



Junos[®] Space

Junos Space Virtual Control User Guide

Release

1.4



Published: 2010-09-22

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Junos Space Junos Space Virtual Control
Release 1.4, Revision 1
Copyright © 2010, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Revision History
September 2010—Junos Space Virtual Control Release 1.4 Revision 1

The information in this document is current as of the date listed in the revision history.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.
- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
- d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14 (ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

	About the Documentation	xiii
	Junos Space Documentation and Release Notes	xiii
	Documentation Conventions	xiii
	Documentation Feedback	xiv
	Requesting Technical Support	xiv
	Self-Help Online Tools and Resources	xv
	Opening a Case with JTAC	xv
Part 1	Junos Space Virtual Control Overview	
Chapter 1	Understanding Junos Space Virtual Control	3
	About Virtual Networks	3
	About Junos Space Virtual Control	4
Chapter 2	Dashboard and Inventory Overview	7
	Dashboard Overview	7
	Inventory Overview	8
	Thumbnail View	9
	Tabbed View	10
Chapter 3	Using the Junos Space Virtual Control Getting Started Assistant	11
	Junos Space Virtual Control Getting Started Assistant Usage Overview	11
	How to manage a Virtual Network	11
	Port Group Profiles	11
Part 2	vNetworks	
Chapter 4	Manage Virtual Switch	15
	Managing Virtual Switches	15
	Manage Virtual Switch Overview	15
	Viewing the vSwitch Inventory	16
	vSwitch Thumbnail View	16
	vSwitch Grid View	17
	Viewing vSwitch Interface Details	18
	Viewing Private VLANs	20
	Managing Private VLANs	20
	Managing Port Groups	21
	Port Groups Overview	21
	Viewing Port Group Details	22
	Creating Port Groups	23
	Modifying Port Groups	26
	Deleting Port Groups	26

Chapter 5	Manage Host	29
	Viewing the Host Inventory	29
	Viewing Host Component Details	30
	Managing Uplink Ports	31
Chapter 6	Manage vNetwork	35
	Manage vNetwork Overview	35
	Viewing Notifications	37
	Purging Event Logs	38
	Managing vNetworks	39
	Viewing the vNetwork Inventory	39
	Adding vNetwork Credentials	40
	Modifying vNetwork Credentials	41
	Deleting vNetworks	42
	Re-synchronizing vNetworks	43
	Orchestrating vNetworks	44
	Orchestration Overview	44
	Physical Switch Configuration	45
	None	45
	Strict	45
	Very Strict	45
	Setting Orchestration Configuration Mode	46
	Importing Switch/Port Associations	46
	Auditing vNetwork Configurations	48
	Configuration Audit Overview	48
	Initiating a Configuration Audit	48
	Viewing Audit Reports	49
	Viewing Audit Reports for Virtual Switches	50
	Viewing Audit Reports for Physical Switches	51
Chapter 7	Discover vNetwork	55
	Discovering vNetworks	55
Part 3	Port Group Profiles	
Chapter 8	Understanding Port Group Profiles	59
	Port Group Profile Overview	59
Chapter 9	Managing Port Group Profiles	63
	Creating a Port Group Profile	64
	Viewing Associations	68
	Modifying a Port Group Profile	69
	Cloning a Port Group Profile	70
	Deleting a Port Group Profile	70
Part 5		
	Index	73

List of Figures

Part 1	Junos Space Virtual Control Overview	
Chapter 1	Understanding Junos Space Virtual Control	3
	Figure 1: Virtualized Server	3
	Figure 2: Network View of Virtual Machines	5
Chapter 2	Dashboard and Inventory Overview	7
	Figure 3: The vNetwork Inventory Dashboard	8
	Figure 4: Thumbnail View of a vNetwork	9
	Figure 5: Tabbed View of a vNetwork	10
Part 2	vNetworks	
Chapter 4	Manage Virtual Switch	15
	Figure 6: Manage Virtual Switch Page	16
	Figure 7: Manage Virtual Switch Page Thumbnail View	17
	Figure 8: Manage Virtual Switch Page Grid View	18
	Figure 9: Manage Virtual Switch Interface Details	19
	Figure 10: Port Group Details	22
	Figure 11: Port Group General Settings	24
	Figure 12: Port Group Failover Order	25
Chapter 5	Manage Host	29
	Figure 13: The Hosts thumbnail view	29
	Figure 14: The Hosts tabular view	30
	Figure 15: Hosts Inventory view	31
	Figure 16: Physical Switch Association Details for the Selected Host	32
Chapter 6	Manage vNetwork	35
	Figure 17: Manage vNetwork page	36
	Figure 18: The Event Details Page	37
	Figure 19: Configure Event Purging Dialog Box	38
	Figure 20: The vNetwork Inventory page	40
	Figure 21: Add vNetwork Credentials dialog box	41
	Figure 22: Modify vNetwork Dialog Box	42
	Figure 23: re-synchronize vNetwork Dialog Box	43
	Figure 24: Job Information Dialog Box	44
	Figure 25: Orchestration Mode Dialog Box	46
	Figure 26: Import Associations Dialog Box	47
	Figure 27: Configuration Audit Dialog Box	49
	Figure 28: Job Information Dialog Box	49
	Figure 29: Virtual Switch Audit Report	50

	Figure 30: Physical Switch Audit Report	52
Chapter 7	Discover vNetwork	55
	Figure 31: The vNetwork Discovery Status View	56
Part 3	Port Group Profiles	
Chapter 8	Understanding Port Group Profiles	59
	Figure 32: Manage Port Group Profile (Thumbnail view)	60
	Figure 33: Manage Port Group Profile (Tabular view)	60
Chapter 9	Managing Port Group Profiles	63
	Figure 34: Port Group Profile: General Settings	64
	Figure 35: Port Group Profile: Traffic Settings	66
	Figure 36: Port Group Profile: Teaming and Failover	67
	Figure 37: View Association	69

List of Tables

	About the Documentation	xiii
	Table 1: Notice Icons	xiv
Part 1	Junos Space Virtual Control Overview	
Chapter 2	Dashboard and Inventory Overview	7
	Table 2: Fields in the vNetwork Summary Information	9
Part 2	vNetworks	
Chapter 4	Manage Virtual Switch	15
	Table 3: Manage vSwitch Page Summary View Fields Descriptions	17
	Table 4: Manage Virtual Switch Page Field Description (Grid View)	18
	Table 5: View Interface Details Page Field Descriptions	19
	Table 6: Viewing Private VLANs page field description	20
	Table 7: Manage Private VLANs Page Field Descriptions	21
	Table 8: Port Group General Parameters	24
Chapter 5	Manage Host	29
	Table 9: Physical Switch Association Details	32
Chapter 6	Manage vNetwork	35
	Table 10: Event Details Information	37
	Table 11: Configure Event Purging Parameters	38
	Table 12: vNetwork Inventory Page field Descriptions	40
	Table 13: Add vNetwork Credentials dialog box field description	41
	Table 14: Fields in the CSV Association File	47
	Table 15: Information in the Virtual Switch Audit Report	51
	Table 16: Information in the Physical Switch Audit Report	52
Part 3	Port Group Profiles	
Chapter 9	Managing Port Group Profiles	63
	Table 17: Port Group Profile: General Settings	64
	Table 18: Port Group Profile: Traffic Settings	66
	Table 19: Port Group Profile: Teaming and Failover	67

About the Documentation

- Junos Space Documentation and Release Notes on page xiii
- Documentation Conventions on page xiii
- Documentation Feedback on page xiv
- Requesting Technical Support on page xiv

Junos Space Documentation and Release Notes

For a list of related Junos Space documentation, see

http://www.juniper.net/techpubs/en_US/release-independent/junos-space/index.html .

If the information in the latest release notes differs from the information in the documentation, follow the *Junos Space Release Notes*.

To obtain the most current version of all Juniper Networks technical documentation, see the technical documentation page at the Juniper Networks website at

<http://www.juniper.net/techpubs/> .

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at <http://www.juniper.net/books> .

Documentation Conventions

Table 1 on page xiv defines notice icons used in this documentation.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/> .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html> .

PART 1

Junos Space Virtual Control Overview

- Understanding Junos Space Virtual Control on page 3
- Dashboard and Inventory Overview on page 7

CHAPTER 1

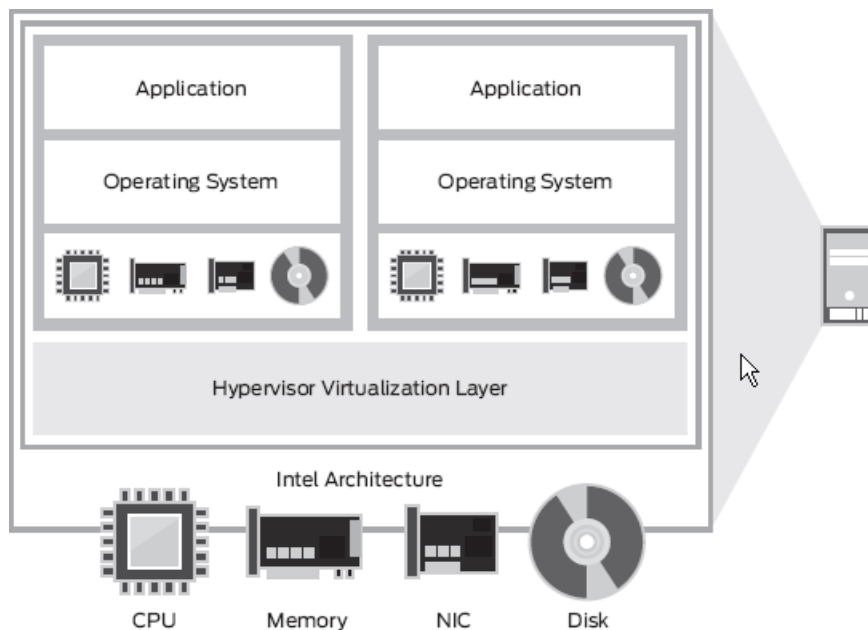
Understanding Junos Space Virtual Control

- About Virtual Networks on page 3
- About Junos Space Virtual Control on page 4

About Virtual Networks

Virtual networks are completely or partially made up of virtual devices that are connected together in a virtual environment. System virtual machines (VM), rendered by hypervisors, allow the sharing of the underlying hardware resources between different VMs.

Figure 1: Virtualized Server



Hypervisors (virtual machine monitors) are small-footprint software applications that reside between the hardware and the installed operating system, sometimes behaving as an extension of the bios. These applications divide the hardware resources (or host) into logical partitions (LPAR), allocating dedicated or shared slices of these resources

to each LPAR. Each VM (or guest) shares the physical resources of the host system. These include the CPU, memory, network interface card (NIC), and storage space. Figure 1 on page 3 illustrates the logical partitioning of hardware resources into virtual devices.

Each VM is assigned a MAC address, is logically connected to virtual ports or switches, and seems to initiate traffic from a virtual NIC. Virtual switches allow VMs on the same host to communicate with each other using the same protocols as physical switches. In addition, VMs can be configured with one or more virtual Ethernet adapters, each with its own MAC address and IP address. Virtual networks and virtual machines, therefore, have the same networking capabilities as physical networks built around physical devices.

The proliferation of virtual switches in the data center presents Data Center (DC) operators with the challenge of having to manage these virtual network resources in conjunction with their physical networks. Network operators are unable to apply the tools that they currently use for managing the physical infrastructure to managing the virtual infrastructure.

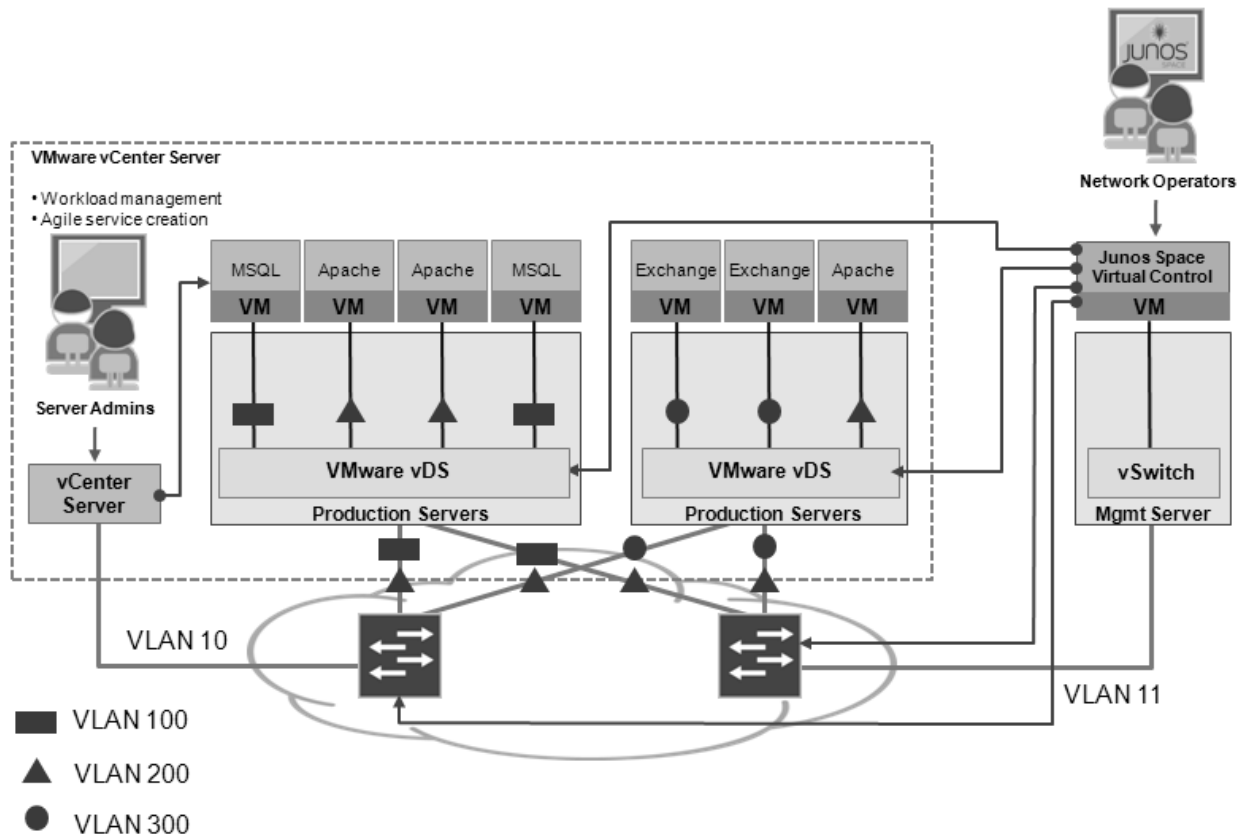
Related Documentation

- About Junos Space Virtual Control on page 4

About Junos Space Virtual Control

Junos Space Virtual Control (JSVC) unifies the physical and virtual networks, providing network operators with a comprehensive view into the complete end-to-end network infrastructure. Junos Space Virtual Control is a web-based solution that enables you to manage virtual networks deployed in virtualized environments in data centers. It provides a single management interface for you to monitor and control the virtual and physical elements of the virtual environment. This ensures that network policies are consistently and automatically applied across physical and virtual networks. Figure 2 on page 5 illustrates how virtual machines and physical interfaces in a virtual network.

