



Cisco Prime Network Services Controller 3.0 User Guide

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-28179-01

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface xv

Audience xv

Organization xv

Conventions xvi

Related Documentation xvii

Documentation Feedback xviii

Obtaining Documentation and Submitting a Service Request xviii

CHAPTER 1

Overview 1

CHAPTER 2

GUI Overview 5

Firewall Access 5

Login URL 6

User Interface Components 6

Toolbar 8

Field Aids 9

Idle Timeout Period 10

Search 10

Clone 11

CHAPTER 3

Configuring Primary Authentication 13

Primary Authentication 13

Remote Authentication Providers 14

Creating an LDAP Provider 14

Editing an LDAP Provider 16

Deleting an LDAP Provider 17

Selecting a Primary Authentication Service 17

CHAPTER 4**Configuring RBAC 19**

RBAC 19

User Accounts 19

Username Guidelines 20

Password Guidelines 20

User Roles 21

Privileges 23

User Locales 24

Configuring User Roles 25

Creating a User Role 25

Editing a User Role 26

Deleting a User Role 26

Configuring User Locales 26

Creating a Locale 26

Editing a Locale 27

Deleting a Locale 28

Assigning an Organization to a Locale 28

Deleting an Organization from a Locale 29

Configuring Locally Authenticated User Accounts 29

Creating a User Account 29

Changing the Locales or Roles Assigned to a Locally Authenticated User 33

Monitoring User Sessions 33

CHAPTER 5**Configuring Trusted Points 35**

Trusted Points 35

Configuring Trusted Points 35

Creating a Trusted Point 35

Editing a Trusted Point 36

Deleting a Trusted Point 36

CHAPTER 6**Configuring System Profiles 37**

Profiles 37

Policies in System Profiles 37

Configuring Policies 38

| | |
|---|----|
| Configuring a Core File Policy | 38 |
| Adding a Core File Policy to the System Profile | 38 |
| Editing a Core File Policy for a System Profile | 39 |
| Deleting a Core File Policy from the System Profile | 40 |
| Configuring a Fault Policy | 40 |
| Adding a Fault Policy to the System Profile | 40 |
| Editing a Fault Policy for a System Profile | 41 |
| Deleting a Fault Policy from the System Profile | 43 |
| Configuring a Logging Policy | 43 |
| Adding a Logging Policy to the System Profile | 43 |
| Editing a Logging Policy for System Profile | 44 |
| Deleting a Logging Policy from the System Profile | 45 |
| Configuring a Syslog Policy | 46 |
| Adding a Syslog Policy to the System Profile | 46 |
| Editing a Syslog Policy for the System Profile | 49 |
| Deleting a Syslog Policy from a System Profile | 52 |
| Adding a Syslog Server to the System Profile | 53 |
| Editing a Syslog Server for the System Profile | 55 |
| Deleting a Syslog Server from a System Profile | 57 |
| Configuring the Default Profile | 58 |
| Editing the System Default Profile | 58 |
| Configuring a DNS Server | 60 |
| Adding a DNS Server | 60 |
| Deleting a DNS Server | 60 |
| Configuring an NTP Server | 60 |
| Adding an NTP Server | 60 |
| Deleting an NTP Server | 61 |
| Configuring a DNS Domain | 61 |
| Editing a DNS Domain | 61 |

CHAPTER 7

| | |
|--------------------------------|-----------|
| Configuring VM Managers | 63 |
| VM Manager Overview | 63 |
| Adding a VM Manager | 63 |
| Editing a VM Manager | 65 |
| Deleting a VM Manager | 67 |

CHAPTER 8**Configuring Tenants 69**

- Tenant Management 69
 - Tenant Management and Multi-Tenant Environments 69
 - Name Resolution in a Multi-Tenant Environment 70
- Configuring Tenants 71
 - Creating a Tenant 71
 - Editing a Tenant 71
 - Deleting a Tenant 72
- Configuring Virtual Data Centers 72
 - Creating a Virtual Data Center 72
 - Editing a Virtual Data Center 73
 - Deleting a Virtual Data Center 73
- Configuring Applications 73
 - Creating an Application 73
 - Editing an Application 74
 - Deleting an Application 74
- Configuring Tiers 75
 - Creating a Tier 75
 - Editing a Tier 75
 - Deleting a Tier 76

CHAPTER 9**Configuring InterCloud Resources 77**

- InterCloud Resources 77
- InterCloud Configuration Workflow 78
- InterCloud Management User Privileges 78
- Preparing to Configure InterCloud Links and Cloud VMs 79
 - Configuring Profiles, Policies, and Pools 80
 - Configuring VSM Port Profiles 80
 - Configuring an InterCloud Device Profile 80
 - Adding a MAC Address Pool 82
 - Policies and Profiles for InterCloud Tunnels 82
 - Configuring a Connection Parameter Policy 83
 - Adding a Key Policy 84
 - Configuring a Tunnel Profile 84

| | |
|---|-----|
| Creating a Provider Account | 85 |
| Importing Infrastructure Images | 86 |
| Configuring InterCloud Links and Cloud VMs | 87 |
| Configuring an InterCloud Link | 88 |
| Field Descriptions | 89 |
| Configure VPC Screen | 89 |
| Configure InterCloud Link Screen | 90 |
| Configure Extender Properties Screen | 91 |
| Configure Extender Network Interfaces Screen | 91 |
| Configure Switch Properties Screen | 94 |
| Configure Switch Network Interfaces Screen | 94 |
| Configure Tunnel Profile Screen | 95 |
| Importing an InterCloud Agent Image | 95 |
| Importing a VM Image | 96 |
| Field Descriptions | 97 |
| Import VM Image Dialog Box | 97 |
| Creating Cloud VM Templates | 98 |
| Creating a Template from a VM Image | 98 |
| Field Descriptions | 99 |
| Template Properties Screen | 99 |
| Configure Application Parameters Screen for ISO Templates | 99 |
| Creating a Cloud Template from an Enterprise Template | 100 |
| Field Descriptions | 100 |
| Template Properties Screen | 100 |
| Creating a Template Under a VPC | 101 |
| Field Descriptions | 102 |
| Template Properties Screen | 102 |
| Instantiating Cloud VMs | 102 |
| Instantiating a Cloud VM from a Cloud Template | 103 |
| Field Descriptions | 103 |
| VM Properties Screen | 103 |
| Instantiating a Cloud VM from a Deployed Template or Local VM | 104 |
| Field Descriptions | 105 |
| VM Properties Screen | 105 |
| Instantiating a Cloud VM by Migrating an Enterprise VM | 106 |

| | |
|---|-----|
| Field Descriptions | 107 |
| VM Properties Screen | 107 |
| Managing InterCloud Links | 107 |
| Updating an InterCloud Link | 108 |
| Updating an InterCloud Link in High Availability Mode | 108 |
| Deleting an InterCloud Link | 109 |
| Monitoring InterCloud Resources and Status | 110 |
| Recent Jobs Table | 110 |
| Monitoring Tab | 111 |
| Status Fields and Labels | 112 |
| Task Tabs | 112 |
| Faults Table | 113 |
| Events Table | 114 |
| Audit Logs | 114 |
| Troubleshooting InterCloud Issues | 115 |
| InterCloud Clients Lose Connectivity to Prime Network Services Controller | 115 |
| Prime Network Services Controller Does Not Display IP Addresses for Cloud VMs | 115 |
| Creating AMI Images from VMs | 116 |
| Creating an AMI Image from a Windows VM | 116 |
| Creating an AMI Image from a Linux VM | 117 |

CHAPTER 10

| | |
|--|------------|
| Configuring Service Policies and Profiles | 123 |
| Configuring Service Policies | 123 |
| Configuring ACL Policies and Policy Sets | 123 |
| Adding an ACL Policy | 124 |
| Add ACL Policy Rule Dialog Box | 124 |
| Time Ranges in ACL Policy Rules | 128 |
| Adding an ACL Policy Set | 130 |
| Configuring Connection Timeout Policies | 130 |
| Add Connection Timeout Policy Rule Dialog Box | 131 |
| Configuring DHCP Policies | 132 |
| Adding a DHCP Relay Server | 132 |
| Add DHCP Relay Server Dialog Box | 133 |
| Configuring a DHCP Relay Policy | 133 |

| | |
|--|-----|
| Add DHCP Relay Policy Dialog Box | 133 |
| Configuring a DHCP Server Policy | 134 |
| Add DHCP Server Policy Dialog Box | 134 |
| Configuring IP Audit and IP Audit Signature Policies | 135 |
| Configuring IP Audit Policies | 136 |
| Add IP Audit Policy Rule Dialog Box | 136 |
| Configuring IP Audit Signature Policies | 137 |
| Configuring NAT/PAT Policies and Policy Sets | 138 |
| Configuring NAT/PAT Policies | 138 |
| Add NAT Policy Rule Dialog Box | 139 |
| Add NAT Policy Rule Dialog Box | 139 |
| Configuring NAT Policy Sets | 141 |
| Configuring PAT for Edge Firewalls | 141 |
| Configuring Source Dynamic Interface PAT | 142 |
| Configuring Destination Static Interface PAT | 142 |
| Configuring Packet Inspection Policies | 143 |
| Protocols Supported for Packet Inspection Policies | 143 |
| Add Packet Inspection Policy Rule Dialog Box | 144 |
| Configuring Routing Policies | 144 |
| Configuring TCP Intercept Policies | 145 |
| Add TCP Intercept Policy Rule Dialog Box | 145 |
| Configuring Site-to-Site IPsec VPN Policies | 146 |
| Configuring Crypto Map Policies | 146 |
| Add Crypto Map Policy Dialog Box | 147 |
| Add Crypto Map Policy Rule Dialog Box | 149 |
| Configuring IKE Policies | 149 |
| IKE V1 Policy Dialog Box | 150 |
| IKE V2 Policy Dialog Box | 150 |
| Configuring Interface Policy Sets | 151 |
| Add Interface Policy Set Dialog Box | 151 |
| Configuring IPsec Policies | 152 |
| IPsec IKEv1 Proposal Dialog Box | 153 |
| IPsec IKEv2 Proposal Dialog Box | 154 |
| Configuring Peer Authentication Policies | 155 |
| Add Policy to Authenticate Peer Dialog Box | 155 |

| | |
|---|-----|
| Configuring VPN Device Policies | 156 |
| Add VPN Device Policy Dialog Box | 157 |
| Working with Profiles | 159 |
| Configuring Compute Security Profiles | 159 |
| Add Compute Security Profile Dialog Box | 160 |
| Verifying Compute Firewall Policies | 161 |
| Configuring Edge Device Profiles | 161 |
| Edge Device Profile Dialog Box | 162 |
| Configuring Edge Security Profiles | 163 |
| Add Edge Security Profile Dialog Box | 164 |
| Applying an Edge Device Profile | 165 |
| Applying an Edge Security Profile | 165 |
| Verifying Edge Firewall Policies | 166 |
| Configuring Security Profiles | 166 |
| Editing a Security Profile for a Compute Firewall | 166 |
| Editing a Security Profile for an Edge Firewall | 168 |
| Deleting a Security Profile | 170 |
| Deleting a Security Profile Attribute | 170 |
| Assigning a Policy | 170 |
| Unassigning a Policy | 171 |
| Configuring Security Policy Attributes | 171 |
| Configuring Object Groups | 171 |
| Adding an Object Group | 171 |
| Adding an Object Group Expression | 172 |
| Editing an Object Group | 173 |
| Editing an Object Group Expression | 174 |
| Deleting an Object Group | 174 |
| Deleting an Object Group Expression | 175 |
| Configuring Security Profile Dictionary | 175 |
| Adding a Security Profile Dictionary | 175 |
| Adding a Security Profile Dictionary Attribute | 176 |
| Editing a Security Profile Dictionary | 176 |
| Editing a Security Profile Dictionary Attribute | 177 |
| Deleting a Security Profile Dictionary | 177 |
| Deleting a Security Profile Dictionary Attribute | 178 |

| | |
|----------------------------|-----|
| Working with vZones | 178 |
| Adding a vZone | 178 |
| Editing a vZone | 179 |
| Deleting a vZone Condition | 180 |
| Deleting a vZone | 180 |

CHAPTER 11

| | |
|---|------------|
| Configuring Device Policies and Profiles | 181 |
| Device Policies and Profiles | 181 |
| Device Profiles | 181 |
| Policies | 182 |
| Device Configuration | 182 |
| Device Policies | 183 |
| Configuring Device Policies | 183 |
| Configuring AAA Policies | 183 |
| Field Descriptions | 184 |
| Add Auth Policy Dialog Box | 184 |
| Remote Access Method Dialog Box | 185 |
| Configuring Core File Policies | 186 |
| Adding a Core File Policy for a Device | 186 |
| Editing a Core File Policy for a Device Profile | 187 |
| Deleting a Core File Policy from a Device Profile | 187 |
| Configuring Fault Policies | 188 |
| Adding a Fault Policy for a Device Profile | 188 |
| Editing a Fault Policy for a Device Profile | 189 |
| Deleting a Fault Policy for a Device Profile | 190 |
| Configuring Log File Policies | 191 |
| Adding a Logging Policy for a Device Profile | 191 |
| Editing a Logging Policy for a Device Profile | 192 |
| Deleting a Logging Policy for a Device Profile | 193 |
| Configuring SNMP Policies | 194 |
| Adding an SNMP Policy | 194 |
| Editing an SNMP Policy | 195 |
| Deleting an SNMP Policy | 196 |
| Adding an SNMP Trap Receiver | 197 |
| Editing an SNMP Trap Receiver | 197 |

| | |
|---|-----|
| Deleting an SNMP Trap Receiver | 198 |
| Configuring Syslog Policies | 198 |
| Adding a Syslog Policy for a Device | 198 |
| Field Descriptions | 198 |
| Add Syslog Policy Dialog Box | 198 |
| Editing a Syslog Policy for a Device Profile | 201 |
| Deleting a Syslog Policy for a Device Profile | 204 |
| Adding a Syslog Server for a Device Profile | 204 |
| Field Descriptions | 204 |
| Add Syslog Server Dialog Box | 204 |
| Editing a Syslog Server for a Device Profile | 207 |
| Deleting a Syslog Server for a Device Profile | 209 |
| Configuring Device Profiles | 209 |
| Adding a Firewall Device Profile | 209 |
| Editing a Firewall Device Profile | 211 |
| Deleting a Firewall Device Profile | 214 |
| Configuring NTP | 214 |
| Creating a Device Profile with NTP | 214 |
| Field Descriptions | 215 |
| Add NTP Server Dialog Box | 215 |
| Applying Device Profiles to Compute Firewalls | 216 |
| Applying Device Profiles to Edge Firewalls | 216 |
| Associating Device Policies with Profiles | 217 |

CHAPTER 12

| | |
|--------------------------------------|------------|
| Configuring Managed Resources | 219 |
| Resource Management | 219 |
| Resource Manager | 220 |
| Virtual Machines | 220 |
| Virtual Security Gateways | 220 |
| ASA 1000V Cloud Firewalls | 221 |
| Managing Compute Firewalls | 221 |
| Adding a Compute Firewall | 221 |
| Editing a Compute Firewall | 222 |
| Deleting a Compute Firewall | 225 |
| Assigning a VSG | 225 |

| | |
|--|-----|
| Unassigning a VSG | 226 |
| Managing Edge Firewalls | 226 |
| Adding an Edge Firewall | 226 |
| Add Edge Firewall Dialog Box | 227 |
| Adding a Data Interface | 227 |
| Add Data Interface Dialog Box | 227 |
| Assigning an ASA 1000V | 228 |
| Unassigning an ASA 1000V | 229 |
| Verifying VM Registration | 229 |
| Examining Fault Details | 229 |
| Examining Faults and Configuration Errors for Edge Firewalls | 230 |
| Examining Faults for Compute Firewalls | 230 |
| Launching ASDM | 231 |
| Managing Pools | 232 |
| Adding a Pool | 232 |
| Assigning a Pool | 233 |
| Editing a Pool | 234 |
| Unassigning a Pool | 234 |
| Deleting a Pool | 235 |

CHAPTER 13

| | |
|--|------------|
| Configuring Administrative Operations | 237 |
| Administrative Operation Conventions | 237 |
| Managing Backup Operations | 237 |
| Creating a Backup Operation | 238 |
| Running a Backup Operation | 239 |
| Editing a Backup Operation | 240 |
| Deleting a Backup Operation | 242 |
| Restoring a Backup Configuration | 242 |
| Managing Export Operations | 244 |
| Creating an Export Operation | 244 |
| Editing an Export Operation | 246 |
| Deleting an Export Operation | 247 |
| Configuring Import Operations | 248 |
| Creating an Import Operation | 248 |
| Editing an Import Operation | 249 |

[Deleting an Import Operation](#) 251



Preface

This preface includes the following sections:

- [Audience, page xv](#)
- [Organization, page xv](#)
- [Conventions, page xvi](#)
- [Related Documentation, page xvii](#)
- [Documentation Feedback, page xviii](#)
- [Obtaining Documentation and Submitting a Service Request, page xviii](#)

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following areas:

- Server administration
- Storage administration
- Network administration
- Network security

Organization

This document includes the following chapters:

| Chapter | Title | Description |
|-----------|--------------|--|
| Chapter 1 | Overview | Contains an overview of Cisco Prime Network Services Controller (Prime Network Services Controller). |
| Chapter 2 | GUI Overview | Provides an overview of the Prime Network Services Controller GUI. |

| Chapter | Title | Description |
|------------|---|---|
| Chapter 3 | Configuring Primary Authentication | Describes how to configure LDAP providers and select a primary authentication service. |
| Chapter 4 | Configuring RBAC | Describes how to configure role-based access control including user locales, user roles, and locally authenticated user accounts. This chapter also describes how to monitor user sessions. |
| Chapter 5 | Configuring Trusted Points | Describes how to configure trusted points. |
| Chapter 6 | Configuring System Profiles | Describes how to configure Prime Network Services Controller policies and profiles. |
| Chapter 7 | Configuring VM Managers | Describes how to configure VM Managers. |
| Chapter 8 | Configuring Tenants | Describes how to configure tenants, data centers, applications, and tiers. |
| Chapter 9 | Configuring InterCloud Resources | Describes how to configure cloud-related policies, VM images, links, templates, and cloud VMs. This chapter also describes how to monitor InterCloud resources and status. |
| Chapter 10 | Configuring Service Policies and Profiles | Describes how to configure service policies and policy sets, verify policies, configure compute and edge firewall security policies, and apply profiles to firewalls. |
| Chapter 11 | Configuring Device Policies and Profiles | Describes how to configure device policies and device profiles, and associate device policies with profiles. |
| Chapter 12 | Configuring Managed Resources | Describes how to configure managed resources including compute and edge firewalls, and pools. |
| Chapter 13 | Configuring Administrative Operations | Describes how to configure backup operations, export operations, and import operations. |

Conventions

This document uses the following conventions:

| Convention | Indication |
|------------------|---|
| bold font | Commands, keywords, GUI elements, and user-entered text appear in bold font. |

| Convention | Indication |
|--------------------------|--|
| <i>italic font</i> | Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> . |
| [] | Elements in square brackets are optional. |
| {x y z} | Required alternative keywords are grouped in braces and separated by vertical bars. |
| [x y z] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |
| string | A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks. |
| Courier font | Terminal sessions and information that the system displays appear in Courier font. |
| Bold Courier font | Information that you enter appears in bold Courier font . |
| <> | Nonprinting characters such as passwords are in angle brackets. |
| [] | Default responses to system prompts are in square brackets. |
| !, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line. |

**Note**

Means *reader take note*.

**Tip**

Means *the following information will help you solve a problem*.

**Caution**

Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Related Documentation

Cisco Prime Network Services Controller

The following Cisco Prime Network Services Controller documents are available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html

- *Cisco Prime Network Services Controller 3.0 Documentation Overview*
- *Cisco Prime Network Services Controller 3.0 Release Notes*
- *Cisco Prime Network Services Controller 3.0 Quick Start Guide*
- *Cisco Prime Network Services Controller 3.0 CLI Configuration Guide*
- *Cisco Prime Network Services Controller 3.0 User Guide*
- *Cisco Prime Network Services Controller 3.0 XML API Reference Guide*
- *Open Source Used in Cisco Prime Network Services Controller 3.0*

Cisco ASA 1000V Documentation

The Cisco Adaptive Security Appliance (ASA) documentation is available on [Cisco.com](http://www.cisco.com) at the following URL:

http://www.cisco.com/en/US/products/ps12233/tsd_products_support_series_home.html

Cisco Nexus 1000V InterCloud Documentation

The Cisco Nexus 1000V InterCloud documentation is available on [Cisco.com](http://www.cisco.com) at the following URL:

http://www.cisco.com/en/US/products/ps12904/tsd_products_support_series_home.html

Cisco Nexus 1000V Series Switch Documentation

The Cisco Nexus 1000V Series switch documentation is available on [Cisco.com](http://www.cisco.com) at the following URL:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Cisco Virtual Security Gateway Documentation

The Cisco Virtual Security Gateway (VSG) documentation is available on [Cisco.com](http://www.cisco.com) at the following URL:

http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to cpnsc-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



Overview

Cisco Prime Network Services Controller (Prime Network Services Controller) is the primary management element for Cisco Nexus 1000V (Nexus 1000V) Switches and Services that can enable a transparent, scalable, and automation-centric network management solution for virtualized data center and hybrid cloud environments. Nexus 1000V switches and services deliver a highly secure multitenant environment by adding virtualization intelligence to the data center network. These virtual switches are built to scale for cloud networks. Support for Virtual Extensible LAN (VXLAN) helps enable a highly scalable LAN segmentation and broader virtual machine (VM) mobility.

Prime Network Services Controller enables the centralized management of Cisco virtual services to be performed by an administrator, through its GUI, or programmatically through its XML API. Prime Network Services Controller is built on an information-model architecture in which each managed device is represented by its subcomponents (or objects), which are parametrically defined. This model-centric approach enables a flexible and simple mechanism for provisioning and securing virtualized infrastructure using Cisco VSG and Cisco Adaptive Security Appliance 1000V (ASA 1000V) Cloud Firewall virtual security services.

InterCloud

With Cisco Nexus 1000V InterCloud, the enterprise network can be securely extended to the cloud, with its enterprise network and security configurations such as VLANs and policies extended to the cloud. Using Prime Network Services Controller, workloads can be migrated from the enterprise data center to the public cloud while retaining the same IP addresses and other networking parameters, thus avoiding the need to redesign the application.

Using Prime Network Services Controller, workloads in the public cloud can use the same security policies as their counterparts in the enterprise data center. System administrators get the policy consistency and network visibility that they require while retaining control of the cloud environment as a transparent extension of the enterprise data center.

With Prime Network Services Controller, customers have a unified view of the workloads across the enterprise data center (private cloud) and public cloud. They can select and migrate workloads from the enterprise data center to the public cloud.

Hypervisor Support

The Prime Network Services Controller platform supports multiple VM Managers through their APIs and through tight integration with Nexus 1000V Virtual Supervisor Modules (VSMs) and Virtual Ethernet Modules (VEMs).

Consistent and Efficient Security Policies

Prime Network Services Controller uses security profiles for template-based configuration of security policies. A security profile is a collection of security policy sets and integrated policies and rules that can be predefined and applied on demand at the time of virtual machine instantiation. This profile-based approach significantly simplifies authoring, deployment, and management of security policies, including dense multi-tenant environments, while enhancing deployment agility and scaling. Security profiles also help reduce administrative errors and simplify audits.

The XML API for Prime Network Services Controller facilitates integration with northbound network provisioning tools for programmatic network and security provisioning and management of Cisco VSG (VSG) and ASA 1000V. The option of programmatic control of those virtual appliances can greatly simplify operational processes and reduce infrastructure management costs.

Nondisruptive Administration Model

By providing visual and programmatic controls, Prime Network Services Controller can enable the security operations team to author and manage security policies for virtualized infrastructure and enhance collaboration with the server and network operations teams. This nondisruptive administration model helps ensure administrative segregation of duties to reduce errors and simplify regulatory compliance and auditing:

- Security administrators can author and manage security profiles and manage VSG and ASA 1000V instances. Security profiles are referenced in Nexus 1000V port profiles.
- Network administrators can author and manage port profiles, and manage Nexus 1000V switches. Port profiles with referenced security profiles are available in VMware vCenter through the Nexus 1000V VSM programmatic interface with VMware vCenter.
- Server administrators can select an appropriate port profile in VMware vCenter when instantiating a virtual machine.

Efficient Management for Easier Scalability

Prime Network Services Controller implements an information-model architecture in which each managed device, such as VSG or Cisco ASA 1000V, is represented by the device's object-information model. This model-based architecture helps enable the use of:

- Stateless managed devices—Security policies (security templates) and object configurations are abstracted into a centralized repository and used as templates against any virtual device type.
- Dynamic device allocation—A centralized resource management function manages pools of devices that are commissioned (deployed) in service and a pool of devices that are available for commissioning. This approach simplifies large-scale deployments because managed devices can be preinstantiated and then configured on demand, and devices can be allocated and deallocated dynamically across commissioned and noncommissioned pools.
- Scalable management—A distributed management-plane function is implemented using an embedded agent on each managed device that helps enable greater scalability.

The following table describes the features and benefits of Prime Network Services Controller.

Table 1: Features and Benefits

| Features | Description | Benefits |
|---------------------------------|---|--|
| InterCloud Management | Prime Network Services Controller extends your enterprise data center into a public cloud through the configuration and management of InterCloud resources. | <ul style="list-style-type: none"> • Provides secure connections to the cloud via InterCloud links using VMware ESXi hypervisors. • Enables easy creation of templates and VMs on the cloud. • Supports high availability across the InterCloud link. |
| Multiple-Device Management | Prime Network Services Controller provides central management of VSG and ASA 1000V for Nexus 1000V switches. | Simplifies provisioning and troubleshooting in a scaled-out data center. |
| Security Profiles | A security profile represents the VSG or ASA 1000V security policy configuration in a profile (template). | Simplifies provisioning, reduces administrative errors during security policy changes, reduces audit complexities, and helps enable a highly scaled-out data center environment. |
| Stateless Device Provisioning | The management agents in VSG and ASA 1000V are stateless, receiving information from Prime Network Services Controller. | <ul style="list-style-type: none"> • Enhances scalability. • Provides robust endpoint failure recovery without loss of configuration state. |
| Security Policy Management | Security policies are authored, edited, and provisioned centrally. | <ul style="list-style-type: none"> • Simplifies operation and management of security policies. • Helps ensure that security intent is accurately represented in the associated security policies. |
| Context-Aware Security Policies | Prime Network Services Controller obtains virtual machine contexts from VMware vCenter. | Allows a security administrator to institute highly specific policy controls across the entire virtual infrastructure. |

| Features | Description | Benefits |
|---|---|---|
| Dynamic Security Policy and Zone Provisioning | Prime Network Services Controller interacts with the Nexus 1000V VSM to bind the security profile to the corresponding Nexus 1000V port profile. When virtual machines are dynamically instantiated by server administrators and appropriate port profiles applied, their association with trust zones is also established. | Helps enable security profiles to stay aligned with rapid changes in the virtual data center. |
| Multi-Tenant (Scale-Out) Management | Prime Network Services Controller is designed to manage VSG and ASA 1000V security policies in a dense multi-tenant environment so that administrators can rapidly add and delete tenants and update tenant-specific configurations and security policies. | Reduces administrative errors, helps ensure segregation of duties in administrative teams, and simplifies audit procedures. |
| Role-Based Access Control (RBAC) | RBAC simplifies operational tasks across different types of administrators, while allowing subject-matter experts to continue with their normal procedures. | <ul style="list-style-type: none"> • Reduces administrative errors. • Enables detailed control of user privileges. • Simplifies auditing requirements. |
| XML-Based API | Prime Network Services Controller XML API allows external system management and orchestration tools to programmatically provision VSG and ASA 1000V. | <ul style="list-style-type: none"> • Allows the use of the best-in-class management software. • Offers transparent and scalable operation management. |



GUI Overview

Prime Network Services Controller provides a browser-based interface that enables you to configure managed endpoints, perform administrative operational tasks, and define and apply policies and profiles. You can also use the GUI to manage and provision compute and edge firewalls, such as VSGs and ASA 1000Vs.

The following topics provide an overview of the Prime Network Services Controller user interface.

- [Firewall Access, page 5](#)
- [Login URL, page 6](#)
- [User Interface Components, page 6](#)
- [Toolbar, page 8](#)
- [Field Aids, page 9](#)
- [Idle Timeout Period, page 10](#)
- [Search, page 10](#)
- [Clone, page 11](#)

Firewall Access

If the Prime Network Services Controller server is protected by a firewall, the following ports must be enabled:

- 22—TCP
- 80—HTTP
- 443—HTTPS
- 843—Adobe Flash
- 6644—TCP, UDP

Login URL

The default HTTPS URL for logging into the Prime Network Services Controller user interface is `https://server-ip-address`, where *server-ip-address* is the IP address assigned to the Prime Network Services Controller server. The IP address is the address for the management port.



Note If you log in using HTTP, you are automatically redirected to the HTTPS link.

User Interface Components

When you log into Prime Network Services Controller, the user interface is displayed with the components described in the following table:

Table 2: Prime Network Services Controller User Interface Components

| Component | Description |
|-----------------|--|
| Title | Displays "Cisco Prime Network Services Controller." |
| Toolbar | Allows you to set an idle timeout value, obtain Prime Network Services Controller version information, access online help, provide product feedback, and log out. |
| Tabs | Provide access to the following primary components for managing your environment: <ul style="list-style-type: none"> • Tenant Management • Resource Management • Policy Management • InterCloud Management • Administration |
| Navigation pane | Provides navigation to all objects in the Prime Network Services Controller instance. The navigation pane is displayed on the left side of the screen below the tabs. The objects that are displayed in the navigation pane depend on the selected tab. |
| Content pane | Displays information and provides options for the object that is selected in the navigation pane. |

The following table provides information about the tabs in the Prime Network Services Controller GUI:

Table 3: Tabs in the Prime Network Services Controller GUI

| Tab | Description |
|-----------------------|---|
| Tenant Management | <p>Enables you to manage tenants in the current Prime Network Services Controller instance.</p> <p>A system or server administrator can use this tab to create organizational hierarchies and enable multi-tenant management domains. The organizational hierarchy levels are Tenant > Virtual Data Center > Application > Tier.</p> |
| Resource Management | <p>Enables you to manage logical resources, such as VSGs, ASA 1000Vs, VSMs, and vCenters.</p> <p>Resource Management subtabs are:</p> <ul style="list-style-type: none"> • Managed Resources • Resources • Capabilities • Diagnostics |
| Policy Management | <p>Enables you to configure service and device policies and profiles, and to assign policies to profiles.</p> <p>Policy Management subtabs are:</p> <ul style="list-style-type: none"> • Service Profiles • Service Policies • Device Configurations • Capabilities • Diagnostics |
| InterCloud Management | <p>Enables you to configure and monitor InterCloud resources.</p> <p>InterCloud Management subtabs are:</p> <ul style="list-style-type: none"> • Enterprise • Public Cloud • InterCloud Link • InterCloud Policies • Diagnostics |

| Tab | Description |
|----------------|---|
| Administration | <p>Provides the tools needed for administering Prime Network Services Controller.</p> <p>Administration subtabs are:</p> <ul style="list-style-type: none"> • Access Control • System Profile • VM Managers • Diagnostics • Operations • Service Registry |

Toolbar

The Prime Network Services Controller toolbar displays in the upper-right portion of the user interface. The following table describes the toolbar options:

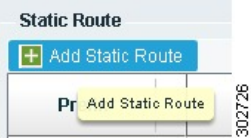

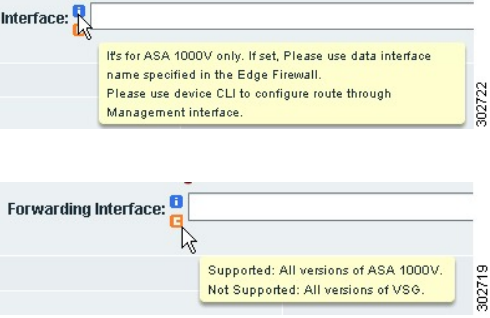
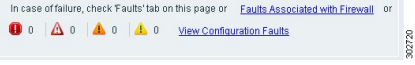
Table 4: Toolbar Options


| Option | Description |
|-------------|---|
| (username) | Username of the current Prime Network Services Controller session. |
| Preferences | Enables you to specify the amount of time that the Prime Network Services Controller session can remain inactive before the session times out. The value that you specify applies to the system from which you logged into Prime Network Services Controller. |
| Log Out | Logs you out of the current session. |
| About | Provides Prime Network Services Controller version information. |
| Help | Launches online help for the currently displayed screen. |
| Feedback | Allows you to provide feedback on Prime Network Services Controller. |

Field Aids

Prime Network Services Controller includes the following aids to assist you in your tasks, whether configuring policies and profiles, troubleshooting faults, or looking for additional information for a particular window or dialog box.

Table 5: Prime Network Services Controller Field Aids

| Feature | Description | Example |
|------------------|---|--|
| Tooltips | Pause your cursor over a field to view additional information about the field. |  |
| Red field or box | Indicates that information is required. If you have entered information and the field remains red, the entry contains an error (such as an incomplete IP address). You can pause your mouse over the field to obtain information about the error. |  |
| Field icons | <p>Two field icons (i and c) provide additional information for the field:</p> <ul style="list-style-type: none"> • The "i" icon provides additional information for the field. • The "c" icon identifies the feature support for the field. For example, a feature might be supported on ASA 1000Vs but not on VSGs. <p>Pause your cursor over the icon to view the information.</p> |  |
| Fault links | <p>Fault information and links to fault information are available for each edge and compute firewall in Resource Management.</p> <p>Navigate to a specific compute or edge firewall to view the object state, number of faults, and severity of faults. The same pane provides links to the relevant fault page.</p> |  |

| Feature | Description | Example |
|-------------|---|--|
| Online help | Context-sensitive online help is available for each Prime Network Services Controller pane and dialog box. To access help, click Help in the active pane or ? in the active dialog box. |  |

Idle Timeout Period

The Preferences dialog box allows you to specify the length of time, from 5 to 60 minutes, that a Prime Network Services Controller session on your current machine can remain idle before the session is closed. The value that you enter applies to the system that you used to log into Prime Network Services Controller.

Search

The Search tab enables you to search for instances of organizations in Prime Network Services Controller. From the search result, you can expand an organization's hierarchy and launch devices and policies in that organization.



Note

Searching for organization names does not work if the organization names contain special characters.

Procedure

Step 1 Do any of the following to launch the Search tab:

- Choose **Policy Management > Service Policies > root > Search**.
- Choose **Policy Management > Service Profiles > root > Search**.
- Choose **Policy Management > Device Configurations > root > Search**.
- Choose **Tenant Management > root > Search**.
- Choose **Resource Management > Managed Resources > root > Search**.

Note You can perform the Search operation at any level in the organizational hierarchy.

Step 2 Enter organization names as a *pattern or a regular expression. The Search feature is case-sensitive. When you enter a name as a regular expression, it can contain regex wildcards such as *, +, ? and so on. For example, "*" will match the previous character zero or more times. Searching myVdc* will return all names that contain "myVd" and "myVDC".

Use the following the guidelines when you enter a pattern:

- To fetch organization names starting with "ABC", enter "ABC*".

- To fetch organization names ending with "ABC", enter "*ABC".
- To fetch organizations names starting with "A" and ending with "BC" but with other characters in between, enter "A*BC".

Step 3 Click **Search**.
The search results are displayed in the table.

Clone

You can create a clone for an organization, policy, policy set, or profile at a destination of your choice. The hierarchy of an organization's clone or the names of the elements in it cannot be changed. After a clone is created, it cannot be renamed or moved to another location.

Procedure

Step 1 Based on the element you want to clone, do one of the following:

- To clone an organization, choose **Tenant Management > root > tenant > organization**.
- To clone a policy, policy set, or profile, choose **Policy Management > Service Polices > root > tenant > Policies > policy** or **Policy Management > Service Profiles > root > tenant > Profiles > profile**.

Step 2 Right-click the element to be cloned and choose **Clone**.

Step 3 In the Clone dialog box that appears:

- a) Enter the name and destination of the clone.
- b) Click **OK**.

The clone appears in the destination you chose.



Configuring Primary Authentication

This section includes the following topics:

- [Primary Authentication, page 13](#)
- [Remote Authentication Providers, page 14](#)
- [Creating an LDAP Provider, page 14](#)
- [Editing an LDAP Provider, page 16](#)
- [Deleting an LDAP Provider, page 17](#)
- [Selecting a Primary Authentication Service, page 17](#)

Primary Authentication

Prime Network Services Controller supports two methods to authenticate user logins:

- Local to Prime Network Services Controller
- Remote through LDAP

The role and locale assignment for a local user can be changed on Prime Network Services Controller. The role and locale assignment for a remote user can be changed on LDAP. If any of the following information assigned to a user is modified, the administrator must delete all the existing sessions of that user so that the new privileges take effect:

- Role
- Privilege for a role
- Locale
- Organization in a locale

Remote Authentication Providers

If a system is configured for a supported remote authentication service, you must create a provider for that service to ensure that Prime Network Services Controller and the system configured with the service can communicate.

User Accounts in Remote Authentication Services

You can create user accounts in Prime Network Services Controller or in the remote authentication server.

The temporary sessions for users who log in through remote authentication services can be viewed through the Prime Network Services Controller GUI.

User Roles and Locales in Remote Authentication Services

If you create user accounts in the remote authentication server, you must ensure that the accounts include the roles and locales those users require for working in Prime Network Services Controller and that the names of those roles and locales match the names used in Prime Network Services Controller. If an account does not have the required roles and locales, the user is granted only read-only privileges.

LDAP Attribute for User

In Prime Network Services Controller, the LDAP attribute that holds the LDAP user roles and locales is preset. This attribute is always a name-value pair. For example, by default CiscoAvPair specifies the role and locale information for the user, and if the filter is specified, the LDAP search is restricted to those values that match the defined filter. By default, the filter is sAMAccountName=\$userid. The user can change these values to match the setting on the LDAP server. When a user logs in, Prime Network Services Controller checks for the value of the attribute when it queries the remote authentication service and validates the user. The value should be identical to the username.

An example of LDAP property settings is as follows:

- Timeout—30
- Retries—1
- Attribute—CiscoAvPair
- Filter—sAMAccountName=\$userid
- Base DN—DC=cisco, DC=com (The specific location in the LDAP hierarchy where Prime Network Services Controller starts the query for the LDAP user.)

Creating an LDAP Provider

Before You Begin

Configure users with the attribute that holds the user role and locale information for Prime Network Services Controller. You can use an existing LDAP attribute that is mapped to the Prime Network Services Controller user roles and locales, or you can create a custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1. When you add the LDAP user to the LDAP server, specify the role and locale in the attribute (for example, shell:roles=network,aaa shell:locale=sanjose,dallas).

Procedure

- Step 1** Choose **Administration > Access Control > LDAP**.
- Step 2** In the content pane, click **Create LDAP Provider**.
- Step 3** In the Create LDAP Provider dialog box, provide the following information:

| Field | Description |
|---------------------|--|
| Hostname/IP Address | <p>Hostname or IP address of the LDAP provider.</p> <p>If SSL is enabled, this field must match a Common Name (CN) in the security certificate of the LDAP database.</p> <p>Note If you use a hostname instead of an IP address, you must configure a DNS server in the Prime Network Services Controller server.</p> |
| Key | <p>Password for the LDAP database account specified in the Root DN field.</p> <p>The maximum is 32 characters.</p> |
| Root DN | <p>Distinguished Name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN.</p> <p>The maximum supported string length is 127 characters.</p> |
| Port | <p>Port through which Prime Network Services Controller communicates with the LDAP database.</p> <p>The default port number is 389.</p> |
| Enable SSL | Check to enable SSL. |

Note Depending on the object you select in the table, different options appear above the table.

- Step 4** Click **OK**, then click **Save**.

Following is an example of creating an LDAP provider:

- **Hostname/IP Address**—Provider-blr-sam-aaa-10.cisco.com
- **Key**—xxxxxx (The password of the LDAP database account specified in the **Root DN** field.)
- **Root DN**— CN=bob,DC=cisco,DC=com (The value of CN is the name of a user with query privileges. DC refers to the location in the LDAP directory where a user is created.)
- **Port**—389

- **Enable SSL**—check box

What to Do Next

Select LDAP as the primary authentication service. For more information, see [Selecting a Primary Authentication Service](#), on page 17.

