Cisco Remote Integrated Service Engine for Citrix NetScaler Appliances and Cisco Nexus 7000 Series Switches Configuration Guide

First Published: 2016-12-23

Last Modified: 2019-10-31

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

CONTENTS

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Preface

This preface describes the audience, organization, and conventions of the Book Title. It also provides information on how to obtain related documentation.

This chapter includes the following topics:

Preface

This preface describes the audience, organization, and conventions of the Book Title. It also provides information on how to obtain related documentation.

This chapter includes the following topics:

Audience

This publication is for experienced network administrators who configure and maintain Cisco NX-OS on Cisco Nexus 7000 Series Platform switches.

Document Conventions

Note

- As part of our constant endeavor to remodel our documents to meet our customers' requirements, we have modified the manner in which we document configuration tasks. As a result of this, you may find a deviation in the style used to describe these tasks, with the newly included sections of the document following the new format.
- The Guidelines and Limitations section contains general guidelines and limitations that are applicable to all the features, and the feature-specific guidelines and limitations that are applicable only to the corresponding feature.

Command descriptions use the following conventions:

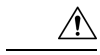
Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen 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.

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Documentation for Cisco Nexus 7000 Series Switches is available at:

- Configuration Guides

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-installation-and-configuration-guides-list.html

- Command Reference Guides

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-command-reference-list.html

- Release Notes

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html

- Install and Upgrade Guides

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-installation-guides-list.html

- Licensing Guide

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-licensing-information-listing.html

Documentation for Cisco Nexus 7000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders is available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-2000-series-fabric-extenders/products-installation-and-configuration-guides-list.html

Documentation Feedback

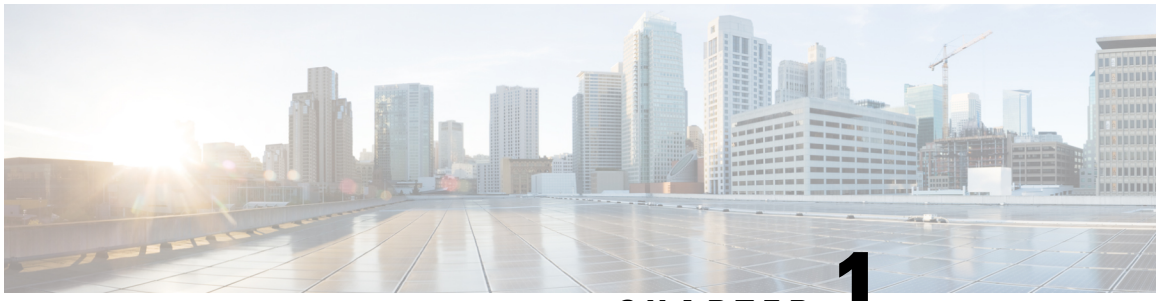
To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus7k-docfeedback@cisco.com. We appreciate your feedback.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

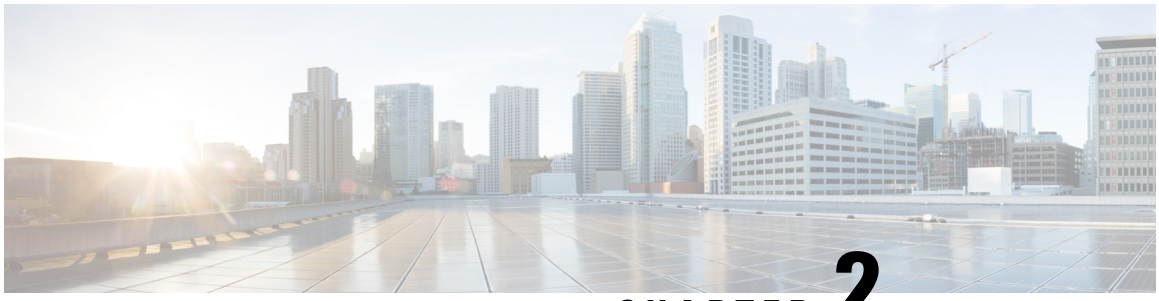
New and Changed Information

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to the configuration guide or of the new features in this release.

New and Changed Information for RISE Integration

This section provides release-specific information for each new and changed feature in the *Cisco Remote Integrated Service Engine for Citrix NetScaler Appliances and Cisco Nexus 7000 Series Switches Configuration Guide*.

Feature	Description	Release	Where Documented
Configuring RISE	Replaced the keyword ISCM with the keyword SC_ENGINE in all commands. For information on Configuring RISE on previous Cisco NX-OS Releases, refer Configuring RISE.	Cisco NX-OS Release 8.0(1)	“Configuring RISE”



CHAPTER 2

Cisco RISE Integration Overview

This chapter provides an overview of the Cisco Remote Integrated Service Engine (RISE) protocol with an external service appliance and the Cisco Nexus Series switches.