Figure 2: Network View of Virtual Machines



Virtual machines residing on a host connect to ports in a virtual switch. Virtual switches, in turn, are associated with port groups that have a fixed number of ports. You can increase the number of ports on a virtual switch by adding more port groups. Ethernet adapters (also called Uplink adapters) connect the virtual environment to the physical network. These elements constitute the inventory of the virtual network.

You can use Junos Space Virtual Control to discover, configure, and monitor the virtual resources in your virtual environment. JSVC also provides consistent orchestration and operation of the physical and virtual components of the environment.

Junos Space Virtual Control allows you to use the services and functionality of other Junos Space applications to manage and monitor the virtual network just as you would a physical network.

Related Documentation

- Port Group Profile Overview on page 59

CHAPTER 2

Dashboard and Inventory Overview

- Dashboard Overview on page 7
- Inventory Overview on page 8

Dashboard Overview

The vNetwork workspace provides a single page snapshot of the current status of your virtual network. The vNetwork Inventory dashboard is the default landing page when Junos Space Virtual Control is launched.

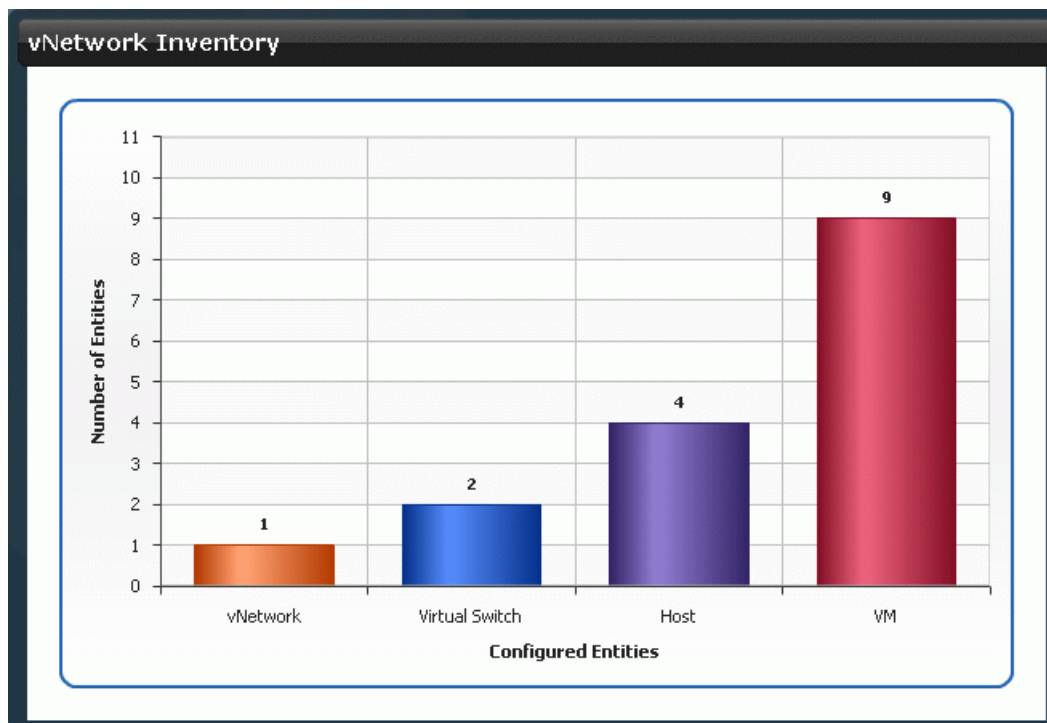
To launch Junos Space Virtual Control, do one of the following:

- Click **Virtual Control** on the **Junos Space Network Application Platform** landing page.
- From the Junos Space Network Application Platform landing page, or any of the Junos SSpace platforms, select **Application Selector > Virtual Control**.

The Virtual Network (vNetwork) Inventory dashboard displays a graphical depiction of the elements in the vNetwork, as shown in Figure 3 on page 8.

Junos Space Virtual Control recognizes the environment of virtual networks and virtual switches as a single physical network environment. This enables the administrator to dynamically configure, manage, and monitor the virtual components according to real time demands. The virtual machines, virtual networks, virtual switches, and hosts make up the inventory of the virtual network environment.

Figure 3: The vNetwork Inventory Dashboard



Related Documentation

- Inventory Overview on page 8

Inventory Overview

From the Junos Space Virtual Control inventory page, you can view and manipulate the managed virtual and physical components of the virtual network individually or collectively. You can also browse, zoom, filter, tag, and sort objects. You can select one or more objects and perform actions on them using the actions in the **Actions** drawer or from the right-click context menu.

Junos Space Virtual Control enables you to manage the virtual network inventory at various levels of granularity, including:

- **Virtual Network:** This includes viewing a graphical representation of the elements in the virtual network, viewing a list of virtual machines in the network and associated details, and adding a VMWare vCenter server.
- **Hosts:** This includes viewing the virtual machines on a host, and drilling down to the details for each host.
- **Virtual Switches and VLANs:** This includes viewing the virtual switches in the network, and the details for each switch. It also includes viewing and configuring VLANs.
- **Port Groups:** This includes viewing the ports in port groups and configuring port and port group settings.

From the vNetwork Inventory page, you can display the managed vNetwork elements in two views:

Thumbnail View

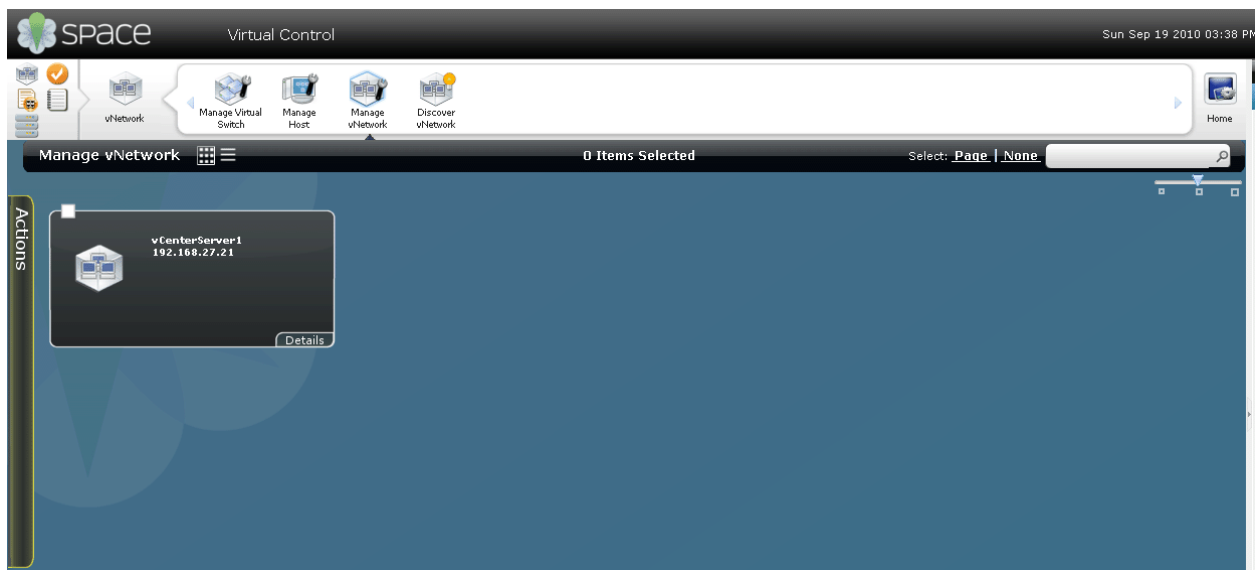
The Thumbnail View of the virtual network displays a representative image of the vNetwork.

To display the thumbnail view of the vNetwork:

- From the Junos Space task ribbon, select **vNetwork > Manage vNetwork**.

The Thumbnail view is displayed, as shown in Figure 4 on page 9.

Figure 4: Thumbnail View of a vNetwork



While in thumbnail view, to get summary information for a specific VMWare vCenter server, click **Details** (the bottom right corner of the thumbnail), or drag the zoom slider to the right. The summary information appears in the main display area. Table 2 on page 9 explains each of the fields in summary view.

Table 2: Fields in the vNetwork Summary Information

Field	Meaning
IP Address	IP address used by this server
vNetwork Name	Name assigned to the vNetwork as configured by the server administrator
Vendor Name	Name of the vendor for the virtual network

Table 2: Fields in the vNetwork Summary Information (*continued*)

Field	Meaning
Orchestration Mode	One of the following: <ul style="list-style-type: none"> • None • Strict • Very Strict
Version	Software version of the virtualization infrastructure

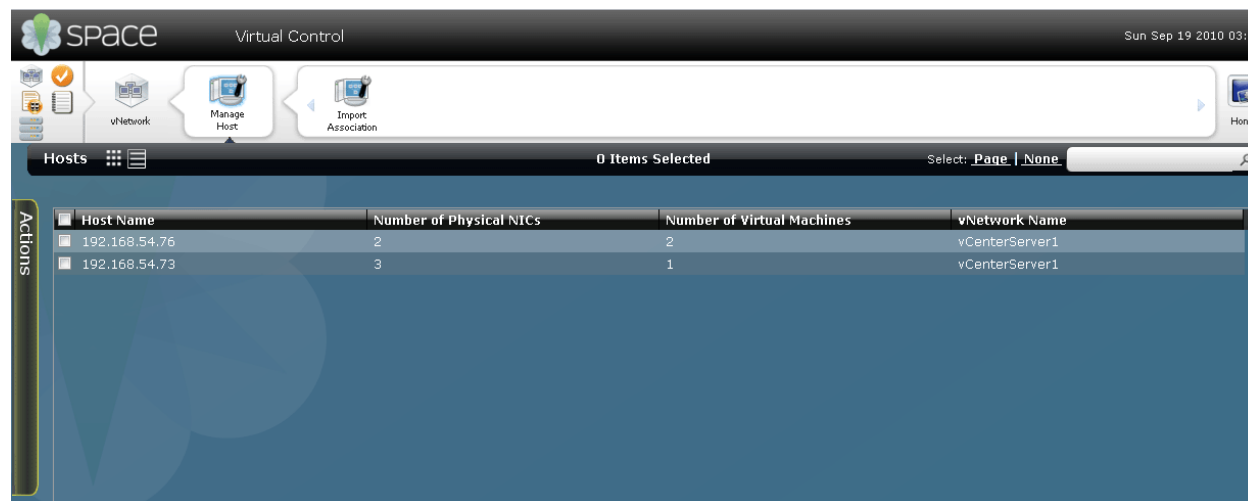
Tabbed View

The tabbed view of the Virtual Network displays a tabbed list of information for the selected vNetwork. To display the tabbed view of the vNetwork, from the Thumbnail view, click the tabbed icon in the title bar.

The Tabbed view is displayed, as shown in Figure 5 on page 10. The information displayed in the tabbed view is the same as that in the Thumbnail View summary, as explained in Table 2 on page 9.

You can toggle between Thumbnail and Tabbed views by clicking the icon in the title bar for the other view. The thumbnail and tabbed views for each of the vNetwork elements will be explained in greater details in subsequent topics, in the context of the elements they portray.

Figure 5: Tabbed View of a vNetwork



Related Documentation

- Dashboard Overview on page 7

CHAPTER 3

Using the Junos Space Virtual Control Getting Started Assistant

- Junos Space Virtual Control Getting Started Assistant Usage Overview on page 11

Junos Space Virtual Control Getting Started Assistant Usage Overview

The Getting Started assistant is a panel in the Junos Space sidebar that guides you through the tasks that you can perform as part of the initial setup for every application. It is displayed when you log in to Junos Space and the **Show Getting Started on Startup** check box is selected.

Every step in the Getting Started assistant contains a task link, and alongside the task links are help icons that provide information about the individual tasks. To execute the steps, click the task links of every step. The inventory page displays the page where you can execute the tasks.

To use the Junos Space Virtual Control Getting Started assistant, navigate to Junos Space Virtual Control, click the **Help** icon, and expand the **Getting Started** assistant. The **Getting Started** assistant displays the following links:

- How to manage a Virtual Network on page 11
- Port Group Profiles on page 11

How to manage a Virtual Network

To manage a virtual network you must first add a vNetwork. Click the **How to manage a Virtual Network** link to display the following links in the Getting Started assistant.

1. The required step is: **Add vNetwork**. See “Adding vNetwork Credentials” on page 40.
2. The optional step is: **Manage vNetwork**. See “Manage vNetwork Overview” on page 35.

Port Group Profiles

To port group profiles you must first create a port group profile. Click the **Port Group Profiles** link to display the following links in the Getting Started assistant.