Editing an LDAP Provider

Procedure

- Step 1** Choose **Administration > Access Control > LDAP**.
- Step 2** In the content pane, select the required LDAP provider.
- Step 3** Click **Edit**.
- Step 4** In the Edit dialog box, modify the settings as required, using the following table as a guide:

| Field | Description |
|---------|--|
| Name | <p>Hostname or IP address of the LDAP provider (read-only).</p> <p>If SSL is enabled, this field must match a Common Name (CN) in the security certificate of the LDAP database.</p> <p>Note If you use a hostname instead of an IP address, you must configure a DNS server in the Prime Network Services Controller server.</p> |
| Key | <p>Password for the LDAP database account specified in the Root DN field.</p> <p>The maximum is 32 characters.</p> |
| Set | <p>Whether or not the preshared key has been set and is properly configured (read-only).</p> <p>If the Set value is Yes, and the Key field is empty, it indicates that a key was provided previously.</p> |
| Root DN | <p>Distinguished Name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN.</p> <p>The maximum supported string length is 127 characters.</p> |
| Port | <p>Port through which Prime Network Services Controller communicates with the LDAP database.</p> <p>The default port number is 389.</p> |

| Field | Description |
|------------|----------------------|
| Enable SSL | Check to enable SSL. |

Step 5 Click **OK**, then click **Save**.

Deleting an LDAP Provider

Procedure

- Step 1** In the Administration tab, choose **Access Control > LDAP**.
- Step 2** In the Work pane, select the LDAP provider that you want to delete, then click **Delete**.
- Step 3** Confirm the deletion, then click **Save**.

Selecting a Primary Authentication Service



Note If the default authentication is set to LDAP, and the LDAP servers are not operating or are unreachable, the local admin user can log in at any time and make changes to the authentication, authorization, and accounting (AAA) system.

Procedure

- Step 1** Choose **Administration > Access Control > Authentication**.
- Step 2** In the Properties tab, specify the information as described in the following table, then click **OK**.

| Field | Description |
|------------------------|---|
| Default Authentication | Default method by which a user is authenticated during remote login: <ul style="list-style-type: none"> • LDAP—The user must be defined on the LDAP server specified for this Prime Network Services Controller instance. • Local—The user must be defined locally in this Prime Network Services Controller instance. • None—A password is not required when the user logs in remotely. |

| Field | Description |
|-----------------------------|--|
| Role Policy to Remote Users | <p data-bbox="732 300 1469 363">Action taken when a user attempts to log in and the LDAP server does not supply a user role with the authentication information:</p> <ul data-bbox="776 384 1469 531" style="list-style-type: none"><li data-bbox="776 384 1469 447">• assign-default-role—The user is allowed to log in with a read-only user role.<li data-bbox="776 468 1469 531">• no-login—The user is not allowed to log into the system, even if the user name and password are correct. |



Configuring RBAC

This section contains the following topics:

- [RBAC, page 19](#)
- [User Accounts, page 19](#)
- [User Roles, page 21](#)
- [Privileges, page 23](#)
- [User Locales, page 24](#)
- [Configuring User Roles, page 25](#)
- [Configuring User Locales, page 26](#)
- [Configuring Locally Authenticated User Accounts, page 29](#)
- [Monitoring User Sessions, page 33](#)

RBAC

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.

A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the Engineering organization could update server configurations in the Engineering organization but could not update server configurations in the Finance organization unless the locales assigned to the user include the Finance organization.

User Accounts

User accounts are used to access the system. Up to 128 local user accounts can be configured in each Prime Network Services Controller instance. Each user account must have a unique username.

A local user can be authenticated using a password or an SSH public key. The public key can be set in either of the two formats: OpenSSH and SECSH.

Default User Account

Each Prime Network Services Controller instance has a default user account, admin, which cannot be modified or deleted. This account is the system administrator or superuser account and has full privileges. There is no default password assigned to the admin account; you must choose the password during the initial system setup.

Expiration of User Accounts

User accounts can be configured to expire at a predefined time. When the expiration time is reached, the user account is disabled.

By default, user accounts do not expire.

Username Guidelines

The username is also used as the login ID for Prime Network Services Controller. When you assign usernames to Prime Network Services Controller user accounts, consider the following guidelines and restrictions:

- The login ID can contain from 1 to 32 characters, including the following:
 - Any alphanumeric character
 - Period (.)
 - Underscore (_)
 - Dash (-)
 - At symbol (@)
- Neither the unique username nor a local user's username can consist solely of numbers.
- The unique username cannot start with a number.
- If an all-numeric username exists on a AAA server (LDAP) and is entered during login, Prime Network Services Controller cannot log in the user.

After you create a user account, you cannot change the username. You must delete the user account and create a new one.

**Note**

You can create up to 128 user accounts in a Prime Network Services Controller instance.

Password Guidelines

For authentication purposes, a password is required for each user account. To prevent users from choosing insecure passwords, each password must be strong. If the Password Strength Check option is enabled, Prime Network Services Controller rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters.

- Must contain at least three of the following:
 - Lowercase letters
 - Uppercase letters
 - Digits
 - Special characters
- Must not contain a character that is repeated more than three times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: dollar sign (\$), question mark (?), or equals sign (=).
- Should not be blank for local user and admin accounts.

**Note**

The Password Strength Check option is enabled by default. You can disable it from the Locally Authenticated Users pane (Administration > Access Control > Locally Authenticated Users).

**Note**

If Prime Network Services Controller is configured to use remote authentication with LDAP, passwords for those remote accounts can be blank. With this configuration, the remote credentials store is used for authentication only, not authorization. The definition of the local user role definition applies to the remotely authenticated user.

User Roles

User roles contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has policy-related privileges, and Role2 has tenant-related privileges, users who are assigned to both Role1 and Role2 have policy- and tenant-related privileges.

All roles include read access to all configuration settings in the Prime Network Services Controller instance. The difference between the read-only role and other roles is that a user who is assigned only the read-only role cannot modify the system state. A user assigned another role can modify the system state in that user's assigned area or areas.

The system contains the following default user roles:

aaa

Users have read and write access to users, roles, and AAA configuration, and read access to the rest of the system.

admin

Users have read and write access to the entire system and has most privileges. However, users cannot create or delete files, or perform system upgrades. These functions can be done only through the default admin account. The default admin account is assigned this role by default, and it cannot be changed.

intercloud-infra

Users have read and write access for InterCloud operations, including creating InterCloud links, creating provider accounts, managing InterCloud Extender and Switch images, and importing InterCloud Agent images. Users with this role are limited to InterCloud functionality.

intercloud-server

Users have read and write access for cloud VMs. User can create or move VMs from the enterprise to the cloud. Users can monitor cloud VMs for multiple tenants. Users with this role are limited to InterCloud functionality.

network

Users can create organizations, security policies, and device profiles.

operations

Users can acknowledge faults and perform some basic operations such as logging configuration.

read-only

Users have read-only access to system configuration and operational status with no privileges to perform any operations.

Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Network and Operations roles have different sets of privileges, but a new Network and Operations role can be created that combines the privileges of both roles.

If a role is deleted after it has been assigned to users, it is also deleted from those user accounts.

The role and locale assignment for a local user can be changed on Prime Network Services Controller. The role and locale assignment for a remote user can be changed on LDAP. If any of the following information assigned to a user is modified, the administrator must delete all the existing sessions of that user so that the new privileges take effect:

- Role
- Privilege for a role
- Locale
- Organization in a locale

Privileges

User Privileges

Privileges give users assigned to user roles access to specific system resources and permission to perform specific tasks. The following table lists each privilege and its description.

| Privilege Name | Description |
|---------------------------|--|
| AAA | System security and AAA. |
| Admin | System administration. |
| InterCloud-Infrastructure | InterCloud infrastructure management. |
| InterCloud-Server | InterCloud VM management. |
| read-only | Read-only access. Read-only cannot be selected as a privilege; it is assigned to every user role. |
| Resource Configuration | Edge and compute firewall configuration. |
| Policy Management | Edge and compute firewall policies. |
| Fault Management | Alarms and alarm policies. |
| Operations | Logs, core file management, and show tech-support command. |
| Tenant Management | Create, delete, and modify tenants and organization containers. |

Privileges and Role Assignments

The following table lists the out-of-box default role name for each privilege.

| Default Role Name | Privilege Name |
|-------------------|----------------------------|
| aaa | aaa |
| admin | admin |
| intercloud-infra | InterCloud-Infrastructure |
| intercloud-server | InterCloud-Server |
| network | policy, res-config, tenant |

| Default Role Name | Privilege Name |
|-------------------|-------------------|
| operations | fault, operations |
| read-only | read-only |

User Locales

A user can be assigned one or more locales. Each locale defines one or more organizations or domains (collectively referred to as *resources*) to which the user is allowed access. In addition, the user has read-only access privileges outside their assigned locale and going up the organization tree. This enables the user to use these resources when creating policies. One exception to this rule is a locale without any organizations, which gives unrestricted access to system resources in all organizations. Only the objects under organizations are controlled by locales. Access to other objects such as users, roles, and resources that are not present in the organization tree are not affected by locales.



Note

Users not assigned to a locale have access to all resources in all organizations. For users assigned to a locale, access is restricted to the objects that reside under the organizations that belong to that locale.

Users with AAA privileges (AAA role) can assign organizations to the locale of other users. The assignment of organizations is restricted to only those in the locale of the user assigning the organizations. For example, if a locale contains only the Engineering organization, then a user assigned that locale can assign only the Engineering organization to other users.



Note

AAA privileges must be carefully assigned because they allow a user to manage other users' privileges and role assignments.

You can hierarchically manage organizations. A user who is assigned to a top-level organization has automatic access to all organizations under it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization; however, a locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

The role and locale assignment for a local user can be changed on Prime Network Services Controller. The role and locale assignment for a remote user can be changed on LDAP. If any of the following information assigned to a user is modified, the administrator must delete all the existing sessions of that user so that the new privileges take effect:

- Role
- Privilege for a role
- Locale
- Organization in a locale

Configuring User Roles

Creating a User Role

Procedure

Step 1 Choose **Administration > Access Control > Roles**.

Step 2 Click **Create Role**.

Step 3 In the Create Role dialog box, complete the following fields, then click **OK**:

| Field | Description |
|------------|--|
| Name | User role name. |
| Privileges | <p>Available privileges. To assign a privilege to the selected role, check one or more of the following check boxes:</p> <ul style="list-style-type: none"> • Admin • AAA • Fault Management • InterCloud-Infrastructure • InterCloud-Server • Operations • Policy Management • Resource Configuration • Tenant Management <p>Note You can assign the Admin privilege, which includes all privileges, or you can assign privileges individually.</p> |

Editing a User Role

Procedure

- Step 1** Choose **Administration > Access Control > Roles**.
 - Step 2** Select the role you want to edit, then click **Edit**.
 - Step 3** In the Edit dialog box, check or uncheck the boxes for the privileges you want to add to or remove from the role, then click **OK**.
-

Deleting a User Role

Except for the admin and read-only roles, you can delete user roles that are not appropriate for your environment.

Procedure

- Step 1** Choose **Administration > Access Control > Roles**.
 - Step 2** Select the user role you want to delete, then click **Delete**.
 - Note** You cannot delete the admin or read-only role.
 - Step 3** In the Confirm dialog box, click **Yes**.
-

Configuring User Locales

Creating a Locale

Before You Begin

Verify that one or more organizations (tenants) exist; if none exist, create one. For information on creating tenants, see [Creating a Tenant](#), on page 71.

Procedure

- Step 1** Choose **Administration > Access Control > Locales**.
- Step 2** Click **Create Locale**.
- Step 3** In the Create Locale dialog box, complete the following fields, then click **OK**:

| Field | Description |
|-------------------------------|--|
| Name | Locale name, containing 2 to 255 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change this name after it is saved. |
| Description | Brief locale description, containing 1 to 256 characters. The description can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). |
| Assigned Organizations | |
| Assign Organization | Click to assign organizations to locales. |
| Assigned Organization | List of organizations assigned to the locale. |

What to Do Next

Add the locale to one or more user accounts. For more information, see [Changing the Locales or Roles Assigned to a Locally Authenticated User](#), on page 33.

Editing a Locale

Procedure

- Step 1** Choose **Administration > Access Control > Locales**.
- Step 2** In the list of locales, select the locale you want to edit, then click **Edit**.
- Step 3** In the Description field, change the description as appropriate.
- Step 4** Click **Assign Organization**.
- Step 5** In the Assign Organization dialog box:
 - a) Expand the root node to view the available organizations.
 - b) Check the check boxes of the organizations to assign to the locale.
- Step 6** Click **OK** in the open dialog boxes to save your changes.

Deleting a Locale

Before You Begin

**Caution**

If the locale you want to delete is assigned to any user/s, remove the locale from the user list of locales.

Procedure

- Step 1** In the Navigation pane, click the **Administration** tab.
 - Step 2** In the Navigation pane, click the **Access Control** subtab.
 - Step 3** In the **Navigation** pane, click the **Locales** node.
 - Step 4** In the **Work** pane, click the locale you want to delete.
 - Step 5** Click **Delete**.
 - Step 6** In the **Confirm** dialog box, click **Yes**.
-

Assigning an Organization to a Locale

Procedure

- Step 1** Choose **Administration > Access Control > Locales > locale**.
 - Step 2** Click **Assign Organization**.
 - Step 3** In the Assign Organization dialog box:
 - a) Expand root to view the available organizations.
 - b) Check the check boxes for the organizations you want to add to the locale.
 - Step 4** Click **OK** in the open dialog boxes, then click **Save** to save the locale.
-

Deleting an Organization from a Locale

Procedure

- Step 1** Choose **Administration > Access Control > Locales > locale**.
 - Step 2** In the content pane, click the **General** tab.
 - Step 3** In the Assigned Organizations area, select the organization you want to delete, then click **Delete Organization**.
 - Step 4** When prompted, confirm the deletion.
 - Step 5** Click **Save**.
-

Configuring Locally Authenticated User Accounts

Creating a User Account

Procedure

- Step 1** Choose **Administration > Access Control > Locally Authenticated Users**.
- Step 2** Click **Create Locally Authenticated Users**.
- Step 3** In the Properties area, complete the following fields:

| Field | Description |
|-------------|--|
| Login ID | <p>Login name.</p> <p>This name must be unique and meet the following guidelines and restrictions for Prime Network Services Controller user accounts:</p> <ul style="list-style-type: none"> • The login ID can be between 1 and 32 characters, including the following: <ul style="list-style-type: none"> ◦ Any alphanumeric character ◦ Underscore (_) ◦ Dash (-) ◦ At symbol (@) • The user name for each user account cannot be all-numeric. • The user name cannot start with a number. <p>After you save the user name, it cannot be changed. You must delete the user account and create a new one.</p> |
| Description | User description. |
| First Name | User first name. This field can contain up to 32 characters. |
| Last Name | User last name. This field can contain up to 32 characters. |
| Email | User email address. |
| Phone | User telephone number. |

| Field | Description |
|------------------|---|
| Password | <p>Password associated with this account.</p> <p>For maximum security, each password must be strong. If the Password Strength Check check box is checked, the system rejects any password that does not meet the following requirements:</p> <ul style="list-style-type: none"> • Contains a minimum of eight characters • Contains at least three of the following: <ul style="list-style-type: none"> ◦ Lowercase letters ◦ Uppercase letters ◦ Digits ◦ Special characters • Does not contain a character that is repeated more than three times consecutively, such as aaabbb. • Is not the user name or the reverse of the user name. • Passes a password dictionary check. For example, the password must not be based on a standard dictionary word. • Does not contain the following symbols: dollar sign (\$), question mark (?), equals sign (=). • The password must not be blank for local user and admin accounts. <p>Note The password strength check box on the Locally Authenticated Users pane can be unchecked, indicating that the password is not required to be strong. It must, however, contain a minimum of eight characters. The password field is a required field, and a user cannot be created without providing a password.</p> |
| Confirm Password | Reenter the password for confirmation purposes. |
| Password Expires | Indicates whether or not password expiration is enabled. Check the check box to enable password expiration. |
| Expiration Date | Available if password expiration is enabled. Date that the password expires. |

Step 4 In the **Roles/Locales** tab area, complete the following fields:

| Field | Description |
|-----------------|---|
| Assigned Roles | Check the applicable check boxes to assign one or more roles to the user: <ul style="list-style-type: none"> • aaa • admin • intercloud-infra • intercloud-server • network • operations • read-only |
| Assigned Locale | Check the applicable check boxes to assign one or more locales to the user. |

Step 5 In the **SSH** tab area, complete the following fields:

| Field | Description |
|----------|--|
| Key | SSH key. If you choose the Key radio button, the SSH Data field is displayed. |
| Password | SSH password. |
| SSH Data | Available if Key is selected. Enter the SSH public key. |

Step 6 Click **OK**.

Changing the Locales or Roles Assigned to a Locally Authenticated User

Procedure

-
- Step 1** Choose **Administration > Access Control > Locally Authenticated Users > user**.
- Step 2** In the General tab, click the **Roles/Locales** tab.
- Step 3** Check or uncheck the appropriate check boxes to assign or remove a locale or role.
- Step 4** Click **Save**.
-

Monitoring User Sessions

You can monitor sessions for both locally and remotely authenticated users.

Procedure

-
- Step 1** Choose **Administration > Access Control**, then choose one of the following:
- **Locally Authenticated Users > user**.
 - **Remotely Authenticated Users > user**.
- Step 2** Click the **Sessions** tab to view the user session.

| Field | Description |
|---------------|---|
| Host | IP address from which the user is logged in. |
| Login Time | Date and time the session started. |
| UI | User interface for this session: <ul style="list-style-type: none"> • web—GUI login • shell—CLI login • ep—End point |
| Terminal Type | Kind of terminal through which the user is logged in. |



Configuring Trusted Points

This section includes the following topics:

- [Trusted Points, page 35](#)
- [Configuring Trusted Points, page 35](#)

Trusted Points

When setting up LDAP over Secure Sockets Layer (SSL) protocol for Prime Network Services Controller user authentication, you need to create a trusted point for each LDAP server. The certificate in the trusted point can be any one of the following:

- The certificate of the certificate authority (CA) that issued the LDAP server certificate.
- If the CAs are organized in a hierarchy, the certificate of any of the CAs in the hierarchy.
- The certificate of the LDAP server.

Configuring Trusted Points

Creating a Trusted Point

Procedure

- Step 1** Choose **Administration > Access Control > Trusted Point**.
- Step 2** Click **Create Trusted Point**.
- Step 3** In the Create Trusted Point dialog box, complete the following fields, then click **OK**.

| Field | Description |
|-------|---------------------|
| Name | Trusted point name. |

| Field | Description |
|-------------------|---|
| Certificate Chain | Certificate information for this trusted point. |

Editing a Trusted Point

Procedure

- Step 1** Choose **Administration > Access Control > Trusted Point**.
 - Step 2** In the content pane, choose the required trusted point, then click **Edit**.
 - Step 3** In the Edit dialog box, modify the certificate chain as appropriate, then click **OK**.
The Name and Fingerprint fields cannot be modified.
-

Deleting a Trusted Point

Procedure

- Step 1** Choose **Administration > Access Control > Trusted Point**.
 - Step 2** In the content pane, select the trusted point you want to delete, then click **Delete**.
 - Step 3** When prompted, confirm the deletion.
-



Configuring System Profiles

This section includes the following topics:

- [Profiles, page 37](#)
- [Policies in System Profiles, page 37](#)
- [Configuring Policies, page 38](#)
- [Configuring the Default Profile, page 58](#)

Profiles

Prime Network Services Controller profiles are configurable.

Prime Network Services Controller provides default profiles. Default profiles are system generated and can be modified, but they cannot be deleted. You can add new policies to a profile, including DNS and NTP policies, or assign existing policies to the a profile.

The Prime Network Services Controller profile includes the DNS domain name that specified at boot configuration. That domain is displayed in the Prime Network Services Controller instance. New DNS domains cannot be created. However, the domain name description can be modified.

Prime Network Services Controller does not support the creation of additional Prime Network Services Controller profiles.

Policies in System Profiles

You can create multiple policies and assign them to the System profile. Policies for the System profile are created and deleted on the **System Profile** tab. Policies can be assigned to the System profile. System profile uses name resolution to resolve policy assignments. For details, see [Name Resolution in a Multi-Tenant Environment, on page 70](#).

The following policies created under root only, in the Device Policies area, will be visible in the System profile:

- Core file
- Fault

- Log file
- Syslog

Policies created under root are visible to both the System profile and the Device profile.

DNS server, NTP server and domain names can be assigned as inline policies. A time zone setting can also be assigned to the profile.

When the system boots up, the following policies already have existing default policies:

- Fault policy
- Log File
- Syslog policy

The default policies cannot be deleted but may be modified.

Configuring Policies

Configuring a Core File Policy

Adding a Core File Policy to the System Profile

Procedure

- Step 1** Choose **Administration > System Profile > root > Policies > Core File**.
- Step 2** In the General tab, click **Add Core File Policy**.
- Step 3** In the Add Core File Policy dialog box, complete the following fields, then click **OK**:

| Field | Description |
|---------------------|--|
| Name | Core file policy name, containing 1 to 32 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.). You cannot change the name after the policy has been saved. |
| Description | Brief policy description, containing 1 to 256 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.). |
| Admin State | Indicate whether the administrative state of the policy is to be enabled or disabled. |
| Hostname/IP Address | Hostname or IP address to use for this policy. If you use a hostname rather than an IP address, you must configure a DNS server in Prime Network Services Controller. |

| Field | Description |
|----------|---|
| Port | Port number for sending the core dump file. This field is read-only for InterCloud policies. |
| Protocol | Protocol for exporting the core dump file (tftp only). |
| Path | Path to use when storing the core dump file on a remote system. The default path is /tftpboot; for example, /tftpboot/test, where <i>test</i> is the subfolder. |

Editing a Core File Policy for a System Profile

Procedure

- Step 1** Choose **Administration > System Profile > root > Policies > Core File**.
- Step 2** In the General tab, click the core file policy you want to edit, then click **Edit**.
- Step 3** In the Edit dialog box, modify the following fields as appropriate, then click **OK**:

| Field | Description |
|-------------|--|
| Name | Name of the core file policy (read-only). |
| Description | Brief policy description. |
| Admin State | Administrative status of the policy: enabled or disabled. |
| Hostname | Hostname or IP address. Note If you use a hostname, you must configure a DNS server. |
| Port | Port number to use when exporting the core dump file. This field is read-only for InterCloud policies. |
| Protocol | Protocol used to export the core dump file (tftp only). |
| Path | Path to use when storing the core dump file on the remote system. The default path is /tftpboot. To specify a subfolder under tftpboot, use the format /tftpboot/ <i>folder</i> where <i>folder</i> is the subfolder. |

Deleting a Core File Policy from the System Profile

Procedure

-
- Step 1** Choose **Administration > System Profile > root > Policies > Core File**.
 - Step 2** In the General tab, click the core file policy you want to delete, then click **Delete**.
 - Step 3** When prompted, confirm the deletion.
-

Configuring a Fault Policy

Adding a Fault Policy to the System Profile

When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

-
- Step 1** Choose **Administration > System Profile > root > Policies > Fault**.
 - Step 2** In the General tab, click **Add Fault Policy**.
 - Step 3** In the Add Fault Policy dialog box, provide the information as described in the following table, then click **OK**:

| Field | Description |
|-------------|---|
| Name | Fault policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created. |
| Description | Brief policy description. |

| Field | Description |
|---------------------------------|---|
| Flapping Interval | <p>Length of time (in hours, minutes, and seconds) that must elapse before the system allows a fault to change its state.</p> <p>Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change.</p> <p>If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the Clear Faults Retention Action field.</p> <p>The default flapping interval is ten seconds.</p> |
| Clear Faults Retention Action | <p>Action to be taken when faults are cleared:</p> <ul style="list-style-type: none"> • retain—Retain the cleared faults. • delete—Delete fault messages as soon as they are marked as cleared. |
| Clear Faults Retention Interval | <p>How long the system is to retain cleared fault messages:</p> <ul style="list-style-type: none"> • Forever—The system retains all cleared fault messages regardless of their age. • Other—The system retains cleared fault message for a specified the length of time. In the spinbox that is displayed when you select this option, enter the length of time (in days, hours, minutes, and seconds) that the system is to retain cleared fault messages. |

Editing a Fault Policy for a System Profile



Note

When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Administration > System Profile > root > Policies > Fault**.

Step 2 In the General tab, select the fault policy you want to edit, then click **Edit**.

Step 3 In the Edit Fault Policy dialog box, modify the fields as needed by using the information in the following table, then click **OK**.

| Field | Description |
|---------------------------------|--|
| Name | Policy name (read-only). |
| Description | Brief policy description. |
| Flapping Interval | <p>Length of time (in hours, minutes, and seconds) that must elapse before the system allows a fault to change its state.</p> <p>Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change.</p> <p>If the condition recurs during the flapping interval, the fault returns to the active state. If the condition does not recur during the flapping interval, the fault is cleared. The next action depends on the setting in the Clear Faults Retention Action field.</p> <p>The default flapping interval is ten seconds.</p> |
| Clear Faults Retention Action | <p>Available fault retention actions:</p> <ul style="list-style-type: none"> • retain—The system retains fault messages. • delete—The system deletes fault messages when they are marked as cleared. |
| Clear Faults Retention Interval | <p>How long the system is to retain cleared fault messages:</p> <ul style="list-style-type: none"> • Forever—The system retains all cleared fault messages regardless of their age. • Other—The system retains cleared fault message for a specified the length of time. In the spinbox that is displayed when you select this option, enter the length of time (in days, hours, minutes, and seconds) that the system is to retain cleared fault messages. |

Deleting a Fault Policy from the System Profile



Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

- Step 1** Choose **Administration > System Profile > root > Policies > Fault**.
- Step 2** In the General tab, select the fault policy you want to delete, then click **Delete**.
- Step 3** When prompted, confirm the deletion.

Configuring a Logging Policy

Adding a Logging Policy to the System Profile

When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

- Step 1** Choose **Administration > System Profile > root > Policies > Log File**.
- Step 2** In the General tab, click **Add Logging Policy**.
- Step 3** In the Add Logging Policy dialog box, complete the following fields:

| Field | Description |
|-------------|---|
| Name | Logging policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created. |
| Description | Brief policy description. |

| Field | Description |
|--------------------|--|
| Log Level | <p>One of the following logging severity levels:</p> <ul style="list-style-type: none"> • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical <p>The default log level is info.</p> |
| Backup Files Count | <p>Number of backup files that are filled before they are overwritten.</p> <p>The range is 1 to 9 files, with a default of 2 files.</p> |
| File Size (bytes) | <p>Backup file size.</p> <p>The range is 1 MB to 100 MB with a default of 5 MB.</p> |

Step 4 Click **OK**.

Editing a Logging Policy for System Profile



Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

- Step 1** Choose **Administration > System Profile > root > Policies > Log File**.
- Step 2** In General tab, select the logging policy that you want to edit, then click **Edit**.
- Step 3** In the Edit Log File Policy dialog box, modify the information as required by using the information in the following table, then click **OK**.

| Field | Description |
|--------------------|---|
| Name | Logging policy name (read-only). |
| Description | Brief policy description. |
| Log Level | <p>One of the following logging levels:</p> <ul style="list-style-type: none"> • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical <p>The default log level is info.</p> |
| Backup Files Count | <p>Number of backup files that are filled before they are overwritten.</p> <p>The range is 1 to 9 files, with a default of 2 files.</p> |
| File Size (bytes) | <p>Backup file size.</p> <p>The range is 1 MB to 100 MB with a default of 5 MB.</p> |

Deleting a Logging Policy from the System Profile



Note

When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

-
- Step 1** Choose **Administration > System Profile > root > Policies > Log File**.
- Step 2** In the General tab, select the logging policy you want to delete, then click **Delete**.
- Step 3** When prompted, confirm the deletion.
-

Configuring a Syslog Policy

Adding a Syslog Policy to the System Profile

When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

The syslog message settings that you configure for the System profile apply to Prime Network Services Controller syslog messages only. These settings do not affect other non-Prime Network Services Controller syslog messages.

Procedure

-
- Step 1** Choose **Administration > System Profile > root > Policies > Syslog**.
- Step 2** In the General tab, click **Add Syslog Policy**.
- Step 3** In the Add Syslog Policy dialog box, provide the information as described in the following table, then click **OK**.

| Field | Description |
|--------------------------|--|
| General Tab | |
| Name | Policy name. |
| Description | Brief policy description. |
| Use Emblem Format | Check the check box to use the EMBLEM format for syslog messages. This option is supported for ASA 1000Vs. It is not supported for VSGs or InterCloud policies. |
| Continue if Host is Down | Check the check box to continue logging if the syslog server is down. This option is supported for ASA 1000Vs. It is not supported for VSGs or InterCloud policies. |
| Servers Tab | |

| Field | Description |
|-------------------------------|--|
| Add Syslog Server | Click to add a new syslog server. |
| Syslog Servers table | List of configured syslog servers. |
| Local Destinations Tab | |
| Console area | <ul style="list-style-type: none"> • Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: alert, critical, or emergency. <p>If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.</p> |
| Monitor area | <ul style="list-style-type: none"> • Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. <p>If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.</p> |

| Field | Description |
|-----------|---|
| File area | <ul style="list-style-type: none">• Admin State—Administrative state of the policy: disabled or enabled.• Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.• File Name—Name of the file to which messages are logged.• Size (bytes)—Maximum size, in bytes, that the file can reach before the system begins to overwrite the messages. |

| Field | Description |
|-------------|--|
| Buffer area | <p>Buffer options are not available for InterCloud policies.</p> <ul style="list-style-type: none"> • Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • Buffer Size (Bytes)—In bytes, the size of the buffer for syslog messages. • Wrap to Flash—Indicates whether or not the buffer contents are saved to flash memory when the buffer wraps (becomes full). Check the check box to save the contents to flash memory if the buffer wraps. • Max File Size in Flash (KB)—Maximum size, in kilobytes, that can be used by the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. • Min Free Flash Size (KB)—Minimum size, in kilobytes, that is allocated for the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. |

Editing a Syslog Policy for the System Profile

The syslog message settings that you configure for the System profile apply to Prime Network Services Controller syslog messages only. These settings do not affect other non-Prime Network Services Controller syslog messages.



Note

When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Administration > System Profile > root > Policies > Syslog**.

Step 2 In the General tab, select the syslog policy you want to edit, then click **Edit**.

Step 3 In the Edit Syslog Policy dialog box, update the information as required by using the information in the following table, then click **OK**.

| Field | Description |
|-------------------------------|--|
| General Tab | |
| Name | Policy name. |
| Description | Brief policy description. |
| Use Emblem Format | Check the check box to use the EMBLEM format for syslog messages. This option is supported for ASA 1000Vs. It is not supported for VSGs or InterCloud policies. |
| Continue if Host is Down | Check the check box to continue logging if the syslog server is down. This option is supported for ASA 1000Vs. It is not supported for VSGs or InterCloud policies. |
| Servers Tab | |
| Add Syslog Server | Click to add a new syslog server. |
| Syslog Servers table | List of configured syslog servers. |
| Local Destinations Tab | |
| Console area | <ul style="list-style-type: none"> • Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: alert, critical, or emergency. <p>If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.</p> |

| Field | Description |
|--------------|---|
| Monitor area | <ul style="list-style-type: none"> • Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. <p>If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.</p> |
| File area | <ul style="list-style-type: none"> • Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. <p>If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.</p> <ul style="list-style-type: none"> • File Name—Name of the file to which messages are logged. • Size (bytes)—Maximum size, in bytes, that the file can reach before the system begins to overwrite the messages. |

| Field | Description |
|-------------|--|
| Buffer area | <p>Buffer options are not available for InterCloud policies.</p> <ul style="list-style-type: none"> • Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • Buffer Size (Bytes)—In bytes, the size of the buffer for syslog messages. • Wrap to Flash—Indicates whether or not the buffer contents are saved to flash memory when the buffer wraps (becomes full). Check the check box to save the contents to flash memory if the buffer wraps. • Max File Size in Flash (KB)—Maximum size, in kilobytes, that can be used by the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. • Min Free Flash Size (KB)—Minimum size, in kilobytes, that is allocated for the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. |

Deleting a Syslog Policy from a System Profile



Note

When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

- Step 1** Choose **Administration > System Profile > root > Policies > Syslog**.
- Step 2** In the General tab, click the syslog policy you want to delete, then click **Delete**.
- Step 3** When prompted, confirm the deletion.

Adding a Syslog Server to the System Profile

This procedure assumes that you have already created a syslog policy for a Prime Network Services Controller profile. For information on creating a syslog policy for a Prime Network Services Controller profile, see [Adding a Syslog Policy to the System Profile, on page 46](#).

Procedure

- Step 1** Choose **Administration > System Profile > root > Policies > Syslog** syslog-policy.
- Step 2** In the Servers tab, click **Add Syslog Server**.
- Step 3** In the Add Syslog Server dialog box, provide the information as described in the following table, then click **OK**:

| Field | Description |
|---------------------|--|
| Server Type | One of the following server types: <ul style="list-style-type: none"> • primary • secondary • tertiary |
| Hostname/IP Address | Hostname or IP address where the syslog file resides. Note If you use a hostname, you must configure a DNS server. |
| Severity | One of the following severity levels: <ul style="list-style-type: none"> • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • information (6) • debugging (7) |

| Field | Description |
|---------------------|--|
| Forwarding Facility | One of the following forwarding facilities: <ul style="list-style-type: none"> • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp |
| Admin State | Administrative state of the server: disabled or enabled. |
| Port | Port to use to send data to the syslog server. The default port selection is 514 for UDP. This option is not available for InterCloud policies. |
| Protocol | Protocol to use: TCP or UDP (default). This option is not available for InterCloud policies. |

| Field | Description |
|------------------------------|---|
| Use Transport Layer Security | Check the check box to use Transport Layer Security. This option is available only for TCP. This option is not available for InterCloud policies. |
| Server Interface | Interface to use to access the syslog server. |

Editing a Syslog Server for the System Profile

Procedure

- Step 1** Choose **Administration > System Profile > root > Policies > Syslog**.
- Step 2** In the General tab, select the syslog policy with the syslog server that you want to edit, then click **Edit**.
- Step 3** In the Edit Syslog Policy dialog box, click the **Servers** tab.
- Step 4** Select the syslog server that you want to edit, then click **Edit**.
- Step 5** In the Edit Syslog Server dialog box, edit the information as required, using the information in the following table, and then click **OK**:

| Field | Description |
|---------------------|--|
| Server Type | One of the following server types: primary, secondary, or tertiary. |
| Hostname/IP Address | Hostname or IP address where the syslog file resides. Note If you use a hostname, you must configure a DNS server. |

| Field | Description |
|---------------------|--|
| Severity | One of the following severity levels: <ul style="list-style-type: none"> • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • information (6) • debugging (7) |
| Forwarding Facility | One of the following forwarding facilities: <ul style="list-style-type: none"> • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp |

| Field | Description |
|------------------------------|--|
| Admin State | Administrative state of the server: enabled or disabled. |
| Port | Port to use to send data to the syslog server. The default port selection is 514 for UDP. |
| Protocol | Protocol to use: TCP or UDP (default). |
| Use Transport Layer Security | Check the check box to use Transport Layer Security. This option is available only for TCP. |
| Server Interface | Interface to use to access the syslog server. If the syslog server is for a device instead of the System profile, keep the following in mind: <ul style="list-style-type: none"> • This option applies to ASA 1000V only. Enter the data interface name specify in the edge firewall. • Use the device CLI to configure a route through the management interface. |

Deleting a Syslog Server from a System Profile

Procedure

- Step 1** Choose **Administration > System Profile > root > Policies > Syslog**.
- Step 2** In the General tab, select the syslog policy with the server you want to delete, then click **Edit**.
- Step 3** In the Edit Syslog Policy dialog box, click the **Servers** tab.
- Step 4** In the Servers table, select the syslog server you want to delete, then click **Delete**.
- Step 5** When prompted, confirm the deletion.
- Step 6** Click **OK** or **Apply** to apply the change to the syslog policy.

Configuring the Default Profile

Editing the System Default Profile

Procedure

Step 1 Choose **Administration > System Profile > root > Profile > default**.

Step 2 In the General tab, update the information as required:

| Field | Description |
|-------------|--|
| Name | Default profile name (read-only). |
| Description | Brief profile description. |
| Time Zone | Available time zones. The default time zone is UTC. |

Step 3 In the Policy tab, update the information as required:

| Field | Description |
|--------------------|--|
| DNS Servers | |
| Add DNS Server | Click to add a new DNS server. |
| Delete | Deletes the DNS server selected in the DNS Servers table. |
| Up and down arrows | Changes the priority of the selected DNS server. Prime Network Services Controller uses the DNS servers in the order in which they appear in the table. |
| DNS Servers table | Identifies the DNS servers configured in the system. |
| NTP Servers | |
| Add NTP Server | Click to add a new NTP server. |
| Delete | Deletes the NTP server selected in the NTP Servers table. |
| Up and down arrows | Changes the priority of the selected NTP server. Prime Network Services Controller uses the NTP servers in the order in which they appear in the table. |

| Field | Description |
|----------------------|--|
| NTP Servers table | Identifies the NTP servers configured in the system. |
| DNS Domains | |
| Edit | <p>Edits the DNS domain selected in the DNS Domains table. The default DNS domain cannot be deleted.</p> <p>Caution Changing the DNS domain will cause a loss of connectivity that results in an error message, your session closing, and then the display of a new Prime Network Services Controller certificate. This situation occurs when the Prime Network Services Controller hostname, Prime Network Services Controller domain name, or both have changed. The VM Manager Extension file must be exported again and installed on vCenter. To continue, accept the Prime Network Services Controller certificate and log into Prime Network Services Controller again.</p> |
| DNS Domains | Identifies the default DNS domain name and domain configured in the system. |
| Other Options | |
| Syslog | <p>The syslog policies associated with this profile can be selected, added, or edited.</p> <p>Click the Resolved Policy field to review or modify the specified policy.</p> |
| Fault | <p>The fault policies associated with this profile can be selected, added, or edited.</p> <p>Click the Resolved Policy field to review or modify the specified policy.</p> |
| Core File | <p>The core file policies associated with this profile can be selected, added, or edited.</p> <p>Click the Resolved Policy field to review or modify the specified policy.</p> |
| Log File | <p>The log file policies associated with this profile can be selected, added, or edited.</p> <p>Click the Resolved Policy field to review or modify the specified policy.</p> |

Step 4 Click **Save**.

Configuring a DNS Server

Adding a DNS Server

You can specify a maximum of four DNS servers for the System profile. Use the up and down arrows to arrange the servers from highest to lowest priority, with the highest priority server at the top of the list.

Procedure

- Step 1** Choose **Administration > System Profile > root > Profile > default**.
 - Step 2** Click the **Policy** tab.
 - Step 3** In the **DNS Servers** area, click **Add DNS Server**.
 - Step 4** In the Add DNS Server dialog box, enter the DNS server IP address, then click **OK**.
 - Step 5** Click **Save**.
-

Deleting a DNS Server

Procedure

- Step 1** Choose **Administration > System Profile > root > Profile > default**.
 - Step 2** Click the **Policy** tab.
 - Step 3** In the **DNS Servers** area, select the DNS server you want to delete, then click **Delete**.
 - Step 4** When prompted, confirm the deletion.
 - Step 5** Click **Save** to save your changes.
-

Configuring an NTP Server

Adding an NTP Server

You can specify a maximum of four NTP servers for the System profile. Use the up and down arrows to arrange the servers from highest to lowest priority, with the highest priority server at the top of the list.

Procedure

- Step 1** Choose **Administration > System Profile > root > Profile > default**.
 - Step 2** In the Policy tab, click **Add NTP Server**.
 - Step 3** In the Add NTP server dialog box, enter the hostname or IP address of the NTP server, then click **OK**.
 - Step 4** Click **Save**.
-

Deleting an NTP Server

Procedure

- Step 1** Choose **Administration > System Profile > root > Profile > default**.
 - Step 2** Click the **Policy** tab.
 - Step 3** In the NTP Servers area, click the server that you want to delete, then click **Delete**.
 - Step 4** When prompted, confirm the deletion.
 - Step 5** Click **Save**.
-

Configuring a DNS Domain

Editing a DNS Domain

**Caution**

Changing the DNS domain will cause a loss of connectivity that results in an error message, your session closing, and then the display of a new Prime Network Services Controller certificate. This situation occurs when the Prime Network Services Controller hostname, Prime Network Services Controller domain name, or both have changed. The VM Manager Extension file must be exported again and installed on vCenter. To continue, accept the Prime Network Services Controller certificate and log into Prime Network Services Controller again.

