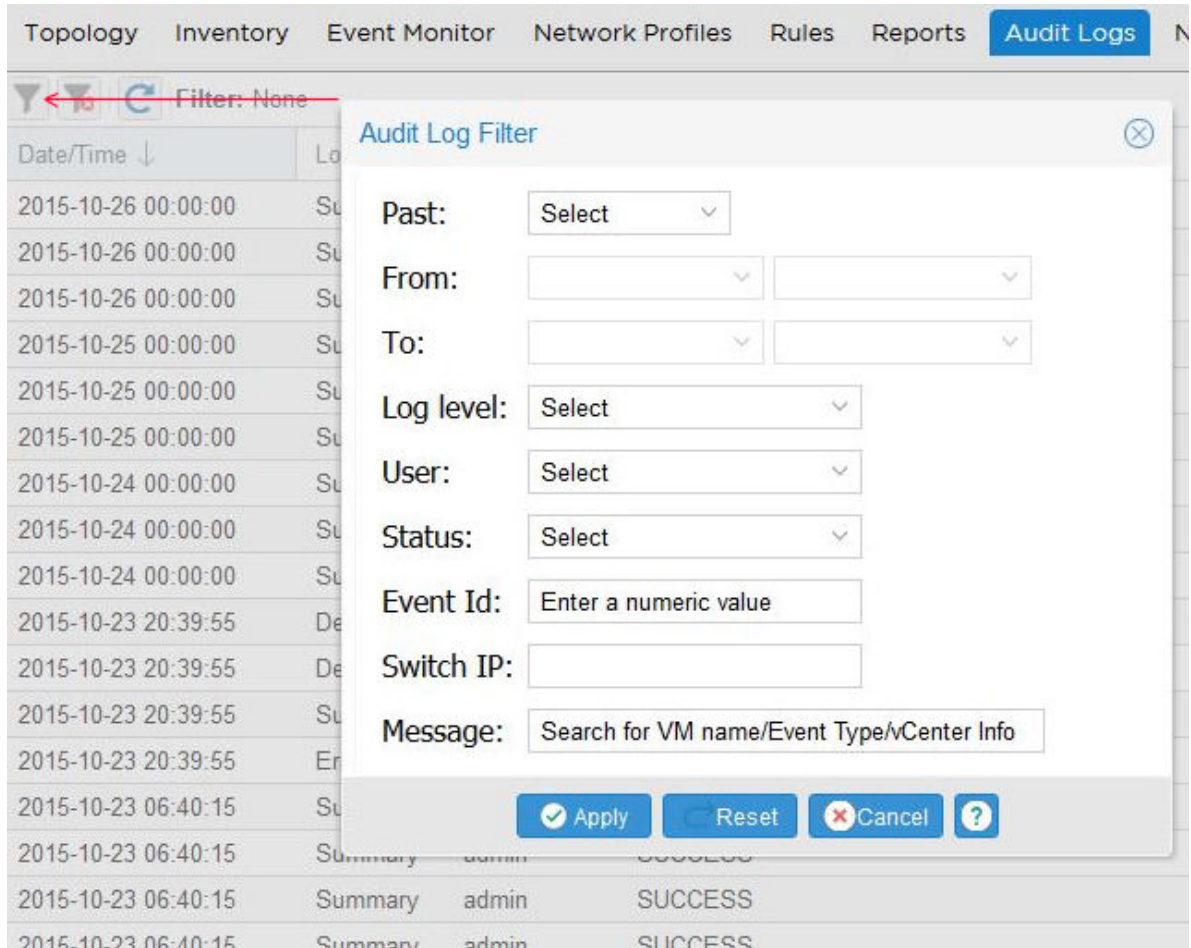
1. From the EFO menu bar, select **Virtualization > Audit Logs**.
2. Click the **Refresh** icon on the **Audit Logs** tab to refresh the audit log.

Filtering Audit Logs

Perform the following steps to apply the Filter option to search for information by fields.

Procedure

1. From the EFO menu bar, select **Virtualization > Audit Logs**.
The Audit Log window displays.
2. Click **Filter**.
The Audit Log Filter window displays.
3. Select the options to filter.



4. Click **Apply**.
5. Click **Clear Filter** to clear the applied filters and restore all the records in the table.

Network Validation procedures

The following sections provide the Network Validation procedures.

Running Network Validation Report

About this task

Perform the following procedure to run a Network Validation Report.

Before you begin

- Configure vCenter Server settings

- Perform Inventory audit and hypervisor connectivity operation

Procedure

1. From the EFO menu bar, select **Virtualization > Network Validation**.
The Network Validation Report displays.
2. **(Optional)** Select **Run Network Validation Report** to rerun a Network Validation Report.

Running network validation tab field descriptions

Field	Description
VM Name	Name of the Virtual Machine
Host Name	Name of the Esxi server
NIC Name	Name of the physical adapter
Virtual Switch	Name of the virtual Switch
Network Label	Name of the Port Group
PG VlanId	Port group Vlan-ID
Device IP	IP Address of the device
State	State of the physical network
Error Msg	Error message

Filtering Network Validation Report

About this task

Perform the following procedure to filter the Network Validation Report based on the network type.