1. The required step is: **Create a Port Group Profile**.
2. The optional step is: **Manage Port Groups**.

PART 2

vNetworks

- Manage Virtual Switch on page 15
- Manage Host on page 29
- Manage vNetwork on page 35
- Discover vNetwork on page 55

CHAPTER 4

Manage Virtual Switch

- Managing Virtual Switches on page 15
- Managing Port Groups on page 21

Managing Virtual Switches

- Manage Virtual Switch Overview on page 15
- Viewing the vSwitch Inventory on page 16
- Viewing vSwitch Interface Details on page 18
- Viewing Private VLANs on page 20
- Managing Private VLANs on page 20

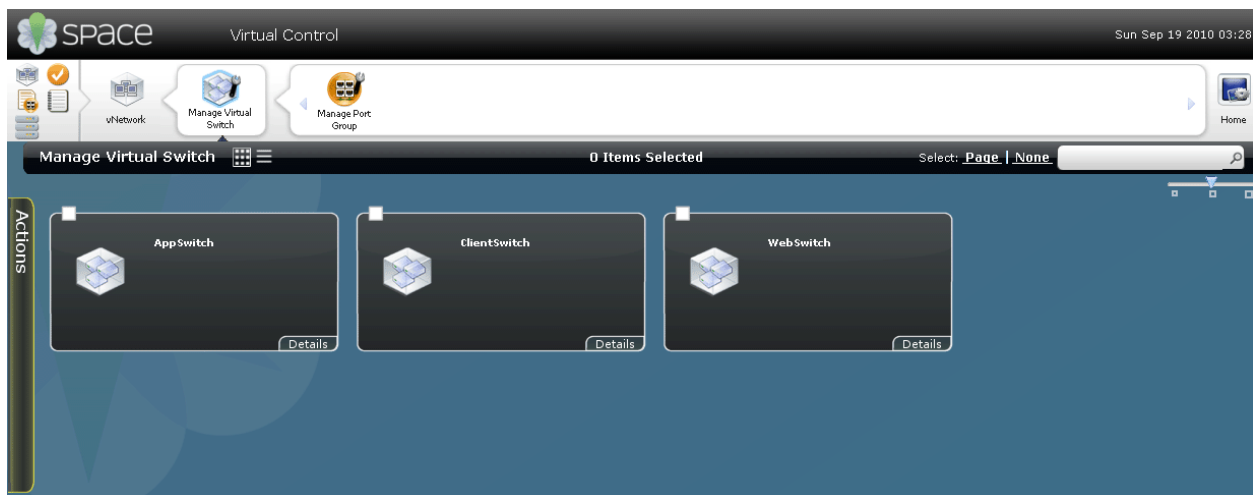
Manage Virtual Switch Overview

Junos Space Virtual Control enables you to manage virtual switches (vSwitches) as part of managing the vNetwork infrastructure. Virtual switches behave much like modular switches.

They are configured with a number of port groups, which in turn determine the number of ports available in a switch.

Figure 6 on page 16 shows the thumbnail view of the **Manage Virtual Switch** page.

Figure 6: Manage Virtual Switch Page



You perform the following tasks using the Manage Virtual Switch page:

- Viewing interfaces, port groups, and private LANs.
- Managing private VLANs.

Related Documentation

- Viewing the vSwitch Inventory on page 16
- Viewing Private VLANs on page 20
- Viewing vSwitch Interface Details on page 18
- Managing Private VLANs on page 20

Viewing the vSwitch Inventory

You can view the Virtual Switch inventory for information about the vSwitches in the vNetwork infrastructure.

To view the vSwitch Inventory:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage Virtual Switch**.
2. In the **Manage Virtual Switch** page, select Thumbnail View or Tabular View from the title bar. The vSwitch inventory thumbnail view is displayed, as shown below.

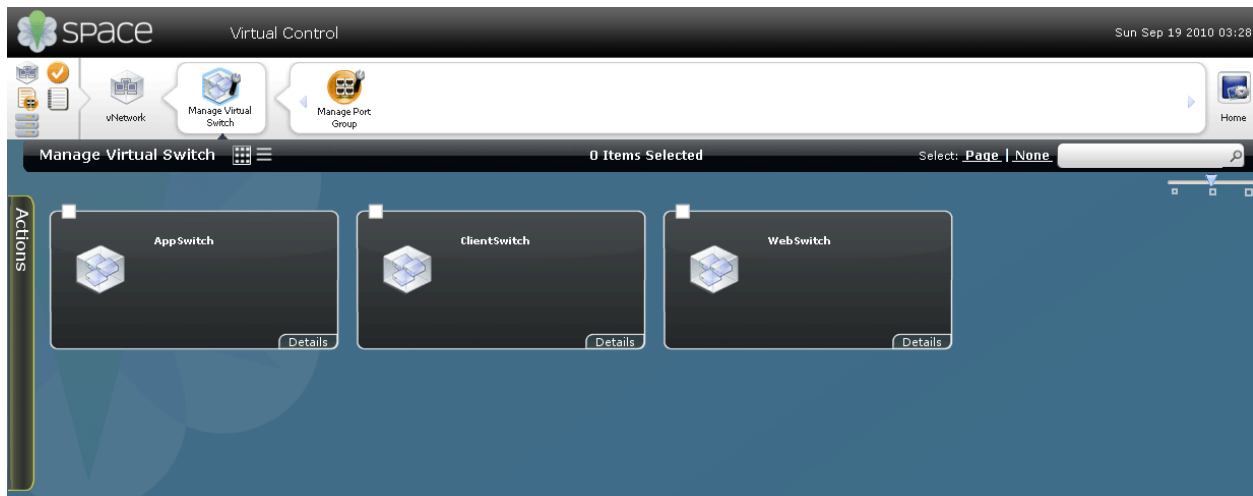
- vSwitch Thumbnail View on page 16
- vSwitch Grid View on page 17

vSwitch Thumbnail View

The thumbnail view of the vSwitch inventory shows thumbnails of all of the vSwitches in the network.

Figure 7 on page 17 represents the thumbnail view of the **Manage Virtual Switch** page.

Figure 7: Manage Virtual Switch Page Thumbnail View



To view a summary for a vSwitch, click **Details** on the thumbnail for a vSwitch. Table 3 on page 17 summarizes the fields displayed in the Thumbnail and Details view of the **Manage Virtual Switch** page.

Table 3: Manage vSwitch Page Summary View Fields Descriptions

Field	Description
Virtual Switch Name	The name assigned to the virtual switch
Number of ports	The total number of ports included in the port groups associated with this vSwitch
Max MTU	Maximum Transmission Unit—the size of the largest packet that can be transmitted.
vNetwork Name	The name of the vNetwork as configured by the server admin.
Type	The type of virtual switch

vSwitch Grid View

The Tabular View of the vSwitch inventory shows the details for all of the vSwitches in the vNetwork as shown in Figure below. This information is explained in Table below

Figure 8 on page 18 shows the Grid view of the **Manage Virtual Switch** page.

Figure 8: Manage Virtual Switch Page Grid View

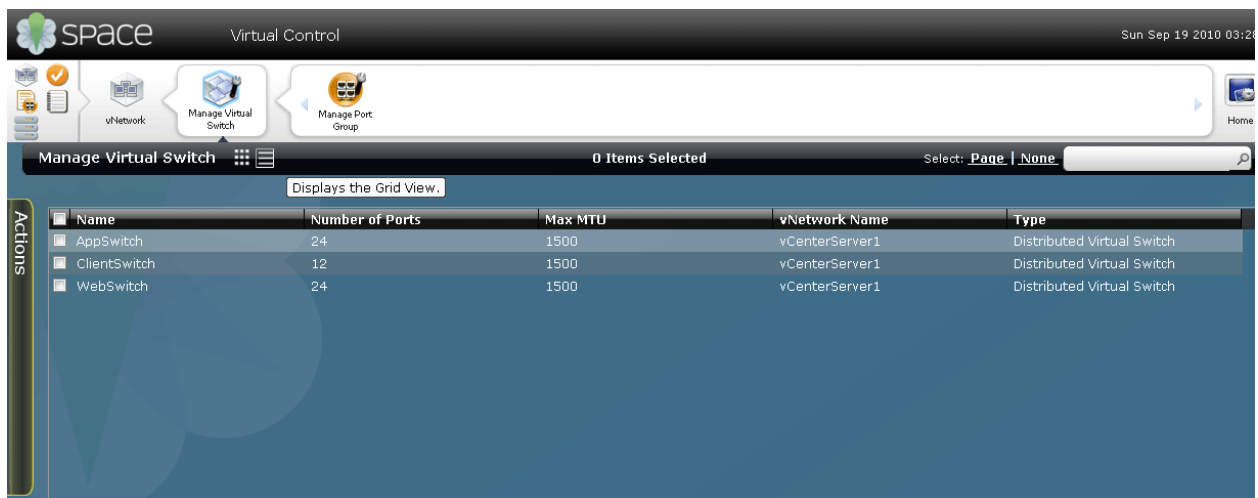


Table 4 on page 18 summarizes the fields in the Grid view of the **Manage Virtual Switch** page.

Table 4: Manage Virtual Switch Page Field Description (Grid View)

Field	Description
Name	Name assigned to the virtual switch.
Number of Ports	The total number of ports held in the port groups configured for this switch.
Max MTU	Maximum Transmission Unit -The maximum size of a protocol data unit that can be transmitted
vNetwork Name	The name of the vNetwork as assigned by the administrator.
Type	Distributed vSwitch

- Related Documentation**
- Manage Virtual Switch Overview on page 15
 - Viewing vSwitch Interface Details on page 18
 - Viewing Private VLANs on page 20

Viewing vSwitch Interface Details

You can view Interface details for each vSwitch in the vNetwork.

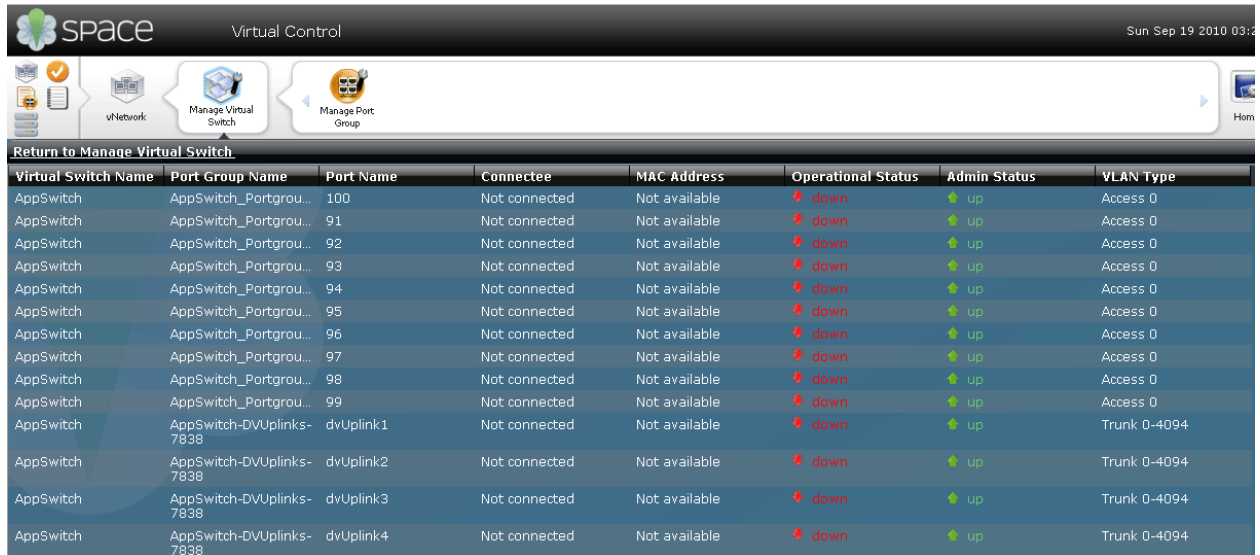
To view vSwitch interface details:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork** > **Manage Virtual Switch**.
2. In the **Manage Virtual Switch** page, select the check box on one or more vSwitch thumbnail.

3. From the **Action** panel, or the right-click context menu, and select **View Interfaces**

The vSwitch interfaces details are displayed, as shown in Figure 9 on page 19 showing the information listed in Table 5 on page 19.

Figure 9: Manage Virtual Switch Interface Details



Virtual Switch Name	Port Group Name	Port Name	Connectee	MAC Address	Operational Status	Admin Status	VLAN Type
AppSwitch	AppSwitch_Portgrou...	100	Not connected	Not available	down	up	Access 0
AppSwitch	AppSwitch_Portgrou...	91	Not connected	Not available	down	up	Access 0
AppSwitch	AppSwitch_Portgrou...	92	Not connected	Not available	down	up	Access 0
AppSwitch	AppSwitch_Portgrou...	93	Not connected	Not available	down	up	Access 0
AppSwitch	AppSwitch_Portgrou...	94	Not connected	Not available	down	up	Access 0
AppSwitch	AppSwitch_Portgrou...	95	Not connected	Not available	down	up	Access 0
AppSwitch	AppSwitch_Portgrou...	96	Not connected	Not available	down	up	Access 0
AppSwitch	AppSwitch_Portgrou...	97	Not connected	Not available	down	up	Access 0
AppSwitch	AppSwitch_Portgrou...	98	Not connected	Not available	down	up	Access 0
AppSwitch	AppSwitch_Portgrou...	99	Not connected	Not available	down	up	Access 0
AppSwitch	AppSwitch-DVUplinks-7838	dvUplink1	Not connected	Not available	down	up	Trunk 0-4094
AppSwitch	AppSwitch-DVUplinks-7838	dvUplink2	Not connected	Not available	down	up	Trunk 0-4094
AppSwitch	AppSwitch-DVUplinks-7838	dvUplink3	Not connected	Not available	down	up	Trunk 0-4094
AppSwitch	AppSwitch-DVUplinks-7838	dvUplink4	Not connected	Not available	down	up	Trunk 0-4094

Table 5: View Interface Details Page Field Descriptions

Field	Description
Virtual Switch Name	Name assigned to the Virtual Port
Port Group name	Name assigned to the Port Group
Port Name	Name assigned to the port.
Connectee	VM or host to which this port is connected.
MAC Address	Unique identifier assigned to the virtual NIC to which the VM connects
Operational Status	Specifies the links status of the virtual port: <ul style="list-style-type: none"> Down--implies that the port is not connected to a VM Up--implies that the port is connected to a VM
Admin Status	Admin Status Specifies the status of the port as set by the admin.
VLAN Type	One of the following <ul style="list-style-type: none"> Private VLAN Access VLAN Trunk VLAN

- Related Documentation**
- Manage Virtual Switch Overview on page 15
 - Viewing the vSwitch Inventory on page 16
 - Viewing Private VLANs on page 20
 - Managing Private VLANs on page 20

Viewing Private VLANs

You can view Private VLAN details for each vSwitch in the vNetwork.

To view details of private VLANs for a vSwitch:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage Virtual Switch**.
2. In the **Manage Virtual Switch** page, select the check box on one or more vSwitch thumbnail.
3. From the **Action** panel, or the right-click context menu, select **View Private VLANs**.