Procedure

- Step 1** Choose **Administration > System Profile > root > Profile > default**.
 - Step 2** Click the **Policy** tab.
 - Step 3** In the DNS Domains table, select the domain that you want to edit, then click **Edit**.
 - Step 4** In the Edit DNS Domains dialog box, edit the Domain Name field as required, then click **OK**.
 - Step 5** Click **Save**.
-



Configuring VM Managers

This section includes the following topics:

- [VM Manager Overview, page 63](#)
- [Adding a VM Manager, page 63](#)
- [Editing a VM Manager, page 65](#)
- [Deleting a VM Manager, page 67](#)

VM Manager Overview

Prime Network Services Controller connects to VM management software on port 80. A VM Manager extension file is required to establish a connection between Prime Network Services Controller and the VM management software. The extension file is exported from Prime Network Services Controller and installed as a plugin on all VM Manager servers to which you want to connect.

You can configure a VM Manager in Prime Network Services Controller under Administration, Resource Management, or InterCloud Management. All VM Managers that you add to Prime Network Services Controller are displayed in all three locations.



Note

In VMware, a VM can be nested within resources. However, when you view the VM properties in Prime Network Services Controller, only the higher level resource is displayed. For example, you can add a VM that is part of a resource pool that resides in a virtual application (vApp). When you view this VM in Prime Network Services Controller, only the vApp name is displayed and not that of the resource pool.

Adding a VM Manager

Adding a VM Manager to Prime Network Services Controller establishes a connection between the selected VM and Prime Network Services Controller and enables you to take advantage of other Prime Network Services Controller features, such as InterCloud Management.

Before You Begin

A VM Manager extension file is required to establish a secure connection between the VM management software and Prime Network Services Controller. Export the VM Manager extension file by clicking **Export vCenter Extension**, and installing the file as a plugin on all VM management servers to which you want to connect.

You can find the Export vCenter Extension option in the following locations:

- **Resource Management > Resources > Virtual Machines > VM Managers.**
- **InterCloud Management > Enterprise > VM Managers.**
- **Administration > VM Managers > VM Managers.**



Note

If you use Internet Explorer, do one of the following to ensure that you can download the extension file:

- Open Internet Explorer in Administrator mode.
- After starting Internet Explorer, choose **Tools > Internet Options > Security**, and uncheck the **Enable Protected Mode** check box.

For detailed information on configuring Prime Network Services Controller connectivity with the VM management software, see the *Cisco Prime Network Services Controller 3.0 Quick Start Guide*, available at http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html.

Procedure

Step 1 Choose any of the following:

- **Resource Management > Resources > Virtual Machines > VM Managers**
- **InterCloud Management > Enterprise > VM Managers**
- **Administration > VM Managers > VM Managers**

Step 2 Click **Add VM Manager**.

Step 3 In the Add VM Manager dialog box, supply the following information, then click **OK**:

| Field | Description |
|---------------------|---|
| Name | VM Manager name, containing 2 to 256 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change the name after it is saved. |
| Description | VM Manager description, containing 1 to 256 characters. The description can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). |
| Hostname/IP Address | Hostname or IP address of the VM Manager. |

| Field | Description |
|-------------|---|
| Port Number | Port to use for communications with the VM Manager. |

Editing a VM Manager

When you edit a VM Manager, you can change its administrative state as long as the VM Manager has the appropriate operational state:

- To change the administrative state to enabled, the operational state must be down.
- To change the administrative state to disabled, the operational state must be up.

If your request to change the administrative state fails, resubmit the request when the system has the correct operational state.

Procedure

Step 1 Choose one of the following:

- **Resource Management > Resources > Virtual Machines > VM Managers**
- **InterCloud Management > Enterprise > VM Managers**
- **Administration > VM Managers > VM Managers**

Step 2 In the VM Managers tab, select the VM Manager you want to edit, then click **Edit**.

Step 3 In the Edit VM Manager dialog box, edit the information as required, then click **OK**.

| Field | Description |
|---------------------|---|
| Name | VM Manager name (read-only). |
| Description | Description of the VM Manager. |
| Hostname/IP Address | VM Manager hostname or IP address (read-only). |
| Port Number | Port to use for communications with the VM Manager (read-only). |

| Field | Description |
|--------------------------|---|
| Admin State | <p>One of the following administrative states for the VM Manager:</p> <ul style="list-style-type: none"> • enable—When a vCenter is added to Prime Network Services Controller with the administrative state of enable, the system fetches all VM inventory from vCenter. Any changes that occur to the VM on vCenter are also fetched. • disable—When a vCenter is added to Prime Network Services Controller with the administrative state of disable, the system displays all discovered VMs from vCenter. Any changes that occur to the VMs on the vCenter are not fetched. The changes will be fetched by Prime Network Services Controller when the admin state is changed to enable. |
| Type | VM Manager vendor (read-only). |
| Version | VM Manager version (read-only). |
| Operational State | <p>One of the following operational states (read-only):</p> <ul style="list-style-type: none"> • up • unreachable • bad-credentials • comm-err • admin-down • unknown |
| Operational State Reason | Provides the reason for the operational state if the operational state is anything other than <i>up</i> (read-only). |

Deleting a VM Manager

Procedure

- Step 1** Choose one of the following:
- **Resource Management > Resources > Virtual Machines > VM Managers**
 - **InterCloud Management > Enterprise > VM Managers**
 - **Administration > VM Managers > VM Managers**
- Step 2** Select the VM Manager that you want to delete, then click **Delete**.
- Step 3** When prompted, confirm the deletion.
-



Configuring Tenants

This section includes the following topics:

- [Tenant Management, page 69](#)
- [Configuring Tenants, page 71](#)
- [Configuring Virtual Data Centers, page 72](#)
- [Configuring Applications, page 73](#)
- [Configuring Tiers, page 75](#)

Tenant Management

Tenant Management and Multi-Tenant Environments

Prime Network Services Controller provides the ability to support multi-tenant environments. A multi-tenant environment enables the division of large physical infrastructures into logical entities called organizations. As a result, you can achieve logical isolation between organizations without providing a dedicated physical infrastructure for each organization.

The administrator can assign unique resources to each tenant through the related organization in the multi-tenant environment. These resources can include different policies, pools, device profiles, firewalls, and so on. The administrator can use locales to assign or restrict user privileges and roles by organization if access to certain organizations needs to be restricted.

Prime Network Services Controller provides a strict organizational hierarchy as follows:

- 1 Root
- 2 Tenant
- 3 Virtual Data Center
- 4 Application
- 5 Tier

The root can have multiple tenants. Each tenant can have multiple data centers. Each data center can have multiple applications, and each application can have multiple tiers.

The policies and pools created at the root level are systemwide and are available to all organizations in the system. However, any policies and pools created in an organization below the root level are available only to those resources that are below that organization in the same hierarchy.

For example, if a system has tenants named Company A and Company B, Company A cannot use any policies created in the Company B organization. Company B cannot access any policies created in the Company A organization. However, both Company A and Company B can use policies and pools in the root organization.

Name Resolution in a Multi-Tenant Environment

In a multi-tenant environment, Prime Network Services Controller uses the hierarchy of an organization to resolve the names of policies and resource pools. The steps Prime Network Services Controller takes to resolve the names of policies and resource pools are as follows:

- 1 Prime Network Services Controller checks the policies and pools for the specified name within an organization assigned to the device profile or security policy.
- 2 If the policy or pool is found, Prime Network Services Controller uses that policy or pool.
- 3 If the policy or pool does not contain available resources at the local level, Prime Network Services Controller moves up the hierarchy to the parent organization and checks for a policy with the specified name. Prime Network Services Controller repeats this step until the search reaches the root organization.



Note

The object name reference resolution takes an object name and resolves an object from an organization container to the object with the same name which is closest in the tree up to the root of the tree. If an object with the specified name is not found, Prime Network Services Controller uses a corresponding default object. For example, there is an SNMP policy under data center called MySNMP, and there is an SNMP policy in the tenant in the same tree that is also MySNMP. In this case, the user cannot explicitly select the MySNMP policy under the tenant. If the user wants to select the SNMP policy under the tenant, they must provide a unique name for the object in the given tree.

- 4 If the search reaches the root organization and an assigned policy or pool is not found, Prime Network Services Controller looks for a default policy or pool starting at the current level and going up the chain to the root level. If a default policy or pool is found, Prime Network Services Controller uses it. If a policy is not available, a fault is generated.

Configuring Tenants

Creating a Tenant

Procedure

-
- Step 1** Choose **Tenant Management > root > Create Tenant**.
- Step 2** In the Create Tenant dialog box, complete the following fields, then click **OK**:

| Field | Description |
|-------------|---|
| Name | Tenant name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created. |
| Description | Brief tenant description. This field can contain between 1 and 256 characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. |

Editing a Tenant

Procedure

-
- Step 1** Choose **Tenant Management > root > tenant**.
- Step 2** In the Sub-Elements tab, select the tenant you want to edit, then click **Edit**.
- Step 3** In the **Edit Tenant** dialog box, modify description, then click **OK**. The Level field identifies the tenant's level in the hierarchy and is read-only.
-

Deleting a Tenant



Note When you delete an organization (such as a tenant, virtual data center, application, or tier), all data contained under the organization is deleted, including sub organizations, compute firewalls, edge firewalls, resource pools, and policies.

Procedure

- Step 1** Choose **Tenant Management > root > Sub-Elements**.
- Step 2** Select the tenant you want to delete, then click **Delete Tenant**.
- Step 3** When prompted, confirm the deletion.

Configuring Virtual Data Centers

Creating a Virtual Data Center

Procedure

- Step 1** Choose **Tenant Management > root > tenant**, where *tenant* is the location for the new virtual data center.
- Step 2** In the General tab, click **Create Virtual Data Center**.
- Step 3** In the Create Virtual Data Center dialog box, complete the following fields, then click **OK**:

| Field | Description |
|-------------|--|
| Name | VDC name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created. |
| Description | Brief VDC description. This field can contain between 1 and 256 characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. |

Editing a Virtual Data Center

Procedure

- Step 1** Choose **Tenant Management > root > tenant > Sub-Elements**.
 - Step 2** In the Sub-Elements tab, select the virtual data center you want to edit, then click **Edit**.
 - Step 3** In the Edit Virtual Data Center dialog box, modify the description, then click **OK**. The Level field indicates the level of the virtual data center in the hierarchy, and is read-only.
-

Deleting a Virtual Data Center



- Note** When you delete a virtual data center, all data contained under the virtual data center is deleted, including sub-organizations, firewalls, resource pools, and policies.
-

Procedure

- Step 1** Choose **Tenant Management > root > tenant > Sub-Elements**, where *tenant* is the tenant with the virtual data center that you want to delete.
 - Step 2** Select the virtual data center that you want to delete, then click **Delete Virtual Data Center**.
 - Step 3** When prompted, confirm the deletion.
-

Configuring Applications

Creating an Application

Procedure

- Step 1** Choose **Tenant Management > root > tenant > vdc** where *vdc* is the location for the new application.
- Step 2** In the General tab, click **Create Application**.
- Step 3** In the Create Application dialog box, complete the following fields, then click **OK**:

| Field | Description |
|-------------|--|
| Name | Application name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created. |
| Description | Brief application description. This field can be between 1 and 256 characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. |

Editing an Application

Procedure

-
- Step 1** Choose **Tenant Management > root > tenant > virtual-data-center > Sub-Elements**, where *virtual-data-center* is the virtual data center with the application that you want to edit.
 - Step 2** Select the application that you want to edit, then click **Edit**.
 - Step 3** In the Edit Application dialog box, modify the description as required, then click **OK**. The Level field identifies the level of the application in the hierarchy, and is read-only.
-

Deleting an Application



Note When you delete an application, all data contained under the application is deleted, including sub-organizations, firewalls, resource pools, and policies.

Procedure

-
- Step 1** Choose **Tenant Management > root > tenant > virtual-data-center > Sub-Elements**, where *virtual-data-center* is the virtual data center with the application you want to delete.
 - Step 2** Select the application that you want to delete, then click **Delete Application**.
 - Step 3** When prompted, confirm the deletion.
-

Configuring Tiers

Creating a Tier

Procedure

- Step 1** Choose **Tenant Management** > **root** > *tenant* > *vdc* > *application*, where *application* is the location for the new tier.
- Step 2** In the General tab, click **Create Tier**.
- Step 3** In the Create Tier dialog box, complete the following fields, then click **OK**:

| Field | Description |
|-------------|--|
| Name | The name of the Tier. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created. |
| Description | A description of the Tier. This field can contain between 1 and 256 characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. |

Editing a Tier

Procedure

- Step 1** Choose **Tenant Management** > **root** > *tenant* > *virtual-data-center* > *application* > *tier* where *tier* is the tier you want to edit.
- Step 2** In the Properties tab, modify the description as required, then click **Save**.

Deleting a Tier



Note When you delete a tier, all data contained under it is also deleted, including sub-organizations, firewalls, resource pools, and policies.

Procedure

-
- Step 1** Choose **Tenant Management > root > tenant > Sub-Elements**, where *tenant* contains the tier you want to delete.
 - Step 2** Navigate to the tier you want to delete, select it, then click **Delete Tier**.
 - Step 3** When prompted, confirm the deletion.
-



Configuring InterCloud Resources

This section includes the following topics:

- [InterCloud Resources, page 77](#)
- [InterCloud Configuration Workflow, page 78](#)
- [InterCloud Management User Privileges, page 78](#)
- [Preparing to Configure InterCloud Links and Cloud VMs, page 79](#)
- [Configuring InterCloud Links and Cloud VMs, page 87](#)
- [Managing InterCloud Links, page 107](#)
- [Creating AMI Images from VMs, page 116](#)

InterCloud Resources

Prime Network Services Controller enables you to extend your enterprise data center into a public cloud through the configuration and management of InterCloud resources. InterCloud resources include the following items:

- **Provider account**—Provider accounts enable users to access and take advantage of cloud resources. Public cloud providers generally own and operate the cloud infrastructure, and provide accounts to those who want to use the cloud resources.
- **Virtual Private Clouds (VPCs)**—VPCs are logical groupings of cloud infrastructure components and resources that enable an enterprise data center to extend into a public cloud. A provider account is required to create a VPC.
- **InterCloud links**—InterCloud links are secure connections between an enterprise data center and a public cloud. An InterCloud link includes two virtual gateways: one on the enterprise network and one on the cloud. The gateway on the enterprise network is referred to as the InterCloud extender, and the gateway on the cloud is referred to as the InterCloud switch. A secure Layer 3 tunnel connects the gateways, thereby extending the Layer 2 enterprise network into the cloud.
- **Cloud VMs**—Cloud VMs are VMs that are instantiated within the context of a VPC and InterCloud link on the public cloud. You can create multiple cloud VMs in a single VPC and InterCloud link.

InterCloud Configuration Workflow

The workflow for configuring and managing InterCloud resources includes the following high-level phases and activities:

| Workflow Phase | Activities | Related Topic |
|--------------------|---|---|
| Preparation | <ul style="list-style-type: none"> • Configuring policies, profiles, and address pools. • Downloading the required images. • Obtaining a provider account. | Preparing to Configure InterCloud Links and Cloud VMs, on page 79 |
| Configuration | <ul style="list-style-type: none"> • Creating an InterCloud link. • Placing VM images on the cloud. • Creating VM instances on the cloud. | Configuring InterCloud Links and Cloud VMs, on page 87 |
| Ongoing management | <ul style="list-style-type: none"> • Updating InterCloud links. • Removing InterCloud links. • Monitoring InterCloud status. • Troubleshooting InterCloud issues. | Managing InterCloud Links, on page 107 |
| Customization | Creating AMI files from VMs in your data center. | Creating AMI Images from VMs, on page 116 |

InterCloud Management User Privileges

Prime Network Services Controller provides the following roles and privileges in support of InterCloud management:

| Role | Default Privileges | Description |
|-------------------|---------------------------|---|
| intercloud-infra | InterCloud-Infrastructure | Ability to create and manage the following InterCloud resources: <ul style="list-style-type: none"> • MAC address pools • Cloud provider accounts • InterCloud Agent image • InterCloud Extender and Switch images • InterCloud links • InterCloud Extenders and Switches |
| intercloud-server | InterCloud-Server | Ability to create and manage the following cloud resources: <ul style="list-style-type: none"> • Cloud VMs • Creation or migration of VM templates on clouds • Instantiation of cloud VMs |

Preparing to Configure InterCloud Links and Cloud VMs

Before you can configure an InterCloud link and cloud VMs, you must complete the following activities:

| Activity | Details | Related Topic |
|---|---|---|
| Adding a VM Manager | — | Adding a VM Manager, on page 63 |
| Configuring policies, profiles, and address pools | <ul style="list-style-type: none"> • Access port profiles and trunk port profiles • Device profiles • MAC address pools • Tunnel profiles | Configuring Profiles, Policies, and Pools, on page 80 |
| Creating a provider account | — | Creating a Provider Account, on page 85 |
| Downloading the required images | <ul style="list-style-type: none"> • InterCloud extender image • InterCloud switch image | Importing Infrastructure Images, on page 86 |

Configuring Profiles, Policies, and Pools

Successful implementation of an InterCloud link depends on the appropriate configuration of the following items:

- Access port profiles and trunk port profiles—See [Configuring VSM Port Profiles](#), on page 80.
- Device profiles—See [Configuring an InterCloud Device Profile](#), on page 80.
- MAC address pools—See [Adding a MAC Address Pool](#), on page 82.
- Policies and profiles for InterCloud tunnels—See [Policies and Profiles for InterCloud Tunnels](#), on page 82.

You can also configure the following additional policies for inclusion in a device profile for InterCloud resources:

- Core File policies
- Log File policies
- Syslog policies

For more information about these policies and how to configure them, see [Configuring Device Policies](#), on page 183.

Configuring VSM Port Profiles

Cisco Virtual Supervisor Modules (VSMs) on Cisco Nexus 1000V Series switches must be properly configured to support InterCloud features. When configuring port profiles on a VSM:

- Configure at least one port profile for the access port and one for the trunk port. For information on configuring port profiles, see the *Cisco Nexus 1000V InterCloud Port Profile Configuration Guide, Release 5.2(1)IC1(1.1)* at http://www.cisco.com/en/US/products/ps12904/products_installation_and_configuration_guides_list.html.
- Add the **org root** command to each port profile so that the port will be included in the results of the **show org port brief** command. For more information, see the command reference guides available on cisco.com at http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html.

VSMs that are capable of registering with InterCloud Extender and InterCloud Switch service modules are automatically displayed when you configure an InterCloud link using either of the following wizards:

- Extend Network to Cloud Wizard
- Add InterCloud Link Wizard

Configuring an InterCloud Device Profile

An InterCloud device profile is a set of custom attributes and device policies that you can apply to an InterCloud extender or switch. You specify device profiles for the InterCloud extender and switch when you create an

InterCloud link or by applying a different device profile to the InterCloud extender or switch after the link is deployed.

Prime Network Services Controller includes a default InterCloud device profile. You can edit the default InterCloud device profile, but you cannot delete it.

Procedure

- Step 1** Choose **InterCloud Management > InterCloud Policies > Device Profiles**.
- Step 2** Click **Add Device Profile**.
- Step 3** In the General tab in the New Device Profile dialog box, enter a profile name and description, and choose the required time zone.
- Step 4** In the Policies tab, provide the following information, then click **OK**:

| Field | Description |
|-------------|---|
| DNS Servers | You can: <ul style="list-style-type: none"> • Add a new server. • Select an existing server and edit or delete it. • Use the arrows to change priority. |
| DNS Domains | You can: <ul style="list-style-type: none"> • Add a new domain. • Select an existing domain and edit or delete it. |
| NTP Servers | You can: <ul style="list-style-type: none"> • Add a new server. • Select an existing server and edit or delete it. • Use the arrows to change priority. |
| Syslog | You can: <ul style="list-style-type: none"> • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned. |
| Core File | You can: <ul style="list-style-type: none"> • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned. |

| Field | Description |
|-----------------------|--|
| Policy Agent Log File | <p>You can:</p> <ul style="list-style-type: none"> • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned. |

Adding a MAC Address Pool

Add a MAC address pool to allocate a group of MAC addresses to a Virtual Private Cloud.

Procedure

-
- Step 1** Choose **InterCloud Management > InterCloud Link > MAC Pools**.
- Step 2** Click **Add MAC Address Pool**.
- Step 3** Enter the following information, then click **OK**:
- In the Name field, enter a name for the MAC address pool.
 - In the Start MAC Address field, enter the starting MAC address for the pool in the 12-digit hexadecimal format.
 - In the Total Count field, enter the number of addresses in the pool. The minimum value is 1000 MAC addresses, and the default value is 10000 MAC addresses.
-

Policies and Profiles for InterCloud Tunnels

A tunnel profile pairs a connection parameter policy with a key policy to ensure secure communications for specific tunnel ports. After you configure tunnel profiles, you can apply them to tunnels between the following elements:

- InterCloud extender and InterCloud switch
- InterCloud switch and cloud VM

For information on first configuring the individual policies and then tunnel profiles, see the following topics:

- [Configuring a Connection Parameter Policy, on page 83](#)
- [Adding a Key Policy, on page 84](#)
- [Configuring a Tunnel Profile, on page 84](#)

You can also configure the following additional policies for inclusion in a device profile for InterCloud resources:

- Core File policies
- Log File policies
- Syslog policies

For more information about these policies and how to configure them, see [Configuring Device Policies](#), on page 183.

Configuring a Connection Parameter Policy

A connection parameter policy specifies the basic attributes for connecting an enterprise network to a cloud. A connection parameter policy is used with a key policy in a tunnel profile to ensure secure communications between the enterprise and the cloud.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Policies > Policies > Connection Parameter Policies**.

Step 2 Click **Add Connection Parameter Policy**.

Step 3 In the Add Connection Parameter Policy dialog box, provide the following information, then click **OK**:

| Field | Description |
|---------------------|---|
| Name | Connection parameter policy name (read-only). |
| Description | Policy description. |
| Protocol | Protocol for this policy (read-only). The default protocol is UDP. |
| Tunnel Port | Tunnel port for this policy (read-only). The default port is 6644. |
| Data Channel Port | Data channel port for this policy (read-only). The default port is 6644. |
| Keep Alive Duration | Length of time, in minutes and seconds, that a connection can exist with no activity before a keepalive message is sent. The default value is one second. |
| Keep Alive Timeout | Length of time, in minutes and seconds, that a connection can remain idle before it closes. The default value is five minutes. |

Adding a Key Policy

A key policy specifies the encryption and hash algorithms, and the length of the rekeying period for a secure connection. A key policy is used with a connection parameter policy in a tunnel profile to ensure secure communications between the enterprise and the cloud.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Policies > Policies > Key Policies**.

Step 2 In the General tab, click **Add Key Policy**.

Step 3 In the Add Key Policy dialog box, provide the following information, then click **OK**:

| Field | Description |
|-------------------|--|
| Name | Policy name. |
| Description | Brief policy description. |
| ReKey Period | Length of time (in days, hours, minutes, and seconds) that can elapse before a new key must be generated. The minimum value is five minutes. The default value of 00:00:00:00 indicates that rekeying does not occur. |
| Encrypt Algorithm | From the drop-down list, choose the encryption method for this policy: AES-128-CBC (default), AES-128-GCM, AES-256-CBC, AES-256-GCM, or None. |
| Hash Algorithm | This option is available if you choose AES-128-CBC, AES-256-CBC, or None in the Encrypt Algorithm field. Hash algorithm for this policy: None, SHA-1 (default), SHA-256, or SHA-384. The None option is available if you choose None in the Encrypt Algorithm field. |

Configuring a Tunnel Profile

A tunnel profile combines a connection parameter policy with a key policy to ensure secure communications for specific tunnel ports. After you configure a tunnel profile, you can apply the profile to tunnels between the following elements:

- InterCloud extender and InterCloud switch
- InterCloud switch and cloud VM

Procedure

Step 1 Choose **InterCloud Management > InterCloud Policies > Tunnel Profiles**.

Step 2 In the General tab, click **Add Tunnel Profile**.

Step 3 In the Add Tunnel dialog box, enter the following information, then click **OK**:

| Field | Description |
|-----------------------------|--|
| Name | Profile name. |
| Description | Brief profile description. |
| Key Policy | Do any of the following: <ul style="list-style-type: none"> • Choose an existing policy from the drop-down list. • Click Add Key Policy to create a new key policy. • Click the Resolved Policy link to review or modify the key policy currently associated with the profile. |
| Connection Parameter Policy | Do any of the following: <ul style="list-style-type: none"> • Choose an existing policy from the drop-down list. • Click Add Connection Parameter Policy to create a new connection parameter policy. • Click the Resolved Policy link to review or modify the connection parameter policy currently associated with the profile. |

Creating a Provider Account

A cloud provider account is required before you can connect to a public cloud.

Before You Begin

Obtain the following information:

- Cloud provider access ID.
- Cloud provider access key.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Link > Provider Accounts**.

Step 2 Click **Create Provider Account**.

Step 3 In the Create Provider Account dialog box, provide the following information, then click **OK**:

| Field | Description |
|---------------|--|
| Name | Provider account name. This name can contain 1 to 16 characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after the object has been saved. |
| Provider Type | Cloud provider (read-only). |
| Access ID | Alphanumeric text string that identifies the account owner. |
| Access Key | Unique key for the account. |

Importing Infrastructure Images

An InterCloud link includes two virtual gateways: one on the enterprise network and one on the cloud. The gateway on the enterprise network is referred to as the InterCloud Extender, and the one on the cloud is referred to as the InterCloud Switch.

Importing the following infrastructure images enables you to create an InterCloud Extender and an InterCloud Switch when you configure an InterCloud link:

- InterCloud Extender image
- InterCloud Switch image



Note

You must install two infrastructure images: an InterCloud Extender image and an InterCloud Switch image.

Procedure

-
- Step 1** Download the InterCloud Extender and InterCloud Switch images from <http://software.cisco.com/download/navigator.html?mdfid=284653427&i=rm> and place them in a location that is accessible from Prime Network Services Controller server.
- Step 2** Choose **InterCloud Management > InterCloud Link > Infrastructure Images**.
- Step 3** Click **Import Infrastructure Image**.
- Step 4** In the Import Infrastructure Image dialog box:
- a) Enter a name and description for the image you are importing.
 - b) In the Type field, select the type of image to import: InterCloud Switch or InterCloud Extender. The Format field is read-only and will display AMI for an InterCloud Switch image and OVA for an InterCloud Extender image.
 - c) In the Version field, enter a version number that you want to assign to this image.
 - d) In the Import area, provide the following information, then click **OK**:
 - Protocol to use for the import operations: FTP, SCP, or SFTP.
 - Hostname or IP address of the remote host to which you downloaded the images.
 - Account username for the remote host.
 - Account password for the remote host.
 - Image path and filename, starting with a slash (/).
 - e) Repeat Step 3 to import the other image.
-

Configuring InterCloud Links and Cloud VMs

To configure an InterCloud link, instantiate one or more VMs in the cloud, and update an InterCloud link, complete the following procedures in the order shown:

| Procedure | Related Topic |
|--|---|
| 1. Configuring an InterCloud link | Configuring an InterCloud Link, on page 88 |
| 2. Importing an InterCloud Agent image | Importing an InterCloud Agent Image, on page 95 |
| 3. Importing a VM image | Importing a VM Image, on page 96 |
| 4. Creating VM templates on the cloud | Creating Cloud VM Templates, on page 98 |
| 5. Instantiating VMs on the cloud | Instantiating a Cloud VM from a Cloud Template, on page 103 |

Configuring an InterCloud Link

The Extend Network to Cloud wizard walks you through the process of configuring an InterCloud link. A configuration summary is displayed at the end of the wizard, allowing you to review the information and choose whether to deploy the InterCloud link immediately or later.

The wizard also enables you to configure the InterCloud link for high availability. If you enable high availability, you can configure the following properties the same for both the primary and secondary InterCloud Extender:

- VM placement
- Port profile for the data trunk interface
- Port profile for the management interface



Note

InterCloud links can be configured only on VMware ESXi hypervisors.

Before You Begin

- Complete the activities described in [Preparing to Configure InterCloud Links and Cloud VMs](#), on page 79.
- Confirm that Prime Network Services Controller has access to a DNS server. If a DNS server is not accessible, Prime Network Services Controller cannot communicate with the Amazon cloud provider. To configure a DNS server, choose **Administration > System Profile > root > Profile > default**, and add a DNS server.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Link > VPCs**.

Step 2 Click **Extend Network to Cloud**.

Step 3 In the Configure VPC screen, provide the information described in [Configure VPC Screen](#), on page 89, then click **Next**.

Note If you select a VPC before choosing to add an InterCloud link, the Configure InterCloud Link screen is displayed initially instead of the Configure VPC screen.

Step 4 In the Configure InterCloud Link screen, provide the information described in [Configure InterCloud Link Screen](#), on page 90, then click **Next**.

Step 5 In the InterCloud Extender screen, select the image to use for the InterCloud Extender, then click **Next**. Prime Network Services Controller automatically selects the data store to use for the InterCloud Extender instance.

Step 6 In the Select VM Placement screen, do one of the following depending on whether or not you enabled high availability, then click **Next**:

- If you did not enable high availability, navigate to and select the ESXi host to use for the InterCloud Extender instance.

- If you enabled high availability, do one of the following:
 - To use the same ESXi host as the primary InterCloud Extender, in the Secondary area, check the **Same as Primary** check box.
 - To use an ESXi host other than the primary InterCloud Extender, in the Secondary area, navigate to and select the ESXi host to use for the secondary InterCloud Extender instance.

- Step 7** In the Configure Properties screen, provide the information described in [Configure Extender Properties Screen, on page 91](#), then click **Next**.
- Step 8** In the Configure Network Interfaces screen, provide the information described in [Configure Extender Network Interfaces Screen, on page 91](#), then click **Next**.
- Step 9** In the InterCloud Switch screen, select the required InterCloud Switch image, then click **Next**.
When you deploy a link, if no template exists for the InterCloud Switch image, Prime Network Services Controller creates one. InterCloud Switch templates are not linked to specific InterCloud links and can be used by other InterCloud links. As a result, if you undeploy an InterCloud link while an InterCloud Switch template is being created, the template creation process continues.
- Step 10** In the Configure Properties screen, provide the information described in [Configure Switch Properties Screen, on page 94](#), then click **Next**.
- Step 11** In the Configure Network Interfaces screen, provide the information described in [Configure Switch Network Interfaces Screen, on page 94](#), then click **Next**.
- Step 12** In the Configure Tunnel Profile screen, provide the information described in [Configure Tunnel Profile Screen, on page 95](#), then click **Next**.
- Step 13** In the Summary screen:
- a) Review the configuration to ensure that it is correct.
 - b) Check the **Deploy** check box to create the InterCloud link when you click **Finish**. Uncheck the **Deploy** check box to create the InterCloud link later.
 - c) Click **Finish**.

Field Descriptions

Configure VPC Screen

| Field | Description |
|-------------|-----------------------------------|
| Name | Virtual Private Cloud (VPC) name. |
| Description | Brief description. |

| Field | Description |
|------------------|--|
| Provider Account | Do any of the following: <ul style="list-style-type: none"> Choose a provider account from the drop-down list. Click Create Provider Account to create a new provider account. Click the Resolved Provider Account link to review and optionally modify the provider account currently associated with the VPC. |
| Location | Provider region in which to create the VPC. If the provider account selected in the previous field is already associated with a region, a check mark and the status Completed are displayed next to the drop-down list. |
| MAC Pool | Do any of the following: <ul style="list-style-type: none"> Choose a MAC address pool from the drop-down list. Click Create MAC Address Pool to create a new MAC address pool. Click the Resolved MAC Pool link to review and optionally modify the MAC address pool currently associated with the VPC. |
| Default VSM | Default VSM to use for the VPC. |

Configure InterCloud Link Screen

| Field | Description |
|----------------------|---|
| InterCloud Link Name | InterCloud link name. |
| Description | Brief description. |
| VSM | Virtual Supervisor Module (VSM) to use for the InterCloud link. This drop-down list is automatically populated with VSMs capable of supporting InterCloud services. |

| Field | Description |
|-------------------|--|
| High Availability | <p>Check the Enable HA check box to indicate that the InterCloud link is in active standby mode. Uncheck the check box to indicate that the InterCloud link is in standalone mode.</p> <p>If you check the check box, subsequent screens will require information for both the primary and secondary InterCloud Extenders and Switches.</p> |

Configure Extender Properties Screen

| Field | Description |
|------------------|---|
| Primary Name | InterCloud Extender name. |
| Secondary Name | (Displayed if high availability is enabled) Secondary InterCloud Extender name. |
| Device Profile | <p>Do one of the following:</p> <ul style="list-style-type: none"> • Click the existing profile to review and optionally modify it. • Click Select to choose a different device profile. |
| SSH User Name | Username for SSH access (read-only). Default value is admin. |
| SSH Password | Password for SSH access. |
| Confirm Password | Confirming entry for SSH password. |

Configure Extender Network Interfaces Screen

| Field | Description |
|---|---|
| General Tab | |
| Primary Data Trunk Interface Port Profile | Select the data trunk interface port profile to use for the InterCloud Extender. |
| Secondary Data Trunk Interface Port Profile | <p>Displayed if you did not check the Same as Primary check box in the Select VM Placement screen.</p> <p>Select the data trunk interface port profile to use for the secondary InterCloud Extender.</p> |

| Field | Description |
|--|---|
| Management Interface | |
| <i>Primary</i> | |
| Port Profile | Select the port profile to use for the primary InterCloud Extender management interface. |
| IP Address | IP address for the management interface. |
| Netmask | Management interface subnet mask. |
| Gateway | Management interface gateway IP address. |
| <i>Secondary</i> | |
| The following fields are displayed only if high availability is enabled. | |
| Port Profile | Displayed if you did not check the Same as Primary check box in the Select VM Placement screen. Select the port profile to use for the secondary InterCloud Extender management interface. |
| IP Address | IP address for the secondary management interface. |
| Netmask | Secondary management interface subnet mask. |
| Gateway | Secondary management interface gateway IP address. |
| Advanced Tab | |
| External Tunnel Interface | Do one of the following: <ul style="list-style-type: none"> • If the external tunnel interface is the same as the Management interface, check the Same as Management Interface check box. • To specify a different external tunnel interface, uncheck the Same as Management Interface check box, and provide the following information for the external tunnel interface: <ul style="list-style-type: none"> • Port profile • Interface IP address • Subnet mask • Gateway IP address |

| Field | Description |
|--|---|
| Primary | |
| The following fields are displayed if the Same as Management Interface check box is unchecked. | |
| Port Profile | Port profile to use for the external tunnel interface. |
| IP Address | External tunnel interface IP address. |
| Netmask | Subnet mask to apply to the external tunnel interface IP address. |
| Gateway | IP address of the gateway for the external tunnel interface. |
| Secondary | |
| The following fields are displayed if the Same as Management Interface check box is unchecked and high availability is enabled. | |
| Port Profile | Port profile to use for the secondary external tunnel interface. |
| IP Address | Secondary external tunnel interface IP address. |
| Netmask | Subnet mask to apply to the secondary external tunnel interface IP address. |
| Gateway | IP address of the gateway for the secondary external tunnel interface. |
| Internal | |
| Use Default Internal Interface | <p>Do one of the following:</p> <ul style="list-style-type: none"> • If the internal interface is the same as the default internal interface, check the Use Default Internal Interface check box. • If the internal interface is not the same as the default internal interface, uncheck the Use Default Internal Interface check box, and choose the port profiles to use for the following trunk ports: <ul style="list-style-type: none"> • Enterprise trunk • Tunnel trunk |

Configure Switch Properties Screen

| Field | Description |
|------------------|--|
| Primary Name | InterCloud Switch name. |
| Secondary Name | (Displayed if high availability is enabled for this link) Secondary InterCloud Switch name. |
| Device Profile | Do one of the following: <ul style="list-style-type: none"> • Click the existing profile to review and optionally modify it. • Click Select to choose a different device profile. |
| SSH User Name | Username for SSH access (read-only). Default value is admin. |
| SSH Password | Password for SSH access. |
| Confirm Password | Confirming entry for SSH password. |

Configure Switch Network Interfaces Screen

| Field | Description |
|---|---|
| General Tab | |
| Port Profile | From the drop-down list, choose the port profile to use for the InterCloud Switch management interface. |
| Primary | |
| IP Address | IP address for the management interface. |
| Netmask | Management interface subnet mask. |
| Gateway | Management interface gateway IP address. |
| Secondary | |
| The following fields are displayed if high availability is enabled. | |
| IP Address | IP address for the secondary management interface. |
| Netmask | Secondary management interface subnet mask. |

| Field | Description |
|--------------------------------|---|
| Gateway | Gateway IP address for the secondary management interface. |
| Advanced Tab | |
| Use Default Internal Interface | Check the check box to use the default internal interface for the InterCloud Switch. Uncheck the check box to select a port profile for the tunnel trunk. |
| Tunnel Trunk Port Profile | Displayed if the Use Default Internal Interface check box is cleared. From the drop-down list, choose the tunnel trunk port profile. |

Configure Tunnel Profile Screen

| Field | Description |
|--|---|
| InterCloud Extender to InterCloud Switch | Do one of the following: <ul style="list-style-type: none"> Click the existing tunnel profile to review and optionally modify it. Click Select to choose a different tunnel profile. |
| InterCloud Switch to VM | Do one of the following: <ul style="list-style-type: none"> Click the existing tunnel profile to review and optionally modify it. Click Select to choose a different tunnel profile. |

Importing an InterCloud Agent Image

An InterCloud Agent image enables you to securely place a VM image, called a *template*, in the cloud. After the VM template is in place, you can create VM instances in the cloud.

The InterCloud Agent image that you choose must match your VM operating system. You can obtain InterCloud Agent images from [http://software.cisco.com/download/release.html?i=!y&mdfid=284653427&softwareid=282088129&release=5.2\(1\)IC1\(1.1\)&os=](http://software.cisco.com/download/release.html?i=!y&mdfid=284653427&softwareid=282088129&release=5.2(1)IC1(1.1)&os=). The zipped file contains a README.txt file that identifies the available InterCloud Agent images and the folder in which they reside. After you download an InterCloud Agent image, do not change the image filename.

Procedure

- Step 1** Download the appropriate InterCloud Agent image for your VM operating system from [http://software.cisco.com/download/release.html?i=!y&mdfid=284653427&softwareid=282088129&release=5.2\(1\)IC1\(1.1\)&os=](http://software.cisco.com/download/release.html?i=!y&mdfid=284653427&softwareid=282088129&release=5.2(1)IC1(1.1)&os=).
- Step 2** Choose **InterCloud Management > InterCloud Link > InterCloud Agent Images**.
- Step 3** Click **Import InterCloud Agent Image**.
- Step 4** In the InterCloud Agent Image dialog box, provide the following information, then click **OK**:

| Field | Description |
|-----------------------|--|
| Name | InterCloud Agent image name. |
| Description | Image description. |
| Import | |
| Protocol | Protocol to use for the import operation: FTP, SCP, or SFTP. |
| Hostname / IP Address | Hostname or IP address of the remote host. |
| User Name | Account username for the remote host. |
| Password | Account password for the remote host. |
| Remote File | Remote filename, starting with a slash (/). |

Importing a VM Image

After you import an InterCloud Agent image, you are ready to import a VM image. The imported image will be used to create a template on the cloud, which will then allow you to create VM instances from the template on the cloud.

Before You Begin

Import the appropriate InterCloud Agent image for your VM operating system, as described in [Importing an InterCloud Agent Image](#), on page 95.