Procedure

1. From the EFO menu bar, select **Virtualization > Network Validation**.
The Network Validation Report displays.
2. Select **Apply Network Validation Report Filter**.
The Network Validation Report Filter dialog box displays.
3. Select the appropriate parameters for filtering.
4. Click **Apply**.
The filtered Network Validation report displays.
5. **(Optional)** Select **Clear Filter** to clear the applied filters and to restore all the records.

Device Management procedures

This section provides the Device Management procedures.

Viewing the Device Management status

About this task

Perform the following procedure to view the Device Management status.

Procedure

1. From the EFO menu bar, select **Virtualization > Device Management**.
The Device Management window displays.
2. Select the desired option in the **View** field to view the device status.
3. **(Optional)** Click the **Refresh** icon to manually refresh the screen.
4. Click **Save Device Management State** icon to save.

Managing devices

About this task

You can manually select devices that are in an unmanaged state within the Device Management window to become managed. Although you can perform this task manually, moving a device from the managed to unmanaged state causes the Virtualization application to recapture all the related inventories and topology of the device. Extreme Networks recommends that you minimize such state changes.

You can also manage or unmanage stacked units under the Stack Units tab. Perform the following procedure to manage or unmanage a device.

Procedure

1. From the EFO menu bar, select **Virtualization > Device Management**.
The Device Management window displays.
2. Determine the device state to be changed.
3. To manage or unmanage a device, click the **State** cell of the selected device row.

A check box displays.

- if the check box is selected, the device is managed. Click the box (the check mark disappears) to unmanage the device.
- if the check box is not selected, the device is unmanaged. Click the box (a check mark appears) to manage the device.

- If a stackable device, you can manage or unmanage stack units using the Stack Units tab.

Unsaved changes of state are indicated by the red marks in the top left corner of the **State** cells.

4. **(Optional)** Click the **Refresh** icon to review the current device states.
5. Click the **Save Device Management State** icon to save the changes to the device States.

Chapter 7: Virtualization backup and restore

The Virtualization database table is the repository of the data that Virtualization updates during backup or recovery. The backup operation makes a backup of the Virtualization system along with Configuration and SMGR to create restoration files in the event that the system state becomes corrupted. Virtualization automatically updates the database tables during a combined backup of Configuration and Virtualization while using scripts for Windows and Linux. You can then restore the system back to the checkpoint created by the backup file.

*** Note:**

Extreme Networks recommends that you backup Configuration along with the Virtualization application.

Virtualization database tables

The Virtualization application has both configured user/system and system discovered data. The following is the list of information that the system or users configures:

- Network profile
- Rules
- Virtualization managed device
- Virtualization historical event information

The Virtualization properties file is found in the following area:

```
{ $JBOSS_HOME } / server / avmgt / conf / vps / VpsPreferences.properties
```

The following table contains a list of database tables that corresponds to the Virtualization during backup:

Table 2: Database tables

Database table	
eem_vps_vnds_uplink	eem_vps_portgrp_vndsport

Table continues...

Database table	
em_vps_serverinfo_vnds	eem_vps_vnic
eem_vps_linkinfo	eem_vps_physicaladaptor
eem_vps_portgroup	eem_vps_vnd_switch
eem_vps_vminfo	eem_vps_serverinfo
eem_vps_clusterinfo	eem_vps_datacenterinfo
eem_vps_rule_variable_condition	eem_vps_rule_variable
eem_vps_rule_condition	eem_vps_rule
eem_vps_networkprofile	eem_vps_monitor_event
eem_vps_monitor_appliedconfig	eem_vps_monitor_action
eem_vps_monitor	eem_vps_device_unit
eem_vps_device	eem_vps_applied_vm_profile_switch
eem_vps_preferences	eem_vps_preferences_element
eem_vps_audit_log	eem_vps_topology_edge
eem_vps_topology_geometry	eem_vps_topology_vertex
eem_vps_vcenterinfo	

Appendix A: Recommendations

The following sections describe how to resolve Virtualization problems, as well as the recommendations for those errors.

Related links

[Rediscoveries and device assignments](#) on page 64

[Updating the virtual MAC of a physical adaptor](#) on page 65

[Internet browser settings](#) on page 66

Rediscoveries and device assignments

When changes in device assignments are not discovered upon Virtualization start up, but the changes exist in the assignment list, then devices are shown as unmanaged in the Device Manager.

The following figure shows the Device Management view.

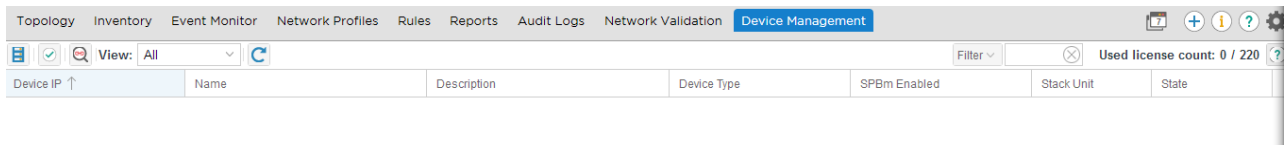


Figure 12: Device Management view

Network rediscoveries can result in the following scenarios.