The vSwitch Private VLANs details are displayed, showing the information listed in Table 6 on page 20.

Table 6: Viewing Private VLANs page field description

Field	Description
Virtual Switch Name	The name assigned to the virtual switch.
Primary Private VLAN ID	The primary ID on the virtual switch
Secondary Private VLAN ID	The secondary ID on the virtual switch
Private VLAN Type	One of the following Private VLAN Types: <ul style="list-style-type: none">• Promiscuous• Isolated• Community

- Related Documentation**
- Manage Virtual Switch Overview on page 15
 - Viewing vSwitch Interface Details on page 18

Managing Private VLANs

You can use Junos Space Virtual Control to add new Private VLANs or delete existing VLANs according to your requirements.

To add a Private VLAN:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage Virtual Switch**.
2. In the **Manage Virtual Switch** page, select one or more vSwitch from the tabbed view.
3. From the **Action** panel, or the right-click context menu, select **Manage Private VLANs**.
4. Click **Add**, in the title bar.
5. Enter information in the fields according to the parameters described in Table 7 on page 21.

Table 7: Manage Private VLANs Page Field Descriptions

Field	Description
Virtual Switch Name	Name of the Virtual Switch
Primary Private VLAN ID	Primary ID on the virtual switch
Secondary Private VLAN ID	Secondary ID on the virtual switch
Private VLAN Type	Select one of the following: <ul style="list-style-type: none"> • Promiscuous • Isolated • Community

- Related Documentation**
- Manage Virtual Switch Overview on page 15
 - Viewing vSwitch Interface Details on page 18
 - Viewing Private VLans on page 20

Managing Port Groups

- Port Groups Overview on page 21
- Viewing Port Group Details on page 22
- Creating Port Groups on page 23
- Modifying Port Groups on page 26
- Deleting Port Groups on page 26

Port Groups Overview

In a virtual switch, a group of ports is collectively identified as a Port Group. New port groups can be added to increase the number of ports available on a virtual switch.

- Related Documentation**
- Creating Port Groups on page 23
 - Viewing Port Group Details on page 22

- Modifying Port Groups on page 26
- Deleting Port Groups on page 26

Viewing Port Group Details

You can view a list of Port Groups configured for each vSwitch in the vNetwork.

To view vSwitch Port Group details:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage Virtual Switch**.
2. In the **Manage Virtual Switch** page, select the check box on one or more vSwitch thumbnail.
3. From the **Action** Drawer, or the right-click context menu, select **View Port Groups**. The vSwitch Port Groups details are displayed as shown in Figure 10 on page 22, showing the information listed in

Figure 10: Port Group Details

Virtual Port Group Name	Virtual Switch Name	Number of Ports	VLAN Type	Port Group Profile Name	vNetwork Name	Synchronization Status
AppSwitch-DVUplinks-7838	AppSwitch	4	Trunk 0-4094	AppSwitch-DVUplinks-7838	vCenterServer1	In Sync
AppSwitch_Portgroup_1	AppSwitch	10	Access 0	AppSwitch_Portgroup_1	vCenterServer1	In Sync
AppSwitch_Portgroup_2	AppSwitch	10	Access 0	AppSwitch_Portgroup_2	vCenterServer1	In Sync
ClientSwitch-DVUplinks-7726	ClientSwitch	4	Trunk 0-4094	ClientSwitch-DVUplinks-7726	vCenterServer1	In Sync
ClientSwitch_Portgroup...	ClientSwitch	4	Access 888	ClientSwitch_Portgroup...	vCenterServer1	In Sync
ClientSwitch_Portgroup...	ClientSwitch	4	Access 999	ClientSwitch_Portgroup...	vCenterServer1	In Sync
WebSwitch-DVUplinks-7849	WebSwitch	4	Trunk 0-4094	WebSwitch-DVUplinks-7849	vCenterServer1	In Sync
WebSwitch_Portgroup...	WebSwitch	10	Access 0	WebSwitch_Portgroup...	vCenterServer1	In Sync
WebSwitch_Portgroup...	WebSwitch	10	Access 0	WebSwitch_Portgroup...	vCenterServer1	In Sync

Field	Description
Virtual Port Group Name	The name assigned to the port group
Virtual Switch name	The name assigned to the virtual switch to which this port group is configured
Number of Ports	The total number of ports in this port group
VLAN Type	Type of VLAN. From among: <ul style="list-style-type: none"> • Private VLAN • Access VLAN • Trunk VLAN
Port Group Profile Name	The name of the port group profile assigned to this port group

vNetwork Name	The name assigned to the vNetwork
Synchronization Status	<p>One of the following:</p> <ul style="list-style-type: none"> • In Sync—the port group is in sync with the VMWare vCenter server • Create Requested—a Create Port Group request has been sent to the VMWare vCenter server for this port group • Edit Requested—an Edit Port Group request has been sent to the VMWare vCenter for this port group

**Related
Documentation**

- Port Groups Overview on page 21
- Creating Port Groups on page 23
- Modifying Port Groups on page 26
- Deleting Port Groups on page 26

Creating Port Groups

Virtual switches are associated with port groups, not individual ports. A virtual machine can be associated with one of the port groups available. When a virtual machine is associated with a port group, the configuration of the port group applies to the virtual port assigned to the virtual machine.

A single port group can be assigned to multiple virtual machines. To increase the number of ports on a virtual switch, you need to add new port groups. The characteristics of these port groups are set by associating them with a port group profile.

To create a port group:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage Virtual Switch > Manage Port Group > Create Port Group**.

The Port Group General Settings property sheet is displayed, as shown in Figure 11 on page 24.

Figure 11: Port Group General Settings

Port Group: General Settings

Port group name:

Virtual switch name:

Number of ports:

VLAN type:

VLAN ID/range:

Port group profile name:

Profile description:

2. In the Port Group General Settings property sheet, enter the port group parameters as explained in Table 8 on page 24.

Table 8: Port Group General Parameters

Field	Description
Port Group Name	Provide a unique name for the new port group.
Virtual Switch Name	Enter the name of the virtual switch with which the port group is associated.
Number of Ports	Enter the number of ports configured on this port group.

Table 8: Port Group General Parameters (*continued*)

VLAN Type	Select one of the following as appropriate: <ul style="list-style-type: none"> • Private VLAN • Access VLAN • Trunk VLAN The Trunk VLAN is recommended for uplink port groups.
VLAN ID/range	Based on the type of VLAN selected, enter the appropriate range.
Port Group Profile Name	Select the required port group profile name from the drop down list. The attributes of the selected port group profile will apply to this port group.
Profile Description	The description of the port group profile selected in the previous field is displayed here.

3. Click **Next**

The Port Group: Failover Order property sheet is displayed, as shown in Figure 12 on page 25.

Figure 12: Port Group Failover Order

4. In the Port Group: Failover Order property sheet, enter the required information as explained in

Field	Description
-------	-------------

Active Uplinks	List the uplink ports assigned to this port group, which are to be used when the connectivity is up and active
Standby Uplinks	List the uplink ports that are assigned to this port group, on failure of one of the active adapter's connectivity. Select the uplink ports from the list and use the Move Up and Move Down buttons to prioritize the ports in the list.
Unused Uplinks	List the uplink ports that will not be assigned to this port group.

5. Click Create

Related Documentation

- Port Groups Overview on page 21
- Viewing Port Group Details on page 22
- Modifying Port Groups on page 26
- Deleting Port Groups on page 26

Modifying Port Groups

Junos Space Virtual Control enables you to modify port group parameters for existing port groups according to your requirements.

To modify port group parameters:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage Virtual Switch > Manage Port Groups**.
2. Select the required port group and click **Modify Port Group** in the **Action** panel. The Port Group: General Settings property sheet is displayed. See “Creating Port Groups” on page 23 for an explanation of the parameters in the Port Group General Settings property sheet. Besides Port Group Name and Virtual Switch Name, all of the other fields can be modified as required.
3. When you have entered your modifications in both of the property sheets, click **Modify**.

Related Documentation

- Port Groups Overview on page 21
- Creating Port Groups on page 23
- Viewing Port Group Details on page 22
- Deleting Port Groups on page 26

Deleting Port Groups

Junos Space Virtual Control enables you to delete port groups that are no longer in use or required.

To delete one or more such port groups:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage Virtual Switch > Manage Port Group**.

2. Select the required port group(s) and click **Delete Port Groups** in the **Action** panel.



NOTE: Only port groups that are not associated can be deleted.

3. Click **Continue** to confirm the deletion of the selected port groups.

The port group is deleted.

**Related
Documentation**

- Port Groups Overview on page 21
- Creating Port Groups on page 23
- Viewing Port Group Details on page 22
- Modifying Port Groups on page 26

CHAPTER 5

Manage Host

- Viewing the Host Inventory on page 29
- Viewing Host Component Details on page 30
- Managing Uplink Ports on page 31

Viewing the Host Inventory

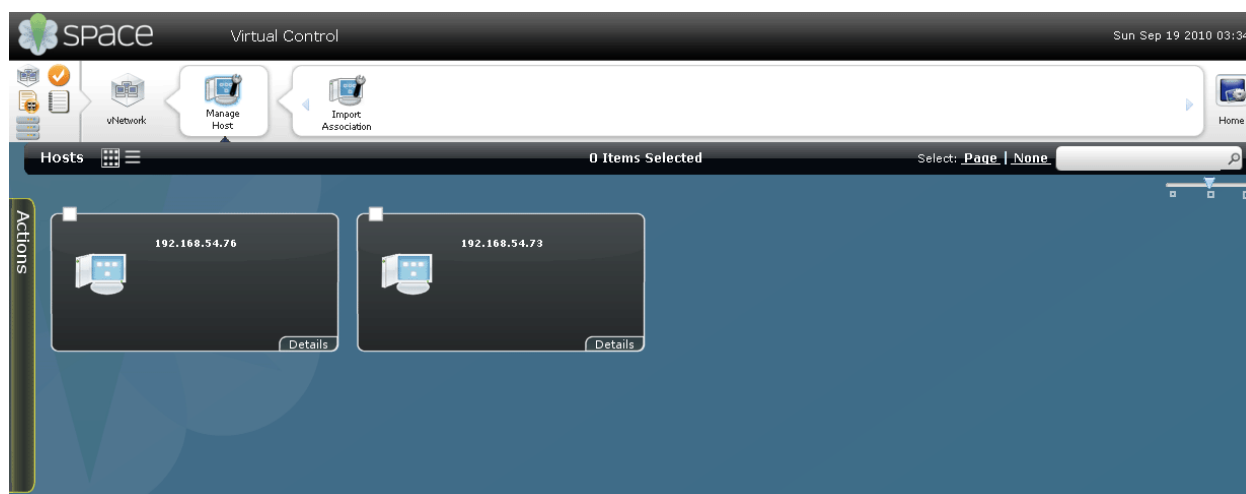
The inventory for hosts lists the virtual machines on a host and the physical NICs that serve the virtual infrastructure.

The Host view lists all of the hosts in the infrastructure. For each host, the detailed inventory provides information on the name of the vNetwork it belongs to, the port number, MAC Address and virtual switch for each virtual machine in the host.

To view the Host inventory:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage Host**.
A thumbnail view of the Host inventory is displayed as shown in Figure 13 on page 29.

Figure 13: The Hosts thumbnail view



2. Click the tabular view icon to display a tabular view of the host inventory details.

The tabular view of the host inventory details is displayed, as shown in Figure 14 on page 30. This view lists the Host by name, and lists the Number of Physical NICs, Number of Virtual machines, and the vNetwork Name against each host in the network.

Figure 14: The Hosts tabular view

Host Name	Number of Physical NICs	Number of Virtual Machines	vNetwork Name
192.168.54.76	2	2	vCenterServer1
192.168.54.73	3	1	vCenterServer1

While in thumbnail view, to view summary information for hosts, drag the zoom slider to the right. The summary information (similar to the information displayed in the tabular format) appears in the main display area.

Related Documentation

- Viewing Host Component Details on page 30

Viewing Host Component Details

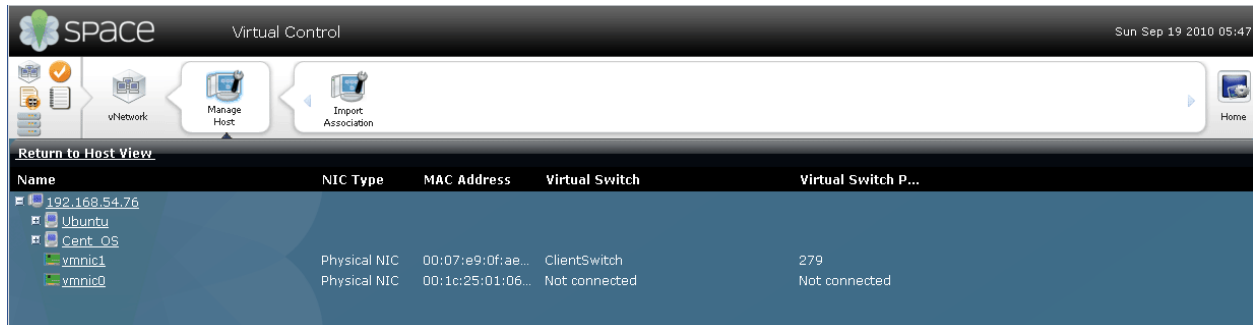
While in the host inventory thumbnail view, to view summary information for hosts, drag the zoom slider to the right. The summary information (similar to the information displayed in the tabular format) appears in the main display area.



To view the details of network components on a host:

1. While in the host inventory thumbnail view, select the required host(s) and click **View Inventory** in the **Action** drawer.

A detailed tabbed view of the components on the host is displayed, as shown in Figure 15 on page 31.

Figure 15: Hosts Inventory view



Field	Explanation
	Indicating that the row of details pertains to a host/VM
	Indicating that the row of details pertains to a physical NIC
Name	The name assigned to the Host/Virtual Machine.
NIC Type	One of the following: <ul style="list-style-type: none"> • Physical • Virtual
MAC Address	MAC address assigned to the virtual NIC to which the VM connects.
Virtual Switch	Virtual Switch to which the Virtual Machine connects.
Virtual Switch Port	Port in the virtual switch serving VM -related traffic.