Procedure

-
- Step 1** Choose **InterCloud Management > Enterprise > VM Images**.
- Step 2** Click **Import VM Image**.
- Step 3** In the Import VM Image dialog box, provide the information described in [Import VM Image Dialog Box](#), on page 97, then click **OK**.
-

Field Descriptions

Import VM Image Dialog Box

| Field | Description |
|--|---|
| Name | VM image name. |
| Description | VM image description. |
| Format | VM image format: AMI, ISO, or OVA. |
| Properties | |
| The Properties area is not displayed for OVA images. | |
| Number of NICs | (AMI images only) Number of NICs for the VM. The value in this field must match the value for the image being imported. |
| OS | (AMI images only) VM operating system: CommunityEnterprise OS (CentOS), Red Hat Enterprise Linux (RHEL), Windows, or Unknown. The value in this field must match the value for the image being imported. |
| Architecture | (AMI images only) VM architecture: 32-bit, 64-bit, or Unknown. The value in this field must match the value for the image being imported. |
| Disk (GB) | Amount of disk space (in gigabytes) for the VM. |
| CPU Cores | Number of CPU cores for the VM. |
| Memory (MB) | Amount of memory (in megabytes) for the VM. |
| Import | |

| Field | Description |
|-----------------------|--|
| Protocol | Protocol to use for the import operation: FTP, SCP, or SFTP. |
| Hostname / IP Address | Hostname or IP address of the remote host. |
| User Name | Account username on the remote host. |
| Password | Account password on the remote host. |
| Remote File | Remote filename, starting with a slash (/). |

Creating Cloud VM Templates

After you establish an InterCloud link and download the required InterCloud Agent and VM images, you are ready to create VM templates in the cloud. After they are created, these VM templates are used to instantiate cloud VMs.

You can create VM templates in a cloud in the following ways:

- From an imported VM image—See [Creating a Template from a VM Image](#), on page 98.
- From an existing template in your enterprise data center—See [Creating a Cloud Template from an Enterprise Template](#), on page 100.
- From an imported VM image or a VM in the data center under a specific VPC—[Creating a Template Under a VPC](#), on page 101.

Creating a Template from a VM Image

Use this procedure to create a template in a cloud from an existing VM image. The template is created in the specified VPC and can then be used to create VM instances in the cloud.

Procedure

-
- Step 1** Choose **InterCloud Management > Enterprise > VM Images > image**.
 - Step 2** Click **Create Template in Cloud**.
 - Step 3** In the Infrastructure screen in the Create Template in Cloud Wizard, select the VPC in which the template is to reside, then click **Next**.
 - Step 4** In the Template Properties screen, provide the information described in [Template Properties Screen](#), on page 99, then click **Next**.
 - Step 5** In the Network Properties screen, optionally add a port profile to each NIC as follows, then click **Next**:
 - a) Right-click the NIC, then choose **Edit**.

- b) In the Edit NIC dialog box, choose the required port profile from the Port Profile drop-down list, then click **OK**.
- Step 6** In the Configure Application Parameters screen, provide the information described in [Configure Application Parameters Screen for ISO Templates](#), on page 99, then click **Next**.
- Step 7** In the Summary and Apply screen, confirm that the information is accurate, then click **Finish**.

Field Descriptions

Template Properties Screen

| Field | Description |
|---|---|
| Template Name | Cloud template name. |
| SSH User | SSH account username. |
| OS Information | |
| OS | VM operating system (read-only): CommunityEnterprise OS (CentOS), Red Hat Enterprise Linux (RHEL), Windows, or Unknown. |
| Architecture | Architecture type (read-only): 32-bit, 64-bit, or Unknown. |
| Template Properties | |
| The following fields display values for the enterprise image and the cloud template. The enterprise values are read-only, but you can modify the values for the cloud template. | |
| Memory (MB) | Amount of memory (in megabytes) for the template. |
| CPU Cores | Number of CPU cores for the template. |
| Disk (GB) | Amount of disk space (in gigabytes) for the template. |

Configure Application Parameters Screen for ISO Templates

| Field | Description |
|------------------|--|
| Timezone | Time zone to use when starting a cloud VM using this template. |
| Hostname | VM hostname. |
| Root Password | Password for the root account. |
| Confirm Password | Confirming password entry. |

| Field | Description |
|-----------------|--|
| Add-on Packages | Additional packages available for the image being imported. The specific packages listed depend on the ISO image being imported. Check the check boxes of any packages you want to include with the ISO image. |

Creating a Cloud Template from an Enterprise Template

You can use an existing VM template in your data center to create a template on the cloud. After you create the template on the cloud, you can use it to instantiate cloud VMs.

Before You Begin

Ensure that at least one VM template is available for you to upload to the cloud.

Procedure

-
- Step 1** Choose **InterCloud Management > Enterprise > VM Managers**.
 - Step 2** In the navigation pane, navigate to the data center, cluster, host, or resource pool with the required template.
 - Step 3** In the Templates table, select the required template, then click **Migrate Template to Cloud**.
 - Step 4** In the Infrastructure screen, select the destination VPC, then click **Next**.
 - Step 5** In the Template Properties screen, provide the information described in [Template Properties Screen](#), on page 100, then click **Next**.
 - Step 6** In the Network Properties screen, optionally assign a port profile to each NIC as follows, then click **Next**:
 - a) Right-click a NIC, then choose **Edit**.
 - b) In the Edit NIC dialog box, select the required port profile from the drop-down list, then click **OK**.
 - Step 7** In the Summary and Apply screen, confirm that the information is correct, then click **Finish**.
-

Field Descriptions

Template Properties Screen

| Field | Description |
|-----------------------|--|
| Template Name | Template name on the cloud. |
| SSH User | Username for SSH access. |
| OS Information | |
| OS | VM operating system (read-only): CommunityEnterprise OS (CentOS), Red Hat Enterprise Linux (RHEL), Windows, or Unknown. |

| Field | Description |
|---|--|
| Architecture | VM architecture (read-only): 32-bit, 64-bit, or Unknown. |
| Template Properties The following fields display values for both the enterprise VM and the cloud template. The enterprise values are read-only, but you can modify the values for the cloud template. | |
| Memory (MB) | Amount of memory (in megabytes) for the template. |
| CPU Cores | Number of CPU cores for the template. |
| Disk (GB) | Amount of disk space (in gigabytes) for the template. |

Creating a Template Under a VPC

Prime Network Services Controller enables you to create a template under a specific VPC from an imported VM image or a VM in the data center.

Procedure

-
- Step 1** Choose **InterCloud Management > Public Cloud > VPCs > vpc > Templates**.
- Step 2** Click **Add New Template**.
The Add New Template wizard opens.
- Step 3** In the Source Image screen, do one of the following, then click **Next**:
- To use an imported VM image as the source for the template:**
- 1 Click the **Images** tab.
 - 2 Select the VM image to upload to the cloud.
- To use a VM in the data center as the source for the template:**
- 1 Click the **Enterprise Data Center** tab.
 - 2 In the left pane, select the data center, cluster, host, or resource pool with the required template.
 - 3 In the right pane, select the template to upload to the cloud.
- Step 4** In the Template Properties screen, provide the information described in [Template Properties Screen](#), on page 102, then click **Next**.
- Step 5** In the Network Properties screen, optionally assign a port profile to each NIC as follows, then click **Next**:
- a) Right-click the NIC, then choose **Edit**.

- b) In the Edit NIC dialog box, choose the required port profile from the Port Profile drop-down list, then click **OK**.

Step 6 In the Summary and Apply screen, confirm that the information is accurate, then click **Finish**.

Field Descriptions

Template Properties Screen

| Field | Description |
|---|---|
| Template Name | Template name on the cloud. |
| SSH User | Username for SSH access. |
| OS Information | |
| OS | VM operating system (read-only): CommunityEnterprise OS (CentOS), Red Hat Enterprise Linux (RHEL), Windows, or Unknown. |
| Architecture | VM architecture (read-only): 32-bit, 64-bit, or Unknown. |
| Template Properties | |
| The following fields display values for both the enterprise VM and the cloud template. The enterprise values are read-only, but you can modify the values for the cloud template. | |
| Memory (MB) | Amount of memory (in megabytes) for the template. |
| CPU Cores | Number of CPU cores for the template. |
| Disk (GB) | Amount of disk space (in gigabytes) for the template. |

Instantiating Cloud VMs

You can instantiate cloud VMs in the following ways:

- From a cloud template—See [Instantiating a Cloud VM from a Cloud Template](#), on page 103.
- From a deployed template or VM in your data center—See [Instantiating a Cloud VM from a Deployed Template or Local VM](#), on page 104.
- By migrating a VM in your data center to the cloud—See [Instantiating a Cloud VM by Migrating an Enterprise VM](#), on page 106.

Instantiating a Cloud VM from a Cloud Template

After you create a VM template on a cloud, you can instantiate one or more cloud VMs.

Procedure

-
- Step 1** Choose **InterCloud Management > Public Cloud > VPCs > vpc > Templates**.
- Step 2** In the Templates table, choose a deployed template, then click **Instantiate VM**.
- Step 3** In the Infrastructure screen, do the following, then click **Next**:
- In the VM Name field, enter a name for the cloud VM.
 - In the InterCloud Link drop-down list, choose the InterCloud link to use for the cloud VM.
- Step 4** In the VM Properties screen, provide the information described in [VM Properties Screen, on page 103](#), then click **Next**.
- Step 5** In the Network Properties screen, provide the following information, then click **Next**:
- In the NICs table, assign a port profile to each NIC by selecting a NIC and then clicking **Edit**. In the Edit NIC dialog box, select the required port profile from the Port Profile drop-down list, then click **OK**.

Note A port profile always belongs to a specific VLAN. Select the port profile according to the VLAN to which the NIC belongs.
 - In the DNS Server 1 and DNS Server 2 fields, enter the IP addresses for the DNS servers.
 - In the Domain Name field, enter the DNS domain name.
- Step 6** In the Review Summary and Apply screen, confirm that the information is accurate, then click **Finish**.
-

Field Descriptions

VM Properties Screen

| Field | Description |
|--|---|
| SSH User | Username for SSH access. |
| OS Information | |
| OS | Cloud VM operating system (read-only): CommunityEnterprise OS (CentOS), Red Hat Enterprise Linux (RHEL), Windows, or Unknown. |
| Architecture | Architecture type (read-only): 32-bit, 64-bit, or Unknown. |
| Template Properties | |
| The following fields display values for both the template and the cloud VM. The values for the template are read-only, but you can modify the values for the cloud VM as needed. | |
| Memory (MB) | Amount of memory (in megabytes) for the cloud VM. |

| Field | Description |
|-----------|---|
| CPU Cores | Number of CPU cores on the cloud VM. |
| Disk (GB) | Amount of disk space (in gigabytes) for the cloud VM. |

Instantiating a Cloud VM from a Deployed Template or Local VM

You can instantiate a cloud VM if the following are available:

- A deployed template on the cloud
- A VM in your data center

If you instantiate a cloud VM from a VM that has a static IP address in the enterprise data center, you can access the cloud VM by using the same enterprise IP address. If you instantiate a cloud VM from a VM that uses DHCP in the enterprise data center, you can access the cloud VM by using the IP address that the VM obtained from the DHCP server. After the cloud VM is created, the Prime Network Services Controller UI displays the enterprise IP address details for your reference.

Procedure

-
- Step 1** Choose **InterCloud Management > Public Cloud > VPCs > vpc > VMs**.
- Step 2** Click **Instantiate New VM**.
The Instantiate New VM Wizard opens.
- Step 3** In the Infrastructure screen, choose the required InterCloud Link from the drop-down list, then click **Next**.
- Step 4** In the Source screen, do one of the following:
- To use a VM in your data center:**
- 1 In the Source VM tab, navigate to and select the required data center, cluster, host, or resource pool.
 - 2 From the list of VMs, select the VM to use for the cloud VM.
 - 3 Click **Next**.
- To use a deployed template:**
- 1 Click the **Source Template** tab.
 - 2 From the list of templates, choose the template you want to use for the cloud VM.
 - 3 Click **Next**.
- Step 5** In the VM Properties screen, provide the information as described in [VM Properties Screen, on page 105](#), then click **Next**.
- Step 6** In the Network Properties screen, provide the following information, then click **Next**. The information you need to enter depends on whether you are using a VM or a template to instantiate the cloud VM:

- a) For both VMs and templates, in the NICs table, right-click a NIC entry and choose **Edit**. In the Edit NIC dialog box, select the required port profile from the drop-down list, then click **OK**.

Note The port profile always belongs to a specific VLAN. Select the port profile according to the VLAN to which the NIC belongs.

- b) For templates, also provide the following DNS information:

- 1 DNS Server 1—Enter the IP address for the first DNS server.
- 2 DNS Server 2—Enter the IP address for the second DNS server. This IP address cannot be the same as that for the first DNS server.
- 3 Domain Name—Enter the DNS domain name.

Step 7 In the Summary and Apply screen, do one of the following, depending to the source of the cloud VM:

If the source is a VM in your data center:

- 1 In the Upon Successful Migration field, indicate whether or not the source VM should be deleted from vCenter after the cloud VM is instantiated. If you choose to delete the VM from vCenter, the deletion is permanent and the VM cannot be retrieved.
- 2 Confirm that the rest of the information is correct.
- 3 Click **Finish**.

If the source is a deployed template:

- 1 Confirm that the information is accurate.
- 2 Click **Finish**.

Field Descriptions

VM Properties Screen

| Field | Description |
|-----------------------|--|
| VM Name | Cloud VM name. |
| SSH User | Username for SSH access. |
| OS Information | |
| OS | VM operating system (read-only): CommunityEnterprise OS (CentOS), Red Hat Enterprise Linux (RHEL), Windows, or Unknown. |
| Architecture | VM architecture (read-only): 32-bit, 64-bit, or Unknown. |

| Field | Description |
|--|---|
| Template Properties | |
| The following fields display values for both the template and the cloud VM. The template values are read-only, but you can modify the values for the cloud VM as needed. | |
| Memory (MB) | Amount of memory (in megabytes) for the VM. |
| CPU Cores | Number of CPU cores for the VM. |
| Disk (GB) | Amount of disk space (in gigabytes) for the VM. |

Instantiating a Cloud VM by Migrating an Enterprise VM

You can migrate an existing VM in your data center to the cloud and thereby create a new cloud VM. After you migrate the enterprise VM to the cloud, you cannot migrate it back to the enterprise data center. However, when you migrate the VM to the cloud, you can retain the original VM in the data center.



Note

Do not make any changes to a VM or its structure in VMware vCenter while the VM is being migrated to the cloud. Similarly, do not make any changes to a VM or its structure in VMware while aborting the migration of the VM to the cloud. If you need to make changes in VMware vCenter that affect the VM, abort or terminate any migration in progress, make the changes in VMware vCenter, and then migrate the VM to the cloud.

Before You Begin

- Ensure that at least one interface is enabled on the VM.
- Disable any service or application on the VM that uses port 22. After migration, the SSH server that is installed on the cloud VM listens on port 22 for communications with Prime Network Services Controller.

Procedure

- Step 1** Choose **InterCloud Management > Enterprise > VM Managers**.
- Step 2** In the navigation pane, navigate to and select the data center, cluster, host, or resource pool with the required template.
- Step 3** In the VMs table, select the VM to use for the VM template, then click **Migrate VM to Cloud**.
- Step 4** In the Infrastructure screen, select the InterCloud link to use for the VM template, then click **Next**.
- Step 5** In the VM Properties screen, provide the information described in [VM Properties Screen, on page 107](#), then click **Next**.
- Step 6** In the Network Properties screen, optionally assign a port profile to each NIC as follows, then click **Next**:
 - a) Right-click the NIC, then click **Edit**.

- b) In the Edit NIC dialog box, choose the required port profile from the Port Profile drop-down list, then click **OK**.

Step 7 In the Summary and Apply screen:

- a) In the Upon Successful Migration field, indicate whether or not the data center VM is to be deleted after the template is successfully created on the cloud.
- b) Confirm that the rest of information is correct.
- c) Click **Finish**.

Field Descriptions

VM Properties Screen

| Field | Description |
|---|---|
| VM Name | Original VM name. |
| SSH User | Username for SSH access. |
| OS Information | |
| OS | VM operating system (read-only): CommunityEnterprise OS (CentOS), Red Hat Enterprise Linux (RHEL), Windows, or Unknown. |
| Architecture | VM architecture (read-only): 32-bit, 64-bit, or Unknown. |
| Template Properties | |
| The following fields display values for both the enterprise VM and the cloud template. The enterprise values are read-only, but you can modify the values for the cloud template. | |
| Memory (MB) | Amount of memory (in megabytes) for the VM. |
| CPU Cores | Number of CPU cores for the VM. |
| Disk (GB) | Amount of disk space (in gigabytes) for the VM. |

Managing InterCloud Links

In addition to creating InterCloud links, you can update them, delete them, monitor their status, or troubleshoot related issues. For more information, see the following topics:

- [Updating an InterCloud Link, on page 108](#)
- [Updating an InterCloud Link in High Availability Mode, on page 108](#)

- [Deleting an InterCloud Link](#), on page 109
- [Monitoring InterCloud Resources and Status](#), on page 110
- [Troubleshooting InterCloud Issues](#), on page 115

Updating an InterCloud Link

Prime Network Services Controller enables you to update the images for an InterCloud Extender and Switch for a deployed link.



Note

If you undeploy an InterCloud link while the InterCloud link is being upgraded, the InterCloud Switch might not be terminated on the cloud. If this occurs, you will need to manually remove the InterCloud Switch from the cloud when the link is undeployed.

Before You Begin

Ensure that a VM Manager is configured in Prime Network Services Controller.

Procedure

- Step 1** Choose **InterCloud Management > InterCloud Link > VPCs > vpc > intercloud-link**.
- Step 2** Click **Update**.
The InterCloud Link Update Wizard is displayed.
- Step 3** In the InterCloud Link screen, check the check boxes of the images to update, then click **Next**. You can update one or both images.
The screens that are displayed in the wizard depend on the images that you select. For example, if you select to update the InterCloud extender image, the screen for the InterCloud switch image is not displayed.
- Step 4** In the InterCloud Extender screen, select the image for the update, then click **Next**.
- Step 5** In the Select VM Placement screen, navigate to and select the VM host to use for the update, then click **Next**.
- Step 6** In the InterCloud Switch screen, select the image for the update, then click **Next**. Whether you update one or both images, the images must have the same version.
- Step 7** In the Summary screen, confirm that the information is correct, then click **Finish**.

Updating an InterCloud Link in High Availability Mode

Use this procedure to update both the primary and secondary devices in an InterCloud link that is configured for high availability.

Procedure

- Step 1** Update the InterCloud link as described in [Updating an InterCloud Link](#), on page 108.
- Step 2** Trigger a switchover as follows:
- Choose **InterCloud Management > InterCloud Link > VPCs > vpc**.
 - In the InterCloud Links table, select the link that you updated in Step 1, and click **Switchover**.
- Step 3** Update the InterCloud link again.
-

Deleting an InterCloud Link

If you need to delete an InterCloud link, you can safely do so after terminating all VMs that are associated with the link and moving the link to the Undeployed state.

If you undeploy an InterCloud link, the InterCloud Switch template used by this InterCloud link is not deleted because it can be used by other InterCloud links. Instead, if you undeploy an InterCloud link while the creation of InterCloud Switch template is in progress, the template creation process continues.

If desired, you can delete the InterCloud Switch template while it is being deployed, which will stop the template deployment. To delete an InterCloud Switch template, choose **InterCloud Management > InterCloud Link > InterCloud Switch Templates > switch-template**, and then click **Delete**.

In rare situations, you might encounter a scenario in which the following events occur:

- 1 You create an InterCloud link that refers to an InterCloud Extender that is registered to Prime Network Services Controller.
- 2 The InterCloud Extender client is in the *lost-visibility* operational state in the Service Registry (**Administration > Service Registry > Clients**).
- 3 You delete the InterCloud Extender client from the Service Registry and then try to deploy the InterCloud link, which fails because the InterCloud Extender no longer exists.

If you encounter this situation, after you delete the InterCloud Extender client from the Service Registry, also delete the InterCloud link that refers to the deleted InterCloud Extender.

Procedure

-
- Step 1** Choose **InterCloud Management > Public Cloud > VPCs > vpc > VMs**.
- Step 2** In the VMs table, select each VM that is associated with the link you want to delete, then click **Abort** or **Terminate**. The Abort option is available while the VM is being created, and the Terminate option is available after the VM has been created.
- Step 3** After the VMs have been terminated or aborted, choose **InterCloud Management > InterCloud Link > VPCs > vpc**.
- Step 4** In the InterCloud Links table, select the link that you want to delete, then click **Undeploy**.
- Step 5** After Prime Network Services Controller displays Undeployed in the Deploy State column for that link, select the link and click **Delete**.
- Step 6** When prompted, confirm the deletion.
-

Monitoring InterCloud Resources and Status

Prime Network Services Controller provides the following options for monitoring InterCloud resources and status:

- [Recent Jobs Table](#), on page 110
- [Monitoring Tab](#), on page 111
- [Status Fields and Labels](#), on page 112
- [Task Tabs](#), on page 112
- [Faults Table](#), on page 113
- [Events Table](#), on page 114
- [Audit Logs](#), on page 114

Recent Jobs Table

The Recent Jobs table appears by default for the following tabs under InterCloud Management:

- Enterprise
- Public Cloud
- InterCloud Link

The table displays recent jobs submitted with the most recent job at the top, and the number of job records in the table. The jobs are displayed for 12 hours. Each job contains the following information:

| Field | Description |
|-------|-------------|
| Name | Job name. |

| Field | Description |
|-------------|---|
| Status | Job status and duration (in days, hours, minutes, and seconds). |
| Description | Job description. |
| Message | Associated message issued for the job. |
| Retry Count | Number of retries for the job. |
| Start Time | Date and time when the job started. |
| End Time | Date and time when the job completed. |

Some jobs, such as creating an InterCloud link, contain subordinate tasks. Expand the icon next to the job name in the Recent Jobs table to view subordinate tasks and their status.

You can resize the table as needed to view more or fewer jobs, and you can minimize the table until needed by clicking the icon next to the table name or the Minimize icon.

Monitoring Tab

Prime Network Services Controller monitors and displays statistical information for InterCloud links and cloud VMs. This information is displayed in a Monitoring tab that is available by choosing either of the following:

- **InterCloud Management > Public Cloud > VPCs > vpc > intercloud-link > Monitoring tab**
- **InterCloud Management > Public Cloud > VPCs > vpc > InterCloud Links tab > intercloud-link > Edit > Monitoring tab**

The following table describes the information that is displayed in the Monitoring tab:

| Field | Description |
|-------------------|--|
| Last Refresh Time | Date and time that the information was last updated. |
| Refresh | Refreshes the information that is displayed. |
| Table | |
| Name | Cloud VM name. |
| CPU | Percent CPU used. |
| Memory | Percent memory used. |
| Collection Time | Time that the statistics were collected. |
| Rx Errors | Number of receive errors. |

| Field | Description |
|------------|---------------------------------|
| Rx Packets | Number of receive packets. |
| Tx Errors | Number of transmission errors. |
| Tx Packets | Number of transmission packets. |

Status Fields and Labels

Status fields with labels and icons are available in many screens and dialog boxes throughout Prime Network Services Controller. In InterCloud Management, depending on the object, common statuses are:

- Deploying
- Deployed
- Undeploying
- Undeployed
- In-progress
- Completed
- Failed
- Aborted
- Success

Icons accompany these statuses for quick visual reference.

Task Tabs

Task tabs are available in many of the Edit and Properties dialog boxes for InterCloud resources. These dialog boxes include:

- Edit InterCloud Extender
- Edit InterCloud Switch
- Edit Infrastructure Image
- Edit InterCloud Agent Image
- InterCloud Switch Template Properties
- Edit Provider Account
- Edit VM Image
- InterCloud Switch Template Properties

The Task tab includes the following information, enabling you to monitor the status of the specific object:

| Field | Description |
|------------------------|--|
| Description | Task description. |
| Status | Task status. |
| Stage Descriptor | Description of the current stage. |
| Tries | Number of times the task has been tried. |
| Previous Status | Status of the previous task only. This field does not provide the status of the current task. |
| Remote Err Code | Remote error code. |
| Remote Err Description | Description of the remote error. |
| Remote Inv Result | Remote error result. |
| Time Stamp | Date and time when the task completed. |
| Progress | Progress of the current task, indicated by the percent complete, a progress bar, or both. |

Faults Table

Faults tables are present throughout the Prime Network Services Controller UI in main screens and many dialog boxes. Fault tables assist in troubleshooting and monitoring status by providing the following information:

| Field | Description |
|-----------------|--|
| Severity | One of the following fault severities: <ul style="list-style-type: none"> • Critical • Major • Minor • Warning • Info • Condition • Cleared |
| Affected Object | Managed object that is affected by this fault. Click the object name to view the properties for this object. |
| Cause | Unique identifier associated with the event that caused the fault. |

| Field | Description |
|-----------------|---|
| Last Transition | Date and time when the severity last changed. If the severity has not changed, the original creation date is displayed. |
| Ack | Acknowledged state. |
| Type | One of the following fault types: <ul style="list-style-type: none"> • fsm • environmental • equipment |
| Description | Fault description. |

To view more information about a fault and optionally acknowledge it, double-click the fault. The Fault Properties dialog box is displayed with additional details.

Events Table

Events tables are available throughout the Prime Network Services Controller UI. Events tables provide the following information:

- Unique event identifier
- User type associated with the event
- Event creation date and time
- Identifier associated with the event cause
- Event description

Audit Logs

The InterCloud Management tab includes a Diagnostics subtab with an Audit Logs entry. When monitoring InterCloud status or troubleshooting InterCloud issues, the Audit Logs table can provide the following information:

- Unique entry identifier
- Object associated with the entry
- User associated with the entry
- Date and time the fault occurred
- Action associated with the entry: Creation, Modification, or Deletion
- Cause associated with the entry
- Description

Troubleshooting InterCloud Issues

The following topics describe how to resolve problems that can arise when using InterCloud resources:

- [Prime Network Services Controller Does Not Display IP Addresses for Cloud VMs](#), on page 115
- [InterCloud Clients Lose Connectivity to Prime Network Services Controller](#), on page 115

InterCloud Clients Lose Connectivity to Prime Network Services Controller

InterCloud clients might lose connectivity to Prime Network Services Controller upon occasion. For example, if the Prime Network Services Controller server's IP address and shared secret are changed via the CLI while an InterCloud link is configured, the InterCloud clients will lose connectivity with the Prime Network Services Controller server and will not be able to reconnect.

Use the following procedure to reestablish connectivity for the VSM, InterCloud Extender, and InterCloud Switch clients.

**Note**

You must manually update the IP address of the VSM whether or not an InterCloud link is deployed.

Procedure

- Step 1** Using SSH, connect to the VSM, and update the IP address and shared secret password for Prime Network Services Controller.
- Step 2** Using SSH, connect to the InterCloud Extender and update the Prime Network Services Controller IP address.
- Step 3** Using the GUI:
 - a) Choose **InterCloud Management > InterCloud Link > VPCs > vpc > intercloud-link**.
 - b) Click the **InterCloud Link** tab.
 - c) In the InterCloud Switch table, select the required switch and click **Reboot**.
After the InterCloud Switch reboots, it will reestablish connectivity.

Prime Network Services Controller Does Not Display IP Addresses for Cloud VMs

Occasionally, Prime Network Services Controller does not display IP addresses for cloud VM instances. For example, this situation occurs if you instantiate a cloud VM from a VM that uses DHCP in the enterprise data center. If this occurs, you can view the cloud VM IP addresses by entering the **show org port brief** command on the VSM or by using the following procedure.

Procedure

-
- Step 1** Create a port profile and include the **org root** command.
 - Step 2** When creating a cloud VM, assign a port profile that has the org defined.
 - Step 3** After the cloud VM is instantiated, initiate traffic on the DHCP IP address so that it appears in the IP database (IPDB) on the InterCloud Switch.
 - Step 4** On the InterCloud Switch, enter the following command to obtain the IP address:

```
show intercloud vm vm-name system info
```

Creating AMI Images from VMs

Prime Network Services Controller enables you to create AMI images from Windows and Linux VMs in your enterprise data center.

For both Windows and Linux VMs, you can obtain a virtual machine VMDK file by completing the following steps:

- 1 Power off the VM on the vCenter Client.
- 2 Select the VM.
- 3 In the vCenter Client, choose **File > Export OVF Template** to export the VM as a single OVA file.
- 4 Use the **tar** utility to untar the exported file and obtain the VM's disk.

For more information on creating AMI images from VMs, see the following topics:

- [Creating an AMI Image from a Windows VM, on page 116](#)
- [Creating an AMI Image from a Linux VM, on page 117](#)

Creating an AMI Image from a Windows VM

This procedure enables you to create an AMI from a Windows VM and import it as a VM image into Prime Network Services Controller.

Before You Begin

- Confirm that the following firewall ports are open on the Windows firewall on any third-party firewall installed in the VM:
 - 22—TCP
 - 6644—TCP, UDP
- Ensure that IPv4 is enabled on the VM's NICs as follows:

- 1 Open `nepa.cpl`.
- 2 For each NIC in the VM, right-click and confirm that IPv4 is enabled.

Procedure

- Step 1** Download `icami.exe` from <http://www.cisco.com/go/services-controller>.
 - Step 2** In VMware vCenter, upload the downloaded `icami.exe` file to your Windows VM running on vCenter.
 - Step 3** Run `icami.exe` with admin privileges.
 - Step 4** Shut down the Windows VM.
 - Step 5** Using vCenter, export the OVF template as OVA.
 - Step 6** Extract the VMDK from the OVA.
 - Step 7** Using `dd` or a similar utility, convert the VMDK to raw images.
 - Step 8** Using `gzip` or `bzip`, compress the images.
 - Step 9** Using the Prime Network Services Controller GUI, import the VM image by choosing **InterCloud Management > Enterprise > VM Images > Import VM Image**.
-

Creating an AMI Image from a Linux VM

This procedure describes how to create an AMI image from a Linux VM. After you create the AMI image, you can import it as a VM image into Prime Network Services Controller.

This procedure uses the `vmware-mount` utility, which is a part of the vSphere disk development tool that you can download from <https://my.vmware.com/web/vmware/details?productId=2&downloadGroup=VDDK50>.

Procedure

- Step 1** Download the VM disk image (VMDK) onto a Linux host.
- Step 2** Mount the VMDK as a flat file by using the `vmware-mount` command, as follows:

```
# vmware-mount -f vmdk-image /mount/point
```

where *vmdk-image* is the VMDK filename and */mount/point* is the desired directory.

- Step 3** Attach a loop device to the flat file by using the `losetup` command:

```
# losetup /dev/loopn /mnt/vmdk/file
```

where *loopn* is the loop device and *file* is the name of the flat file.

- Step 4** Access partitions on the disk image as follows:
 - a) Enter the `fdisk` command to view the disk partitions as shown in the following example for loop device `/dev/loop0` :

```
# fdisk -l /dev/loop0
```

| Device | Boot | Start | End | Blocks | Id | System |
|--------------|------|-------|-----|---------|----|-----------|
| /dev/loop0p1 | * | 1 | 64 | 512000 | 83 | Linux |
| /dev/loop0p2 | | 64 | 784 | 5778432 | 8e | Linux LVM |

- b) Create a device for each partition on the disk image by entering the **kpartx** command, as follows:

```
# kpartx -a /dev/loop0
# ls /dev/mapper/
control loop0p1 loop0p2
```

This command creates device files for all physical partitions on the disk file and maps the logical volumes that reside in the partition.

- c) (Optional) Enter the **pvscan** command to identify the volume groups that are present on the disk image. The command with example output resembles the following:

```
# pvscan
PV /dev/mapper/loop0p2 VG vg_mowgli lvm2 [5.51 GiB / 0 free]
```

In this example, the second partition (/dev/mapper/loop0p2) contains the volume group `vg_mowgli`.

- d) (Optional) View the logical volumes by entering the **lvscan** command as shown in the following example:

```
# lvscan
inactive          '/dev/vg_mowgli/lv_root'[1.85 GiB] inherit
inactive          '/dev/vg_mowgli/lv_swap'[3.66 GiB] inherit
```

Step 5 Mount the partitions and logical volume to recreate the Linux file system hierarchy under / (root) by completing the following steps:

Note In this example, the logical volume /dev/vg_mowgli/lv_root is the root (/) partition.

- a) Activate the logical volume by using the **lvchange** command so that it can be mounted:

```
# lvchange -ay /dev/vg_mowgli/lv_root
```

- b) Mount the logical volume on a directory on the host system (/mnt/fs in this example):

```
# mount /dev/vg_mowgli/lv_root /mnt/fs/
```

- c) List the contents of the logical volume to confirm that this is the root of the filesystem:

```
# ls /mnt/fs/
bin boot cgroup dev etc home lib lib64 lost+found media mnt opt proc
root sbin selinux
srv sys tmp usr var
```

- d) Obtain the filesystem mount points by entering the **cat** command:

```
# cat /mnt/fs/etc/fstab
```

```

/dev/mapper/vg_mowgli-lv_root / ext4 defaults 1 1
UUID=44cb64be-62bc-4297-9a8d-beb3493a2362 /boot ext4 defaults
1 2
/dev/mapper/vg_mowgli-lv_swap swap swap defaults 0 0

```

In this example:

- /dev/mapper/vg_mowgli-lv_root mounts at /.
- /dev/mapper/vg_mowgli-lv_swap is the swap partition.
- The partition with the UUID 44cb64be-62bc-4297-9a8d-beb3493a2362 mounts at /boot.

- e) Obtain the UUID and LABEL of a partition by entering the **blkid** command on the partition device file:

```

# blkid /dev/mapper/loop0p1

/dev/mapper/loop0p1:UUID="44cb64be-62bc-4297-9a8d-beb3493a2362"
TYPE="ext4"

```

- f) Recreate the filesystem by using the information gained from the **fstab** command:

```
# mount /dev/mapper/loop0p1 /mnt/fs/boot/
```

The Linux file system is successfully recreated with all partitions mounted as in fstab. That is, the file system present on vmdk has been recreated inside the /mnt/fs directory on the host system.

Step 6 Validate the image for the Amazon Xen Hypervisor by completing the following steps:

- a) Verify that the operating system and version are supported by Prime Network Services Controller by checking the contents of the file etc/redhat-release:

```

# cat /mnt/fs/edt/redhat-release
Red Hat Enterprise Linux Server release 6.2 (Santiago)

```

- b) Review the contents of grub.conf to determine the version of Linux kernel present on the filesystem that is set to boot by default. The following example displays the contents of a grub.conf file and provides the following information:

- The value of the parameter default identifies the default entry (0).
- A single kernel is present in the disk image and is set to boot by default.
- The version of the kernel that is set to boot by default is displayed in the kernel entry. In this example, the version is 2.6.32-220.el6.x86_64.

```

# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this
file
# NOTICE: You have a /boot partition. This means that
# all kernel and initrd paths are relative to /boot/, eg.
# root (hd0,0)
# kernel /vmlinuz-version ro root=/dev/mapper/vg-mowgli-lv_root
# initrd /initrd-[generic-]version.img

```

```
# boot
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xmp.gz
hiddenmenu
title Red Hat Enterprise Linux (2.6.32-220.el6.x86_64)
    root (hd0,0)
    kernel /vmlinuz-2.6.32.220.el6.x86_64 ro
root=/dev/mapper/vg_mowgli-lv_root
initrd /initramfs-2.6.32-220.el6.x86_64.img
```

c) In the file `/mnt/fs/boot/config-kernel-version`, verify that the following flags are set to y:

- `CONFIG_PARAVIRT_GUEST=y`
- `CONFIG_XEN=y`
- `CONFIG_PARAVIRT=y`
- `CONFIG_NETFILTER=y`

Step 7 Create a new disk image to copy the filesystem present on the VMDK by completing the following steps:

a) Create a new disk by using the `qemu-img` command:

```
qemu-img create -f raw myami.img 6G
Formatting 'myami.img', fmt=raw size=6442450944
```

b) Attach the new image file to a loop device and format it so that it is the same as the source VMDK image filesystem:

```
# losetup /dev/loop1 myami.img
# mkfs.ext4 /dev/loop1
```

c) Label the new image, as in the following example:

```
# e4label /dev/loop1 _/
# blkid /dev/loop1
/dev/loop1: LABEL="_/"  UUID="9cf14199-a0ff-4501-bb2f-9a7bc020b1e2"
TYPE="ext4"
```

d) Mount the new image file:

```
# mkdir /mnt/amifs
# mount /dev/loop1 /mnt/amifs
```

Step 8 Copy the file system contents from the source image to the new image:

```
# cp -ar /mnt/fs/* /mnt/amifs/
```

Step 9 Configure the new image as described in the following steps:

a) Modify `/mnt/amifs/etc/fstab` so that it reflects the partitioning on the new image. For example:

```
LABEL=_/ ext4 defaults 1 1
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
```

- b) Create a udev rule to change the first Ethernet interface to csc0 by creating the file `/mnt/amifs/etc/udev/rules.d/70-persistent-net.rules` and adding the following content:

```
SUBSYSTEM=="net", DRIVERS=="vif", ATTRS{nodename}=="device/vif/0",
NAME="csc0"
```

- c) Create an interface file named `/mnt/p1/etc/sysconfig/network-scripts/ifcfg-csc0` and add the following content:

```
ONBOOT=yes
DEVICE=csc0
BOOTPROTO=dhcp
```

- d) Enable networking by editing the file `/mnt/amifs/etc/sysconfig/network` and setting `NETWORKING` to `yes`.
- e) Edit `grub.conf` so that it looks similar to the following:

```
default=0
timeout=2
title Red Hat Enterprise Linux (2.6.32-71.el6.x86_64)
    root (hd0)
    kernel /boot/vmlinuz-2.6.32-71.el6.x86_64 ro root=LABEL=_/
    selinux=0 console=hvc0
```

Step 10 Add the driver RPM by completing the following steps:

- a) Create the directory `/mnt/amifs/opt/.cisco` and copy the driver RPM into this directory:

```
mkdir -p /mnt/amifs/opt/.cisco
cp csw.1.1.2.rhel6_2.x86-64.rpm /mnt/amifs/opt/.cisco
```

- b) Create the files `version_cur` and `version_gold` in `/opt/.cisco` and place the driver version in each file. You can obtain the driver version from the name of the file. For example, a file with the name `csw.1.1.2.rhel6_2.x86_64` has the driver version 1.1.2.

```
cat /mnt/amifs/opt/.cisco/version_cur
1.1.2
cat /mnt/amifs/opt/.cisco/version_gold
1.1.2
```

- c) For each `ifcfg-ethn` file in `/mnt/amifs/sysconfig/network-scripts/`, create an entry in `interface.conf` using the syntax `interface-interface-number,interface-name,random-mac-address` where:
- *interface-number* is the number assigned to the interface, starting with 1.
 - *interface-name* is the name assigned to the interface.
 - *random-mac-address* is a MAC address.

The following is an example interface.conf file for two interfaces:

```
cat /mnt/amifs/opt/.cisco/interface.conf

interface-1,ether0,00:0f:f7:dd:8a:37
interface-2,ether1,00:0f:f7:34:40:ae
```

Step 11 Add the initialization scripts for starting the subagent:

```
# cp csw /mnt/amifs/etc/init.d/
# chroot /mnt/amifs/ chkconfig --level 34 csw on
```

Step 12 Add the getkeys script for fetching Amazon keys:

```
# cp getkeys /mnt/amifs/etc/init.d/
# chroot /mnt/amifs/ chkconfig --34 getkeys on
```

Step 13 Unmount and close the AMI image by entering the following commands:

```
//Unmount the disk image file
# umount /mnt/amifs/

//Detach the loop device
# losetup -d dev/loop0
```

Step 14 Unmount and close the VMDK by entering the following commands:

```
//Unmount partitions
# umount /mnt/fs/boot
# umount /mnt/fs

//Deactivate all logical volumes present
# lvchange -an /dev/vg-mowgli/lv_root

//Delete device mappings
# kpartx -d /dev/loop0

//Detach the loop device
# losetup -d /dev/loop0

//Unmount the VMDK file
# vmware-mount -d /mnt/vmdk
```



Configuring Service Policies and Profiles

This section includes the following topics:

- [Configuring Service Policies, page 123](#)
- [Working with Profiles, page 159](#)
- [Configuring Security Profiles, page 166](#)
- [Configuring Security Policy Attributes, page 171](#)

Configuring Service Policies

The following topics describe concepts and options for configuring service policies and policy sets:

- [Configuring ACL Policies and Policy Sets, on page 123](#)
- [Configuring Connection Timeout Policies, on page 130](#)
- [Configuring DHCP Policies, on page 132](#)
- [Configuring IP Audit and IP Audit Signature Policies, on page 135](#)
- [Configuring NAT/PAT Policies and Policy Sets, on page 138](#)
- [Configuring Packet Inspection Policies, on page 143](#)
- [Configuring Routing Policies, on page 144](#)
- [Configuring TCP Intercept Policies, on page 145](#)
- [Configuring Site-to-Site IPsec VPN Policies, on page 146](#)

Configuring ACL Policies and Policy Sets

The following topics describe how to configure ACL policies and policy sets:

- [Adding an ACL Policy](#)
- [Time Ranges in ACL Policy Rules, on page 128](#)

- [Adding an ACL Policy Set, on page 130](#)

Adding an ACL Policy

Prime Network Services Controller enables you to implement access control lists based on the time of day and frequency, or inclusion in a defined group. Benefits of this feature include:

- Providing closer control of access to network resources throughout the day or week.
- Enhancing policy-based routing and queuing functions.
- Automatically rerouting traffic at specific times of the day to ensure cost-effectiveness.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > ACL > ACL Policies**.