- There is a fault in the discovery or configuration, and you must modify the list accordingly to allow proper device management.
- You can verify if there were changes made to the Virtualization licensing by accessing the Configuration network discovery.

In case of a rediscovery, you must take the following measures:

- [Viewing the Device Management status](#) on page 60.
- [Displaying a summary of Network Discovery status](#) on page 35.

Related links

[Recommendations](#) on page 64

Updating the virtual MAC of a physical adaptor

Before you begin

This procedure is optional.

Ensure you perform an inventory audit before performing this task.

About this task

If the virtual MAC of a vmnic is set to use a prefix other than the standard IOU, then the switch information may not be populated correctly during link discovery.. Complete the following procedure to populate the data switch connection information for the physical adaptors. The physical adaptors include the switch IP address, as well as the slot and port of the switch to which the ESX or ESXi server physical adaptor is connected. You can use this tool if you want to populate either the virtual MAC, or the switch information, or both.

Procedure

1. Extract the vmac_populate_tool.tar or vmac_populate_tool.zip to a temporary folder.
A folder vmac_populate_tool is created.
2. In the CSV file VirtualMacInput.csv from the vmac_populate_tool folder, populate the CSV entries of each of the physical adaptor virtual MAC using the following format:
<EsxServerName>,<physicalMac>,<virtualMac>,<switchIp>,<switchSlot>,<switchPort>.
3. Complete the following steps:
 - a. With Telnet or SSH, login to each of the ESX Server and Esxi Server managed by Virtualization.
 - b. In the su mode, type the following command: `esxcfg-info | egrep 'MAC Address'`.
 - c. From the output, get the virtual MAC address of each physical adaptor of the Esx Server.
 - d. For each mapping, update the CSV file with the entry.

* Note:

Remove any sample entries from the file before you add new entries.

4. After changing the directory vmac_populate_tool, and depending on which operating system you are running, type the following command:

- On Linux, run the following command: `./parseVMac.sh`.

If the script does not have executable permission, run the following command: `chmod 0554 parseVMac.sh`.

- On Windows, run the following command: `ParseVMac.bat`.

Before you run the script, update the JAVA_HOME path in the script(ParseVMac.bat) to the path where JRE 6 is installed, for example, `C:\Program Files (x86)\Java\jre6`. This is required for java command to run.

Related links

[Recommendations](#) on page 64

Internet browser settings

Some security settings in Internet Explorer do not allow Java script execution. In this case, the login page does not show the login button. The following settings are recommended for Internet Explorer.

- Set the Internet Explorer security settings to medium high or lower to allow Java script execution, as shown in the following figure.

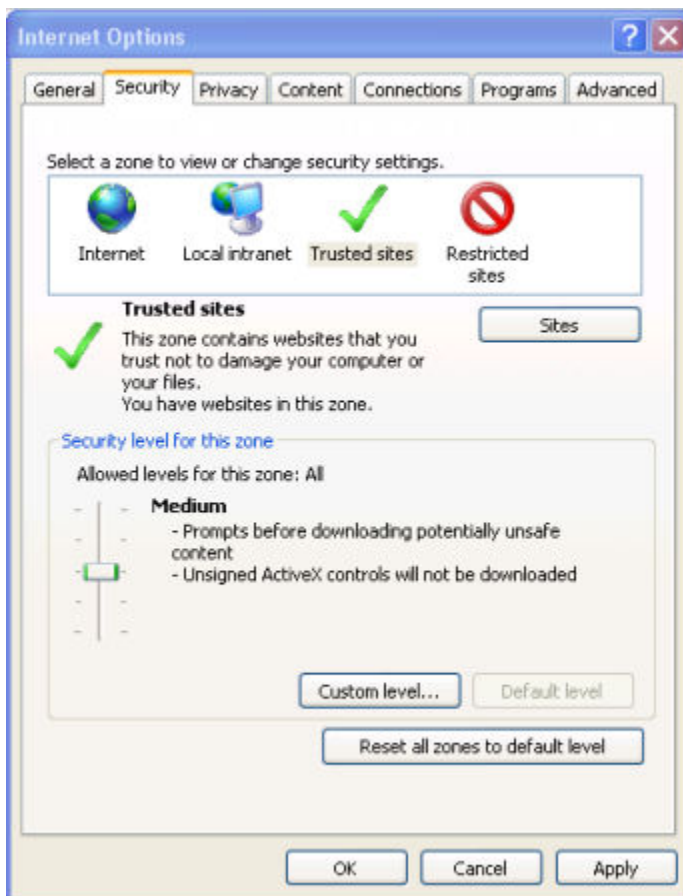


Figure 13: Internet Options dialog box

- There are additional settings for group policies that disable execution of scripts. Extreme Networks recommends that you set the same functionality in Firefox, in case the problem persists.

Related links

[Recommendations](#) on page 64