Related Documentation

- Viewing the Host Inventory on page 29

Managing Uplink Ports

You need to group uplink ports just as you would group virtual ports. You need to have at least one NIC port each hosts to support vMotion. It is normally recommended to have two physical NICs from each Host as part of an Uplink Port Group.



NOTE: If a host is not included in an Uplink Port Group of a VDS, Virtual Machines cannot be migrated to or from this host.

Junos Space Virtual Control application displays the Uplink Ports and the parameters that define the connectivity of the uplink port to the physical switch port.

To view the current configuration:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage Host**.
2. Select the required host(s) and click **View Physical Switch Association** in the **Actions** drawer, or the right-click context menu.

A tabbed view of Physical Switch Association information for the selected host is displayed, as shown in Figure 16 on page 32.

Figure 16: Physical Switch Association Details for the Selected Host

Host Name	Uplink MAC Address	NIC Name	Virtual Switch	Virtual Switch Port	External Switch	External Interface
192.168.54.76	00:07:e9:0f:ae:8d	vmmic1	ClientSwitch	279	EX4200	ge-0/0/12
192.168.54.76	00:1c:25:01:06:6f	vmmic0	Not connected	Not connected	Not connected	Not connected

Table 9 on page 32 describes the fields displayed in the tabbed view.

Table 9: Physical Switch Association Details

Fields	Description
Host Name	Name/IP of the host
Uplink MAC Address	Unique identifier assigned to the virtual NIC to which the VM connects
Virtual Switch	Name of the virtual switch
Virtual Switch Ports	ID of the virtual port on the above virtual switch
External Switch	Name of the physical switch
External Switch Ports	ID of the port on the above switch

When you manually connect the uplink ports on a virtual switch with physical switches, you need to create an association between the two.

To create or modify an association between physical and virtual switch ports:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage Host**.
2. Select the required host(s) and click **Associate Physical Switch Ports** in the **Actions** drawer.
3. Edit the configuration using one of the following methods:
 - Double-click on any entry in that row.
 - Click the edit icon at the beginning (left) of the row.
4. Select the required External Switch name from the drop down box.
5. Select the required External Switch ports from the drop down box.
6. Click **Update** to apply the configuration parameters.

These parameters are validated by Junos Space Virtual Control, and validation errors are displayed.

**Related
Documentation**

- Viewing the Host Inventory on page 29
- Viewing Host Component Details on page 30

CHAPTER 6

Manage vNetwork

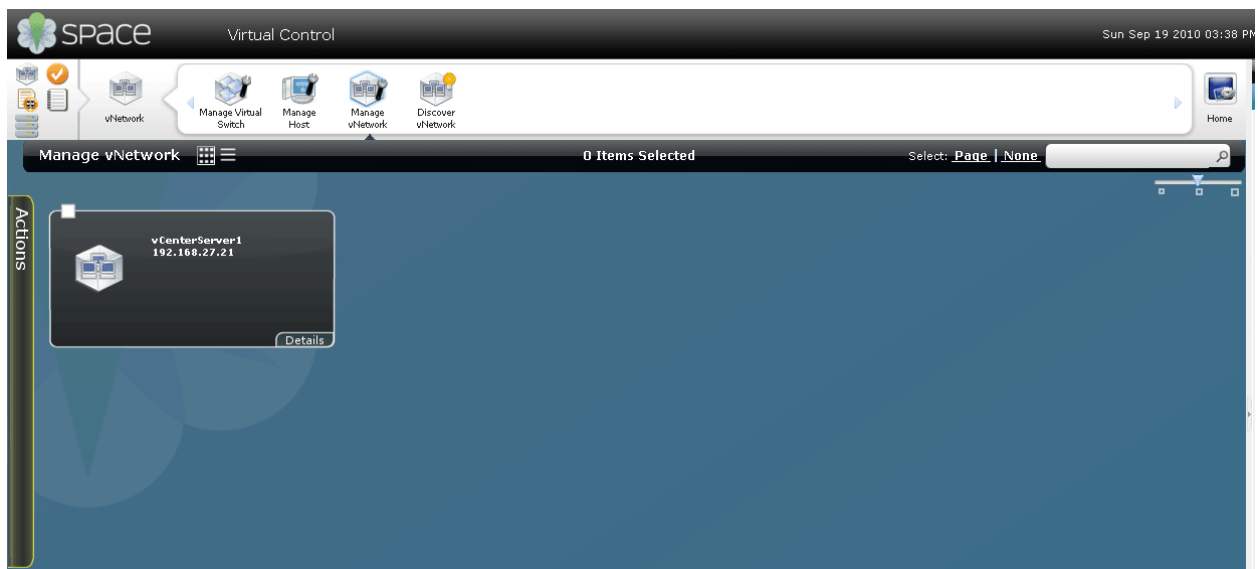
- Manage vNetwork Overview on page 35
- Viewing Notifications on page 37
- Purging Event Logs on page 38
- Managing vNetworks on page 39
- Orchestrating vNetworks on page 44
- Auditing vNetwork Configurations on page 48

Manage vNetwork Overview

Junos Space Virtual Control displays all of the VMWare vCenter servers (vNetwork) managed by the application. Based on information received from the VMWare vCenter server, the inventory views for each VMWare vCenter server presents a detailed list of all of the elements in the VMWare vCenter server. This includes all of the hosts and all of the virtual machines configured on each host, along with their key parameters such as MAC addresses, names of the virtual switches, and port numbers.

Figure 17 on page 36 shows the thumbnail view of the **Manage vNetwork** page.

Figure 17: Manage vNetwork page



You can perform the following tasks from the **Manage vNetwork** page:

- Viewing the vNetwork inventory.
- Modifying vNetworks.
- Deleting vNetworks.
- Re-synchronizing vNetworks
- Configuring orchestration modes.
- Viewing event details.
- Auditing vNetwork configuration.
- Viewing virtual and physical switch audit report.
- Configuring event purging.

Related Documentation

- Viewing the vNetwork Inventory on page 39
- Viewing Notifications on page 37
- Adding vNetwork Credentials on page 40
- Re-synchronizing vNetworks on page 43
- Modifying vNetwork Credentials on page 41
- Deleting vNetworks on page 42
- Orchestration Overview on page 44
- Setting Orchestration Configuration Mode on page 46
- Configuration Audit Overview on page 48
- Initiating a Configuration Audit on page 48

- Viewing Audit Reports on page 49
- Purging Event Logs on page 38

Viewing Notifications

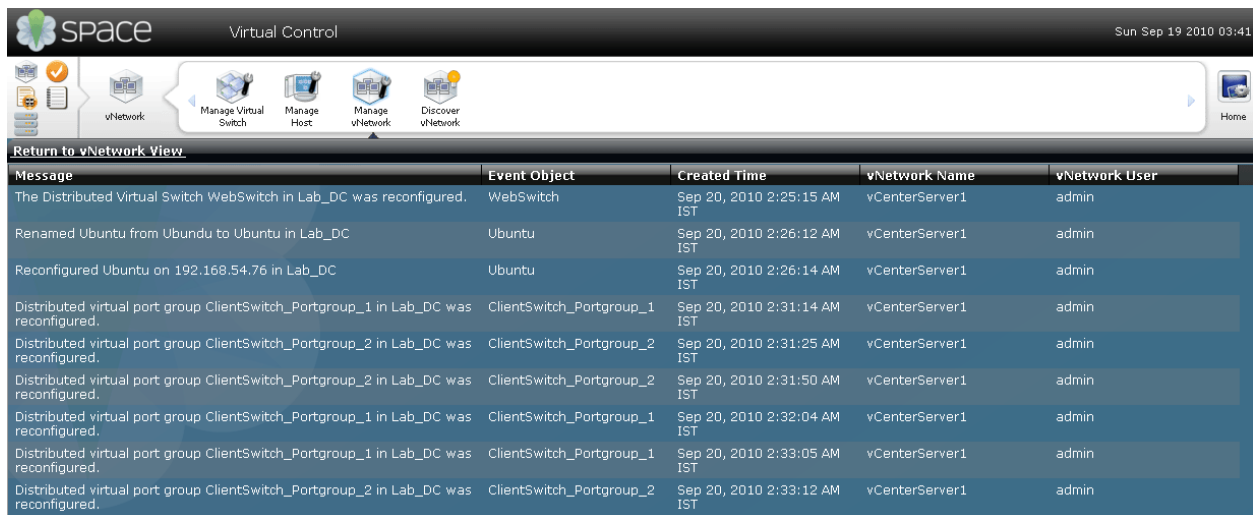
Junos Space Virtual Control works with the VMWare vCenter server to receive regular updates and notification about configuration information.

To view the notifications received:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork** > **Manage vNetwork**.
2. Select the required virtual network(s) and from the **Actions** drawer, or the right-click context menu, click **View Event Details**.

The **Event Details** page is displayed, as shown in Figure 18 on page 37

Figure 18: The Event Details Page



Message	Event Object	Created Time	vNetwork Name	vNetwork User
The Distributed Virtual Switch WebSwitch in Lab_DC was reconfigured.	WebSwitch	Sep 20, 2010 2:25:15 AM IST	vCenterServer1	admin
Renamed Ubuntu from Ubuntu to Ubuntu in Lab_DC	Ubuntu	Sep 20, 2010 2:26:12 AM IST	vCenterServer1	admin
Reconfigured Ubuntu on 192.168.54.76 in Lab_DC	Ubuntu	Sep 20, 2010 2:26:14 AM IST	vCenterServer1	admin
Distributed virtual port group ClientSwitch_Portgroup_1 in Lab_DC was reconfigured.	ClientSwitch_Portgroup_1	Sep 20, 2010 2:31:14 AM IST	vCenterServer1	admin
Distributed virtual port group ClientSwitch_Portgroup_2 in Lab_DC was reconfigured.	ClientSwitch_Portgroup_2	Sep 20, 2010 2:31:25 AM IST	vCenterServer1	admin
Distributed virtual port group ClientSwitch_Portgroup_2 in Lab_DC was reconfigured.	ClientSwitch_Portgroup_2	Sep 20, 2010 2:31:50 AM IST	vCenterServer1	admin
Distributed virtual port group ClientSwitch_Portgroup_1 in Lab_DC was reconfigured.	ClientSwitch_Portgroup_1	Sep 20, 2010 2:32:04 AM IST	vCenterServer1	admin
Distributed virtual port group ClientSwitch_Portgroup_1 in Lab_DC was reconfigured.	ClientSwitch_Portgroup_1	Sep 20, 2010 2:33:05 AM IST	vCenterServer1	admin
Distributed virtual port group ClientSwitch_Portgroup_2 in Lab_DC was reconfigured.	ClientSwitch_Portgroup_2	Sep 20, 2010 2:33:12 AM IST	vCenterServer1	admin

The information displayed in the **Event Details** page is explained in Table 10 on page 37.

Table 10: Event Details Information

Fields	Description
Message	Message notified by the VMWare vCenter server.
Event Object	The ID/name of the object in focus.
Created Time	Time of the event.
vNetwork Name	Name of the vNetwork that the object belongs to.
vNetwork User	User name.

- Related Documentation**
- Purging Event Logs on page 38

Purging Event Logs

The records held in the event log are purged periodically. You can schedule the purging of event logs based on the number of records in the logs, or a time frame.

To schedule the purging of event logs:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage vNetwork**.
2. Select the required virtual network(s) and from the **Action** panel, or the right-click context menu, click **Purge Configuration**.
The **Configure Event Purging** dialog box pops up as shown in Figure 19 on page 38.

Figure 19: Configure Event Purging Dialog Box

3. In the **Configure Event Purging** dialog box, enter the required information according to the explanation given in Table 11 on page 38.

Table 11: Configure Event Purging Parameters

Fields	Entry
Days	Select this option to schedule an event log purge based on a time frame
Purge entries older than ___ days	Specify the number of days for which the event records are to be maintained. Records older than the specified age will be periodically purged.
Records	Select this option to schedule an event log purge based on the number of records in the log.

Table 11: Configure Event Purging Parameters (*continued*)

Fields	Entry
Purge oldest entries	Enter the number of records to be purged. This schedule follows a FIFO purge sequence.
Purge immediately	Select this option to override the existing configuration and purge immediately.

Related Documentation

- Viewing Notifications on page 37

Managing vNetworks

- Viewing the vNetwork Inventory on page 39
- Adding vNetwork Credentials on page 40
- Modifying vNetwork Credentials on page 41
- Deleting vNetworks on page 42
- Re-synchronizing vNetworks on page 43

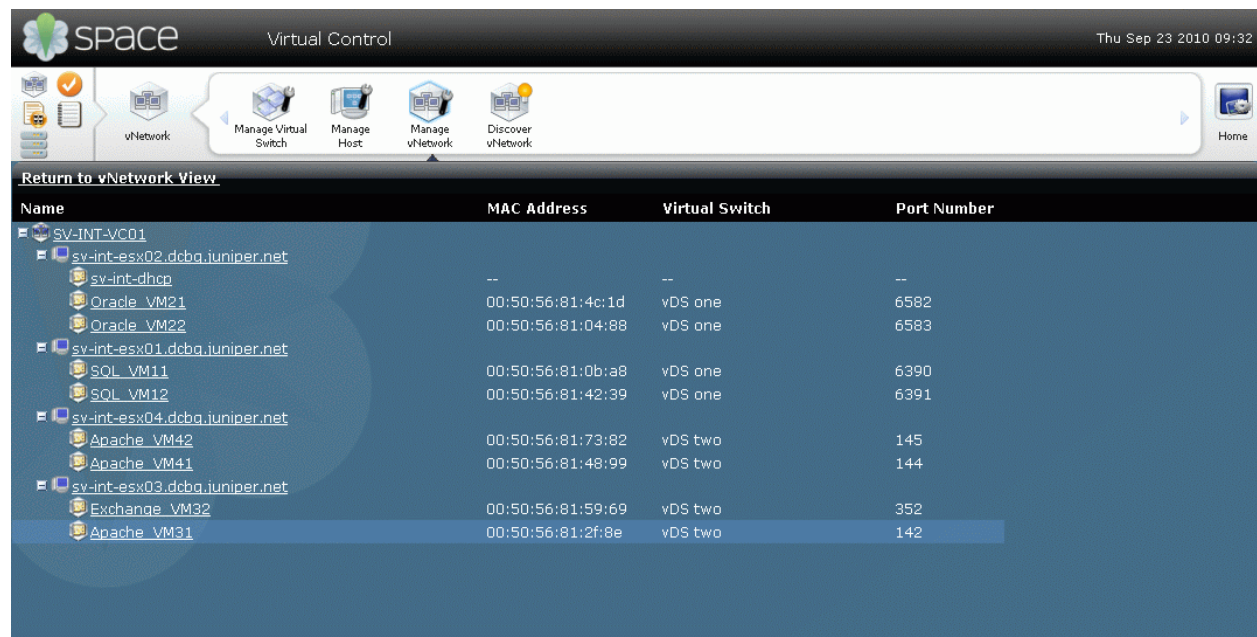
Viewing the vNetwork Inventory

The components of any of the listed virtual networks can be viewed in one of the following ways:

- Right click on the required virtual network and click **View vNetwork Inventory**.
- Select the required vNetwork(s) and click **View vNetwork Inventory** in the **Action** panel.