Step 2 In the General tab, click **Add ACL Policy**.

Step 3 In the Add ACL Policy dialog box, enter a name and brief description for the policy, then click **Add Rule**.

Step 4 In the Add Rule dialog box, specify the required information as described in [Add ACL Policy Rule Dialog Box, on page 124](#), then click **OK**.

Note All Network Port conditions in a single ACL rule must have the same value selected in the Attribute Value field. For example, you would choose FTP from the Attribute Value drop-down list for all rule conditions that specify the Attribute Name of Network Port.

The Add Rule dialog box contains settings for time rules for ACL policies. For more information about using time ranges with ACL policies, see [Time Ranges in ACL Policy Rules, on page 128](#).

Add ACL Policy Rule Dialog Box

| Field | Description |
|-------------|--|
| Name | Rule name, containing 2 to 32 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change the name after it is saved. |
| Description | Rule description, containing 1 to 256 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). |

| Field | Description |
|--------------------------|---|
| Action | <p>1 Select the action to take if the rule conditions are met:</p> <ul style="list-style-type: none"> • Drop—Drops traffic or denies access. • Permit—Forwards traffic or allows access. • Reset—Resets the connection. <p>2 Check the Log check box to enable logging.</p> |
| Condition Match Criteria | <p>Choose the match option to use:</p> <ul style="list-style-type: none"> • Match-all—Match all of the conditions (AND). • Match-any—Match any one of the conditions (OR). |
| Src-Dest-Service | |
| Source Conditions | <p>Source attributes that must be met for the rule to apply.</p> <p>1 Click Add.</p> <p>2 Enter values for the following, then click OK:</p> <ul style="list-style-type: none"> • Attribute Name • Operator • Attribute Value |
| Destination Conditions | <p>Destination attributes that must be met for the rule to apply.</p> <p>1 Click Add.</p> <p>2 Enter values for the following, then click OK:</p> <ul style="list-style-type: none"> • Attribute Type • Attribute Name • Operator • Attribute Value |

| Field | Description |
|--------------------------------|---|
| Service | <p>Service attributes that must be met for the rule to apply.</p> <ol style="list-style-type: none"> 1 Click Add. 2 Enter values for the following, then click OK: <ul style="list-style-type: none"> • Operator • Protocol • Port |
| Protocol | <p>Specify the protocols to which the rule applies:</p> <ul style="list-style-type: none"> • To apply the rule to any protocol, check the Any check box. • To apply the rule to specific protocols: <ol style="list-style-type: none"> 1 Uncheck the Any check box. 2 From the Operator drop-down list, choose a qualifier: Equal, Not Equal, Member, Not Member, In range, or Not in range. 3 In the Value fields, specify the protocol, object group, or range. |
| Ether Type | <p>Specify the encapsulated protocols to be examined for this rule:</p> <ul style="list-style-type: none"> • To examine all encapsulated protocols, check the Any check box. • To examine specific encapsulated protocols: <ol style="list-style-type: none"> 1 Uncheck the Any check box. 2 From the Operator drop-down list, choose a qualifier: Equal, Not Equal, Member, Not Member, In range, or Not in range. 3 In the Value fields, specify the hexadecimal value, object group, or hexadecimal range. |
| Time Range | |
| To apply the rule all the time | Check the Always check box. |

| Field | Description |
|--|--|
| To apply the rule for a specific time range | <ol style="list-style-type: none"> 1 Uncheck the Always check box. 2 Check the Range check box. 3 In the Absolute Start Time fields, provide the start date and time. 4 In the Absolute End Time fields, provide the end date and time. |
| To apply the rule based on membership in an object group | <ol style="list-style-type: none"> 1 Uncheck the Always check box. 2 Check the Pattern check box. 3 From the Operator drop-down list, choose member (Member of). 4 Do any of the following : <ul style="list-style-type: none"> • Choose an existing object group from the drop-down list. • Click Add Object Group to create a new object group. • Click the Resolved Object Group link to review or modify the specified object group. |

| Field | Description |
|---|---|
| To apply the rule on a periodic basis, with the frequency you specify | <ol style="list-style-type: none"> 1 Uncheck the Always check box. 2 Check the Pattern check box. 3 From the Operator drop-down list, choose range (In range). 4 In the Begin fields: <ol style="list-style-type: none"> 1 From the Begin drop-down list, choose the beginning day of the week or the frequency of the time range. 2 Choose the beginning hour and minute, and AM or PM. 5 In the End fields: <ol style="list-style-type: none"> 1 From the End drop-down list, choose the ending day of the week or frequency. 2 Choose the ending hour and minute, and AM or PM. <p>Note If you choose a frequency in the Begin drop-down list, choose the same frequency in the End drop-down list. For example, choose Weekdays from both the Begin and End drop-down lists.</p> |
| Advanced | <p>Source port attributes that must be matched for the rule to apply. To add a source port:</p> <ol style="list-style-type: none"> 1 Click Add. 2 Enter the required information, then click OK. |

Time Ranges in ACL Policy Rules

Prime Network Services Controller enables you to configure time ranges for ACL policy rules in either of the following ways:

- By specifying a time range for the ACL policy rule.
- By associating an ACL object group with the ACL policy rule.

Prime Network Services Controller supports the following types of time ranges:

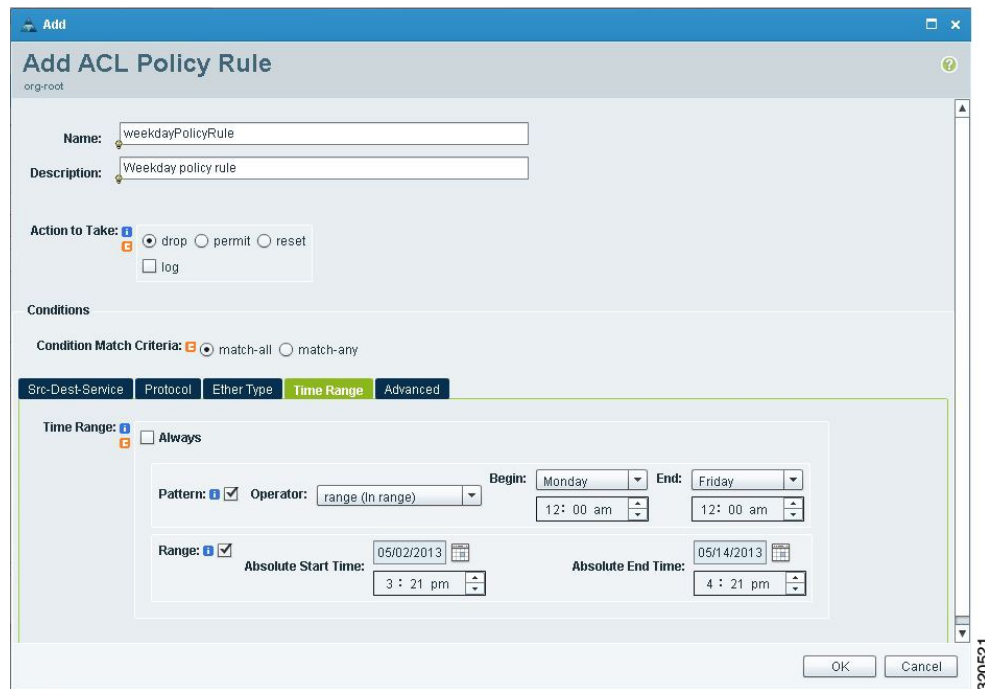
- Periodic—Specified by day-of-week start and end times (such as Sunday to Sunday), or a frequency (such as Daily, Weekdays, or Weekends). Periodic range start and end times also include options for hours and minutes.
- Absolute—Specified by a calendar date and time for start and end times, such as 01 Sep 2013 12:00 AM to 31 Dec 2013 12:00 AM.

For each ACL policy rule, you can have:

- One absolute time range.
- Any number of periodic time ranges, or none.
 - To specify a single periodic time range, add it to an ACL policy rule.
 - To specify multiple periodic time ranges, use an ACL policy object group.

The following figure shows the Time Range fields for an ACL policy rule.

Figure 1: Time Range Fields in an ACL Policy Rule



320521

Adding an ACL Policy Set

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policies > ACL > ACL Policy Sets**.
- Step 2** In the General tab, click **Add ACL Policy Set**.
- Step 3** In the Add ACL Policy Set dialog box, enter the required information as described in the following table, then click **OK**:

| Field | Description |
|--------------------|--|
| Name | Policy set name, containing 2 to 32 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change the name after it is saved. |
| Description | Policy set description, containing 1 to 256 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). |
| Admin State | Administrative state of the policy: enabled or disabled. This field is not available for all policy sets. |
| Policies | |
| Add Policy | Click to add a new policy. |
| Available | Policies that can be assigned to the policy set. Use the arrows between the columns to move policies between columns. |
| Assigned | Policies assigned to the policy set. |
| Up and down arrows | Changes the priority of the selected policies. Arrange the policies from highest to lowest priority, with the highest priority policy at the top of the list. |

Configuring Connection Timeout Policies

Prime Network Services Controller enables you to configure connection timeout policies so that you can establish timeout limits for different traffic types.

After you create a connection timeout policy, you can associate it with an edge security profile. For more information, see [Configuring Edge Security Profiles](#), on page 163.

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policies > Connection Timeout**.
- Step 2** In the General tab, click **Add Connection Timeout Policy**.
- Step 3** In the Add Connection Timeout Policy dialog box:
- a) Enter a policy name and description.
 - b) Choose whether the administrative status of the policy is to be enabled or disabled.
- Step 4** To add a rule to the policy, click **Add Rule**.
- Step 5** In the Add Connection Timeout Policy Rule dialog box, provide the information as described in [Add Connection Timeout Policy Rule Dialog Box](#), on page 131.
-

Add Connection Timeout Policy Rule Dialog Box

Table 6: Add Connection Timeout Policy Rule Dialog Box

| Field | Description |
|-------------------------------|--|
| Name | Policy name. |
| Description | Brief policy description. |
| Action | |
| Idle TCP | Length of time (in days, hours, minutes, and seconds) a TCP connection can remain idle before it is closed. |
| Half-Closed | Length of time (in days, hours, minutes, and seconds) a half-closed TCP connection can remain idle before it is freed. |
| Send Reset To Idle Connection | Check the check box to send a reset to the TCP endpoints when a TCP connection times out. |
| Idle UDP | Length of time (in days, hours, minutes, and seconds) a UDP connection can remain idle before it closes. The duration must be at least one minute, and the default value is two minutes. Enter 00:00:00:00 to disable timeout. |
| ICMP | Length of time (in days, hours, minutes, and seconds) an ICMP state can remain idle before it is closed. |

| Field | Description |
|------------------------|----------------------------------|
| Protocol | Not available for configuration. |
| Source Conditions | |
| Destination Conditions | |

Configuring DHCP Policies

Prime Network Services Controller enables you to create the following DHCP policies and apply them to edge firewalls:

- DHCP relay policy
- DHCP server policy

You can also configure DHCP relay servers for inclusion in DHCP relay policies.

The DHCP relay and DHCP server policies can be authored at the organization level and can be applied only to the inside interface of an edge firewall. When they are applied, DHCP policies allow the edge firewall to act either as a DHCP server or a DHCP relay for all VMs in the inside network.

You can apply only one DHCP server or relay profile at a time to the inside interface of the edge firewall.

For more information, see the following topics:

- [Adding a DHCP Relay Server, on page 132](#)
- [Configuring a DHCP Relay Policy, on page 133](#)
- [Configuring a DHCP Server Policy, on page 134](#)

Adding a DHCP Relay Server

DHCP relay servers are used to forward DHCP requests and replies between clients and servers when they are not on the same physical subnet. In contrast to IP router forwarding, where IP datagrams are switched between networks, DHCP relay servers receive DHCP messages and then generate a new message to send out on a different interface.

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Relay Server**.
 - Step 2** In the General tab, click **Add DHCP Relay Server**.
 - Step 3** In the New DHCP Relay Server dialog box, provide the information described in the [Add DHCP Relay Server Dialog Box, on page 133](#), then click **OK**.
-

Add DHCP Relay Server Dialog Box

| Field | Description |
|-----------------|---|
| Name | Relay server name. |
| Description | Brief description of the relay server. |
| Relay Server IP | IP address of the relay server. |
| Interface Name | Interface to use to reach the relay server. |

Configuring a DHCP Relay Policy

Prime Network Services Controller enables you to associate a DHCP relay server with a DHCP relay policy, as described in this procedure.

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Relay**.
- Step 2** In the General tab, click **Add DHCP Relay Policy**.
- Step 3** In the New DHCP Relay Policy dialog box, provide the information described in [Add DHCP Relay Policy Dialog Box](#), on page 133, then click **OK**.
-

Add DHCP Relay Policy Dialog Box

| Name | Description |
|------------------------------|--|
| Name | Policy name. |
| Description | Brief policy description. |
| DHCP Relay Server Assignment | <p>Assign a DHCP relay server in one of the following ways:</p> <ul style="list-style-type: none"> • Click Add DHCP Relay Server to add a new DHCP relay server. • In the Available Relay Servers list, select one of the available relay servers and move it to the Assigned Relay Servers list <p>You must assign at least one DHCP relay server to the policy.</p> |

Configuring a DHCP Server Policy

A DHCP server policy enables you to define the characteristics of the policy, such as ping and lease timeouts, IP address range, and DNS and WINS settings.

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Server**.
- Step 2** In the General tab, click **Add DHCP Server Policy**.
- Step 3** In the New DHCP Server Policy dialog box, provide the information as described in [Add DHCP Server Policy Dialog Box](#), on page 134, then click **OK**.
-

Add DHCP Server Policy Dialog Box

| Field | Description |
|--|---|
| General Tab | |
| Name | Policy name. |
| Description | Brief policy description. |
| Ping Timeout (Milliseconds) | Amount of time (in milliseconds) that the DHCP server waits for a ping reply before it stops attempting to reach a pool address for client assignment. The valid range is 10 to 10000 milliseconds. |
| Lease Timeout | Amount of time (in days, hour, minutes, and seconds) that the DHCP server allocates an IP address to a DHCP client before reclaiming and then reallocating it to another client. The default value is 00:01:00:00 (one hour). |
| Edge Firewall Interface Using the DHCP Client for DHCP Server Auto Configuration | To enable DHCP server automatic configuration, enter the name of the edge firewall interface that uses the DHCP client. For ASA 1000V instances, this interface is always an outside interface. Leaving this field empty indicates that the automatic configuration feature is disabled. |
| Policies Tab | |

| Field | Description |
|------------------|--|
| DNS Settings | <p>DNS settings used by the edge firewall when configuring DHCP clients.</p> <p>To add a new entry, click Add DNS Setting and add the required information.</p> |
| WINS Servers | <p>Windows Internet Naming Service (WINS) name servers that are available to DHCP clients.</p> <p>To add a new WINS server, click Add WINS Server and enter the WINS server IP address.</p> <p>WINS servers are listed in the order of preference, with the most preferred WINS server at the top. Select an entry in the table, and then use the arrows above the table to change server priority.</p> |
| IP Address Range | <p>Enter the following information for the DHCP address pool:</p> <ul style="list-style-type: none"> • Start IP Address—Beginning IP address of the pool. • End IP Address—Ending IP address of the pool. • Subnet Mask—Subnet mask to apply to the address pool. |

Configuring IP Audit and IP Audit Signature Policies

The IP audit feature provides basic Intrusion Prevention System (IPS) support for ASA 1000V instances. Prime Network Services Controller supports a basic list of signatures, and enables you to configure policies that specify one or more actions to apply to traffic that matches a signature.

The following IP audit policies are available:

- Audit policies
- Signature policies

When you associate an IP audit policy with a device, the policy is applied to all traffic on the outside interface of the device.

The following topics describe how to configure these policies.

Configuring IP Audit Policies

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policies > IP Audit > Audit Policies**.
- Step 2** In the General tab, click **Add IP Audit Policy**.
- Step 3** In the Add IP Audit Policy dialog box provide the following information:
- Policy name
 - Policy description
 - In the Admin State field, choose whether the administrative state of the policy is to be enabled or disabled.
- Step 4** To add a rule to the policy, click **Add Rule** in the Rule Table toolbar.
- Step 5** In the Add IP Audit Policy Rule dialog box, provide the information as described in [Add IP Audit Policy Rule Dialog Box](#), on page 136, then click **OK** in the open dialog boxes.
-

Add IP Audit Policy Rule Dialog Box

Table 7: IP Audit Policy Rule Dialog Box

| Field | Description |
|---------------------|--|
| Name | Rule name. |
| Description | Brief rule description. |
| Attack-Class Action | <p>Check the check boxes of the actions to take for signature type Attack if the conditions of the rule are met:</p> <ul style="list-style-type: none"> • Log—Send a message indicating that a packet matched the signature. • Drop—Drop the packet. • Reset Flow—Drop the packet and reset the connection. |

| Field | Description |
|----------------------------|---|
| Informational-Class Action | <p>Check the check boxes of the actions to take for signature type Informational if the conditions of the rule are met:</p> <ul style="list-style-type: none"> • Log—Send a message indicating that a packet matched the signature. • Drop—Drop the packet. • Reset Flow—Drop the packet and reset the connection. |
| Protocol | Not available for configuration. |
| Source Conditions | |
| Destination Conditions | |

Configuring IP Audit Signature Policies

An IP audit signature policy identifies the signatures that are enabled and disabled. By default, all signatures are enabled. You can disable a signature when legitimate traffic matches the signature in most situations, resulting in false alarms. However, disabling the signature is performed at a global level, meaning that no traffic will trigger the signature (even bad traffic) when it is disabled.

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policies > IP Audit > Signature Policies**.
- Step 2** In the General tab, click **Add IP Audit Signature Policy**.
- Step 3** In the Add IP Audit Signature Policy dialog box, enter a name and description for the policy.
- Step 4** In the Signatures area, move signatures between the Enabled Signatures and Disabled Signatures lists as required.
- Note** We recommend that you do not disable signatures unless you are sure you understand the consequences of doing so.
- You can view additional information about a signature by selecting the required signature and clicking **Properties**.
- Step 5** After you have made all adjustments, click **OK**.
-

Configuring NAT/PAT Policies and Policy Sets

Prime Network Services Controller supports Network Address Translation (NAT) and Port Address Translation (PAT) policies for controlling address translation in the deployed network. These policies support both static and dynamic translation of IP addresses and ports.

Prime Network Services Controller enables you to configure the following policy items:

- NAT policy—Can contain multiple rules, which are evaluated sequentially until a match is found.
- NAT policy set—Group of NAT policies that can be associated with an edge security profile. When the profile is applied, the NAT policies are applied only to ingress traffic.
- PAT policy—Supports source dynamic and destination static interface PAT on edge firewalls.

The following topics describe how to configure NAT and PAT policies, and NAT policy sets.

Configuring NAT/PAT Policies

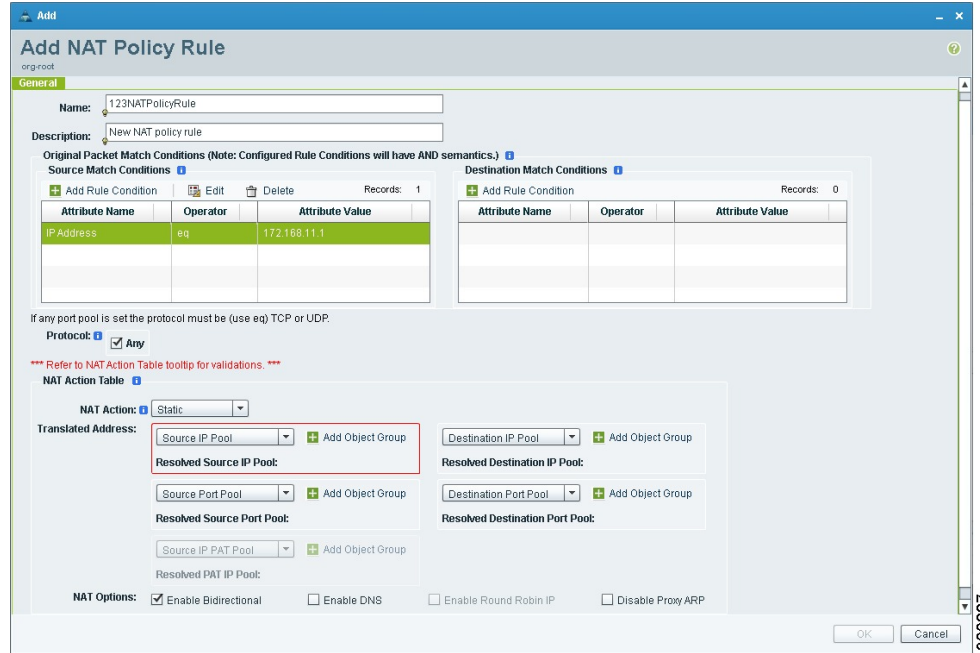
This procedure describes how to configure NAT/PAT policies with Prime Network Services Controller.

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.
 - Step 2** In the General tab, click **Add NAT Policy**.
 - Step 3** In the Add NAT Policy dialog box, enter a name and description for the policy.
 - Step 4** In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.
 - Step 5** To add a rule to the policy, click **Add Rule**.
 - Step 6** In the Add NAT Policy Rule dialog box, provide the information as described in [Add NAT Policy Rule Dialog Box](#), on page 139, then click **OK** in the open dialog boxes.
-

Add NAT Policy Rule Dialog Box

Figure 2: Add NAT Policy Rule Dialog Box



Add NAT Policy Rule Dialog Box

Add NAT Policy Rule Dialog Box

| Field | Description |
|---|---|
| Name | Rule name. |
| Description | Brief rule description. |
| Original Packet Match Conditions | |
| Source Match Conditions | Source attributes that must be matched for the current policy to apply. To add a new condition, click Add Rule Condition . Available source attributes are IP Address and Network Port. |

300987

| Field | Description |
|------------------------------|--|
| Destination Match Conditions | <p>Destination attributes that must be matched for the current policy to apply.</p> <p>To add a new condition, click Add Rule Condition. Available destination attributes are IP Address and Network Port.</p> |
| Protocol | <p>Specify the protocols to which the rule applies:</p> <ul style="list-style-type: none"> • To apply the rule to any protocol, check the Any check box. • To apply the rule to specific protocols: <ol style="list-style-type: none"> 1 Uncheck the Any check box. 2 From the Operator drop-down list, choose a qualifier: Equal, Not equal, Member, Not Member, In range, or Not in range. 3 In the Value fields, specify the protocol, object group, or range. |
| NAT Action Table | |
| NAT Action | From the drop-down list, choose the required translation option: Static or Dynamic. |
| Translated Address | <p>Identify a translated address pool for each original packet match condition from the following options:</p> <ul style="list-style-type: none"> • Source IP Pool • Source Port Pool • Source IP PAT Pool • Destination IP Pool • Destination Port Pool <p>For example, if you specify a source IP address match condition, you must identify a Source IP Pool object group. Similarly, a destination network port match requires a Destination Port Pool object group.</p> <p>The Source IP PAT Pool option is available only if you choose dynamic translation.</p> <p>Click Add Object Group to add object groups for the translation actions.</p> |

| Field | Description |
|-------------|---|
| NAT Options | <p>Check and uncheck the check boxes as required:</p> <ul style="list-style-type: none"> • Enable Bidirectional—Check the check box for connections to be initiated bidirectionally; that is, both to and from the host. Available only for static address translation. • Enable DNS—Check the check box to enable DNS for NAT. • Enable Round Robin IP—Check the check box to allocate IP addresses on a round-robin basis. Available only for dynamic address translation. • Disable Proxy ARP—Check the check box to disable proxy ARP. Available only for static address translation. |

Configuring NAT Policy Sets

Policy sets enable you to group multiple policies of the same type (such as NAT, ACL, or Interface) for inclusion in a profile. NAT policy sets are groups of NAT policies that can be associated with an edge security profile.

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policy Sets**.
 - Step 2** In the General tab, click **Add NAT Policy Set**.
 - Step 3** In the Add NAT Policy Set dialog box, enter a name and description for the policy set.
 - Step 4** In the Admin State field, indicate whether the administrative status of the policy is to be enabled or disabled.
 - Step 5** In the Policies area, select the policies to include in this policy set:
 - a) In the Available list, select one or more policies and move them to the Assigned list.
 - b) Adjust the priority of the assigned policies by using the arrow keys above the list.
 - c) If required, click **Add NAT Policy** to add a new policy and include it in the Assigned list.
For information on configuring a NAT policy, see [Configuring NAT/PAT Policies, on page 138](#).
 - Step 6** Click **OK**.
-

Configuring PAT for Edge Firewalls

Prime Network Services Controller enables you to configure source and destination interface PAT for edge firewalls, such as the ASA 1000V. For more information, see the following topics.

Configuring Source Dynamic Interface PAT

Prime Network Services Controller enables you to configure source dynamic interface PAT for edge firewalls, such as ASA 1000Vs.

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.
 - Step 2** In the General tab, click **Add NAT Policy**.
 - Step 3** In the Add NAT Policy dialog box, enter a name and description for the policy.
 - Step 4** In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.
 - Step 5** Click **Add Rule** to add a rule to this policy.
 - Step 6** In the Add NAT Policy Rule dialog box, provide the information described in [Add NAT Policy Rule Dialog Box](#), on page 139 with the following specific settings, then click **OK**:
 - a) From the NAT Action drop-down list, choose **Dynamic**.
 - b) In the Translated Address area, add a Source IP Pool object group that contains the ASA 1000V outside interface IP address.
 - Step 7** Click **OK**.
-

Configuring Destination Static Interface PAT

Prime Network Services Controller enables you to configure destination static interface PAT for edge firewalls, such as ASA 1000Vs, as described in the following procedure.

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.
 - Step 2** In the General tab, click **Add NAT Policy**.
 - Step 3** In the Add NAT Policy dialog box, enter a name and description for the policy.
 - Step 4** In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.
 - Step 5** Click **Add Rule** to add a rule to this policy.
 - Step 6** In the Add NAT Policy Rule dialog box, enter the IP address of the ASA 1000V outside interface as a rule condition for Destination Match Conditions.
 - Step 7** Configure other options in the Add NAT Policy Rule dialog box as described in [Add NAT Policy Rule Dialog Box](#), on page 139, then click **OK**.

Note If any of the IP address fields includes a range that starts or ends with the IP address of the outside interface of the ASA 1000V, an error message will be displayed that identifies an overlap with the ASA 1000V interface IP address.
 - Step 8** Click **OK**.
-

Configuring Packet Inspection Policies

Prime Network Services Controller enables you to configure policies for application-layer protocol inspection. Inspection is required for services that embed IP addressing information in the user data packet, or that open secondary channels on dynamically assigned ports. When inspection is configured, the end device performs a deep packet inspection instead of quickly passing the packet on. As a result, inspection can affect overall device throughput.

[Protocols Supported for Packet Inspection Policies, on page 143](#) lists the application-layer protocols supported by Prime Network Services Controller.

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policies > Packet Inspection**.
 - Step 2** In the General tab, click **Add Packet Inspection Policy**.
 - Step 3** In the Add Packet Inspection Policy dialog box, enter a name and description for the policy.
 - Step 4** In the Admin State field, indicate whether the administrative status of the policy is enabled or disabled.
 - Step 5** To add a rule to the policy, click **Add Rule**.
 - Step 6** In the Add Packet Inspection Policy Rule Dialog box, provide the information as described in [Add Packet Inspection Policy Rule Dialog Box, on page 144](#), then click **OK** in the open dialog boxes.
-

Protocols Supported for Packet Inspection Policies

Protocols Supported for Packet Inspection Policies

| | | | |
|-----------|--------------------|--------|----------|
| CTIQBE | ICMP | PPTP | SQL *Net |
| DCE/RPC | ICMP Error | RSH | SunRPC |
| DNS | ILS | RSTP | TFTP |
| FTP | IP Options | SIP | WAAS |
| H323 H225 | IPsec Pass-Through | Skinny | XDMCP |
| H323 RAS | MGCP | SMTP | |
| HTTP | NetBIOS | SNMP | |

Add Packet Inspection Policy Rule Dialog Box

Table 8: Add Packet Inspection Policy Rule Dialog Box

| Field | Description |
|------------------------|--|
| Name | Rule name. |
| Description | Brief rule description. |
| Action | Under Enable Inspections, check the check boxes of protocols to be inspected if the rule conditions are met. |
| Protocol | Not available for configuration. |
| Source Conditions | |
| Destination Conditions | |

Configuring Routing Policies

Prime Network Services Controller enables you to use routing policies to configure static routes for managed endpoints on an edge firewall.



Note You can configure only inside and outside interfaces on edge firewalls by using Prime Network Services Controller. Use the CLI to configure routes on the edge firewall management interface.

After you configure a static route routing policy, you can implement the policy by:

- Including the routing policy in an edge device profile.
- Applying the edge device profile to an edge firewall that has managed endpoints.

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policies > Routing**.
- Step 2** In the General tab, click **Add Routing Policy**.
- Step 3** In the Add Routing Policy dialog box, enter a name and brief description for the routing policy.
- Step 4** To add a new static route, click **Add Static Route**.
- Step 5** In the Add Static Route dialog box, enter the following information:
 - a) In the Destination Network fields, enter the IP route prefix and prefix mask for the destination.
 - b) In the Forwarding (Next Hop) fields, enter the IP address of the next hop that can be used to reach the destination network.

Note The Forwarding Interface field applies only to ASA 1000V data interfaces. Use the CLI to configure routes on the ASA 1000V management interface.

c) (Optional) In the Distance Metric field, enter the distance metric.

Step 6 Click **OK**.

Configuring TCP Intercept Policies

Prime Network Services Controller enables you to configure TCP intercept policies that you can then associate with an edge security profile. TCP intercept policies that you associate with a device via an edge security profile are applied to all traffic on the outside interface of the device.

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policies > TCP Intercept**.
- Step 2** In the General tab, click **Add TCP Intercept Policy**.
- Step 3** In the Add TCP Intercept Policy dialog box, enter a name and brief description for the policy.
- Step 4** In the Admin State field, indicate whether the administrative status of the policy is to be enabled or disabled.
- Step 5** To add a rule to the policy, click **Add Rule**.
- Step 6** In the Add TCP Intercept Policy Rule dialog box, provide the information as described in [Add TCP Intercept Policy Rule Dialog Box](#), on page 145.

Add TCP Intercept Policy Rule Dialog Box

| Field | Description |
|---|--|
| Name | Rule name. |
| Description | Brief rule description. |
| Maximum Number of Embryonic TCP Connections (0-65535) | <p>Number of embryonic TCP connections allowed overall and per client:</p> <ol style="list-style-type: none"> 1 In the Total field, enter the maximum number of embryonic TCP connections allowed. 2 In the client field, enter the maximum number of embryonic TCP connections allowed per client. <p>The default value 0 (zero) indicates unlimited connections.</p> |
| Protocol | Not available for configuration. |

| Field | Description |
|------------------------|----------------------------------|
| Source Conditions | Not available for configuration. |
| Destination Conditions | Not available for configuration. |

Configuring Site-to-Site IPsec VPN Policies

Prime Network Services Controller enables you to configure site-to-site IPsec VPNs. In addition, you can configure a crypto map policy and attach it to an edge profile. For ease of configuration and to keep logical IPsec entities separate, configuration is divided into the following sections:

- Configuring Crypto Map Policies
- Configuring IKE Policies
- Configuring Interface Policy Sets
- Configuring IPsec Policies
- Configuring Peer Authentication Policies
- Configuring VPN Device Policies

To access VPN policies, choose **Policy Management > Service Policies > root > Policies > VPN**.

Configuring Crypto Map Policies

Prime Network Services Controller enables you to create crypto map policies that include:

- Rules for source and destination conditions.
- IP Security (IPsec) options, including an IPsec policy.
- Internet Key Exchange (IKE) options, including a peer device.

Crypto map policies are applied to interfaces by means of their inclusion in interface policy sets and edge security policies.

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policies > VPN > Crypto Map Policies**.
 - Step 2** In the General tab, click **Add Crypto Map Policy**.
 - Step 3** In the Add Crypto Map Policy dialog box, provide the information as described in [Add Crypto Map Policy Dialog Box](#), on page 147, then click **OK**.
 - Step 4** To add a policy rule, click **Add Rule** in the General tab and provide the required information as described in [Add Crypto Map Policy Rule Dialog Box](#), on page 149.
-

Add Crypto Map Policy Dialog Box

| Field | Description |
|-----------------------------------|---|
| General Tab | |
| Name | Policy name. |
| Description | Brief policy description. |
| Admin State | Whether the administrative status of the policy is enabled or disabled. |
| Rule Table | |
| Add Rule | Click Add Rule to add a new rule to the current policy. |
| IPsec Settings Tab | |
| SA Lifetime | Length of time (in days, hours, minutes, and seconds) that a security association (SA) lives before expiring. |
| SA Lifetime Traffic (KB) | Volume of traffic, in kilobytes, that can pass between IPsec peers using a given SA before that association expires. |
| Enable Perfect Forwarding Secrecy | Whether or not Perfect Forward Secrecy (PFS) is enabled. PFS is a cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. |
| Diffie-Hellman Group | Available if PFS is enabled. Choose the Diffie-Hellman (DH) group for this policy: <ul style="list-style-type: none"> • Group 1—The 768-bit DH group. • Group 2—The 1024-bit DH group. • Group 5—The 1536-bit DH group. |
| IPsec Policies | The IPsec policy that applies to the current policy. Select an existing IPsec policy or click Add IPsec Policy to create a new policy. |

| Field | Description |
|--------------------------------|--|
| Peer Device | Peer device. Choose an existing peer or click Add Peer Device to add a new peer. In the Add Peer Device dialog box, enter the peer device IP address or hostname. |
| Other Settings Tab | |
| Enable NAT Traversal | Whether or not IPsec peers can establish a connection through a NAT device. |
| Enable Reverse Route Injection | Whether or not static routes are automatically added to the routing table and then announced to neighbors on the private network. |
| Connection Type | Connection type for this policy: <ul style="list-style-type: none"> • Answer-Only—Responds only to inbound IKE connections during the initial proprietary exchange to determine the appropriate peer to which to connect. • Bidirectional—Accepts and originates connections based on this policy. • Originate-Only—Initiates the first proprietary exchange to determine the appropriate peer to which to connect. |
| Negotiation Mode | Mode to use for exchanging key information and setting up SAs: <ul style="list-style-type: none"> • Aggressive Mode—Faster mode, using fewer packets and exchanges, but does not protect the identity of the communicating parties. • Main Mode—Slower mode, using more packets and exchanges, but protects the identities of the communicating parties. |
| DH Group for Aggressive Mode | DH group to use when in aggressive mode: Group 1, Group 2, or Group 5. |

Add Crypto Map Policy Rule Dialog Box

| Field | Description |
|------------------------|--|
| Name | Rule name. |
| Description | Brief rule description. |
| VPN Action | Action to take based on this rule: Permit or Deny. |
| Protocol | <p>Protocols to examine for this rule:</p> <ul style="list-style-type: none"> • To examine all protocols, check the Any check box. • To examine specific protocols: <ol style="list-style-type: none"> 1 Uncheck the Any check box. 2 From the Operator drop-down list, choose a qualifier: Equal, Not equal, Member, Not Member, In range, or Not in range. 3 In the Value fields, specify the protocol, object group, or range. |
| Source Conditions | <p>Source attributes that must be matched for the rule to apply.</p> <p>To add a new condition, click Add Rule Condition.</p> <p>Available source attributes are IP Address and Network Port.</p> |
| Destination Conditions | <p>Destination attributes that must be matched for the rule to apply.</p> <p>To add a new condition, click Add Rule Condition.</p> <p>Available destination attributes are IP Address and Network Port.</p> |

Configuring IKE Policies

The Internet Key Exchange (IKE) protocol is a hybrid protocol that implements Oakley and SKEME key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. The initial IKE implementation used the IPsec protocol, but IKE can be used with other protocols. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates the IPsec Security Associations (SAs).

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policies > VPN > IKE Policies**.
- Step 2** In the General tab, click **Add IKE Policy**.
- Step 3** In the Add IKE Policy dialog box, enter a name and description for the policy.
- Step 4** Configure either an IKE V1 or IKE V2 policy:
- IKE V1 Policy
 - 1 Click **Add IKE V1 Policy**.
 - 2 In the Add IKE V1 Policy dialog box, provide the information described in [IKE V1 Policy Dialog Box](#), on page 150, then click **OK**.
 - IKE V2 Policy
 - 1 Click **Add IKE V2 Policy**.
 - 2 In the Add IKE V2 Policy dialog box, provide the information described in [IKE V2 Policy Dialog Box](#), on page 150, then click **OK**.
- Step 5** Click **OK**.
-

IKE V1 Policy Dialog Box

| Field | Description |
|----------------|---|
| DH Group | Diffie-Hellman group: Group 1, Group 2, or Group 5. |
| Encryption | Encryption method: 3DES, AES, AES-192, AES-256, or DES. |
| Hash | Hash algorithm: MD5 or SHA. |
| Authentication | Authentication method is Preshared key. |
| SA Lifetime | Length of time (in days, hours, minutes, and seconds) that an SA lives before expiring. |

IKE V2 Policy Dialog Box

| Field | Description |
|----------|---|
| DH Group | Diffie-Hellman group: Group 1, Group 2, Group 5, or Group 14. |

| Field | Description |
|-----------------------------|---|
| Encryption | Encryption method: 3DES, AES, AES-192, AES-256, or DES. |
| Hash | Hash integrity algorithm: MD5, SHA, SHA256, SHA384, or SHA512. |
| Pseudo Random Function Hash | Pseudo-random function (PRF) has algorithm: MD5, SHA, SHA256, SHA384, or SHA512. |
| SA Lifetime | Length of time (in days, hours, minutes, and seconds) that an SA lives before expiring. |

Configuring Interface Policy Sets

Interface policy sets enable you to group multiple policies for inclusion in an edge security profile.

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policies > VPN > Interface Policy Sets**.
 - Step 2** In the General tab, click **Add Interface Policy Set**.
 - Step 3** In the Add Interface Policy Set dialog box, provide the information as described in [Add Interface Policy Set Dialog Box](#), on page 151, then click **OK**.
-

Add Interface Policy Set Dialog Box

General Tab

| Field | Description |
|-----------------------|--|
| Name | Policy set name. |
| Description | Brief description of the policy set. |
| Admin State | Administrative state of the policy set: enabled or disabled. |
| Policies Area | |
| Add Crypto Map Policy | Click to add a new policy. |

| Field | Description |
|--------------------|--|
| Available | Policies that can be assigned to the policy set. Use the arrows between the columns to move policies between columns. |
| Assigned | Policies assigned to the policy set. |
| Up and down arrows | Changes the priority of the selected policies. Arrange the policies from highest to lowest priority, with the highest priority policy at the top of the list. |

Domain Settings Tab

| Field | Description |
|--------------------------------------|--|
| Enable IKE (Must check at least one) | Check the appropriate check box to specify IKE V1 or IKE V2. |
| Enable IPsec Pre-fragmentation | Check the check box to fragment packets before encryption. Pre-fragmentation minimizes post-fragmentation (fragmentation after encryption) and the resulting reassembly before decryption, thereby improving performance. |
| Do Not Fragment | Available only if the Enable IPsec Pre-fragmentation check box is checked. From the drop-down list, choose the action to take with the Don't Fragment (DF) bit in the encapsulated header: <ul style="list-style-type: none"> • Clear • Copy • Set |

Configuring IPsec Policies

IPsec policies define the IPsec policy objects used to create a secure IPsec tunnel for a VPN.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > VPN > IPsec Policies**.

Step 2 In the General tab, click **Add IPsec Policy**.

Step 3 In the Add IPsec Policy dialog box, enter a name and description for the policy.

You must configure either an IKE V1 or IKE V2 proposal for an IPsec policy.