The vNetwork Inventory view is displayed, as shown in Figure 20 on page 40.

Figure 20: The vNetwork Inventory page



The vNetwork Inventory page displays information about the elements in the selected vNetwork, as explained in Table 12 on page 40.

Table 12: vNetwork Inventory Page field Descriptions

Field	Description
Name	Name assigned to the virtual network or the component described i.e. Host or Virtual Machine
MAC Address	Unique identifier assigned to the virtual NIC to which the VM connects.
Virtual Switch	Virtual Switch to which the Virtual Machine connects to.
Port Number	Port in the virtual switch serving the VM related traffic.

Related Documentation

- Manage vNetwork Overview on page 35
- Adding vNetwork Credentials on page 40
- Re-synchronizing vNetworks on page 43
- Modifying vNetwork Credentials on page 41

Adding vNetwork Credentials

You need to add a vNetwork to Junos Space Virtual Control to be able to manage it using the application. This involves assigning a set of credentials to the vNetwork.

To add a vNetwork to Junos Space Virtual Control:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Discover vNetwork > Add vNetwork Credentials**. The **Add vNetwork Credentials** dialog box is displayed, as shown in Figure 21 on page 41.

Figure 21: Add vNetwork Credentials dialog box

2. In the **Add vNetwork Credentials** dialog box, enter the credentials for the vNetwork as explained in Table 13 on page 41.
3. Click **Discover** to proceed with the process of discovering the new virtual network. On successful discovery the VMWare vCenter server is added to Junos Space Virtual Control.

Table 13: Add vNetwork Credentials dialog box field description

Field	Description
Host Name/IP	The name of the host machine (or its IP address) to be used as the VMWare vCenter server.
Port	The port used for connection. Default value is set as 443
User Name	The user name to be used to connect to the VMWare vCenter server.
Password	The password to be used with the name provided in the previous field.
Confirm Password	Repeat the password provided in the previous field, to confirm.

- Related Documentation**
- Manage vNetwork Overview on page 35
 - Viewing Notifications on page 37
 - Deleting vNetworks on page 42
 - Re-synchronizing vNetworks on page 43

Modifying vNetwork Credentials

You can change some of the credentials for an existing vNetwork.

To modify credentials for a vNetwork:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage vNetwork**.
2. Select the required vNetwork(s) and from the **Action** panel, or the right-click context menu, click **Modify vNetwork**. The **Modify vNetwork Credentials** dialog box is displayed, with the same fields as the Add vNetwork pop-up, shown in Figure 22 on page 42.

Figure 22: Modify vNetwork Dialog Box

3. In the **Modify vNetwork Credentials** dialog box, you can modify the port information, the username and password.
4. Click **Modify**, to submit the modification.

Related Documentation

- Manage vNetwork Overview on page 35
- Adding vNetwork Credentials on page 40
- Re-synchronizing vNetworks on page 43
- Deleting vNetworks on page 42

Deleting vNetworks

You can dissociate a vNetwork from Junos Space Virtual Control by deleting it in the system.

To delete a vNetwork:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage vNetwork**.
2. Select the required vNetwork(s) and from the **Action** panel, or the right-click context menu, click **Delete vNetwork**.
The **Delete vNetwork** dialog box is displayed, with the name of the selected vNetwork(s) listed.
3. In the **Delete vNetwork** dialog box, click **Confirm**, to delete the vNetwork from Junos Space Virtual Control.

- Related Documentation**
- Manage vNetwork Overview on page 35
 - Adding vNetwork Credentials on page 40

Re-synchronizing vNetworks

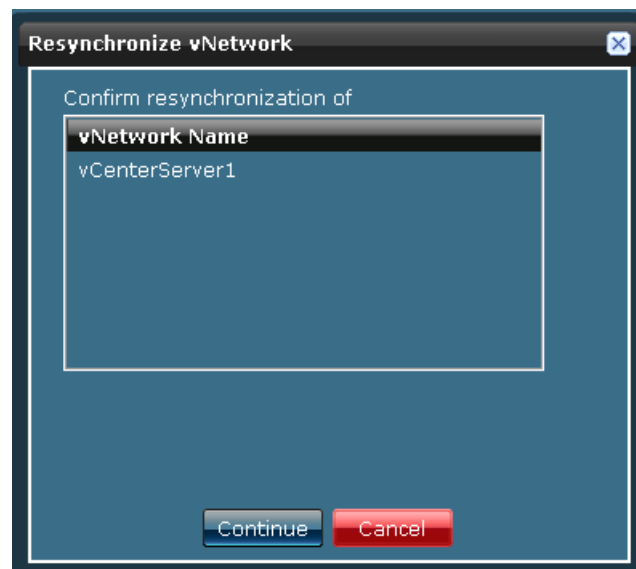
You can re-synchronize vNetworks registered with Junos Space Virtual Control. Synchronization is run as a job, and is managed by the Job Manager in Junos Space.

To initiate re-synchronizing vNetworks:

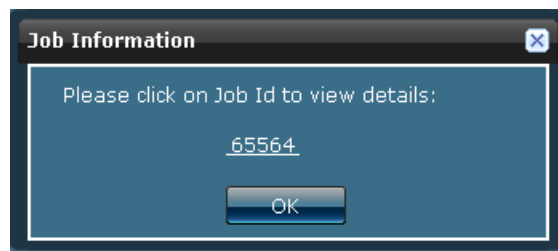
1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage vNetwork**.
2. Select the required vNetwork(s) and from the **Action** panel, or the right-click context menu, click **re-synchronize with vNetwork**.

The **re-synchronize vNetwork** dialog box is displayed, with the name of the selected vNetwork displayed, as shown in Figure 23 on page 43.

Figure 23: re-synchronize vNetwork Dialog Box



3. In the **re-synchronize vNetwork** dialog box, click **Continue**. The **Job Information** dialog box is displayed as shown in Figure 24 on page 44.

Figure 24: Job Information Dialog Box

4. In the **Job Information** dialog box, click the job ID link. The **Job Details** page displays details about the re-synchronization job.

Related Documentation

- Manage vNetwork Overview on page 35
- Adding vNetwork Credentials on page 40
- Modifying vNetwork Credentials on page 41

Orchestrating vNetworks

- Orchestration Overview on page 44
- Physical Switch Configuration on page 45
- Setting Orchestration Configuration Mode on page 46
- Importing Switch/Port Associations on page 46

Orchestration Overview

Junos Space Virtual Control seamlessly orchestrates across physical and virtual network elements. Orchestration applies aggregated VLAN configurations of the required port group profiles to the appropriate port(s) of the physical switch.

Each virtual switch can span multiple hosts, and is configured to have a minimum of one uplink port per host. While port groups are assigned to single virtual switches, the ports associated with the port group can be configured to the different hosts that share this virtual switch.

Each Physical NIC in a host is connected to an access port in the EX switch. Any configuration or restrictions to be applied to the physical NIC in order to manage traffic, is applied to the access port of the EX switch.

Related Documentation

- Physical Switch Configuration on page 45
- Setting Orchestration Configuration Mode on page 46
- Importing Switch/Port Associations on page 46

Physical Switch Configuration

VMWare vSphere components such as Distributed Resource Scheduler (DRS), High Availability (HA), Fault Tolerance, and Network vMotion manage automatic migration of VMs across hosts based on the strategy configured by the server administrator.

The migration of VMs triggered by any of these four components, have a direct impact on the networking infrastructure. You need to update virtual port configurations to ensure un-interrupted application traffic for the applications running on the virtual machines.

In order to achieve uninterrupted traffic, Junos Space Virtual Control ensures that the configuration of the networking infrastructure (vDS and physical switches) is in line with the latest location of the virtual machine.

The EX4200 physical switch is configured based on the modes, listed below as chosen by the Administrator:

- None
- Strict
- Very Strict

None

The physical switch is not configured if the orchestration mode is set to None.

Strict

In Strict mode, the ports limit the set of VLAN metrics to those currently required for the port group profiles configured in the virtual machines. All of the access ports of the physical switch will, however, be configured with the same configuration. This ensures that the configuration need not be changed during VM Migration.

This mode offers better traffic control as it allows only the traffic related to the virtual machines to pass through. When a new VM is added (or) when one of the port group profiles of the VDS is changed, the configuration for all these physical switch ports will be automatically updated by JSVC.

Very Strict

This is the most secure mode. In this mode, Junos Space Virtual Control maintains a track of the VMs using the EX port for its data traffic and configure the ports to only allow traffic related to the VMs using this EX port.

All of the access ports of a virtual switch from a single host have the same configuration. This prevents the traffic configured for VMs on other hosts from entering this hosts. In this mode, the EX ports will be re-configured by JSVC during a VM Migration, new VM Addition, Change in Port Group Profile configuration etc.

Junos Space Virtual Control adds value to the entire operation of configuring virtual switches with external switches by enabling efficient and automatic configuration of physical switches like the EX4200. When a VM migrates from one host to another, you need to configure the ports of the physical EX appropriately, to offer uninterrupted traffic.

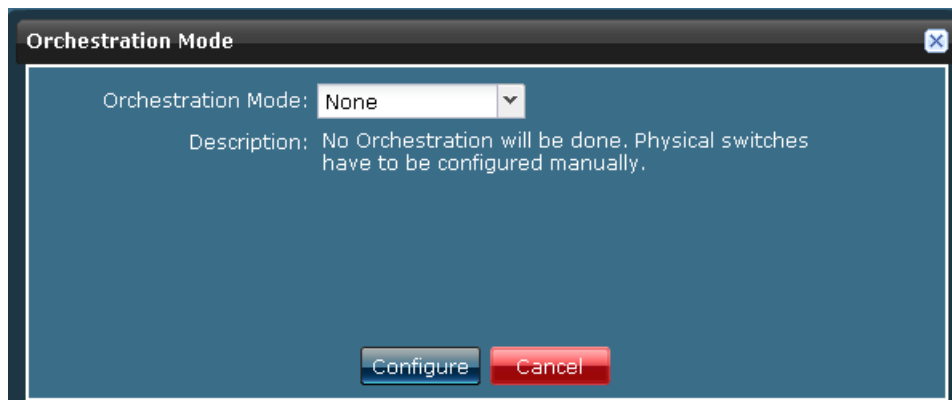
- Related Documentation**
- [Orchestration Overview on page 44](#)
 - [Setting Orchestration Configuration Mode on page 46](#)
 - [Importing Switch/Port Associations on page 46](#)

Setting Orchestration Configuration Mode

To set the orchestration mode operable on the host:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage vNetwork**.
2. Select the required host(s) and click **Configure Orchestration Mode** in the **Actions** panel. The **Orchestration Mode** dialog box is displayed, as shown in Figure 25 on page 46.

Figure 25: Orchestration Mode Dialog Box



3. In the **Orchestration Mode** dialog box, select the Orchestration Mode from among None, Strict and Very Strict.
4. Click **Configure**.

- Related Documentation**
- [Orchestration Overview on page 44](#)
 - [Physical Switch Configuration on page 45](#)
 - [Importing Switch/Port Associations on page 46](#)

Importing Switch/Port Associations

Besides explicitly setting up associations for individual switches/ports, Junos Space Virtual Control enables you to create physical port association en bloc. You can do this by importing the switch port association information in a CSV file.

The data in the file is validated against the existing environment, and only those settings that are feasible are applied.

To import switch/port association information:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage Host > Import Association**.

The **Import** dialog box pops up as shown in Figure 26 on page 47.

Figure 26: Import Associations Dialog Box

Host Name	NIC Name	External Switch	External Interface
192.168.54.74	vmnic3	192.168.27.20	ge-0/0/2
192.168.54.74	vmnic0	192.168.27.20	ge-0/0/0
192.168.54.74	vmnic2	192.168.27.20	ge-0/0/1

View Sample CSV Upload CSV Configure Cancel

2. Click **Upload CSV** to locate the required file and upload it to the system.

The valid records in the CSV file are displayed, as listed in Table 14 on page 47.

Table 14: Fields in the CSV Association File

Fields	Meaning
Host Name	Name of the host
PNIC Name	Name of the physical NIC
External Switch	Name of the External Switch
External Interface	Name of the port on the External Switch

3. To proceed with the bulk association, click **Configure**.

- Related Documentation**
- [Orchestration Overview on page 44](#)
 - [Setting Orchestration Configuration Mode on page 46](#)
 - [Physical Switch Configuration on page 45](#)

Auditing vNetwork Configurations

- [Configuration Audit Overview on page 48](#)
- [Initiating a Configuration Audit on page 48](#)
- [Viewing Audit Reports on page 49](#)

Configuration Audit Overview

A Configuration Audit analyzes the virtual network environment and summarizes the audit results in a report. The audits uncover any existing mismatch or conflict between the virtual and physical infrastructure in the vNetwork. The auditing process analyzes the configuration of the access ports on the Juniper Networks EX Series Ethernet Switch to which the hosts are connected, and uplink ports of the virtual switches.

Configuration audits can be scheduled as jobs using the Job Manager in Junos Space. Audits can be scheduled to either follow periodic synchronization jobs, or be initiated manually.

The outcome of the audit is available as two reports:

- Virtual switch audit report
- Physical switch audit report

- Related Documentation**
- [Initiating a Configuration Audit on page 48](#)
 - [Viewing Audit Reports on page 49](#)
 - [Purging Event Logs on page 38](#)

Initiating a Configuration Audit

To manually initiate a Configuration Audit:

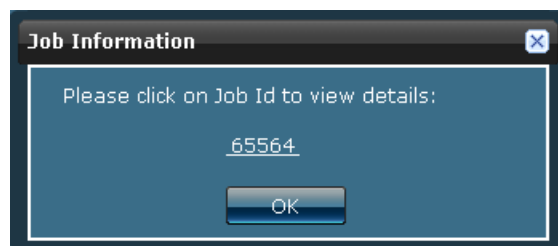
1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage vNetwork**.
2. Select the required virtual network(s) and from the **Action** panel, or the right-click context menu, click **Audit vNetwork Configuration**.
The Configuration Audit dialog box pops up as shown in Figure 27 on page 49.

Figure 27: Configuration Audit Dialog Box



3. Click **Continue** to proceed with the audit process.
4. The **Job Information** dialog box appears displaying the job ID, as shown in Figure 28 on page 49.
To view the details of the job, click the job ID link.

Figure 28: Job Information Dialog Box



- Related Documentation**
- Configuration Audit Overview on page 48
 - Viewing Audit Reports on page 49
 - Purging Event Logs on page 38

Viewing Audit Reports

Configuration Audit Reports list the compatibility between the physical and virtual network infrastructure. It reports the feasibility for the flow of traffic from and to the virtual machines through:

- Access ports of the EX Series switch to which the hosts are connected.

- Uplink ports of the virtual switches.
- Viewing Audit Reports for Virtual Switches on page 50
- Viewing Audit Reports for Physical Switches on page 51

Viewing Audit Reports for Virtual Switches

The audit report for virtual switches shows status information about the uplink ports configured for the hosts in the selected vNetwork.

To view the audit report for a virtual switch:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage vNetwork**.
2. Select the required virtual network(s) and from the **Action** panel, or the right-click context menu, click **View Virtual Switch Audit Report**.
The audit report for the selected virtual switch is displayed, as shown in Figure 29 on page 50.

Figure 29: Virtual Switch Audit Report

Virtual Switch Name	Uplink Port Group Name	Host Name	PNIC Name	Created Time	Current VM Traffic	VM Migration	New Port Group	Remarks
ClientSwitch	ClientSwitch-DVUplinks-7726	192.168.54.76	vmnic1	Sep 21, 2010 1:00:07 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
WebSwitch	WebSwitch-DVUplinks-7849	192.168.54.73	vmnic0	Sep 21, 2010 1:00:07 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
WebSwitch	WebSwitch-DVUplinks-7849	192.168.54.73	vmnic1	Sep 21, 2010 1:00:07 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
ClientSwitch	ClientSwitch-DVUplinks-7726	192.168.54.76	vmnic1	Sep 21, 2010 1:00:02 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
WebSwitch	WebSwitch-DVUplinks-7849	192.168.54.73	vmnic0	Sep 21, 2010 1:00:02 AM IST	Ready	Ready	Ready	Current configuration will allow uninterrupted VM traffic after migration of VMs across hosts and also after addition of new VMs.
WebSwitch	WebSwitch-DVUplinks-7849	192.168.54.73	vmnic1	Sep 21, 2010 1:00:02 AM IST	Ready	Ready	Ready	Current configuration will allow uninterrupted VM traffic after migration of VMs across hosts and also after addition of new VMs.
ClientSwitch	ClientSwitch-DVUplinks-7726	192.168.54.76	vmnic1	Sep 21, 2010 12:57:53 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
WebSwitch	WebSwitch-DVUplinks-7849	192.168.54.73	vmnic0	Sep 21, 2010 12:57:53 AM IST	Ready	Ready	Ready	Current configuration will allow uninterrupted VM traffic after migration of VMs across hosts and also after addition of new VMs.
WebSwitch	WebSwitch-DVUplinks-7849	192.168.54.73	vmnic1	Sep 21, 2010 12:57:52 AM IST	Ready	Ready	Ready	Current configuration will allow uninterrupted VM traffic after migration of VMs across hosts and also after addition of new VMs.
ClientSwitch	ClientSwitch-DVUplinks-7726	192.168.54.76	vmnic1	Sep 21, 2010 12:57:09 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.

The information displayed in the virtual switch audit report is explained in Table 15 on page 51.

Table 15: Information in the Virtual Switch Audit Report

Fields	Description
Virtual Switch Name	Name of the virtual switch whose ports are being audited.
Uplink Port Group Name	Name of the port group configured to the uplink port being audited.
Host Name	Name of the host to which this uplink port belongs.
PNIC Name	Name of the Physical NIC on the uplink port.
Created Time	Time when this report was created.
Current VM Traffic	Values are: <ul style="list-style-type: none"> • Ready • Not Ready
VM Migration	Values are: <ul style="list-style-type: none"> • Ready • Not Ready
New Port Group	Values are: <ul style="list-style-type: none"> • Ready • Not Ready
Remarks	Comprehensive summary on the status of traffic through this uplink port, based on the current VLAN configuration.

Viewing Audit Reports for Physical Switches

The audit report for physical switches shows status information about the access ports configured on the EX Series switch.

To view the audit report for physical switches:

1. From the Junos Space Virtual Control task ribbon, select **vNetwork > Manage vNetwork**.
2. Select the required virtual network(s) and from the **Action** panel, or the right-click context menu, click **View Physical Switch Audit Report**.
The physical switch audit report is displayed, as shown in Figure 30 on page 52.

Figure 30: Physical Switch Audit Report

Ex Switch Name	Interface Name	Created Time	Current VM Traffic	VM Migration	New Port Group	Remarks
EX4200	ge-0/0/3	Sep 21, 2010 12:57:53 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/5	Sep 21, 2010 12:57:53 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/2	Sep 21, 2010 12:57:53 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/3	Sep 21, 2010 12:57:09 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/5	Sep 21, 2010 12:57:09 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/2	Sep 21, 2010 12:57:09 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/3	Sep 21, 2010 12:57:03 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/5	Sep 21, 2010 12:57:03 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/2	Sep 21, 2010 12:57:03 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/3	Sep 21, 2010 12:56:43 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/5	Sep 21, 2010 12:56:43 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/2	Sep 21, 2010 12:56:42 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/3	Sep 21, 2010 12:56:38 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/5	Sep 21, 2010 12:56:37 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/2	Sep 21, 2010 12:56:37 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/3	Sep 21, 2010 12:55:45 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.
EX4200	ge-0/0/5	Sep 21, 2010 12:55:45 AM IST	Ready	Not Ready	Not Ready	Current configuration permits uninterrupted VM traffic only for currently hosted VMs.

The information displayed in the physical switch audit report is explained in Table 16 on page 52.

Table 16: Information in the Physical Switch Audit Report

Fields	Description
Ex Switch Name	Name of the external EX switch.
Interface Name	Name of the interface.
Created Time	Time when this report was created.
Current VM Traffic	Values are: <ul style="list-style-type: none"> • Ready • Not Ready
VM Migration	Values are: <ul style="list-style-type: none"> • Ready • Not Ready

Table 16: Information in the Physical Switch Audit Report (*continued*)

Fields	Description
New Port Group	Values are: <ul style="list-style-type: none">• Ready• Not Ready
Remarks	Comprehensive summary on the status of traffic through this external switch, based on the current VLAN configuration. In case of failure, this summary lists the VM to/from which traffic cannot flow.

- Related Documentation**
- Configuration Audit Overview on page 48
 - Initiating a Configuration Audit on page 48
 - Purging Event Logs on page 38

CHAPTER 7

Discover vNetwork

- Discovering vNetworks on page 55

Discovering vNetworks

Junos Space Virtual Control discovers hosts, virtual machines, virtual switches, and port groups to provide a complete picture of the virtual infrastructure.

The vNetwork discovery process uncovers:

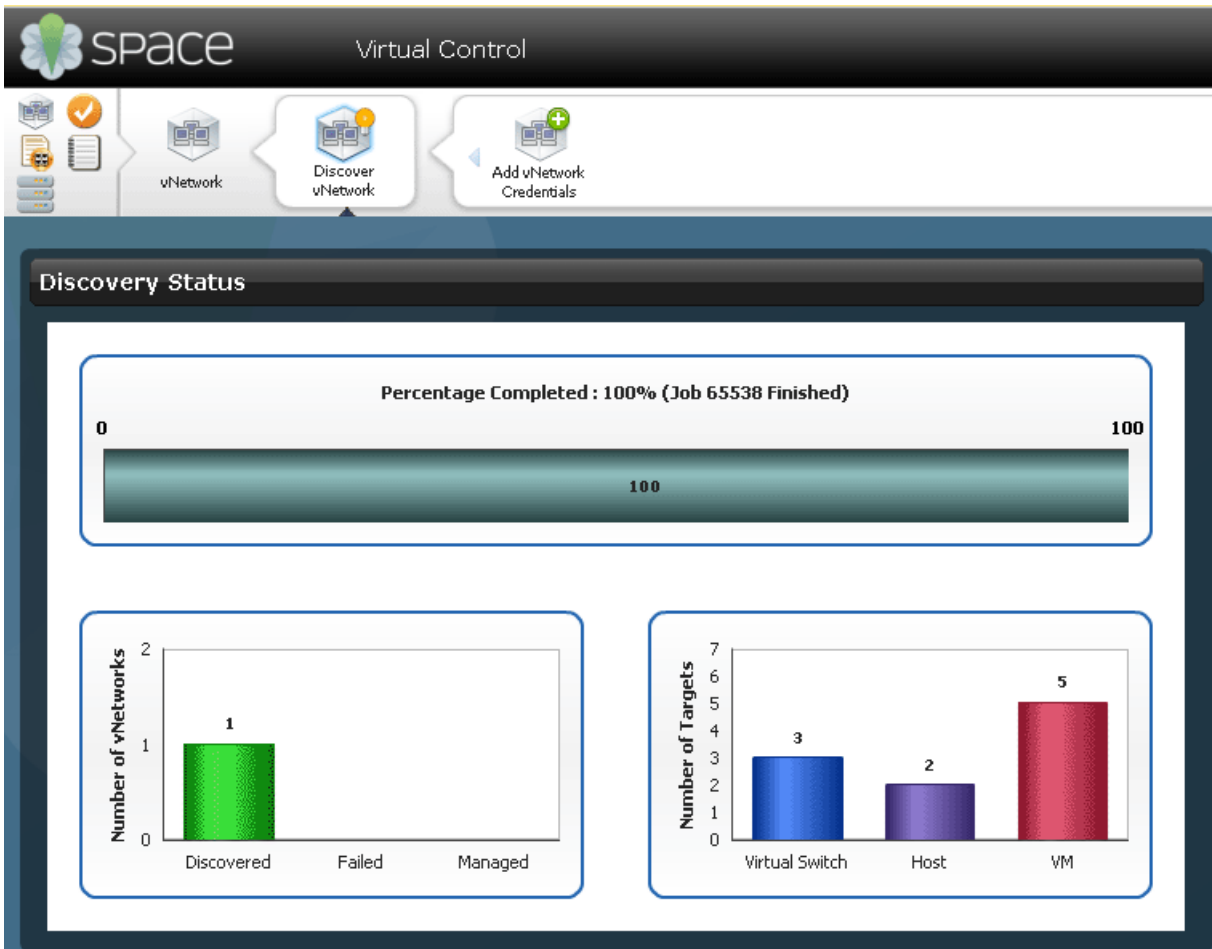
- Virtual switches and virtual machines connected to each virtual port of the virtual switch.
- Connectivity between virtual machines and the physical NIC in the host.

To view the vNetwork Discovery Status page:

- From the Junos Space Virtual Control task ribbon, select **vNetwork** > **Discover vNetwork**.

The **Discovery Status** information is displayed as shown in Figure 31 on page 56.

Figure 31: The vNetwork Discovery Status View



Related Documentation

- Manage vNetwork Overview on page 35
- Viewing Notifications on page 37
- Adding vNetwork Credentials on page 40
- Deleting vNetworks on page 42
- Re-synchronizing vNetworks on page 43

PART 3

Port Group Profiles

- Understanding Port Group Profiles on page 59
- Managing Port Group Profiles on page 63

CHAPTER 8

Understanding Port Group Profiles

- Port Group Profile Overview on page 59

Port Group Profile Overview

You need to configure ports on virtual and physical switches in order to regulate data packet traffic. Traffic regulation ensures security, a guaranteed rate of packet flow, and prevents unsolicited traffic. You can use port group profiles to set up parameters and then apply them to multiple port groups across different virtual switches.

Junos Space Virtual Control synchronizes the entire virtual network. This permits administrators to make changes in port group related parameters in the VMWare vCenter server or through Junos Space Virtual Control. You can create port group profiles by using Junos Space Virtual Control (JSVC), and you can configure port groups in a VMWare vCenter server. JSVC synchronizes the infrastructure with both of these kinds of profiles. The port groups you create in a VMWare vCenter server are called **Discovered profiles**, while those you create using JSVC are called “**user defined profiles**.”

JSVC uses a profile to enable ing of multiple port groups with the same set of parameters as defined by the profile. Port group profiles set rules for:

- Security
- Quality of Service
- Teaming and Failover policy that enables the port groups to share the load of traffic and/or provide a passive failover in event of failure.

You can edit port group profiles and apply them to ports across virtual switches to suit your requirements.

JSVC provides you with a workspace called **Port Group Profile** where you can create and manage port group profiles.

To get to the **Port Group Profile** workspace, select **Virtual Control** from the application switcher and click **Port Group Profile** in the **Virtual Control** task ribbon.

The **Port Group Profile** dashboard opens displaying the **Port Group Profile Statistics** and **Port Group Profile by Profile Type** dashboard gadgets.

From the task ribbon, click **Manage Port Group Profile**. This opens the **Manage Port Group Profile** page which displays the existing port group profiles. These profiles can be displayed in either the thumbnail view (Figure 32 on page 60) or tabular form (Figure 33 on page 60).