Step 4 To configure an IKE V1 proposal:

- a) In the IKE v1 Proposal Table area, click **Add IPsec IKEv1 Proposal**.
- b) In the IPsec IKEv1 Proposal dialog box, provide the information described in [IPsec IKEv1 Proposal Dialog Box, on page 153](#), then click **OK**.

Step 5 To configure an IKE V2 proposal:

- a) In the IKE v2 Proposal Table area, click **Add IPsec IKE v2 Proposal**.
- b) In the IPsec IKEv2 Proposal dialog box, provide the information described in [IPsec IKEv2 Proposal Dialog Box, on page 154](#), then click **OK**.

Step 6 Click **OK** to save the policy.

IPsec IKEv1 Proposal Dialog Box

| Field | Description |
|----------------|---|
| Mode | Mode in which the IPsec tunnel operates. In Tunnel mode, the IPsec tunnel encapsulates the entire IP packet. |
| ESP Encryption | Encapsulating Security Protocol (ESP) encryption method: <ul style="list-style-type: none"> • 3DES—Encrypts three times according to the Data Encryption Standard (DES) using 56-bit keys. • AES—Encrypts according to the Advanced Encryption Standard (AES) using 128-bit keys. • AES-192—Encrypts according to the AES using 192-bit keys. • AES-256—Encrypts according to the AES using 256-bit keys. • DES—Encrypts according to the DES using 56-bit keys. • Null—Null encryption algorithm. Transform sets defined with ESP-Null provide authentication without encryption; this method is typically used for testing purposes only. |

| Field | Description |
|--------------------|---|
| ESP Authentication | <p>Hash authentication algorithm:</p> <ul style="list-style-type: none"> • MD5—Produces a 128-bit digest. • Null—Does not perform authentication. • SHA—Produces a 160-bit digest. |

IPsec IKEv2 Proposal Dialog Box

| Field | Description |
|--------------------------------|---|
| ESP Encryption Algorithm Table | <p>To add an ESP encryption method:</p> <ol style="list-style-type: none"> 1 Click Add ESP Encryption Algorithm. 2 From the ESP Encryption drop-down list, choose the encryption method: <ul style="list-style-type: none"> • 3DES—Encrypts three times according to the Data Encryption Standard (DES) using 56-bit keys. • AES—Encrypts according to the Advanced Encryption Standard (AES) using 128-bit keys. • AES-192—Encrypts according to the AES using 192-bit keys. • AES-256—Encrypts according to the AES using 256-bit keys. • DES—Encrypts according to the DES using 56-bit keys. • Null—Null encryption algorithm. Transform sets defined with ESP-Null provide authentication without encryption; this method is typically used for testing purposes only. |

| Field | Description |
|---------------------------|---|
| Integrity Algorithm Table | <p>To add an integrity algorithm:</p> <ol style="list-style-type: none"> 1 Click Add Integrity Algorithm. 2 From the Integrity Algorithm drop-down list, choose the authentication algorithm: <ul style="list-style-type: none"> • MD5—Produces a 128-bit digest. • Null—Does not perform authentication. • SHA—Produces a 160-bit digest. |

Configuring Peer Authentication Policies

Use a peer authentication policy to define the method used to authenticate a peer.

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policies > VPN > Peer Authentication Policies**.
 - Step 2** In the General tab, click **Add Peer Authentication Policy**.
 - Step 3** In the Add Peer Authentication Policy dialog box, enter a name and description for the policy.
 - Step 4** Click **Add Policy to Authenticate Peer**.
 - Step 5** In the Add Policy to Authenticate Peer dialog box, provide the information described in [Add Policy to Authenticate Peer Dialog Box](#), on page 155, then click **OK**.
 - Step 6** Click **OK** to save the policy.
-

Add Policy to Authenticate Peer Dialog Box

| Field | Description |
|----------------------|---|
| Peer Device (Unique) | Unique IP address or hostname of the peer. |
| IKEv1 Area | |
| Local | Preshared key. |
| Confirm | Preshared key for confirmation. |
| Set | Whether or not the preshared key has been set and is properly configured (read-only). |
| IKEv2 Area | |

| Field | Description |
|---------|--|
| Local | Local preshared key. |
| Confirm | Local preshared key for confirmation. |
| Set | Whether or not the local preshared key has been set and is properly configured (read-only). |
| Remote | Remote preshared key. |
| Confirm | Remote preshared key for confirmation. |
| Set | Whether or not the remote preshared key has been set and is properly configured (read-only). |

Configuring VPN Device Policies

A VPN device policy enables you to specify VPN global settings, such as:

- IKE policy
- IKE global settings
- IPsec global settings
- Peer authentication policy

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policies > VPN > VPN Device Policies**.
- Step 2** In the General tab, click **Add VPN Device Policy**.
- Step 3** In the Add VPN Device Policy dialog box, provide the information as described in [Add VPN Device Policy Dialog Box](#), on page 157.
- Step 4** As needed, provide the information described in the following tables:
- [Configuring IKE Policies](#), on page 149
 - [Configuring Peer Authentication Policies](#), on page 155
- Step 5** Click **OK** to create the policy.
-

Add VPN Device Policy Dialog Box

General Tab


Note

A VPN device policy requires both an IKE policy and a peer authentication policy.

| Field | Description |
|----------------------------|--|
| Name | Policy name. |
| Description | Brief policy description. |
| IKE Policy | Choose an existing policy from the drop-down list, or click Add IKE Policy to add a new policy. |
| Peer Authentication Policy | Choose an existing policy from the drop-down list, or click Add Peer Authentication Policy to add a new policy. |

IKE Settings Tab

| Field | Description |
|---|---|
| Enable IPsec over TCP | Whether or not IPsec traffic is allowed over TCP. If IPsec over TCP is enabled, this method takes precedence over all other connection methods. |
| Send Disconnect Notification | Whether or not clients are notified that sessions will be disconnected. |
| Allow Inbound Aggressive Mode | Whether or not inbound aggressive mode is permitted. |
| Wait for Termination before Rebooting | Whether or not a reboot can occur only when all active sessions have terminated voluntarily. |
| Threshold for Cookie Challenge (0-100 Percent) | Percentage of the maximum number of allowed Security Associations (SAs) that can be in-negotiation (open) before cookie challenges are issued for future SA negotiations. |
| Negotiation Threshold for Maximum SAs (0-100 Percent) | Percentage of the maximum number of allowed SAs that can be in-negotiation before additional connections are denied. The default value is 100 percent. |

| Field | Description |
|---|--|
| IKE Identity | Phase 2 identification method: <ul style="list-style-type: none"> • Automatic—Determines ISAKMP negotiation by connection type: <ul style="list-style-type: none"> ◦ IP address for a preshared key. ◦ Cert DN for certificate authentication. • IP Address—IP address of the host exchanging ISAKMP identity information. • Hostname—Fully qualified domain name of the host exchanging ISAKMP identity information. • Key ID—String used by the remote peer to look up the preshared key. |
| Key for IKE Identity | The key to use for IKE identify if the IKE identification method is Key ID. |
| NAT Traversal | Whether or not IPsec peers can establish a connection through a NAT device. |
| Keep-Alive Time for NAT Traversal | Length of time (in hours, minutes, and seconds) that a tunnel can exist with no activity before the device sends keepalive messages to the peer. Values range from 10 to 3600 seconds, with a default of 20 seconds. |
| IKEv2 IPsec Maximum Security Associations | Whether or not the total number of IKE V2 SAs on the node can be set. |
| Maximum Number of SA | Maximum number of SA connections allowed. |
| IKEv1 over TCP Port Table | <ol style="list-style-type: none"> 1 Click Add IKE V1 Over TCP Port to add a new port. 2 In the Port field, enter the TCP port to use for IKE V1. |

IPsec Settings Tab

| Field | Description |
|-------------|---|
| Anti Replay | Whether or not SA anti-replay is enabled. |

| Field | Description |
|-------------------------|--|
| Anti Replay Window Size | Window size to use to track and prevent duplication of packets. Using a larger window size allows the decryptor to track more packets. |
| SA Lifetime | Length of time (in days, hours, minutes, and seconds) that an SA can live before expiring. |
| SA Lifetime Volume (KB) | Volume of traffic, in kilobytes, that can pass between IPsec peers using a given SA before the association expires. |

Working with Profiles

A profile is a collection of policies. By creating a profile with policies that you select, and then applying that profile to multiple objects, such as edge firewalls, you can ensure that those objects have consistent policies.

A device must be registered to Prime Network Services Controller before you can apply a profile to it.

Prime Network Services Controller enables you to create and apply the following types of profiles:

- Compute security profiles—Compute firewall profiles that include ACL policies and user-defined attributes.
- Edge device profiles—Edge firewall profiles that include routing, VPN, DHCP, and IP Audit policies.
- Edge security profiles—Edge firewall profiles that include access and threat mitigation policies.

The following topics describe how to configure and apply profiles.

Configuring Compute Security Profiles

Prime Network Services Controller enables you to create compute security profiles at the root or tenant level. Creating a compute security profile at the root level enables you to apply the same profile to multiple tenants.

Procedure

-
- Step 1** Choose **Policy Management > Service Profiles > root > Compute Firewall > Compute Security Profiles**.
 - Step 2** In the General tab, click **Add Compute Security Profile**.
 - Step 3** In the Add Compute Security Profile dialog box, provide the information as described in [Add Compute Security Profile Dialog Box](#), on page 160, then click **OK**.
-

Add Compute Security Profile Dialog Box

General Tab

| Field | Description |
|-------------------------------|--|
| Name | Profile name. This name can be between 2 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved. |
| Description | Brief profile description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. |
| Policy Set | Drop-down list of policy sets. |
| Add ACL Policy Set | Click the link to add an ACL policy set. |
| Resolved Policy Set | Click the link to edit the resolved policy set. |
| Resolved Policies Area | |
| (Un)assign Policy | Click the link to assign or unassign a policy. |
| Name | Rule name. |
| Source Condition | Source condition for the rule. |
| Destination Condition | Destination condition for the rule. |
| Service/Protocol | Service or protocol to which the rule applies. |
| EtherType | Encapsulated protocol to which the rule applies. |
| Action | Action to take if the rule conditions are met. |
| Description | Rule description. |

Attributes Tab

| Field | Description |
|----------------------------|---|
| Add User Defined Attribute | Opens a dialog box for adding an attribute. |

| Field | Description |
|-------|------------------|
| Name | Attribute name. |
| Value | Attribute value. |

Verifying Compute Firewall Policies

Use this procedure to verify active policies and optionally modify policy objects for compute firewalls.

Procedure

-
- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Compute Firewalls > compute-firewall**.
 - Step 2** In the Compute Security Profiles tab, select the required policy, then click **Show Resolved Policies**.
 - Step 3** In the Edit dialog box, click the required policy in the Resolved Policies table to view the policy details, such as source and destination conditions.
 - Step 4** To modify a policy, in the Policy Set area, either choose a different policy from the drop-down list, or click **Add ACL Policy Set** to configure a new policy.
 - Step 5** Click **Apply** to accept any changes or **OK** when you have finished reviewing the policies.
-

Configuring Edge Device Profiles

Edge device profiles contain the following policies in addition to a timeout value for address translation:

- DHCP
- IP audit signature
- Routing
- VPN device

You can create an edge device profile at any level of the organization hierarchy (root, tenant, virtual data center (VDC), app, or tier). Creating an edge device profile at the root level enables you to apply it to multiple edge firewalls for different tenants.

Procedure

-
- Step 1** Choose **Policy Management > Service Profiles > root > Edge Firewall > Edge Device Profiles**.
 - Step 2** In the General tab, click **Add Edge Device Profile**.
 - Step 3** In the Add Edge Device Profile dialog box, enter the information as described in [Edge Device Profile Dialog Box](#), on page 162, then click **OK**.
-

Edge Device Profile Dialog Box

| Field | Description |
|------------------------------|---|
| Toolbar | |
| Clone | Clones the current profile. |
| General Tab | |
| Name | Profile name. |
| Description | Brief profile description. |
| Policies Tab | |
| Routing Policy | Choose an existing policy or click Add Routing Policy to add a new policy. Click the Resolved Policy link to review or modify the assigned policy. |
| IP Audit Signature Policy | Choose an existing policy or click Add IP Audit Signature Policy to add a new policy. Click the Resolved Policy link to review or modify the assigned policy. |
| VPN Device Policy | Choose an existing policy or click Add VPN Device Policy to add a new policy. Click the Resolved Policy link to review or modify the assigned policy. |
| Address Translations Timeout | Length of time (in days, hours, minutes, and seconds) that a translation can remain unused before it expires. |
| DHCP Policy Table | |
| Edge DHCP Policy | Click to add a new DHCP policy. |
| Type | Type of DHCP service: relay or server. |
| Interface Name | Interface to which the DHCP policy is applied. |
| Server/Relay Policy | DHCP policy name. |

Events Tab

| Field | Description |
|-------------|--|
| ID | Unique event identifier. |
| User | One of the following user types: <ul style="list-style-type: none"> • admin • internal |
| Created at | Date and time at which the fault occurred. |
| Cause | Unique identifier associated with the event cause. |
| Description | Event description. |

Configuring Edge Security Profiles

Edge security profiles can include any of the following:

- ACL policy sets (ingress and egress)
- Connection timeout policies
- IP audit policies
- NAT policy sets
- Packet inspection policies
- TCP intercept policies
- VPN interface policy sets

You can create an edge security profile at any level of the organizational hierarchy (root, tenant, VDC, app, or tier). Creating an edge security profile at the root level enables you to apply it to multiple edge firewalls for different tenants.

Procedure

-
- Step 1** Choose **Policy Management > Service Profiles > Edge Firewall > Edge Security Profiles**.
 - Step 2** In the General tab, click **Add Edge Security Profile**.
 - Step 3** In the Add Edge Security Profile dialog box provide the information as described in [Add Edge Security Profile Dialog Box](#), on page 164.
-

Add Edge Security Profile Dialog Box

| Field | Description |
|---------------------|---|
| General Tab | |
| Name | Profile name. |
| Description | Brief profile description. |
| Ingress Tab | |
| Policy Set | Choose an existing policy set or click Add ACL Policy Set to add a new policy set. Click the Resolved Ingress Policy Set link to modify the assigned policy set. |
| Resolved Policies | Click (Un)assign Policy to assign or remove a policy for the current policy set. |
| Egress Tab | |
| Policy Set | Choose an existing policy set or click Add ACL Policy Set to add a new policy set. Click the Resolved Egress Policy Set link to modify the assigned policy set. |
| Resolved Policies | Click (Un)assign Policy to assign or remove a policy for the current policy set. |
| NAT Tab | |
| Policy Set | Choose an existing policy set or click Add NAT Policy Set to add a new policy set. Click the Resolved NAT Policy Set link to modify the assigned policy set. |
| Resolved Policies | Click (Un)assign Policy to assign or remove a policy for the current policy set. |
| VPN Tab | |
| Policy Set | Choose an existing policy set or click Add Interface Policy Set to add a new policy set. Click the Resolved VPN Interface Policy Set link to modify the assigned policy set. |
| Advanced Tab | |

| Field | Description |
|---------------------------|--|
| Packet Inspection Policy | Choose an existing policy or click Add Packet Inspection Policy to add a new policy. Click the Resolved Policy link to modify the assigned policy. |
| Connection Timeout Policy | Choose an existing policy or click Add Connection Timeout Policy to add a new policy. Click the Resolved Policy link to modify the assigned policy. |
| TCP Intercept Policy | Choose an existing policy or click Add TCP Intercept Policy to add a new policy. Click the Resolved Policy link to modify the assigned policy. |
| IP Audit Policy | Choose an existing policy or click Add IP Audit Policy to add a new policy. Click the Resolved Policy link to modify the assigned policy. |

Applying an Edge Device Profile

After you have created an edge device profile, you can apply the profile to multiple edge firewalls to ensure consistent policies across the firewalls.

Procedure

-
- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Edge Firewalls > edge-firewall**.
 - Step 2** In the General tab, click **Select** in the Edge Device Profile field.
 - Step 3** In the Select Edge Device Profile dialog box, select the required profile, then click **OK**.
 - Step 4** Click **Save**.
-

Applying an Edge Security Profile

After you have created an edge security profile, you can apply it to edge firewall instances to ensure consistent policies on the interfaces.



Note Edge security profiles can be applied only on outside interfaces of edge firewalls.

Procedure

- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Edge Firewalls > edge-firewall**.
 - Step 2** In the Interfaces table, select the required outside interface, then click **Edit**.
 - Step 3** In the Edit dialog box, click **Select** in the Edge Security Profile field.
 - Step 4** In the Select Edge Security Profile dialog box, select the required profile, then click **OK**.
 - Step 5** Click **OK** in the open dialog boxes, then click **Save**.
-

Verifying Edge Firewall Policies

Use this procedure to verify active policies and optionally modify policy objects for edge firewalls.

Procedure

- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Edge Firewalls > edge-firewall**.
 - Step 2** In the Edge Security Profiles tab, select the required policy, then click **Show Resolved Policies**.
 - Step 3** To view policy or policy set details, use the tabs in the Edit dialog box to navigate to the required policy or policy set, then click the required policy or policy set in Resolved field
 - Step 4** To use a different policy or policy set, navigate to the required policy or policy set, then either choose a different policy or policy set from the drop-down list, or add a new policy or policy set.
 - Step 5** Click **Apply** to accept any changes or **OK** when you have finished reviewing the policies.
-

Configuring Security Profiles

Editing a Security Profile for a Compute Firewall

Procedure

- Step 1** Choose **Policy Management > Service Profiles > root > Compute Firewalls > Compute Security Profiles**.
- Step 2** In the General tab, select the profile you want to edit, then click **Edit**.
- Step 3** In the Edit Compute Security Profile dialog box, edit the fields as required by using the information in the following tables, then click **OK**.

Table 9: General Tab

| Field | Description |
|--------------------------|---|
| Name | Profile name. |
| Description | Brief policy description. |
| Policy Set | List of available policy sets. |
| Add ACL Policy Set | Click to add a new ACL policy set. |
| Resolved Policy Set | Click the link to view and optionally edit the resolved policy set. |
| Resolved Policies | |
| (Un)assigned Policy | Click to assign or unassign policies. |
| Name | Policy name. |
| Source Condition | Source condition for the policy. |
| Destination Condition | Destination condition for the policy. |
| Service/Protocol | Protocol specify by the policy. |
| EtherType | EtherType specified by the policy. |
| Action | Action to take if the specified condition is met. |
| Description | Brief policy description. |

Table 10: Attributes Tab

| Field | Description |
|----------------------------|----------------------------------|
| Add User Defined Attribute | Click to add a custom attribute. |
| Name | Attribute name. |
| Value | Attribute value. |

Editing a Security Profile for an Edge Firewall

This procedure enables you to edit a security profile associated with an edge firewall.

Procedure

- Step 1** Choose **Policy Management > Service Profiles > root > Edge Firewall > Edge Security Profiles**.
- Step 2** In the General tab, select the edge security profile that you want to edit, then click **Edit**.
- Step 3** In the Edit Edge Security Profile dialog box, edit the entries as required by using the information in the following table, then click **OK**.

| Field | Description |
|--------------------|---|
| General Tab | |
| Name | Profile name (read-only). |
| Description | Brief profile description. |
| ID | Unique profile identifier (read-only). |
| Ingress Tab | |
| Policy Set | Choose an existing policy set or click Add ACL Policy Set to add a new policy set. Click the Resolved Ingress Policy Set link to modify the assigned policy set. |
| Resolved Policies | Click (Un)assign Policy to assign or remove a policy for the current policy set. |
| Egress Tab | |
| Policy Set | Choose an existing policy set or click Add ACL Policy Set to add a new policy set. Click the Resolved Egress Policy Set link to modify the assigned policy set. |
| Resolved Policies | Click (Un)assign Policy to assign or remove a policy for the current policy set. |
| NAT Tab | |
| Policy Set | Choose an existing policy set or click Add NAT Policy Set to add a new policy set. Click the Resolved NAT Policy Set link to modify the assigned policy set. |

| Field | Description |
|---------------------------|---|
| Resolved Policies | Click (Un)assign Policy to assign or remove a policy for the current policy set. |
| VPN Tab | |
| Policy Set | Choose an existing policy set or click Add Interface Policy Set to add a new policy set. Click the Resolved VPN Interface Policy Set link to modify the assigned policy set. |
| Advanced Tab | |
| Packet Inspection Policy | Choose an existing policy or click Add Packet Inspection Policy to add a new policy. Click the Resolved Policy link to modify the assigned policy. |
| Connection Timeout Policy | Choose an existing policy or click Add Connection Timeout Policy to add a new policy. Click the Resolved Policy link to modify the assigned policy. |
| Threat Migration | Choose an existing policy or click Add TCP Intercept Policy to add a new policy. Click the Resolved Policy link to modify the assigned policy. |
| IP Audit Policy | Choose an existing policy or click Add IP Audit Policy to add a new policy. Click the Resolved Policy link to modify the assigned policy. |

Deleting a Security Profile

Procedure

- Step 1** In the **Navigation** pane, choose **Policy Management > Security Policies > root > Security Profiles**.
 - Step 2** In the **Work** pane, click the security profile you want to delete.
 - Step 3** Click **Delete**.
 - Step 4** In the Confirm dialog box, click **OK**.
-

Deleting a Security Profile Attribute

Procedure

- Step 1** In the **Navigation** pane, choose **Policy Management > Security Profiles > root > Security Profiles > security profile**. The security profile is the profile that contains the attribute you want to delete.
 - Step 2** In the **Work** pane, click the **Attributes** tab.
 - Step 3** Click the attribute you want to delete.
 - Step 4** Click **Delete**.
 - Step 5** In the Confirm dialog box, click **OK**.
-

Assigning a Policy

Procedure

- Step 1** In the **Navigation** pane, expand **Policy Management > Security Profiles > root > Security Profiles**.
 - Step 2** Click the profile where you want to assign the policy.
 - Step 3** In the **Work** pane, click the **(Un)assign Policy** link.
 - Step 4** In the **(Un)assign Policy** dialog box, move the policy you want assigned to the **Assigned** list.
 - Step 5** Click **OK**.
-

Unassigning a Policy

Procedure

-
- Step 1** In the **Navigation** pane, expand **Policy Management > Security Profiles > root > Security Profiles**.
 - Step 2** Click the profile where you want to unassign the policy.
 - Step 3** In the **Work** pane, click the **(Un)assign Policy** link.
 - Step 4** In the **(Un)assign Policy** dialog box, move the policy you want unassigned to the **Available** list.
 - Step 5** Click **OK**.
-

Configuring Security Policy Attributes

Configuring Object Groups

An object group defines a collection of condition expressions on a system-defined or user-defined attribute. An object group can be referred to in a policy rule condition when the member or not-member operator is selected. A rule condition that refers to an object group resolves to true if any of the expressions in the object group are true.

Object groups can be created at any level in the organizational hierarchy.

Adding an Object Group

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > tenant > Policy Helpers > Object Groups**.
 - Step 2** In the **General** tab, click **Add Object Group**.
 - Step 3** In the **Object Group** dialog box, provide the information as described in the following table, then click **OK**.

| Field | Description |
|-------------|---|
| Name | Object group name. This name can be between 2 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved. |
| Description | Brief description of the object group. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. |

| Field | Description |
|-----------------------------|--|
| Attribute Type | Available attribute types: Network, VM, User Defined, vZone, and Time Range. You must configure an attribute type and name to add an object group expression. |
| Attribute Name | Available attribute names for the selected attribute type. |
| Expression Table | |
| Add Object Group Expression | Click to add an object group expression. |
| Operator | Operator for the selected expression. |
| Value | Value for the selected expression. |

Adding an Object Group Expression

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.
- Step 2** In the General tab, select the object group you want to add an object group expression to, then click **Edit**.
- Note** For new object groups, you must specify the attribute type and name before adding an object group expression.
- Step 3** In the Edit Object Group dialog box, click **Add Object Group Expression**.
- Step 4** In the Add Object Group Expression dialog box, specify the object group expression by using the information in the following table, then click **OK** in the open dialog boxes.

| Field | Description |
|-----------------|---|
| Attribute Name | Attribute (read-only). |
| Operator | Available operators for this attribute. |
| Attribute Value | Attribute value for this expression. |

Editing an Object Group

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > tenant > Policy Helpers > Object Groups**.
- Step 2** In the General tab, select the object group you want to edit, then click **Edit**.
- Step 3** In the Edit Object Group dialog box, update the fields as follows, then click **OK** in the open dialog boxes:

| Field | Description |
|-----------------------------|--|
| Name | Object group name (read-only). |
| Description | Object group description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. |
| Attribute Type | Specified attribute type (read-only). |
| Attribute Name | Specified attribute name (read-only). |
| Expression Table | |
| Add Object Group Expression | Click to add a new object group expression. |
| Edit | Enables you to edit the selected object group expression. |
| Delete | Deletes the selected object group expression. |
| Operator | Expression operator. |
| Value | Expression attribute value. |

Editing an Object Group Expression

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.
 - Step 2** In the General tab, select the object group with the expression you want to edit, then click **Edit**.
 - Step 3** In the Expression table in the Edit Object Group dialog box, select the expression you want to edit, then click **Edit**.
 - Step 4** In the Edit Object Group Expression dialog box, edit the fields as required, then click **OK** in the open dialog boxes.

| Field | Description |
|-----------------|--|
| Attribute Name | Attribute name (read-only). |
| Operator | Available operators for this expression. |
| Attribute Value | Attribute value for this expression. |

Deleting an Object Group

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.
 - Step 2** In the General tab, select the Object Group you want to delete, then click **Delete**.
 - Step 3** When prompted, confirm the deletion.
-

Deleting an Object Group Expression

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.
 - Step 2** In the General tab, select the object group that contains the expression you want to delete, then click **Edit**.
 - Step 3** In the Edit Object Group dialog box, select the expression that you want to delete In the Expression table, then click **Delete**.
 - Step 4** When prompted confirm the deletion.
 - Step 5** Click **OK** in the open dialog box to save the change.
-

Configuring Security Profile Dictionary

Adding a Security Profile Dictionary

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > tenant > Policy Helpers > Security Profile Dictionary**.
 - Note** You can have one security profile dictionary at the root level and one for each tenant.
 - Step 2** In the General tab, click **Add Security Profile Dictionary**.
 - Step 3** In the Add Security Profile Dictionary dialog box, complete the following fields as appropriate, then click **OK**:

| Field | Description |
|---------------------------------------|---|
| Name | Name of the security profile dictionary. This name can contain 1 to 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved. Note You can have one security profile dictionary at the root level and one for each tenant. |
| Description | A description of the security profile dictionary. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. |
| Attributes Table | |
| Add Security Profile Custom Attribute | Click to add a new attribute. |

| Field | Description |
|-------------|-------------------------------|
| Name | Custom attribute name. |
| Description | Custom attribute description. |

Adding a Security Profile Dictionary Attribute

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > tenant > Policy Helpers > Security Profile Dictionary**.
- Step 2** In the General tab, select the security profile dictionary that you want to add an attribute to, then click **Edit**.
- Step 3** In the Edit Security Profile Dictionary dialog box, click **Add Security Profile Custom Attribute**.
- Step 4** In the Add Security Profile Custom Attribute dialog box, complete the following fields, then click **OK**:

| Field | Description |
|-------------|---|
| Name | Attribute name. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved. |
| Description | Attribute description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. |

Editing a Security Profile Dictionary

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.
- Step 2** In the General tab, select the security profile dictionary you want to edit, then click **Edit**.
- Step 3** In the Edit Security Profile Dictionary dialog box, modify the fields as appropriate, then click **OK**:

| Field | Description |
|---------------------------------------|--|
| Name | Name of the security profile dictionary (read-only). |
| Description | Description of the security profile dictionary. |
| Attributes | |
| Add Security Profile Custom Attribute | Click to add a custom attribute. |
| Name | Attribute name. |
| Description | Attribute description. |

Editing a Security Profile Dictionary Attribute

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.
- Step 2** In the General tab, select the security profile dictionary that contains the attribute you want to edit, then click **Edit**.
- Step 3** In the Edit Security Profile Dictionary dialog box, select the attribute you want to edit, then click **Edit**.
- Step 4** In the Edit Security Custom Attribute dialog box, edit the Description field as required, then click **OK** in the open dialog boxes to save the change.

Deleting a Security Profile Dictionary

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.
- Step 2** In the General tab, select the security profile dictionary you want to delete, then click **Delete**.
- Step 3** When prompted, confirm the deletion.

Deleting a Security Profile Dictionary Attribute

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**. In the General tab, select the dictionary that contains the attribute you want to delete, then click **Edit**.
- Step 2** In the Edit Security Profile Dictionary dialog box, in Attributes table, select the attribute you want to delete, then click **Delete**.
- Step 3** When prompted, confirm the deletion.
-

Working with vZones

A virtual zone (vZone) is a logical grouping of VMs or hosts. vZones facilitate working with policies and profiles because vZones enable you to write policies based on vZone attributes by using vZone names.

The high level flow for working with vZones in Prime Network Services Controller is as follows:

1. Define a vZone, each with one or more conditions for inclusion in the vZone.
2. Define a service policy with the rules based on zone or network conditions.
3. Create a policy set that includes the service policy defined in Step 2.
4. Create a security profile that includes the policy set created in Step 3.
5. Bind the security profile to the ASA 1000V or VSG port profile.
6. Assign the security profile to the ASA 1000V or VSG in Prime Network Services Controller.

See the following topics for more information about working with vZones.

Adding a vZone

Procedure

-
- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.
- Step 2** In the General tab, click **Add vZone**.
- Step 3** In the Add vZone dialog box, provide the information as described in the following table, then click **OK**:

| Field | Description |
|-------|--|
| Name | vZone name. The name can be between 2 and 32 characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change the name after it is saved. |

| Field | Description |
|--------------------------|---|
| Description | vZone description. The description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. |
| Condition Match Criteria | Choose the required match criteria: <ul style="list-style-type: none"> • Match-all—Match all of the criteria (AND). • Match-any—Match any one of the criteria (OR). |
| vZone Condition | |
| Attribute Type | Condition type. |
| Attribute Name | Condition attribute name. Note vZone conditions cannot be created using the service attribute. |
| Operator | Condition operator. |
| Attribute Value | Condition attribute value. |

Editing a vZone

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.
- Step 2** In the General tab, select the vZone that you want to edit, then click **Edit**.
- Step 3** In the Edit vZone dialog box in the General tab, edit the fields as required, click **OK** in the open dialog boxes.

| Field | Description |
|--------------------------|---|
| Name | vZone name (read-only). |
| Description | vZone description. |
| Condition Match Criteria | Choose the required match option: <ul style="list-style-type: none"> • Match-all—Match all of the criteria (AND). • Match-any—Match any one of the criteria (OR). |

| Field | Description |
|------------------------|--|
| vZone Condition | |
| Attribute Type | Attribute type for the selected vZone condition (read-only). |
| Attribute Name | Attribute name for the selected vZone condition (read-only). |
| Operator | Operator for the selected vZone condition. |
| Attribute Value | Attribute value for the selected vZone condition. |
| Object Group | Enables you to add or edit an object group. |

Deleting a vZone Condition

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.
- Step 2** In the General tab, select the vZone with the condition that you want to delete, then click **Edit**.
- Step 3** In the Edit vZone dialog box, select the condition in the vZone Condition table that you want to delete, then click **Delete**.
- Step 4** Confirm the deletion.
- Step 5** In the Edit vZone dialog box, click **OK** or **Apply**.

Deleting a vZone

Procedure

- Step 1** Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.
- Step 2** In the General tab, select the vZones that you want to delete, then click **Delete**.
- Step 3** Confirm the deletion.



Configuring Device Policies and Profiles

This section includes the following topics:

- [Device Policies and Profiles, page 181](#)
- [Device Configuration, page 182](#)
- [Device Policies, page 183](#)
- [Configuring Device Policies, page 183](#)
- [Configuring Device Profiles, page 209](#)
- [Configuring NTP, page 214](#)
- [Associating Device Policies with Profiles, page 217](#)

Device Policies and Profiles

Prime Network Services Controller enables you to create device profiles and policies at any organizational level.

Device Profiles

A Prime Network Services Controller device profile is a set of custom security attributes and device policies. For Nexus 1000V VSMs, the device profile is added to the port profile. The port profile is assigned to the Nexus 1000V VSM vNIC, making the device profile part of the virtual machine (VM). Adding a device profile to the VM allows the addition of custom attributes to the VM. Firewall rules can be written using custom attributes such that traffic between VMs can be allowed to pass or be dropped.

You apply device profiles to compute and edge firewalls by choosing Resource Management > Managed Resources and then navigating to the required compute or edge firewall at the root or tenant level. The Firewall Settings area of the firewall pane includes the Device Profile option.

Prime Network Services Controller includes a default device profile at root level. The default device profile can be edited but cannot be deleted.

Policies

Prime Network Services Controller supports the following objects related to policies:

- **Policy set**—Contains policies. After a policy set is created, it can be assigned to a profile. An existing default policy set is automatically assigned at system boot up.
- **Policy**—Contains rules that can be ordered. An existing default policy is automatically assigned at system boot up. The default policy contains a rule with an action of **drop**.
- **Rule**—Contains conditions for regulating traffic. The default policy contains a rule with an action of **drop**. Conditions for a rule can be set using the network, custom, and virtual machine attributes.
- **Object group**—Can be created under an organization node. An object group defines a collection of condition expressions on a system-defined or user-defined attribute. An object group can be referred to in a policy rule condition when the member or not-member operator is selected. A rule condition that refers to an object group resolves to true if any of the expressions in the object group are true.
- **Security Profile Dictionary**—Logical collection of security attributes. You define dictionary attributes for use in a security profile. A security profile dictionary is created at the root or tenant node. You can create only one dictionary for a tenant and one for root. The security profile dictionary allows the user to define names of custom attributes. Custom attribute values are specified on security profile objects. Custom attributes can be used to define policy rule conditions. Attributes configured in a root level dictionary can be used by any tenant. You cannot create a dictionary below the tenant level.
- **Zone**—Set of VMs based on conditions. The zone name is used in the authoring rules.

Security policies are created and then pushed to the Cisco VSG or ASA 1000V.

Device Configuration

Prime Network Services Controller enables you to configure devices by adding policies to a device profile and then applying that profile to a device. Device profiles contain options for the following policies and settings:

- DNS server and domain
- NTP server
- SNMP policy
- Syslog policy
- Fault policy
- Core policy
- Log file policy
- Policy engine logging
- Authentication policy

Device Policies

Prime Network Services Controller enables you to create the following policies and assign them to device profiles for application to compute firewalls, edge firewalls, and VSGs:

- AAA policy
- Core file policy
- Fault policy
- Logging policy
- SNMP policy
- Syslog policy

Prime Network Services Controller provides default policies for fault, logging, SNMP, and syslog. The default policies cannot be deleted but can be modified. A device profile uses name resolution to resolve policy assignments. For details, see [Name Resolution in a Multi-Tenant Environment](#), on page 70.

Policies created under root are visible to both the Prime Network Services Controller profile and the Device profile.

Configuring Device Policies

Prime Network Services Controller enables you to configure and manage the following types of device policies:

- AAA
- Core File
- Fault
- Log File
- SNMP
- Syslog

Configuring AAA Policies

AAA authentication policies verify users before they are allowed access to a network and network services. By creating AAA authentication policies in Prime Network Services Controller and associating the policies with objects through device profiles, you can ensure that only authenticated users can access the objects.

Prime Network Services Controller supports AAA authentication and authorization for edge firewalls, and server groups using the following protocols:

- Kerberos
- Lightweight Directory Access Protocol (LDAP)
- Windows NT

- RADIUS
- RSA SecurID (SDI)
- TACACS+

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > AAA > Auth Policies**.

Step 2 In the General tab, click **Add Auth Policy**.

Step 3 In the Add Auth Policy dialog box, enter the information as described in [Add Auth Policy Dialog Box](#), on page 184, then click **OK**.

Note If you add a remote server group with a new server group with a new server host, the information that you must provide for the host depends on the protocol used. For example, the information required for a RADIUS server host is different from the information required for an LDAP server host.

See the online help for the information required for the selected protocol.

Field Descriptions

Add Auth Policy Dialog Box

| Field | Description |
|------------------------------|---|
| Name | Policy name. |
| Description | Brief policy description. |
| Authorization | Check the Enable check box to enable authorization via server authentication. |
| Remote Access Methods | |
| Add Remote Access Method | Adds a remote access method to the policy. For more information, see Remote Access Method Dialog Box , on page 185. |
| Access Method | One of the following access methods: <ul style="list-style-type: none"> • Enable Mode • HTTP • Serial • SSH • Telnet |

| Field | Description |
|---------------------|--|
| Admin State | Whether the administrative state of the policy is enabled or disabled. |
| Remote Server Group | Remote server group name. |
| Local Auth | This column is not used. |

Remote Access Method Dialog Box

| Field | Description |
|---------------|---|
| Access Method | One of the following access methods: <ul style="list-style-type: none"> • Enable Mode • HTTP • Serial • SSH • Telnet |
| Admin State | Whether the administrative state of the access method is enabled or disabled. |
| Server Group | <p>Indicate the server group to use:</p> <ol style="list-style-type: none"> 1 In the Protocol for Creation field, choose the required protocol. 2 In the Server Group fields, do one of the following: <ul style="list-style-type: none"> • From the drop-down list, choose an available remote server group. • Click Add Remote Server Group - <i>protocol</i> to add a new remote server group. <p>Note If you add a new remote server group, the information that you must provide for the server group and host depends on the protocol used. For example, the information required for a RADIUS server group and host is different from the information required for an LDAP server group and host.</p> |

Configuring Core File Policies

Adding a Core File Policy for a Device

You can add a core file policy at any organizational level.

Procedure

-
- Step 1** Choose **Policy Management > Device Configurations > root > Policies > Core File**.
- Step 2** In the General tab, click **Add Core File Policy**.
- Step 3** In the Add Core File Policy dialog box, add the information as described in the following table, then click **OK**:

| Field | Description |
|---------------------|--|
| Name | Core file policy name, containing 1 to 32 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.). You cannot change the name after the policy has been saved. |
| Description | Brief policy description, containing 1 to 256 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.). |
| Admin State | Indicate whether the administrative state of the policy is to be enabled or disabled. |
| Hostname/IP Address | Hostname or IP address to use for this policy. If you use a hostname rather than an IP address, you must configure a DNS server in Prime Network Services Controller. |
| Port | Port number for sending the core dump file. This field is read-only for InterCloud policies. |
| Protocol | Protocol for exporting the core dump file (tftp only). |
| Path | Path to use when storing the core dump file on a remote system. The default path is /tftpboot; for example, /tftpboot/test, where <i>test</i> is the subfolder. |

Editing a Core File Policy for a Device Profile

Procedure

- Step 1** Choose **Policy Management > Device Configurations > root > Policies > Core File**.
- Step 2** In the General tab, select the core file policy you want to edit, then click **Edit**.
- Step 3** In the Edit Core File Policy dialog box, edit the fields as required, using the information in the following table, then click **OK**.

| Field | Description |
|-------------|--|
| Name | Name of the core file policy (read-only). |
| Description | Brief policy description. |
| Admin State | Administrative status of the policy: enabled or disabled. |
| Hostname | Hostname or IP address. Note If you use a hostname, you must configure a DNS server. |
| Port | Port number to use when exporting the core dump file. This field is read-only for InterCloud policies. |
| Protocol | Protocol used to export the core dump file (tftp only). |
| Path | Path to use when storing the core dump file on the remote system. The default path is /tftpboot. To specify a subfolder under tftpboot, use the format /tftpboot/ <i>folder</i> where <i>folder</i> is the subfolder. |

Deleting a Core File Policy from a Device Profile

Procedure

- Step 1** Choose **Policy Management > Device Configurations > root > Policies > Core File**.
- Step 2** In the General tab, select the core file policy you want to delete, then click **Delete**.
- Step 3** When prompted, confirm the deletion.

Configuring Fault Policies

Adding a Fault Policy for a Device Profile

You can add a fault policy at any organizational level.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Fault**.

Step 2 In the General tab, click **Add Fault Policy**.