Figure 32: Manage Port Group Profile (Thumbnail view)

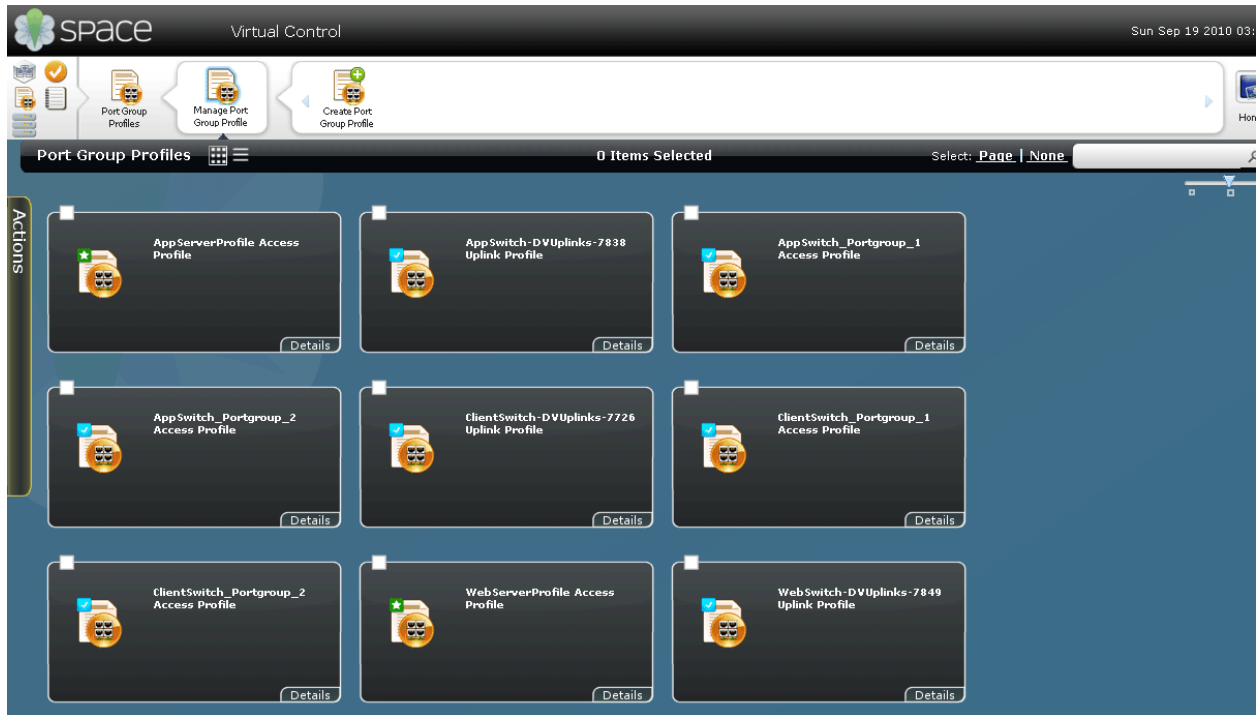


Figure 33: Manage Port Group Profile (Tabular view)

Name	Category	Type	Description	Number of Associated PortGroups
AppServerProfile	Access Profile	User Defined	App Server Profile	0
AppServerProfile_1	Access Profile	User Defined	App Server Profile	0
AppSwitch-DVUplinks-7838	Uplink Profile	Discovered	VMWare Generated Port Group Profiles.	1
AppSwitch_Portgroup_1	Access Profile	Discovered	VMWare Generated Port Group Profiles.	1
AppSwitch_Portgroup_2	Access Profile	Discovered	VMWare Generated Port Group Profiles.	1
ClientSwitch-DVUplinks-7726	Uplink Profile	Discovered	VMWare Generated Port Group Profiles.	1
ClientSwitch_Portgroup_1	Access Profile	Discovered	VMWare Generated Port Group Profiles.	1
ClientSwitch_Portgroup_2	Access Profile	Discovered	VMWare Generated Port Group Profiles.	1
WebServerProfile	Access Profile	User Defined	Web Server Profile	0
WebSwitch-DVUplinks-7849	Uplink Profile	Discovered	VMWare Generated Port Group Profiles.	1
WebSwitch_Portgroup_1	Access Profile	Discovered	VMWare Generated Port Group Profiles.	1
WebSwitch_Portgroup_2	Access Profile	Discovered	VMWare Generated Port Group Profiles.	1

Related Documentation

- Creating a Port Group Profile on page 64
- Viewing Associations on page 68
- Modifying a Port Group Profile on page 69
- Cloning a Port Group Profile on page 70

- Deleting a Port Group Profile on page 70

CHAPTER 9

Managing Port Group Profiles

- Creating a Port Group Profile on page 64
- Viewing Associations on page 68
- Modifying a Port Group Profile on page 69
- Cloning a Port Group Profile on page 70
- Deleting a Port Group Profile on page 70

Creating a Port Group Profile

To create a port group profile:

1. From the Junos Space Virtual Control task ribbon, select **Port Group Profiles > Manage Port Group Profile > Create Port Group Profile**.

The **Port Group Profile: General Settings** (Figure 34 on page 64) page appears.

Figure 34: Port Group Profile: General Settings

2. Enter the values in the fields as described in Table 17 on page 64.

Table 17: Port Group Profile: General Settings

Fields	Descriptions
General Settings	
Profile name	Enter the name of the profile.
Uplink profile	Select if you want to create the profile as an uplink port group profile. If you don't select this option, the profile is saved as an access profile.
Profile description	Enter a description of the port group profile.

Table 17: Port Group Profile: General Settings (*continued*)

Fields	Descriptions
Port Binding Type	<p>Select an option from the list.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Static binding: Assigns a fixed port ID to the virtual machine whenever it connects to a virtual port that exists in a port group associated with this profile. • Dynamic binding: Assigns a port ID to the virtual machine whenever it is first switched on after the virtual machine has connected to a virtual port. • Ephemeral: Does not assign any port ID to the virtual machine.
Security	
Mirroring Mode	Select an option from this list to enable or disable port mirroring.
MAC Address changes	<p>Select an option from the list.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Accept: Accepts requests to change the effective MAC address to an address other than the initial value set. • Reject: Denies requests to change the effective MAC address. This protects the host from any MAC address impersonation.
Forged Transmits	<p>Select an option from the list.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Accept: Stops the comparison of source and effective MAC addresses. • Reject: Allows the comparison of source and effective MAC addresses. This protects the host from any MAC address impersonation.
Block All Ports	Select this option to block all ports assigned to this profile.

3. Click **Next** to go to the next step in the create port group profile wizard.
The **Port Group Profile: Traffic Settings** page (Figure 35 on page 66) appears.

Figure 35: Port Group Profile: Traffic Settings

Port Group Profile: Traffic Settings

Ingress Traffic Shaping

Status: ☒ Enable

Average bandwidth (Kbits/sec): 100000

Peak bandwidth (Kbits/sec): 100000

Burst size (Kbytes): 102400

Egress Traffic Shaping

Status: ☒ Enable

Average bandwidth (Kbits/sec): 100000

Peak bandwidth (Kbits/sec): 100000

Burst size (Kbytes): 102400

◀ Back ▶ Next Create Cancel

4. Enter the values in the fields as described in Table 18 on page 66

Table 18: Port Group Profile: Traffic Settings

Fields	Descriptions
Ingress Traffic Shaping	
Status	Select this option to enable shaping of inbound traffic.
Average Bandwidth	Enter the average load permitted in Kbits/sec
Peak Bandwidth	Enter the maximum load (Kbits/sec) allowed across the port.
Burst Size	Enter the maximum kbytes allowed in a burst. Set a value that enables the port to gain a burst bonus if it does not use all its allocated bandwidth.
Egress Traffic Shaping	
Status	Select this option to enable shaping of outbound traffic.
Average Bandwidth	Enter the average load permitted in Kbits/sec
Peak Bandwidth	Enter the maximum load (Kbits/sec) allowed across the port.
Burst Size	Enter the maximum kbytes allowed in a burst. Set a value that enables the port to gain a burst bonus if it does not use all its allocated bandwidth.

5. Click **Next** to go to the next step in the create port group profile wizard.
The **Port Group Profile: Teaming and Failover** page (Figure 36 on page 67) appears.

Figure 36: Port Group Profile: Teaming and Failover

6. Enter the values in the fields as described in Table 19 on page 67

Table 19: Port Group Profile: Teaming and Failover

Fields	Descriptions
Load Balance Type	<p>Select an option from the list.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Route based on IP hashing: Bases the uplink port on a hash of the source and destination IP addresses in each packet. • Route based on source MAC hash: Bases the uplink port on a hash of the source MAC address of the packet. • Route based on source of the port: Bases the uplink port on the virtual port where the traffic entered the virtual switch. • Use explicit failover order: Uses the highest order uplink from the list of active adapters. •
Network Failover Detection	<p>Select an option from the list.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Link Status only: Detects failovers based on link status provided by the network adapter. This option detects failures but not configuration errors. • Beacon Probing: Detects failovers based on beacon probes that were sent out and listened for by all NICs in the team. This is used in addition to link status.

Table 19: Port Group Profile: Teaming and Failover (*continued*)

Fields	Descriptions
Notify Switches	<p>Select an option for notifying switches in cases of a failover from the list.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Yes: Sends a notification over the network whenever a virtual NIC is connected to the virtual switch, or whenever the traffic of that virtual NIC is routed over a different physical NIC. • No: Does not send out a notification. <p>NOTE: Do not use this option when Microsoft Network Load Balancing is used in unicast mode.</p>
Failback	<p>Select an option to return a physical adapter to active duty, from the list.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • Yes: Returns the adapter to active duty immediately on recovery, • No: Leaves the adapter inactive even after recovery. Returns the adapter to active duty only when another active adapter fails and requires a replacement.

7. Click **Create** to create the port group profile.
The newly created port group profile appears in the **Manage Port Group Profile** page..

Related Documentation

- Port Group Profile Overview on page 59
- Viewing Associations on page 68
- Modifying a Port Group Profile on page 69
- Cloning a Port Group Profile on page 70
- Deleting a Port Group Profile on page 70

Viewing Associations

To view the port group profile associations:

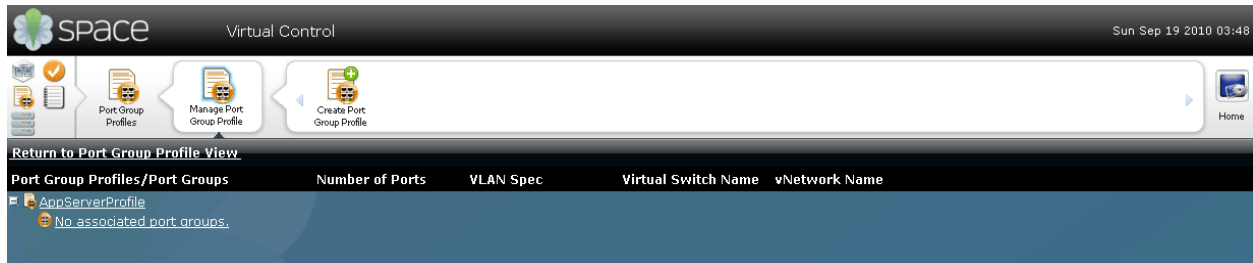
1. From the Junos Space Virtual Control task ribbon, select **Port Group Profiles > Manage Port Group Profile**.
The **Manage Port Group Profile** page appears.
2. Select the required port group profile, and from the **Action** panel or the right-click context menu, click **View Association**.

The **View Association** dialog box appears displaying the

- Port groups,
- Number of ports,
- VLAN type and ID,

- Virtual switches,
- and vNetworks that are associated with the port group profile as shown in Figure 37 on page 69

Figure 37: View Association



3. Click **Return to Port Group Profile View** to go back to the **Manage Port Group Profile** page.

Related Documentation

- Port Group Profile Overview on page 59
- Creating a Port Group Profile on page 64
- Modifying a Port Group Profile on page 69
- Cloning a Port Group Profile on page 70
- Deleting a Port Group Profile on page 70

Modifying a Port Group Profile

To modify a port group profile:

1. From the Junos Space Virtual Control task ribbon, select **Port Group Profiles > Manage Port Group Profile**.
The **Manage Port Group Profile** page appears.
2. Select the required port group profile, and from the **Action** panel or the right-click context menu, click **Modify profile**.
The **Port Group Profile: General Settings** dialog box is displayed, with the same fields as the **Create Port Group Profile** wizard.
3. Enter the appropriate values in the desired fields and click **Modify**.
The **Manage Port Group Profile** page appears displaying the newly modified port group profile.

Related Documentation

- Port Group Profile Overview on page 59
- Creating a Port Group Profile on page 64
- Viewing Associations on page 68
- Cloning a Port Group Profile on page 70
- Deleting a Port Group Profile on page 70

Cloning a Port Group Profile

To clone a port group profile:

1. From the Junos Space Virtual Control task ribbon, select **Port Group Profiles > Manage Port Group Profile**.
The **Manage Port Group Profile** page appears.
2. Select the required port group profile, and from the **Action** panel or the right-click context menu, click **Clone profile**.
The **Port Group Profile: General Settings** dialog box is displayed, with the same fields as the **Create Port Group Profile** wizard.
3. Enter the appropriate values in the desired fields and click **Clone**.
The **Manage Port Group Profile** page appears displaying the newly cloned port group profile.

Related Documentation

- Port Group Profile Overview on page 59
- Creating a Port Group Profile on page 64
- Viewing Associations on page 68
- Modifying a Port Group Profile on page 69
- Deleting a Port Group Profile on page 70

Deleting a Port Group Profile

To delete a port group profile:

1. From the Junos Space Virtual Control task ribbon, select **Port Group Profiles > Manage Port Group Profile**.
The **Manage Port Group Profile** page appears.
2. Select the required port group profile, and from the **Action** panel or the right-click context menu, click **Delete Profiles**.
The **Delete Port Group Profile** dialog box appears listing the profiles that you selected for deletion.
3. Click **Confirm** to delete the port group profile from the Junos Space Virtual Control database.

Related Documentation

- Port Group Profile Overview on page 59
- Creating a Port Group Profile on page 64
- Viewing Associations on page 68
- Modifying a Port Group Profile on page 69
- Cloning a Port Group Profile on page 70

PART 5

- Index on page 73

Index

C

- conventions
 - notice icons.....xiii
- customer support.....xiv
 - contacting JTAC.....xiv

D

- documentation
 - comments on.....xiv

H

- Host Inventory
 - viewing.....29
 - viewing details.....30

J

- Junos Space Virtual Control
 - Overview.....4

M

- manuals
 - comments on.....xiv

N

- notice icons.....xiii

P

- Port Group Details
 - Viewing22
- Port Group Profile
 - overview.....59
- Port Groups
 - creating.....23
 - Deleting.....26
 - modifying.....26
 - Overview.....21

S

- support, technical See technical support

T

- technical support
 - contacting JTAC.....xiv

V

- Virtual Networks
 - Overview.....3