Step 3 In the Add Fault Policy dialog box, enter the information as described in the following table, then click **OK**.

| Field | Description |
|-------------------------------|--|
| Name | Fault policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created. |
| Description | Brief policy description. |
| Flapping Interval | Length of time (in hours, minutes, and seconds) that must elapse before the system allows a fault to change its state. Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the Clear Faults Retention Action field. The default flapping interval is ten seconds. |
| Clear Faults Retention Action | Action to be taken when faults are cleared: <ul style="list-style-type: none"> • retain—Retain the cleared faults. • delete—Delete fault messages as soon as they are marked as cleared. |

| Field | Description |
|---------------------------------|---|
| Clear Faults Retention Interval | <p>How long the system is to retain cleared fault messages:</p> <ul style="list-style-type: none"> • Forever—The system retains all cleared fault messages regardless of their age. • Other—The system retains cleared fault message for a specified the length of time. In the spinbox that is displayed when you select this option, enter the length of time (in days, hours, minutes, and seconds) that the system is to retain cleared fault messages. |

Editing a Fault Policy for a Device Profile



Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

- Step 1** Choose **Policy Management > Device Configurations > root > Policies > Fault**.
- Step 2** In the General tab, select the fault policy you want to edit, then click **Edit**.
- Step 3** In the Edit Fault Policy dialog box, modify the following fields as required, then click **OK**.

| Field | Description |
|-------------|---------------------------|
| Name | Policy name (read-only). |
| Description | Brief policy description. |

| Field | Description |
|---------------------------------|--|
| Flapping Interval | <p>Length of time (in hours, minutes, and seconds) that must elapse before the system allows a fault to change its state.</p> <p>Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change.</p> <p>If the condition recurs during the flapping interval, the fault returns to the active state. If the condition does not recur during the flapping interval, the fault is cleared. The next action depends on the setting in the Clear Faults Retention Action field.</p> <p>The default flapping interval is ten seconds.</p> |
| Clear Faults Retention Action | <p>Available fault retention actions:</p> <ul style="list-style-type: none"> • retain—The system retains fault messages. • delete—The system deletes fault messages when they are marked as cleared. |
| Clear Faults Retention Interval | <p>How long the system is to retain cleared fault messages:</p> <ul style="list-style-type: none"> • Forever—The system retains all cleared fault messages regardless of their age. • Other—The system retains cleared fault message for a specified the length of time. In the spinbox that is displayed when you select this option, enter the length of time (in days, hours, minutes, and seconds) that the system is to retain cleared fault messages. |

Deleting a Fault Policy for a Device Profile



Note

When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

- Step 1** Choose **Policy Management > Device Configurations > root > Policies > Fault**.
 - Step 2** In the General tab, select the fault policy that you want to delete, then click **Delete**.
 - Step 3** When prompted, confirm the deletion.
-

Configuring Log File Policies

Adding a Logging Policy for a Device Profile

You can add a logging policy for a device at any organizational level.

Procedure

- Step 1** Choose **Policy Management > Device Configurations > root > Policies > Log File**.
- Step 2** In the General tab, click **Add Logging Policy**.
- Step 3** In the Add Logging Policy dialog box, complete the following fields, then click **OK**.

| Field | Description |
|-------------|---|
| Name | Logging policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created. |
| Description | Brief policy description. |

| Field | Description |
|--------------------|--|
| Log Level | <p>One of the following logging severity levels:</p> <ul style="list-style-type: none"> • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical <p>The default log level is info.</p> |
| Backup Files Count | <p>Number of backup files that are filled before they are overwritten.</p> <p>The range is 1 to 9 files, with a default of 2 files.</p> |
| File Size (bytes) | <p>Backup file size.</p> <p>The range is 1 MB to 100 MB with a default of 5 MB.</p> |

Editing a Logging Policy for a Device Profile



Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

- Step 1** Choose **Policy Management > Device Configurations > root > Policies > Log File**.
- Step 2** In the General tab, select the log file policy that you want to edit, then click **Edit**.
- Step 3** In the Edit Log File Policy dialog box, edit the fields as required by using the information in the following table, then click **OK**.

| Field | Description |
|--------------------|---|
| Name | Logging policy name (read-only). |
| Description | Brief policy description. |
| Log Level | <p>One of the following logging levels:</p> <ul style="list-style-type: none"> • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical <p>The default log level is info.</p> |
| Backup Files Count | <p>Number of backup files that are filled before they are overwritten.</p> <p>The range is 1 to 9 files, with a default of 2 files.</p> |
| File Size (bytes) | <p>Backup file size.</p> <p>The range is 1 MB to 100 MB with a default of 5 MB.</p> |

Deleting a Logging Policy for a Device Profile



Note

When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

-
- Step 1** Choose **Policy Management > Device Configurations > root > Policies > Log File**.
 - Step 2** In the General tab, select the logging policy you want to delete, then click **Delete**.
 - Step 3** When prompted, confirm the deletion.
-

Configuring SNMP Policies

Adding an SNMP Policy

You can add an SNMP policy at any organizational level.

Procedure

-
- Step 1** Choose **Policy Management > Device Configurations > root > Policies > SNMP**.
 - Step 2** In the General tab, click **Add SNMP Policy**.
 - Step 3** In the Add SNMP dialog box, complete the following fields as appropriate:

Table 11: General Tab

| Field | Description |
|-------------|--|
| Name | SNMP policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created. |
| Description | SNMP policy description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. |
| Admin State | Indicate whether the administrative status of the policy is enabled or disabled. |
| Location | Physical location of the device. |
| Contact | Contact person for the device. |
| SNMP Port | Port that the SNMP agent listens to for requests. You cannot edit this field. |

Step 4 Click the **Communities** tab, then complete the following steps:

- a) Click **Add SNMP Community**.
- b) In the Add SNMP Community dialog box, complete the following fields as appropriate, then click **OK**:

| Name | Description |
|-----------|---|
| Community | SNMP community name. |
| Role | Role associated with the community string. You cannot edit this field. |

Step 5 In the Add SNMP dialog box, click **OK**.

Editing an SNMP Policy



Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the General tab, select the SNMP policy that you want to edit, then click **Edit**.

Step 3 In the Edit SNMP Policy dialog box, edit the information in the General tab as required, using the information in the following table:

| Field | Description |
|-------------|--|
| Name | SNMP policy name (read-only). |
| Description | Brief policy description. |
| Admin State | Administrative state of the policy: enabled (default) or disabled. |
| Location | Physical location of the device. |
| Contact | Contact person for the device. |
| SNMP Port | Port that the SNMP agent listens to for requests (read-only). |

Step 4 In the Communities tab, edit the information as required:

| Field | Description |
|--------------------|--|
| Add SNMP Community | Click to add an SNMP community. |
| Community | SNMP community name. |
| Role | Role associated with the SNMP community. |

Step 5 In the Traps tab, edit the information as required:

| Field | Description |
|---------------------|--|
| Add SNMP Trap | Click to add an SNMP trap. |
| Hostname/IP Address | IP address of the SNMP host. |
| Port | Port where the SNMP agents listens for requests. |
| Community | SNMP community name. |

Step 6 Click **OK**.

Deleting an SNMP Policy



Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the General tab, select the SNMP policy that you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Adding an SNMP Trap Receiver

Procedure

- Step 1** Choose **Policy Management > Device Configurations > root > Policies > SNMP**.
- Step 2** In the General tab, click **Add SNMP Policy > Traps > Add SNMP Trap**.
- Step 3** In the Add SNMP Trap dialog box, enter the following information, then click **OK**:

| Field | Description |
|----------------------|---|
| Hostname/ IP Address | Hostname or IP address of the SNMP host. |
| Port | Port that the SNMP agent listens to for requests. The default port is 162. |
| Community | SNMP community name. |

Editing an SNMP Trap Receiver

Procedure

- Step 1** Choose **Policy Management > Device Configurations > root > Policies > SNMP**.
- Step 2** In the General tab, select the SNMP policy with the SNMP trap that you want to edit, then click **Edit**.
- Step 3** In the Edit SNMP Policy dialog box, click the **Traps** tab.
- Step 4** In the Traps tab, select the entry that you want to edit, then click **Edit**.
- Step 5** In the Edit SNMP Trap dialog box, edit the information in the General tab as required, using the following information:

| Field | Description |
|---------------------|---|
| Hostname/IP Address | Hostname or IP address of the SNMP host (read-only). |
| Port | Port that the SNMP agent listens to for requests. |
| Community | SNMP community name. |

- Step 6** Click **OK** in the open dialog boxes.

Deleting an SNMP Trap Receiver

Procedure

-
- Step 1** Choose **Policy Management > Device Configurations > root > Policies > SNMP**.
 - Step 2** In the General tab, select the SNMP policy with the SNMP trap that you want to delete, then click **Edit**.
 - Step 3** In the Edit SNMP Policy dialog box, click the **Traps** tab.
 - Step 4** In the Traps tab, select the entry that you want to delete, then click **Delete**.
 - Step 5** When prompted, confirm the deletion.
-

Configuring Syslog Policies

Adding a Syslog Policy for a Device

Prime Network Services Controller enables you to configure syslog policies for syslog messages and then attach a created syslog policy to a device profile for implementation on all devices using that profile.

You can create syslog policies for logging syslog messages to a remote syslog server or to a local buffer for later review.

Procedure

-
- Step 1** Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
 - Step 2** In the General tab, click **Add Syslog Policy**.
 - Step 3** In the Add Syslog dialog box, provide the information as described in [Add Syslog Policy Dialog Box, on page 198](#), then click **OK**.
-

Field Descriptions

Add Syslog Policy Dialog Box

| Field | Description |
|--------------------|---------------------------|
| General Tab | |
| Name | Policy name. |
| Description | Brief policy description. |

| Field | Description |
|-------------------------------|--|
| Use Emblem Format | <p>Check the check box to use the EMBLEM format for syslog messages.</p> <p>This option is supported for ASA 1000Vs. It is not supported for VSGs or InterCloud policies.</p> |
| Continue if Host is Down | <p>Check the check box to continue logging if the syslog server is down.</p> <p>This option is supported for ASA 1000Vs. It is not supported for VSGs or InterCloud policies.</p> |
| Servers Tab | |
| Add Syslog Server | Click to add a new syslog server. |
| Syslog Servers table | List of configured syslog servers. |
| Local Destinations Tab | |
| Console area | <ul style="list-style-type: none"> • Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: alert, critical, or emergency. <p>If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.</p> |
| Monitor area | <ul style="list-style-type: none"> • Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. <p>If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.</p> |

| Field | Description |
|-----------|---|
| File area | <ul style="list-style-type: none">• Admin State—Administrative state of the policy: disabled or enabled.• Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.• File Name—Name of the file to which messages are logged.• Size (bytes)—Maximum size, in bytes, that the file can reach before the system begins to overwrite the messages. |

| Field | Description |
|-------------|---|
| Buffer area | <p>Buffer options are not available for InterCloud policies.</p> <ul style="list-style-type: none"> • Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • Buffer Size (Bytes)—In bytes, the size of the buffer for syslog messages. • Wrap to Flash—Indicates whether or not the buffer contents are saved to flash memory when the buffer wraps (becomes full). Check the check box to save the contents to flash memory if the buffer wraps. • Max File Size in Flash (KB)—Maximum size, in kilobytes, that can be used by the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. • Min Free Flash Size (KB)—Minimum size, in kilobytes, that is allocated for the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. |

Editing a Syslog Policy for a Device Profile

Prime Network Services Controller enables you to edit existing syslog policies as described in this procedure.

Procedure

-
- Step 1** Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
 - Step 2** In the General tab, select the policy you want to edit, then click **Edit**.
 - Step 3** In the Edit Syslog Policy dialog box, in the General tab, edit the information as required, using the following information:

| Field | Description |
|--------------------------|---|
| Name | Policy name (read-only). |
| Description | Brief policy description. |
| Use Emblem Format | Check the check box to use the EMBLEM format for syslog messages. This option is supported for ASA 1000Vs. It is not supported for VSGs. |
| Continue if Host is Down | Check the check box to continue logging if the syslog server is down. This option is supported for ASA 1000Vs. It is not supported for VSGs. |

Step 4 In the Servers tab, click **Add Syslog Server** to add a new syslog server, or select an existing server and click **Edit** to edit it.

Step 5 In the Local Destinations tab, edit the information as required, using the following information:

| Field | Description |
|--------------|---|
| Console area | <ul style="list-style-type: none"> • Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alerts, critical, or emergencies. <p>If the Admin State is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.</p> |
| Monitor area | <ul style="list-style-type: none"> • Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, emergency, error, warning, notification, information, or debugging. <p>If the Admin State is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.</p> |

| Field | Description |
|-------------|--|
| File area | <ul style="list-style-type: none"> • Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, emergency, error, warning, notification, information, or debugging. If the Admin State is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console. • File Name—Name of the file to which messages are logged. • Size (bytes)—Maximum size, in bytes, that the file can reach before the system begins to overwrite the messages. |
| Buffer area | <ul style="list-style-type: none"> • Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, emergency, error, warning, notification, information, or debugging. If the Admin State is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console. • Buffer Size (Bytes)—In bytes, the size of the buffer for syslog messages. • Wrap to Flash—Indicates whether or not the buffer contents are saved to flash memory with the buffer wraps (becomes full). Check the check box to save the contents to flash memory if the buffer wraps. • Max File Size in Flash (KB)—Maximum size, in kilobytes, that can be used by the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. • Min Free Flash Size (KB)—Minimum size, in kilobytes, that is allocated for the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. |

Step 6 Click **OK**.

Deleting a Syslog Policy for a Device Profile



Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.

Step 2 In the General tab, select the syslog policy that you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Adding a Syslog Server for a Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.

Step 2 In the General tab, click **Add Syslog Policy**.

Step 3 In the Add Syslog Policy dialog box, click the **Servers** tab, then click **Add Syslog Server**.

Step 4 In the Add Syslog Server dialog box, provide the information as described in [Add Syslog Server Dialog Box, on page 204](#), then click **OK** in the open dialog boxes.

Field Descriptions

Add Syslog Server Dialog Box

| Field | Description |
|-------------|---|
| Server Type | One of the following server types: <ul style="list-style-type: none"> • primary • secondary • tertiary |

| Field | Description |
|---------------------|---|
| Hostname/IP Address | Hostname or IP address where the syslog file resides. Note If you use a hostname, you must configure a DNS server. |
| Severity | One of the following severity levels: <ul style="list-style-type: none">• emergencies (0)• alerts (1)• critical (2)• errors (3)• warnings (4)• notifications (5)• information (6)• debugging (7) |

| Field | Description |
|---------------------|---|
| Forwarding Facility | <p>One of the following forwarding facilities:</p> <ul style="list-style-type: none"> • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp |
| Admin State | Administrative state of the server: disabled or enabled. |
| Port | <p>Port to use to send data to the syslog server. The default port selection is 514 for UDP. This option is not available for InterCloud policies.</p> |
| Protocol | <p>Protocol to use: TCP or UDP (default). This option is not available for InterCloud policies.</p> |

| Field | Description |
|------------------------------|---|
| Use Transport Layer Security | Check the check box to use Transport Layer Security. This option is available only for TCP. This option is not available for InterCloud policies. |
| Server Interface | Interface to use to access the syslog server. |

Editing a Syslog Server for a Device Profile

Procedure

- Step 1** Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
- Step 2** In the General tab, select the required syslog policy, then choose **Edit**.
- Step 3** In the Edit Syslog Policy dialog box, from the **Servers** tab, select the syslog server you want to edit, then click **Edit**.
- Step 4** In the Edit Syslog Server dialog box, edit the fields as required, using the information in the following table.

| Field | Description |
|---------------------|--|
| Server Type | One of the following server types: primary, secondary, or tertiary (read-only). |
| Hostname/IP Address | Hostname or IP address where the syslog file resides. |
| Severity | One of the following severity levels: <ul style="list-style-type: none"> • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • information (6) • debugging (7) |

| Field | Description |
|------------------------------|--|
| Forwarding Facility | One of the following forwarding facilities: <ul style="list-style-type: none"> • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp |
| Admin State | Administrative state of the policy: enabled or disabled. |
| Port | Port to use to send data to the syslog server. Valid port values are 1025 through 65535 for both TCP and UDP. The default TCP port is 1470. The default UDP port is 514. |
| Protocol | Protocol to use: TCP or UDP. |
| Use Transport Layer Security | Check the check box to use Transport Layer Security. This option is available only for TCP. |

| Field | Description |
|------------------|--|
| Server Interface | Interface to use to access the syslog server. This option applies to ASA 1000V only. Enter the data interface name specify in the edge firewall. Use the device CLI to configure a route through the management interface. |

Step 5 Click **OK** in the open dialog boxes to save your changes.

Deleting a Syslog Server for a Device Profile

Procedure

- Step 1** Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
 - Step 2** In the General tab, select the syslog policy with the server you want to delete, then click **Edit**.
 - Step 3** In the Edit Syslog Policy dialog box, click the **Servers** tab.
 - Step 4** In the Servers tab, select the syslog server that you want to delete, then click **Delete**.
 - Step 5** When prompted, confirm the deletion.
 - Step 6** Click **OK** to save the policy.
-

Configuring Device Profiles

Adding a Firewall Device Profile

Procedure

- Step 1** Choose **Policy Management > Device Configurations > root > Device Profiles**.
- Step 2** In the General tab, click **Add Device Profile**.
- Step 3** In the New Device Profile dialog box, enter the required information in the General and Policies tabs, then click **OK**:

| Field | Description |
|-------------|---|
| DNS Servers | <p>You can:</p> <ul style="list-style-type: none"> • Add a new server. • Select an existing server and edit or delete it. • Use the arrows to change priority. |
| DNS Domains | <p>You can:</p> <ul style="list-style-type: none"> • Add a new domain. • Select an existing domain and edit or delete it. |
| NTP Servers | <p>You can:</p> <ul style="list-style-type: none"> • Add a new server. • Select an existing server and edit or delete it. • Use the arrows to change priority. |
| SNMP | <p>You can:</p> <ul style="list-style-type: none"> • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned. <p>This option is not available for InterCloud Management device profiles.</p> |
| Syslog | <p>You can:</p> <ul style="list-style-type: none"> • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned. |
| Fault | <p>You can:</p> <ul style="list-style-type: none"> • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned. <p>This option is not available for InterCloud Management device profiles.</p> |

| Field | Description |
|-----------------------|---|
| Core File | <p>You can:</p> <ul style="list-style-type: none"> • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned. |
| Policy Agent Log File | <p>You can:</p> <ul style="list-style-type: none"> • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned. |
| Policy Engine Logging | <p>Select the appropriate radio button to enable or disable logging.</p> <p>This option is not available for InterCloud Management device profiles.</p> |
| Auth Policy | <p>You can:</p> <ul style="list-style-type: none"> • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned. <p>This option is not available for InterCloud Management device profiles.</p> |

Editing a Firewall Device Profile

After you create a firewall device profile, you can edit it as needed.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Device Profiles**.

Step 2 In the Device Profiles pane, select the profile you want to edit, then click **Edit**.

Step 3 In the Edit Firewall Device Policy dialog box, update the information in the General tab as described in the following table:

| Field | Description |
|-------------|--|
| Name | Profile name. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved. |
| Description | Brief profile description. The description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. |
| Time Zone | Select the required time zone from the drop-down list. |

Step 4 In the Policies tab, update the information as described in the following table, then click **OK**:

| Field | Description |
|--------------------------|---|
| DNS Servers | |
| Add DNS Server | Adds a DNS server. |
| Edit | Enables you to edit the selected DNS server. |
| Delete | Deletes the selected DNS server. |
| Up and down arrows | Change the priority of the selected DNS server. Prime Network Services Controller uses the DNS servers in the order in which they appear in the table. |
| <i>DNS Servers Table</i> | |
| IP Address | IP addresses for the DNS servers configured in the system. |
| Server Interface | Interface to use to access the DNS server. |
| NTP Servers | |

| Field | Description |
|--------------------------|--|
| Add NTP Server | Click to add an NTP server. |
| Edit | Enables you to edit the selected NTP server. |
| Delete | Deletes the selected NTP server. |
| Up and down arrows | Change the priority of the selected NTP Server hostname. Prime Network Services Controller uses the NTP servers in the order in which they appear in the table. |
| <i>NTP Servers Table</i> | |
| Hostname / IP Address | Hostnames or IP addresses for NTP servers configured in the system. |
| Interface Name | Interface to use to access the NTP server. |
| DNS Domains | |
| Add | Click to add a DNS domain name. |
| Edit | Click to edit the DNS domain name selected in the DNS Domains table. The default DNS name cannot be edited. |
| Delete | Click to delete the DNS domain name selected in the DNS Domains table. |
| DNS Domains table | Default DNS domain name and domain in the system. |
| Other Options | |
| SNMP | Select, add, or edit SNMP policies as needed. |
| Syslog | Select, add, or edit syslog policies as needed. |
| Fault | Select, add, or edit fault policies as needed. |
| Core File | Select, add, or edit core file policies as needed. |
| Policy Agent Log File | Select, add, or edit the policy agent log file policies as needed. |
| Policy Engine Logging | Select the appropriate radio button to enable or disable logging. |

| Field | Description |
|-------------|--|
| Auth Policy | Select an available authentication policy, or click Add Auth Policy to add a new authentication policy. |

Deleting a Firewall Device Profile

Procedure

-
- Step 1** Choose **Policy Management > Device Configurations > root > Device Profiles**.
 - Step 2** In the **Work** pane, click the device profile you want to delete.
 - Step 3** Click **Delete**.
 - Step 4** In the Confirm dialog box, click **OK**.
-

Configuring NTP

Network Time Protocol (NTP) is a networking protocol used to synchronize the time on a network of machines. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server.

Prime Network Services Controller enables you to configure NTP for compute firewalls, edge firewalls, and Prime Network Services Controller itself.

Configuring NTP for a compute or edge firewall requires the following steps:

- 1 Configuring a device profile with NTP.
- 2 Applying the device profile to a compute or edge firewall

The following topics describe how to perform these steps.

For information on configuring NTP on Prime Network Services Controller, see [Adding an NTP Server](#), on page 60.

Creating a Device Profile with NTP

This procedure describes how to create a device profile with NTP that you can apply to an edge or compute firewall.

Procedure

-
- Step 1** Choose **Policy Management > Device Configurations > root > Device Profiles**.
- Step 2** In the General tab, click **Add Device Profile**.
- Step 3** In the New Device Profile dialog box, provide the following information:
- Name—Profile name.
 - Description—Brief profile description.
 - Time Zone—From the drop-down list, choose the time zone.
- Step 4** Click the **Policies** tab.
- Step 5** In the NTP servers area, click **Add NTP Server**.
- Step 6** In the Add NTP Server dialog box, enter the information as described in [Add NTP Server Dialog Box](#), on [page 215](#), then click **OK**.
- Step 7** Click **OK**.
-

What to Do Next

After you have configured the device profile, you can apply it to a firewall as described in the following topics:

- [Applying Device Profiles to Edge Firewalls](#), on [page 216](#)
- [Applying Device Profiles to Compute Firewalls](#), on [page 216](#)

Field Descriptions

Add NTP Server Dialog Box

| Field | Description |
|---------------------|--|
| Hostname/IP Address | NTP server name or IP address. For Prime Network Services Controller and VSGs, you can enter either a hostname or IP address. For ASA 1000Vs, you must enter an IP address. |

| Field | Description |
|--------------------|--|
| Interface Name | <p>(Policy Management Device Profiles only) Device interface to reach the NTP server.</p> <p>The following information applies:</p> <ul style="list-style-type: none"> • Only ASA 1000Vs support interface names: <ul style="list-style-type: none"> • If you specify an interface, use the interface name specified by the edge firewall. • To use the management interface, you must configure the route by using the CLI. • VSGs do not support interface names. |
| Authentication Key | <p>(Policy Management Device Profiles only) Authentication key to access the NTP server.</p> <p>The following information applies:</p> <ul style="list-style-type: none"> • Only ASA 1000Vs support authentication keys. • VSGs do not support authentication keys. |

Applying Device Profiles to Compute Firewalls

After you have created a device profile, you can apply the profile to a compute firewall.

Procedure

-
- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Compute Firewalls > compute-firewall**.
- Step 2** In the General tab, click **Select** in the Device Profile field.
- Step 3** In the Select Device Profile dialog box, select the desired profile, then click **OK**.
- Step 4** Click **Save**.
-

Applying Device Profiles to Edge Firewalls

After you have created a device profile, you can apply the profile to an edge firewall.

Procedure

- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Edge Firewalls > edge-firewall**.
 - Step 2** In the General tab, click **Select** in the Device Profile field.
 - Step 3** In the Select Device Profile dialog box, select the desired profile, then click **OK**.
 - Step 4** Click **Save**.
-

Associating Device Policies with Profiles

After you create a device policy, you can associate it with a device profile. By doing so, you can ensure that all devices associated with the device profile use the same policy.

Procedure

- Step 1** Choose **Policy Management > Device Configurations > root > Device Profiles > profile** where *profile* is the device profile that you want to add the device policy to.
 - Step 2** Click the **Policies** tab.
 - Step 3** In the Policies tab, locate the drop-down list for the type of policy you want to associate, such as Syslog or Auth Policy.
 - Step 4** From the drop-down list, choose the policy to add to the profile, then click **Save**. The policy is automatically applied to all devices using the selected profile.
-



Configuring Managed Resources

This section includes the following topics:

- [Resource Management](#), page 219
- [Resource Manager](#), page 220
- [Virtual Machines](#), page 220
- [Virtual Security Gateways](#), page 220
- [ASA 1000V Cloud Firewalls](#), page 221
- [Managing Compute Firewalls](#), page 221
- [Managing Edge Firewalls](#), page 226
- [Verifying VM Registration](#), page 229
- [Examining Fault Details](#), page 229
- [Launching ASDM](#), page 231
- [Managing Pools](#), page 232

Resource Management

The Resource Management tab displays the following resources that are managed by Prime Network Services Controller:

- Virtual Machines (VMs)
- ASA 1000V edge firewalls
- VSG compute firewalls
- Virtual Supervisor Modules (Nexus 1000V VSM)

You manage ASA 1000Vs and VSGs by placing them in service:

- You place an ASA 1000V in service by creating an edge firewall in an organization and assigning the ASA 1000V to that edge firewall.

- You place a VSG in service by creating a compute firewall in an organization and assigning the VSG to that compute firewall.

You manage VMs by discovering those VMs that have at least one network interface configured with a Nexus 1000V port profile.

Resource Manager

Resource Manager manages logical edge and compute firewalls and their association with ASA 1000Vs and VSGs, respectively. When an edge firewall is associated with an ASA 1000V, the device configuration profile information (defined by the edge firewall) is pushed to the ASA 1000V which, in turn, triggers the ASA 1000V to download the security profiles and policies from Policy Manager.

Resource Manager is responsible for the following services:

- Maintaining an inventory of ASA 1000Vs, VSGs, and VSMs.
- With user input, defining compute firewalls and associating them with VSGs for provisioning.
- With user input, defining edge firewalls and associating them with ASA 1000Vs for provisioning.
- Integrating with VMware vCenter instances to retrieve VM attributes.

Virtual Machines

Virtualization allows you to create multiple VMs that run in isolation, side by side on the same physical machine. Each VM has virtual RAM, a virtual CPU and NIC, and an operating system and applications. Because of virtualization, the operating system sees a consistent set of hardware regardless of the actual physical hardware components.

VMs are encapsulated in files for rapid saving, copying, and provisioning, which means that you can move full systems, configured applications, operating systems, BIOS, and virtual hardware within seconds, from one physical server to another. Encapsulated files allow for zero-downtime maintenance and continuous workload consolidation.

Instances of Prime Network Services Controller are installed on VMs.

Virtual Security Gateways

VSGs evaluate Prime Network Services Controller policies based on network traffic. The main functions of a VSG are as follows:

- Receive traffic from Virtual Network Service Data Path (vPath).

For every new flow, the vPath component encapsulates the first packet and sends it to a VSG as specified in the Nexus 1000V port profiles. It assumes that the VSG is Layer 2 adjacent to vPath. The mechanism used for communication between vPath and the VSG is similar to VEM and Nexus 1000V VSM communication on a packet VLAN.

- Perform application fix-up processing such as FTP, TFTP, and RSH.
- Evaluate policies by inspecting the packets sent by vPath using network, VM, and custom attributes.

- Transmit the policy evaluation results to vPath.

Each vPath component maintains a flow table for caching VSG policy evaluation results.

ASA 1000V Cloud Firewalls

The Cisco Adaptive Security Appliance Cisco Adaptive Security Appliance 1000V Cloud Firewall (ASA 1000V) is a virtual appliance that was developed using the ASA infrastructure to secure the tenant edge in multi-tenant environments with Cisco Nexus 1000V Series switch deployments. ASA 1000V firewalls provide the following edge features and functionality:

- Support site-to-site VPN, NAT, and DHCP.
- Act as a default gateway.
- Secure the VMs within a tenant against any network-based attacks.

In Prime Network Services Controller, edge firewall objects are associated to an ASA 1000V instance. After association, all applicable profile types for the ASA 1000V device type are pushed to the ASA 1000V instance. All edge profile objects that are created at the same organization level as the edge firewall object are pushed to the device.

Managing Compute Firewalls

Prime Network Services Controller enables you to add, edit, and delete compute firewalls. In addition, you can assign a VSG to compute firewall, thereby placing the VSG in service. The following topics describe these activities in more detail.

Adding a Compute Firewall

This procedure describes how to add a compute firewall to Prime Network Services Controller so that you can assign it to a VSG, and thereby place the VSG in service.

When you add a new compute firewall, the firewall data IP address can be the same as the data IP address of an existing compute firewall in Prime Network Services Controller as long as the firewalls have different organizational paths. That is, as long as the firewalls do not reside in the same organization, including parent and child organizations.

**Note**

We recommend that you add the compute firewall at the tenant level or below, and not at the root level.

Procedure

- Step 1** In the Resource Management tab, choose **Managed Resources > root > tenant > Compute Firewalls**.
- Step 2** In the General tab, click **Add Compute Firewall**.
- Step 3** In the Add Compute Firewall dialog box, supply the required information as described in the following table, then click **OK**:

| Field | Description |
|-------------------------------|--|
| Name | Object name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created. |
| Description | Brief object description. |
| Firewall Settings Area | |
| Device Profile | To apply a device profile to the firewall: 1 Click Select . 2 In the Select Device Profile dialog box, choose the required profile, then click OK . |
| Management Hostname | Management hostname for the firewall. |
| Data IP Address | Data IP address. The vPath component running on each VEM uses the data IP address to determine the MAC address of the VSG (via ARP). After the VSG MAC address has been resolved, vPath can communicate with the VSG using MAC in MAC encapsulation. Subsequently, for each new flow initiated by a VM, vPath sends the first packet of the flow to the VSG for policy evaluation. vPath caches the VSG policy decision in a flow table. This is the same IP address that is configured in the vservice CLI command on the Nexus 1000V port profile. |
| Data IP Subnet | Data IP subnet. |

Editing a Compute Firewall

You can edit existing compute firewalls as needed.

Procedure

- Step 1** In the Resource Management tab, choose **Managed Resources > root > tenant > Compute Firewalls** where *tenant* is the required tenant.
- Step 2** In the General tab, select the compute firewall you want to edit, then click **Edit**.
- Step 3** In the Edit dialog box, modify the following fields as appropriate, using the information in the following tables, then click **OK**.

General Tab

| Field | Description |
|---------------------------------|---|
| Name | Compute firewall name (read-only). |
| Description | Brief firewall description. |
| Pool Name | The pool assigned to the compute firewall, if any. Only one pool can be assigned to a compute firewall at a time. To change the pool, click Assign Pool . |
| States | |
| Config State | One of the following compute firewall configuration states: not-applied, applying, failed-to-apply, or applied. |
| Association State | One of the following compute firewall association states: unassociated, associating, associated, disassociating, or failed. |
| Faults Associated with Firewall | Displays faults associated with the firewall. This information is available only if the compute firewall has been associated with a VSG. |
| View Device Faults | Displays faults associated with the device. This information is available only if the compute firewall has been associated with a VSG. |
| Firewall Settings | |
| Device Profile | Device profile associated with the firewall. To change the device profile, click Select , then choose the desired profile. |

| Field | Description |
|--|---|
| Management Hostname | Management hostname for the compute firewall. |
| Data IP Address | <p>Compute firewall data IP address.</p> <p>The vPath component running on each VEM uses the data IP address to determine the MAC address of the VSG (via ARP). Once the VSG MAC address has been resolved, vPath can communicate with the VSG using MAC in MAC encapsulation. Subsequently for each new flow initiated by a VM, vPath sends the first packet of the flow to the VSG for policy evaluation. vPath caches the VSG policy decision in a flow table. This is the same IP address which is configured in the vservice CLI command on the Nexus 1000v port profile.</p> |
| Data IP Subnet | Firewall data IP subnet mask. |
| VSG Details This information is available only if the compute firewall has been associated with a VSG. | |
| Task | Click to open the Edit VSG dialog box. |
| VSG Service ID | Internal identification number of the VSG. |
| VSG Mgmt IP | VSG management IP address. |
| HA Role | High availability (HA) role of the VSG: HA or standalone mode. |
| Association | Association state of the VSG: unassociated, associating, associated, disassociating, or failed. |
| Reachable | Whether or not the VSG can be reached. |

Compute Security Profiles Tab

| Field | Description |
|------------------------|---|
| Show Resolved Policies | <p>Click to view and optionally modify the security policies applied to the compute firewall.</p> <p>This option is available only if the selected profile has been configured in the corresponding VSM port profile.</p> |
| Properties | Displays the properties of the port profile associated with the compute firewall. |

| Field | Description |
|--------------------------|--|
| Compute Security Profile | Name of the compute firewall security profile. |
| Port Profile | Name of the associated port profile. |
| Org | Distinguished name (DN) of the organization. |
| VSG Data IP | VSG data IP address. |
| Config State | VSG configuration state. |

Deleting a Compute Firewall

Procedure

-
- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Compute Firewalls**.
 - Step 2** In the General tab, select the compute firewall you want to delete, then click **Delete**.
 - Step 3** When prompted, confirm the deletion.
-

Assigning a VSG

Assigning a VSG to a compute firewall enables you to place a VSG in service and manage it using Prime Network Services Controller. Before you can assign a VSG to a compute firewall, you must:

- Register the VSG with Prime Network Services Controller. For information on registering a VSG with Prime Network Services Controller, see the *Cisco Prime Network Services Controller 3.0 Quick Start Guide*.
- Add a compute firewall to Prime Network Services Controller. For more information, see [Adding a Compute Firewall](#), on page 221.

Procedure

-
- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Compute Firewalls**.
 - Step 2** In the General tab, select the compute firewall to which you want to assign a VSG, then click **Assign VSG**.
 - Step 3** In the Assign VSG dialog box, select the desired IP address from the **VSG Management IP** drop-down list, then click **OK**.
-

Unassigning a VSG

Procedure

- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Compute Firewalls**.
 - Step 2** In the Compute Firewalls table, select the firewall with the VSG you want to unassign.
 - Step 3** Click **Unassign VSG/Pool**.
 - Step 4** In the Confirm dialog box, click **Yes**.
-

Managing Edge Firewalls

Managing edge firewalls involves adding edge firewalls to Prime Network Services Controller, configuring the edge firewall data interfaces, and then assigning an ASA 1000V to the edge firewall to place the ASA 1000V in service. The following topics describe these activities in more detail.

Adding an Edge Firewall

This procedure describes how to add an edge firewall to Prime Network Services Controller so that you can assign it to an ASA 1000V instance, and thereby place the ASA 1000V in service.

When you add a new edge firewall, the firewall data IP address identified as the primary IP address of the inside data interface can be the same as the IP address of an inside data interface for an existing edge firewall in Prime Network Services Controller long as the firewalls have different organizational paths. That is, as long as the edge firewalls do not reside in the same organization, including parent and child organizations.



Note We recommend that you add edge firewalls at the tenant level or lower, and not at the root level.

Procedure

- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Edge Firewalls**.
 - Step 2** Click **Add Edge Firewall**.
 - Step 3** In the Add Edge Firewall dialog box, specify the information as described in [Add Edge Firewall Dialog Box, on page 227](#), then click **OK**.
-

What to Do Next

After you add the edge firewall, assign an ASA 1000V to it so that you can manage the ASA 1000V using Prime Network Services Controller. For more information, see [Assigning an ASA 1000V, on page 228](#).

Add Edge Firewall Dialog Box

| Field | Description |
|---------------------|---|
| Name | Edge firewall name. |
| Description | Brief description of the edge firewall. |
| HA Mode | High Availability (HA) role of the edge firewall: HA or standalone. |
| Device Profile | To apply a device profile: <ol style="list-style-type: none"> 1 Click Select. 2 In the Select Device Profile dialog box, choose the desired profile and click OK. |
| Edge Device Profile | To apply an edge device profile: <ol style="list-style-type: none"> 1 Click Select. 2 In the Select Edge Device Profile dialog box, choose the desired profile, then click OK. |

Adding a Data Interface

When you add an edge firewall, you also need to specify inside and outside interfaces for data communications.

Procedure

-
- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Edge Firewalls**.
 - Step 2** In the Edge Firewalls pane, select the edge firewall to add or modify data interfaces, then click **Edit**.
 - Step 3** In the Edit Edge Firewall dialog box, click **Add Data Interface**.
 - Step 4** For each interface you add, enter the information as described in [Add Data Interface Dialog Box](#), then click **OK**.
-

Add Data Interface Dialog Box

| Field | Description |
|-------------|------------------------------|
| Name | Interface name. |
| Description | Brief interface description. |

| Field | Description |
|-----------------------|---|
| Role | Whether the interface is for inside or outside communications. |
| DHCP | Available for outside interfaces only. Check the Enable DHCP check box to enable DHCP on the interface. |
| Primary IP Address | IP address for this interface. |
| Secondary IP Address | Available if the edge firewall is in High Availability (HA) Mode. Secondary IP address for this interface. |
| Subnet Mask | Mask to apply to the IP address. |
| Edge Security Profile | Available for outside interfaces only. To apply an edge security profile: 1 Click Select . 2 In the Select Edge Security Profile dialog box, choose the desired profile, then click OK . |

Assigning an ASA 1000V

After you add an edge firewall to Prime Network Services Controller, you need to assign an ASA 1000V instance to it so that the ASA 1000V instance is placed in service with the associated policies and profiles. Before you can assign an ASA 1000V to an edge firewall, you must:

- Register the ASA 1000V to Prime Network Services Controller. For more information, see the *Cisco Prime Network Services Controller 3.0 Quick Start Guide*.
- Add an edge firewall to Prime Network Services Controller. For more information, see [Adding an Edge Firewall](#), on page 226.

Procedure

-
- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Edge Firewalls > edge-firewall**.
- Step 2** Click **Assign ASA 1000V**.
- Step 3** In the Assign ASA 1000V dialog box, choose the required ASA 1000V from the drop-down list, then click **OK**.
-

Unassigning an ASA 1000V

If required you can unassign an ASA 1000V from an edge firewall.

Procedure

- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Edge Firewalls > edge-firewall**.
 - Step 2** Click **Unassign ASA 1000V/Pool**.
 - Step 3** In the confirmation dialog box, click **OK**.
-

Verifying VM Registration

Use this procedure to verify that the following VMs are successfully registered in Prime Network Services Controller:

- ASA 1000V
- VSG
- VSM

Procedure

- Step 1** Choose **Administration > Service Registry > Clients**.
 - Step 2** In the Clients table, confirm that the Open State column contains *registered* for the ASA 1000V, VSG, and VSM entries.
-

Examining Fault Details

Prime Network Services Controller enables you to examine the policy and configuration errors that prevent the successful application of a policy. For example, if you apply a policy to an edge firewall and the Config State field displays the Failed-to-Apply state, you can examine the configuration errors to identify the issue and resolve the problem.

The same interface enables you to perform the following tasks:

- Examine the faults and events associated with an edge firewall with applied policies and configurations.
- Examine the faults associated with a compute firewall.

The following topics describe these features in more detail.

Examining Faults and Configuration Errors for Edge Firewalls

Prime Network Services Controller enables you to view the faults and events associated with edge firewalls, and their policies and configurations.

Procedure

- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Edge Firewalls > edge-firewall**.
- Step 2** In the General tab, review the configuration, association, and fault information in the States area.
- Step 3** If faults are indicated, view fault details as follows:
- Click the **Faults** tab.
 - Click the **Events** tab.
 - Click **Faults Associated with Firewall**.
 - Click **View Configuration Faults**.
- Step 4** To view more information, double-click an entry in any of the tables.
In the Faults table in the new browser window, you can click **Refresh Now** to view updated information.
-

Examining Faults for Compute Firewalls

Prime Network Services Controller enables you to examine faults and events for compute firewalls.

Procedure

- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Compute Firewalls > compute-firewall**.
- Step 2** In the General tab, review the configuration, association, and fault information in the States area.
- Step 3** If faults are indicated, view fault details as follows:
- Click the **Faults** tab.
 - Click the **Events** tab.
 - Click **Faults Associated with Firewall**.
 - Click **View Configuration Faults**.
- Step 4** To view more information, double-click an entry in any of the tables.
-

Launching ASDM

Prime Network Services Controller enables you to launch Cisco Adaptive Security Device Manager (ASDM) as a Web Start application on your desktop.

You can set up ASDM to be used by the ASA 1000V when it is configured for either Prime Network Services Controller management mode or ASDM management mode. When the ASA 1000V is configured to use Prime Network Services Controller management mode, you can use ASDM to monitor the status of the ASA 1000V, but you cannot use it to manage configurations.

Before You Begin

You must complete the following tasks before launching ASDM from Prime Network Services Controller:

1 Do one of the following:

- If you have not already deployed the ASA 1000V OVA, do so now; during the deployment, provide the ASDM client IP address.
- If you have already deployed the ASA 1000V OVA, apply the following configuration by using the VM console in the vSphere client:

- Add a route on the management interface to the ASDM client subnet by issuing the following command:

```
ASA1000V(config)# route interface ip subnet next-hop-ip
```

where *interface* is the management interface to the ASDM client subnet, *ip* is the IP address of the host that accesses ASDM, *subnet* is the ASDM client subnet, and *next-hop-ip* is the IP address of the gateway.



Note Perform this step only if the next hop gateway IP address was not specified when deploying the ASA 1000V.

- Allow HTTP access via the management interface for the ASDM client subnet by entering the following command:

```
ASA1000V(config)# http ip subnet interface
```

where *ip* is the IP address of the host that accesses ASDM, and *interface* is the ASDM client interface.



Note Perform this step only if the ASDM client IP address was not specified when deploying the ASA 1000V.

2 Confirm the following:

- The ASA 1000V is registered to Prime Network Services Controller.
- A valid username and password exist for the ASA 1000V VM console.

3 Assign the edge firewall to an ASA 1000V instance. If the edge firewall is not assigned to an ASA 1000V instance, the ASDM options are not displayed in the UI.

- 4 Confirm that your system is configured to run downloaded Java Web Start applications.

For more information about configuring ASDM, see the *Cisco ASA 1000V Cloud Firewall Getting Started Guide*.

Procedure

-
- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Edge Firewalls > edge-firewall** where *edge-firewall* is the edge firewall for which you want to launch ASDM.
- Step 2** In the General tab, click **Launch ASDM** in the ASA 1000V Details area.
The ASDM Launch screen opens in a new browser window.
- Step 3** In the ASDM Launch screen, click **Run ASDM**.
The ASDM Web Start application is automatically downloaded and runs. If prompted, accept the certificates.
- Note** If an ASDM login dialog box is displayed, you can click **OK** without entering login credentials.
-

Managing Pools

Adding a Pool

Procedure

-
- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Pools**.
- Step 2** In the General tab, click **Add Pool**.
- Step 3** In the Add Pool dialog box, enter the information as described in the following table, then click **OK**:

| Field | Description |
|--------------------------|---|
| Name | Pool name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created. |
| Description | Brief pool description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. |
| Pool Members Area | |
| (Un)Assign | Click to add pool members to or remove pool members from the pool. |

| Field | Description |
|-----------------------|---|
| Management IP Address | Management IP address of the pool member. |
| Firewall | Associated compute or edge firewall. |
| Association State | Association state of the pool member: unassociated, associating, associated, disassociating, or failed. |
| Service ID | Unique identifier for the pool member. |
| Operational State | Pool member operational state. |

Step 4 (Optional) Assign pool members to the pool by performing the following tasks:

- a) Click **(Un)Assign**.
- b) In the (Un)Assign Pool Member(s) dialog box, select the firewall that you want to assign, and then click the arrow to move it to the Assigned Firewalls list.
- c) Click **OK**.

Step 5 Click **OK**.

Assigning a Pool

After you have created a pool, you can assign it to a compute or edge firewall.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root > Compute Firewalls** or **Edge Firewalls**.

Step 2 In the list of firewalls, select the required firewall, then click **Assign Pool**.

Step 3 In the Assign Pool dialog box, either choose a pool from the Name drop-down list or click **Add Pool** to add a new pool.

Step 4 Click **OK**.

Editing a Pool

Procedure

- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Pools**.
- Step 2** In the General tab, select the pool that you want to edit, then click **Edit**.
- Step 3** In the Edit Pool dialog box, edit the information as required by using the information in the following table, then click **OK**.

| Field | Description |
|---------------------|--|
| Name | Pool name (read-only). |
| Description | Brief pool description. |
| Pool Members | |
| (Un)Assign | Click to assign or unassign pool members. |
| IP Address | Pool member IP addresses. |
| Compute Firewall | A list of the compute firewalls. |
| Association State | Association state for the pool member. |
| Service ID | Service identification number for the pool member. |
| Operational State | Operational state of the pool member. |

Unassigning a Pool

If required, you can unassign a pool from a compute or edge firewall.

Procedure

- Step 1** Choose **Resource Management > Managed Resources > root > Compute Firewalls** or **Edge Firewalls**.
- Step 2** In the list of firewalls, select the required firewall, then click **Unassign *object*/Pool** where *object* is either ASA 1000V or VSG, depending on whether you selected an edge or compute firewall.
- Step 3** When prompted, confirm the deletion.

Deleting a Pool

Procedure

- Step 1** Choose **Resource Management > Managed Resources > root > tenant > Pools**.
 - Step 2** In the General tab, select the pool you want to delete, then click **Delete**.
 - Step 3** When prompted, confirm the deletion.
-



Configuring Administrative Operations

This section includes the following topics:

- [Administrative Operation Conventions, page 237](#)
- [Managing Backup Operations, page 237](#)
- [Restoring a Backup Configuration, page 242](#)
- [Managing Export Operations, page 244](#)
- [Configuring Import Operations, page 248](#)

Administrative Operation Conventions

The following conventions apply when performing the administrative operations described in this section:

- The remote file location you specify must start with a slash (/) and include the full path and file name. Do not use relative paths.
- The user name and password on the remote system must be correct, and the user specified must have read and write permissions on the remote system.
- The file on the remote system must be a valid file, and the size cannot be zero.
- For backup and export operations, if the Task tab contains a Remote Err Description of *No such file*, reboot the Prime Network Services Controller VM via vCenter.

Managing Backup Operations

We recommend that you use backup and restore operation as a disaster recovery mechanism. To migrate configuration data from one Prime Network Services Controller server to another, use export and import operations.

Creating a Backup Operation

Before You Begin

Obtain the backup server IP address or hostname and authentication credentials.

Procedure

Step 1 Choose **Administration > Operations > Backups**.

Step 2 Click **Create Backup Operation**.

Step 3 In the Create Backup Operation dialog box, complete the following fields, then click **OK**:

| Field | Description |
|---------------------|---|
| Admin State | <p>One of the following administrative states:</p> <ul style="list-style-type: none"> • enabled—Backup is enabled. The system runs the backup operation when you click OK. • disabled—Backup is disabled. The system does not run the backup operation when you click OK. If you choose this option, all fields in the dialog box remain visible. |
| Type | <p>Backup type.</p> <p>The backup creates a copy of the whole database file. You can use this file for disaster recovery if you need to recreate every configuration on your system. This field is not editable.</p> |
| Protocol | <p>Protocol used when communicating with the remote server:</p> <ul style="list-style-type: none"> • FTP • SCP • SFTP |
| Hostname/IP Address | <p>Hostname or IP address of the device where the backup file is stored.</p> <p>This entry cannot be changed when editing the operation.</p> <p>Note If you use a hostname instead of an IP address, you must configure a DNS server.</p> |
| User | <p>Username the system uses to log into the remote server.</p> |

| Field | Description |
|---------------------------|--|
| Password | <p>Password the system uses to log into the remote server.</p> <p>This field is displayed if you choose enabled in the Admin State field.</p> <p>Note Prime Network Services Controller does not store this password. You do not need to enter this password unless you intend to enable and run the backup operation immediately.</p> |
| Absolute Path Remote File | <p>Full path of the backup filename.</p> <p>This entry must start with a slash (/) and must not contain a relative path.</p> |

Running a Backup Operation

Procedure

- Step 1** Choose **Administration > Operations > Backups > Backup-server** where *backup-server* is the server on which the backup file is stored.
- Step 2** In the General tab, enter the following information:
- In the Admin State field, choose **enabled**.
 - In the Password field, enter the password for the identified user.
 - (Optional) Change the content of the other available fields.
- Step 3** Click **Save**.
Prime Network Services Controller takes a snapshot of the configuration type that you selected and uploads the file to the network location.
- Step 4** (Optional) To view the progress of the backup operation, click the **Task** tab. The Task tab provides the information described in the following table. The operation continues to run until it is completed.

| Field | Description |
|------------------|--|
| Description | Task description. |
| Status | Task status. |
| Stage Descriptor | Description of the current stage. |
| Tries | Number of times the task has been tried. |

| Field | Description |
|------------------------|--|
| Previous Status | Status of the previous task only. This field does not provide the status of the current task. |
| Remote Err Code | Remote error code. |
| Remote Err Description | Description of the remote error. |
| Remote Inv Result | Remote error result. |
| Time Stamp | Date and time when the task completed. |
| Progress | Progress of the current task, indicated by the percent complete, a progress bar, or both. |

Editing a Backup Operation

Before You Begin

Obtain the backup server IP address or hostname and authentication credentials.

Procedure

- Step 1** Choose **Administration > Operations > Backups**.
- Step 2** Select the backup operation you want to edit, then click **Edit**.
- Step 3** In the Edit Backup dialog box, modify the information as required, then click **OK**.

| Field | Description |
|-------------|--|
| Admin State | One of the following administrative states: <ul style="list-style-type: none"> • enabled—Backup is enabled. The system runs the backup operation when you click OK. • disabled—Backup is disabled. The system does not run the backup operation when you click OK. If you choose this option, all fields in the dialog box remain visible. |

| Field | Description |
|---------------------------|--|
| Type | <p>Backup type.</p> <p>The backup creates a copy of the whole database file. You can use this file for disaster recovery if you need to recreate every configuration on your system. This field is not editable.</p> |
| Protocol | <p>Protocol used when communicating with the remote server:</p> <ul style="list-style-type: none"> • FTP • SCP • SFTP |
| Hostname/IP Address | <p>Hostname or IP address of the device where the backup file is stored.</p> <p>This entry cannot be changed when editing the operation.</p> <p>Note If you use a hostname instead of an IP address, you must configure a DNS server.</p> |
| User | <p>Username the system uses to log into the remote server.</p> |
| Password | <p>Password the system uses to log into the remote server.</p> <p>This field is displayed if you choose enabled in the Admin State field.</p> <p>Note Prime Network Services Controller does not store this password. You do not need to enter this password unless you intend to enable and run the backup operation immediately.</p> |
| Absolute Path Remote File | <p>Full path of the backup filename.</p> <p>This entry must start with a slash (/) and must not contain a relative path.</p> |

Deleting a Backup Operation

Procedure

-
- Step 1** Choose **Administration > Operations > Backups**.
 - Step 2** Select the backup operation you want to delete, then click **Delete**.
 - Step 3** When prompted, confirm the deletion.
-

Restoring a Backup Configuration

Procedure

-
- Step 1** Install the Prime Network Services Controller virtual machine. For information, see the *Cisco Prime Network Services Controller 3.0 Quick Start Guide*.
 - Step 2** Uninstall the VSG policy agents. Connect the Secure Shell to the VSG console for this task. This step does not cause a traffic disruption.

Example:

```
vsg# conf t
vsg (config)# vnmc-policy-agent
vsg (config-vnmc-policy-agent)# no policy-agent-image
```

Note Perform this step for all VSGs that are associated with the Prime Network Services Controller that you are restoring.

- Step 3** Disable the ASA 1000V policy agent.

Example:

```
ASA-154# conf t
ASA-154 (config)# no vnmc policy-agent
```

- Step 4** Uninstall the VSM policy agents. Connect the Secure Shell to the VSM console for this task. This step does not cause a traffic disruption.

Example:

```
vsm# conf t
vsm (config)# nsc-policy-agent
vsm (config-nsc-policy-agent)# no policy-agent-image
```

Note Perform this step for all VSMs that are associated with the Prime Network Services Controller you are restoring.

- Step 5** Restore the Prime Network Services Controller database. Connect the Secure Shell to the Prime Network Services Controller CLI for this task. Depending upon your Prime Network Services Controller backup location, restore using FTP, SCP, or SFTP.

Example:

```
nsc# connect local-mgmt
nsc(local-mgmt) # restore scp://username@server/path
```

Step 6 In the Prime Network Services Controller UI, choose **Administration > Service Registry > Clients**, and in the General tab, do the following:

- a) Wait until each registered VSM displays the operational status as lost-visibility.
- b) Choose each VSM, and click **Delete Client**.

Step 7 In the Prime Network Services Controller UI, choose **Resource Management > Resources > Virtual Supervisor Modules**, and verify that the deleted VSMS are not visible.

Step 8 Reregister the VSMS associated with Prime Network Services Controller by entering the following commands for each VSM:

Example:

```
VSM# conf t
VSM (config)# nsc-policy-agent
VSM (config-nsc-policy-agent)# registration-ip vsm-ip-address
VSM (config-nsc-policy-agent)# shared-secret password
```

Step 9 Reinstall the VSM policy agents.

Note If the VSM policy agents must be upgraded, install the new software now.

Example:

```
VSM# conf t
VSM (config)# nsc-policy-agent
VSM (config-nsc-policy-agent)# policy-agent-image bootflash:nsc-vsmpa.1.0.1g.bin
```

Step 10 Wait until all the VSMS have registered in the Service Registry and are displayed under **Resource Management > Resources > Virtual Supervisor Modules**.

Step 11 Reregister the VSGs associated with Prime Network Services Controller by entering the following commands for each VSG:

Example:

```
VSG# conf t
VSG (config)# vnmc-policy-agent
VSG (config-vnmc-policy-agent)# registration-ip vsg-ip-address
VSG (config-vnmc-policy-agent)# shared-secret password
```

Step 12 Reinstall the VSG policy agents.

Note If the VSG policy agents must be upgraded, install the new software now.

Example:

```
VSG# conf t
VSG (config)# vnmc-policy-agent
VSG (config-vnmc-policy-agent)# policy-agent-image bootflash:nsc-vsgpa.1.0.1g.bin
```

Step 13 Re-enable the ASA 1000V policy agent.

Example:

```
ASA-154# conf t
ASA-154 (config)# vnmc policy-agent
ASA-154 (config-vnmc-policy-agent)# shared-secret password
ASA-154 (config-vnmc-policy-agent)# registration host host-ip-address
```

Step 14 Verify the following states after the restore process is complete:

Note The restore process could take a few minutes depending upon your setup environment.

- a) Using the VSG CLI, verify that your configurations are restored to their earlier state.
 - b) Using the Prime Network Services Controller UI, verify that your objects and policies are restored to their earlier state.
 - c) Using the ASA 1000V CLI, verify that your configurations are restored to their earlier state.
-

Managing Export Operations

Use export and import operations to migrate data from one Prime Network Services Controller server to another. To back up and restore Prime Network Services Controller data (for example, as a disaster recovery mechanism), use backup and restore operations.

Creating an Export Operation

The associations of compute and edge firewalls with VSGs and ASA 1000Vs, respectively, are not included in export or import data. Only firewall definitions are included, such as device profiles and policies. If an imported firewall did not exist in the system, it will not be associated to a VSG or ASA 1000V after the import operation. If an imported firewall already existed in the system, the association state remains the same.

InterCloud data is not included in export or import operations. The affected InterCloud data includes:

- Provider account information
- InterCloud links and components
- Cloud VMs

Before You Begin

Obtain the remote file server IP address or hostname and authentication credentials before performing an export.

Procedure

Step 1 Choose **Administration > Operations > Backups**.

Step 2 Click **Create Export Operation**.

Step 3 In the Create Export Operation dialog box, provide the required information as described in the following table, then click **OK**:

| Field | Description |
|----------------------------------|---|
| Admin State | <p>One of the following administrative states:</p> <ul style="list-style-type: none"> • enabled—Export is enabled. The system runs the export operation when you click OK. • disabled—Export is disabled. The system does not run the export operation when you click OK. If you choose this option, all fields in the dialog box remain visible. |
| Type | <p>One of the following export types:</p> <ul style="list-style-type: none"> • config-all • config-logical • config-system |
| Protocol | <p>Protocol used when communicating with the remote server:</p> <ul style="list-style-type: none"> • FTP • SCP • SFTP |
| Hostname/IP Address | <p>Hostname or IP address of the device where the export file is stored.</p> <p>This entry cannot be changed when editing the operation.</p> <p>Note If you use a hostname instead of an IP address, you must configure a DNS server.</p> |
| User | <p>Username the system uses to log into the remote server.</p> |
| Password | <p>The password the system uses to log into the remote server.</p> <p>This field is displayed if you choose enabled in the Admin State field.</p> <p>Note Prime Network Services Controller does not store this password. You do not need to enter this password unless you intend to enable and run the export operation immediately.</p> |
| Absolute Path Remote File (.tgz) | <p>Full path of the .tgz filename.</p> <p>This entry must start with a slash (/) and must not contain a relative path.</p> |

Editing an Export Operation



Note The associations of compute and edge firewalls with VSGs and ASA 1000Vs, respectively, are not included in export or import data. Only firewall definitions are included, such as device profiles and policies. If an imported firewall did not exist in the system, it will not be associated to a VSG or ASA 1000V after the import operation. If an imported firewall already existed in the system, the association state remains the same.

Before You Begin

Obtain the remote file server IP address or hostname and authentication credentials before performing an export.

Procedure

- Step 1** Choose **Administration > Operations > Backups**.
- Step 2** In the Backups table, select the export operation you want to edit, then click **Edit**.
- Step 3** In the Edit Export dialog box, modify the fields as appropriate, then click **OK**.

| Field | Description |
|-------------|--|
| Admin State | One of the following administrative states: <ul style="list-style-type: none"> • enabled—Export is enabled. The system runs the export operation when you click OK. • disabled—Export is disabled. The system does not run the export operation when you click OK. If you choose this option, all fields in the dialog box remain visible. |
| Type | One of the following export types: <ul style="list-style-type: none"> • config-all • config-logical • config-system |

| Field | Description |
|----------------------------------|--|
| Protocol | <p>Protocol used when communicating with the remote server:</p> <ul style="list-style-type: none"> • FTP • SCP • SFTP |
| Hostname/IP Address | <p>Hostname or IP address of the device where the export file is stored.</p> <p>This entry cannot be changed when editing the operation.</p> <p>Note If you use a hostname instead of an IP address, you must configure a DNS server.</p> |
| User | <p>Username the system uses to log into the remote server.</p> |
| Password | <p>The password the system uses to log into the remote server.</p> <p>This field is displayed if you choose enabled in the Admin State field.</p> <p>Note Prime Network Services Controller does not store this password. You do not need to enter this password unless you intend to enable and run the export operation immediately.</p> |
| Absolute Path Remote File (.tgz) | <p>Full path of the .tgz filename.</p> <p>This entry must start with a slash (/) and must not contain a relative path.</p> |

Deleting an Export Operation

Procedure

-
- Step 1** In the Navigation pane, choose **Administration > Operation > Backups**.
- Step 2** In the **Work** pane, click the export operation you want to delete.
- Step 3** In the Confirm dialog box, click **Yes**.
-

Configuring Import Operations

Creating an Import Operation

Before You Begin

Obtain the remote file server IP address or hostname and authentication credentials.



Note

The association of compute and edge firewalls with VSGs and ASA 1000Vs, respectively, are not included in the export or import data. Only the compute and edge firewall definitions are included, such as device profiles and policies. Therefore, if an imported firewall did not exist in the system, it will not be associated to a VSG or ASA 1000V after the import operation. If an imported firewall already existed in the system, the association state remains the same.



Caution

When the configuration data is imported into the Prime Network Services Controller server, you might see an error message and get logged out, followed by the display of a new Prime Network Services Controller certificate. This error occurs because the Prime Network Services Controller hostname, domain name, or both have changed. The VM Manager Extension needs to be exported again and installed on vCenter. To continue with the import, accept the Prime Network Services Controller certificate and log into Prime Network Services Controller again.

Procedure

Step 1 Choose **Administration > Operations > Backups**.

Step 2 Click **Create Import Operation**.

Step 3 In the Create Import Operation dialog box, provide the following information as required, then click **OK**:

| Field | Description |
|-------------|--|
| Admin State | One of the following administrative states: <ul style="list-style-type: none"> • enabled—Import is enabled. The system runs the import operation as soon as you click OK. • disabled—Import is disabled. The system does not run the import operation when you click OK. If you choose this option, all fields in the dialog box remain visible. |
| Action | Action to be taken on a file: merge. |

| Field | Description |
|----------------------------------|--|
| Protocol | <p>Protocol used when communicating with the remote server:</p> <ul style="list-style-type: none"> • FTP • SCP • SFTP |
| Hostname/IP Address | <p>Hostname or IP address of the device where the import file is stored.</p> <p>This entry cannot be changed when editing the operation.</p> <p>Note If you use a hostname instead of an IP address, you must configure a DNS server.</p> |
| User | <p>Username the system uses to log into the remote server.</p> <p>This field is displayed if you choose enabled in the Admin State field.</p> |
| Password | <p>Password the system uses to log into the remote server.</p> <p>Note Prime Network Services Controller does not store this password. You do not need to enter this password unless you intend to enable and run the import operation immediately.</p> |
| Absolute Path Remote File (.tgz) | <p>Full path of the .tgz filename.</p> <p>This entry must start with a slash (/) and must not contain a relative path.</p> |

Editing an Import Operation

Before You Begin

Obtain the remote file server IP address or hostname and authentication credentials.

Procedure

Step 1 Choose **Administration > Operations > Backups**.

Step 2 Select the import operation that you want to edit, then click **Edit**.

Step 3 In the Edit dialog box, modify the fields as required, then click **OK**.

| Field | Description |
|---------------------|---|
| Admin State | <p>One of the following administrative states:</p> <ul style="list-style-type: none"> • enabled—Import is enabled. The system runs the import operation as soon as you click OK. • disabled—Import is disabled. The system does not run the import operation when you click OK. If you choose this option, all fields in the dialog box remain visible. |
| Action | Action to be taken on a file: merge. |
| Protocol | <p>Protocol used when communicating with the remote server:</p> <ul style="list-style-type: none"> • FTP • SCP • SFTP |
| Hostname/IP Address | <p>Hostname or IP address of the device where the import file is stored.</p> <p>This entry cannot be changed when editing the operation.</p> <p>Note If you use a hostname instead of an IP address, you must configure a DNS server.</p> |
| User | <p>Username the system uses to log into the remote server.</p> <p>This field is displayed if you choose enabled in the Admin State field.</p> |
| Password | <p>Password the system uses to log into the remote server.</p> <p>Note Prime Network Services Controller does not store this password. You do not need to enter this password unless you intend to enable and run the import operation immediately.</p> |

| Field | Description |
|----------------------------------|---|
| Absolute Path Remote File (.tgz) | Full path of the .tgz filename. This entry must start with a slash (/) and must not contain a relative path. |

Deleting an Import Operation

Procedure

- Step 1** Choose **Administration > Operations > Backups**.
 - Step 2** Select the import operation that you want to delete, then click **Delete**.
 - Step 3** When prompted, confirm the deletion.
-



INDEX

A

- AAA policies [183](#)
 - configuring [183](#)
- ACL policies [124](#)
 - adding [124](#)
- ACL Policy Rule dialog box [124](#)
- ACL policy rules, and time ranges [128](#)
- ACL policy sets [130](#)
 - adding [130](#)
- Add Auth Policy dialog box [184](#)
- Add Compute Security Profile dialog box [160](#)
- Add Connection Timeout Policy Rule dialog box [131](#)
- Add Data Interface dialog box [227](#)
- Add DHCP Server Policy dialog box [134](#)
- Add Edge Firewall dialog box [227](#)
- Add Edge Security Profile dialog box [164](#)
- Add Interface Policy Set dialog box [151](#)
- Add IP Audit Policy Rule dialog box [136](#)
- Add NAT Policy Rule dialog box [139](#)
- Add NTP Server dialog box [215](#)
- Add Policy to Authenticate Peer dialog box [155](#)
- Add Syslog Policy dialog box [198](#)
- Add Syslog Server dialog box [204](#)
- adding [40, 43, 46, 53, 60, 63, 82, 84, 124, 130, 132, 171, 172, 175, 176, 178, 186, 188, 191, 194, 198, 204, 209, 221, 226, 227, 232](#)
 - ACL policies [124](#)
 - ACL policy sets [130](#)
 - compute firewalls [221](#)
 - connection timeout policies [130](#)
 - core file policies [186](#)
 - data interfaces [227](#)
 - DHCP relay servers [132](#)
 - DNS servers [60](#)
 - edge firewalls [226](#)
 - fault policies [40](#)
 - System profile [40](#)
 - fault policy [188](#)
 - device profile [188](#)
 - firewall device profiles [209](#)
 - key policies [84](#)
 - adding (*continued*)
 - logging policies [43](#)
 - System profile [43](#)
 - logging policy [191](#)
 - device profile [191](#)
 - object group expressions [172](#)
 - object groups [171](#)
 - pools [232](#)
 - security profile dictionary [175](#)
 - security profile dictionary attributes [176](#)
 - SNMP community [194](#)
 - SNMP policies [194](#)
 - SNMP trap [194](#)
 - syslog policies [46, 198](#)
 - device profile [198](#)
 - System profile [46](#)
 - syslog server [53](#)
 - System profile [53](#)
 - syslog servers for devices [204](#)
 - VM Managers [63](#)
 - vZones [178](#)
- adding an SNMP trap receiver [197](#)
- administrative operation [237](#)
 - conventions [237](#)
- AMI image [116, 117](#)
 - from Linux VM [117](#)
 - from Windows VM [116](#)
- applying [165](#)
 - edge device profiles [165](#)
 - edge security profiles [165](#)
- ASA 1000V firewalls, overview [221](#)
- ASA 1000Vs [228, 229](#)
 - assigning [228](#)
 - unassigning [229](#)
- ASDM [231](#)
 - launching [231](#)
- assigning [170, 225, 233](#)
 - policy [170](#)
 - pool [233](#)
 - VSGs [225](#)
- associating [217](#)
 - device policies [217](#)

audit logs [114](#)
 monitoring [114](#)

B

backing up [238](#)
 system [238](#)
 backup operations [237](#)
 managing [237](#)

C

changing [33](#)
 locales [33](#)
 roles [33](#)
 clone [11](#)
 cloud VM templates [98](#)
 creating [98](#)
 cloud VMs [87, 102, 104, 105, 115](#)
 configuring [87](#)
 instantiating [102, 104, 105](#)
 IP addresses not shown [115](#)
 clouds [80, 103](#)
 configuring device profiles [80](#)
 instantiating VMs [103](#)
 compute firewalls [216, 221, 222, 230](#)
 adding [221](#)
 applying device profiles [216](#)
 editing [222](#)
 examining faults [230](#)
 compute security profiles [159](#)
 configuring [159](#)
 configuring [78, 79, 80, 83, 84, 87, 88, 132, 135, 136, 137, 138, 141, 142, 143, 144, 145, 146, 149, 151, 152, 155, 156, 159, 161, 163, 171, 183, 214](#)
 AAA policies [183](#)
 cloud VMs [87](#)
 compute security profiles [159](#)
 connection parameter policies [83](#)
 crypto map policies [146](#)
 device policies [183](#)
 device profiles [214](#)
 DHCP policies [132](#)
 edge device profiles [161](#)
 edge security profiles [163](#)
 IKE policies [149](#)
 InterCloud links [87, 88](#)
 InterCloud links, preparing for [79](#)
 InterCloud resources [78](#)
 interface policy sets [151](#)

configuring (*continued*)
 IP audit policies [135, 136](#)
 configuring [136](#)
 IP audit signature policies [137](#)
 IPsec policies [152](#)
 NAT policy sets [141](#)
 NAT/PAT policies [138](#)
 NTP [214](#)
 object groups [171](#)
 packet inspection policies [143](#)
 PAT [142](#)
 PAT for edge firewalls [141, 142](#)
 peer authentication policies [155](#)
 routing policies [144](#)
 TCP intercept policies [145](#)
 tunnel profiles [84](#)
 VPN device policies [156](#)
 VPN policies [146](#)
 VSM port profiles [80](#)
 connection parameter policies [83](#)
 configuring [83](#)
 connection timeout policies [130](#)
 adding [130](#)
 conventions [237](#)
 administrative operations [237](#)
 creating [14, 25, 26, 29, 35, 71, 72, 73, 75, 85, 101, 106, 238, 244, 248](#)
 applications [73](#)
 backups [238](#)
 export operations [244](#)
 import operations [248](#)
 LDAP provider [14](#)
 locales [26](#)
 templates [101, 106](#)
 tenants [71](#)
 tiers [75](#)
 trusted points [35](#)
 user accounts [29](#)
 user roles [25](#)
 virtual data centers [72](#)
 creating AMI images [116](#)
 creating template [100](#)
 from enterprise templates [100](#)
 creating templates [98](#)
 for cloud VMs [98](#)
 creating templates in clouds [98](#)
 crypto map policies [146](#)
 configuring [146](#)

D

data interfaces [227](#)
 adding [227](#)

deleting [17, 26, 28, 29, 36, 40, 43, 45, 52, 57, 60, 61, 67, 72, 73, 74, 76, 109, 170, 174, 175, 177, 178, 180, 187, 190, 193, 196, 198, 204, 209, 214, 225, 235, 242, 247, 251](#)

- application [74](#)
- backup operation [242](#)
- compute firewalls [225](#)
- core file policies [40](#)
 - System profile [40](#)
- core file policy [187](#)
 - device profile [187](#)
- DNS server [60](#)
- export operation [247](#)
- fault policy [43, 190](#)
 - device profile [190](#)
 - system profile [43](#)
- firewall device profile [214](#)
- import operation [251](#)
- InterCloud links [109](#)
- LDAP provider [17](#)
- locales [28](#)
- logging policies [45](#)
 - System profile [45](#)
- logging policy [193](#)
 - device profile [193](#)
- NTP server [61](#)
- object group expressions [175](#)
- object groups [174](#)
- organizations from a locale [29](#)
- pool [235](#)
- security profile [170](#)
- security profile attribute [170](#)
- security profile dictionary [177](#)
- security profile dictionary attribute [178](#)
- SNMP policy [196](#)
- SNMP trap receiver [198](#)
- syslog policy [52, 204](#)
 - device profile [204](#)
 - System profile [52](#)
- syslog server [57, 209](#)
 - device profile [209](#)
 - System profile [57](#)
- tenants [72](#)
- tiers [76](#)
- trusted points [36](#)
- user roles [26](#)
 - deleting [26](#)
- virtual data center [73](#)
- VM Managers [67](#)
- vZone conditions [180](#)
- vZones [180](#)

device configuration [182](#)

device policies [181, 183, 217](#)

- associating with profiles [217](#)
- configuring [183](#)

device profiles [80, 181, 214, 216](#)

- applying to compute firewalls [216](#)
- applying to edge firewalls [216](#)
- configuring [214](#)
- configuring for clouds [80](#)

DHCP policies [132](#)

- configuring [132](#)

DHCP relay policies [133](#)

- configuring [133](#)
 - DHCP relay policies [133](#)

DHCP relay servers [132](#)

- adding [132](#)

DNS server [60](#)

- deleting [60](#)

E

Edge Device Profile dialog box [162](#)

edge device profiles [161, 165](#)

- applying [165](#)
- configuring [161](#)

edge firewall security profiles [168](#)

- configuring [168](#)

edge firewalls [216, 226, 228, 229, 230](#)

- adding [226](#)
 - applying device profiles [216](#)
 - assigning ASA 1000Vs [228](#)
 - examining faults [230](#)
 - unassigning ASA 1000Vs [229](#)

edge security profiles [163, 165](#)

- applying [165](#)
- configuring [163](#)

Edit Security Profile Dictionary dialog box [176](#)

editing [16, 26, 27, 36, 38, 39, 41, 44, 49, 55, 58, 61, 65, 71, 73, 74, 75, 166, 168, 173, 174, 177, 179, 187, 189, 192, 195, 197, 207, 211, 222, 234, 240, 246, 249](#)

- application [74](#)
- backup operations [240](#)
- compute firewalls [222](#)
- core file policies [39](#)
- core file policy [187](#)
 - device profile [187](#)
- default System profile [58](#)
- DNS domains [61](#)
- export operation [246](#)
- fault policies [41](#)
 - System profile [41](#)
- fault policy [189](#)
 - device profile [189](#)
- firewall device profiles [211](#)
- import operations [249](#)
- LDAP provider [16](#)

editing (*continued*)

- locales [27](#)
 - logging policies [38, 44](#)
 - System profile [38, 44](#)
 - logging policy [192](#)
 - device profile [192](#)
 - object group expression [174](#)
 - object groups [173](#)
 - pools [234](#)
 - security profile dictionary attribute [177](#)
 - security profiles [166, 168](#)
 - SNMP policy [195](#)
 - SNMP trap receiver [197](#)
 - syslog policies [49](#)
 - System profile [49](#)
 - syslog policy [49](#)
 - local destinations [49](#)
 - syslog server [55](#)
 - system profile [55](#)
 - syslog servers [207](#)
 - tenants [71](#)
 - tiers [75](#)
 - trusted points [36](#)
 - user roles [26](#)
 - virtual data centers [73](#)
 - VM Manager [65](#)
 - vZones [179](#)
- events [114](#)
- monitoring [114](#)
- export operations [244](#)
- managing [244](#)

F

- faults [113, 229, 230](#)
 - compute firewalls [230](#)
 - edge firewalls [230](#)
 - monitoring [113](#)
 - viewing details [229](#)
- field aids [9](#)
- firewall access [5](#)
- firewall device profiles [211](#)
 - editing [211](#)
- firewalls, using [5](#)

I

- IKE policies [149](#)
 - configuring [149](#)
- IKE V1 Policy dialog box [150](#)
- IKE V2 Policy dialog box [150](#)

- Import VM Image dialog box [97](#)
- importing [86, 95, 96](#)
 - infrastructure images [86](#)
 - InterCloud Agent images [95](#)
 - VM images [96](#)
- infrastructure images [86](#)
 - importing [86](#)
- instantiating [102, 104, 105](#)
 - cloud VMs [102, 104, 105](#)
- InterCloud [110](#)
 - monitoring status [110](#)
- InterCloud Agent images [95](#)
 - importing [95](#)
- InterCloud clients lose connectivity [115](#)
- InterCloud configuration [78](#)
 - workflow [78](#)
- InterCloud link [88, 109](#)
 - configuring [88](#)
 - deleting [109](#)
- InterCloud links [79, 80, 87, 107, 108](#)
 - configuring [87](#)
 - managing [107](#)
 - preparing [80](#)
 - preparing to configure [79](#)
 - updating [108](#)
 - updating when in HA mode [108](#)
- InterCloud management [78, 110](#)
 - Recent Jobs table [110](#)
 - user privileges [78](#)
- InterCloud resources [77, 110, 112](#)
 - monitoring [110](#)
 - Status fields [112](#)
 - Task tab [112](#)
- interface policy sets, configuring [151](#)
- IP audit signature policies [137](#)
 - configuring [137](#)
- IPsec IKEv1 Proposal dialog box [153, 154](#)
- IPsec policies [152](#)
 - configuring [152](#)

K

- key policies [84](#)
 - adding [84](#)

L

- launching [231](#)
 - ASDM [231](#)
- LDAP provider [14, 16, 17](#)
 - creating [14](#)

LDAP provider (*continued*)deleting [17](#)editing [16](#)locales [26, 27, 28](#)assigning organizations [28](#)creating [26](#)editing [27](#)locally authenticated user account [33](#)changing locales [33](#)changing roles [33](#)logging in [6](#)**M**MAC address pool [82](#)adding [82](#)MAC address pools [82](#)managed resources [219](#)managing [107, 237, 244](#)backup operations [237](#)export operations [244](#)InterCloud links [107](#)migrating a VM [106](#)monitoring [33, 110, 111, 112, 113, 114](#)audit logs [114](#)events [114](#)faults [113](#)InterCloud status [110](#)user sessions [33](#)using Status fields [112](#)using Task tabs [112](#)Monitoring Tab [111](#)multi-tenant environments [69](#)**N**name resolution [70](#)NAT policy sets [141](#)configuring [141](#)NAT/PAT policies [138](#)configuring [138](#)New DHCP Relay Policy dialog box [133](#)New DHCP Relay Server dialog box [133](#)not available for cloud VMs [115](#)NTP [60, 214](#)configuring [214](#)configuring for System Profile [60](#)**O**object groups [171, 173](#)adding [171](#)configuring [171](#)editing [173](#)organizations [26](#)creating locales [26](#)overview [63](#)VM Manager [63](#)**P**packet inspection policies [143](#)configuring [143](#)passwords [20](#)guidelines [20](#)PAT [141, 142](#)configuring [141, 142](#)peer authentication policies [155](#)configuring [155](#)policies [37, 161, 166, 182, 183](#)configuring [183](#)System profile [37](#)verifying [161, 166](#)pools [233, 234](#)assigning [233](#)unassigning [234](#)port profiles [80](#)configuring for InterCloud links [80](#)preparing [80](#)for InterCloud links [80](#)privileges [23](#)profiles [37, 159, 161, 163, 165, 216, 217](#)applying [165, 216](#)configuring [159, 161, 163, 217](#)types of [159](#)provider account [85](#)creating [85](#)provider accounts [85](#)public cloud [77](#)resources [77](#)**R**Recent Jobs table [110](#)registration [229](#)verifying [229](#)Remote Access Method dialog box [185](#)remote authentication [14](#)providers [14](#)

resource management [219](#)
 Resource Manager [220](#)
 restoring [242](#)
 backup configuration [242](#)
 System software [242](#)
 roles [23](#)
 routing policies [144](#)
 configuring [144](#)
 running [239](#)
 backups [239](#)

S

Search [10](#)
 security policies [181](#)
 security profiles [168](#)
 configuring [168](#)
 selecting [17](#)
 primary authentication service [17](#)
 service policies [123](#)
 configuring [123](#)
 service policies [123](#)
 setting [10](#)
 idle timeout [10](#)
 Status field [112](#)
 monitoring status [112](#)
 syslog policy [201](#)
 device profile [201](#)
 system [238](#)
 backing up [238](#)
 System Profile [60](#)
 configuring NTP [60](#)

T

Task tab [112](#)
 monitoring status [112](#)
 TCP intercept policies [145](#)
 configuring [145](#)
 templates [98, 100, 101, 106](#)
 creating [100, 101, 106](#)
 creating in clouds [98](#)
 tenant management [69](#)
 tenants [71](#)
 creating [71](#)
 time ranges in ACL policy rules [128](#)
 toolbar [8](#)
 troubleshooting [115](#)
 InterCloud issues [115](#)
 trusted points [35](#)

tunnel profile [84](#)
 configuring [84](#)
 tunnel profiles [82](#)
 policies included [82](#)

U

unassigning [171, 226, 234](#)
 policy [171](#)
 pools [234](#)
 VSGs [226](#)
 updating [108](#)
 InterCloud links [108](#)
 InterCloud Links in HA [108](#)
 user accounts [19](#)
 user interface [6](#)
 user locales [24](#)
 user privileges [23, 78](#)
 InterCloud management [78](#)
 user roles [21, 23](#)
 usernames [20](#)
 guidelines [20](#)

V

verifying [161, 166, 229](#)
 compute firewall policies [161](#)
 edge firewall policies [166](#)
 VM registration [229](#)
 virtual machines [220](#)
 Virtual Security Gateways [220](#)
 VM images [96](#)
 importing [96](#)
 VM Manager [63](#)
 adding [63](#)
 overview [63](#)
 VM Managers [67](#)
 deleting [67](#)
 VMs [103, 106, 229](#)
 instantiating on clouds [103](#)
 migrating to the cloud [106](#)
 verifying registration [229](#)
 VPN device policies [156](#)
 configuring [156](#)
 VPN policies [146](#)
 configuring [146](#)
 VSGs [220, 226](#)
 unassigning pools [226](#)
 VSM port profiles [80](#)
 configuring [80](#)

vZone [178](#)
 adding [178](#)

vZones [179](#)
 editing [179](#)
vZones, overview [178](#)