Cisco RISE is an architecture that logically integrates an external service appliance, such as a Citrix NetScaler Application Delivery Controller (ADC) appliance appears and operates as a service module within the Cisco Nexus switch.

The Cisco NX-OS software in which RISE is supported supports the Cisco Nexus Series switches.

Note Support for the RISE feature has been deprecated in Cisco NX-OS Release 8.4(1).

This chapter includes the following sections:

Licensing Requirements

For a complete explanation of Cisco NX-OS licensing recommendations and how to obtain and apply licenses, see the *Cisco NX-OS Licensing Guide*.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “New and Changed Information” section or the "Feature History" table.

Citrix Netscaler Application Delivery Controller (ADC)

The Citrix Netscaler Application Delivery Controller (ADC) is a network switch that performs application-specific traffic analysis to intelligently distribute, optimize, and secure layer 4 to layer 7 network traffic for web applications. For example, a Citrix Netscaler Application Delivery Controller (ADC) makes load balancing decisions on individual HTTP requests instead of on the basis of long-lived TCP connections, so that the failure or slowdown of a server is managed much more quickly and with less disruption to clients. The feature set can be broadly categorized as consisting of switching features, security and protection features, and server-farm optimization features.

The Cisco Nexus Series switches are used purely as a 1 and 10-Gigabit Ethernet switch, consolidating 10 Gigabit Ethernet connections into a smaller number of server connections trunked to the aggregation layers. These switches are designed for deployment in the core, aggregation, or access layers of a high performance, hierarchical data center network topology.

The Cisco Nexus Series switches run on the Cisco NX-OS software. This software fulfills the routing, switching, and storage networking requirements of data centers and provides an Extensible Markup Language (XML) interface and a command-line interface (CLI) that is similar to Cisco IOS software. As a crucial element in data center I/O consolidation, the switch enables I/O consolidation at the access layer and provides interoperability with the Cisco Nexus Series switches and other standards-based products.

Cisco Prime NAM Appliances

Cisco Prime NAM Appliances are purpose-built devices that uniquely combine application visibility and network performance analytics to help accelerate operational decisions. They help you understand who is using the network, know what applications are running on the network, assess how the applications are performing, and characterize how traffic over the network is being used. And, when there is a problem, Cisco Prime NAM Appliances can help you find it fast, reducing the time it takes to resolve the problem from days to just minutes.

RISE Functionality

Note All features in this section function with IPv4.

This section includes the following topics:

Discovery and Bootstrap

The discovery and bootstrap functionality enables the Cisco Nexus Series switches to communicate with the appliance by exchanging information to set up the Remote Integrated Service Engine (RISE) channel, which transmits control and data packets. Auto-discovery is supported only when you directly connect the service appliance with the Cisco Nexus switch. Once you configure the RISE control channel on the switch, the connected service appliance is set to RISE mode and all of its ports are set to operational mode by default.

In indirect mode (when the appliance is either Layer 2 or Layer 3 adjacent to the switch), you must manually configure the appliance and the Cisco Nexus switches to establish the control channel connectivity and for discovery and bootstrap to occur.

For more information about connection modes, see the “Preparing for RISE Integration” chapter. For configuration information, see the “Configuring RISE” chapter.

Health Monitoring

A RISE-enabled appliance can use its health monitoring feature to track and support server health by sending out health probes to verify server responses.

The Cisco Nexus switch and the appliance also periodically send heartbeat packets to each other. If a critical error occurs and health monitoring detects a service instance failure, or if the heartbeat is missed six times successively, the RISE channel becomes nonoperational. The health monitoring timer is 30 seconds (sec).

Nondisruptive Maintenance

The nondisruptive maintenance feature of the Cisco Remote Integration Services Engine (RISE) maintains the RISE configuration and runtime information on the Cisco Nexus Series switches during maintenance processes, such as an in-service software upgrade (ISSU) or an in-service software downgrade (ISSD), instead of being purged.

In-Service Software Upgrade

During an in-service software upgrade (ISSU), all RISE control channel communications are disabled. The configuration state across all components is restored after the ISSU is completed. Data traffic is not affected during an ISSU.

In-Service Software Downgrade

During an in-service software downgrade (ISSD), when you are downgrading from a Cisco Nexus Series switch software image with RISE support to an image without RISE support, you are notified that you should enter the **no feature rise** command before proceeding with the downgrade. This removes all of the RISE configuration and runtime configuration from the switch.

ISSU Start and Stop Notifications

Cisco Nexus Series switch provides start and stop notifications to the RISE service appliance during an in-service software upgrade (ISSU) or downgrade. This notification includes the hitful and hitless status of the line card to which the appliance is connected.

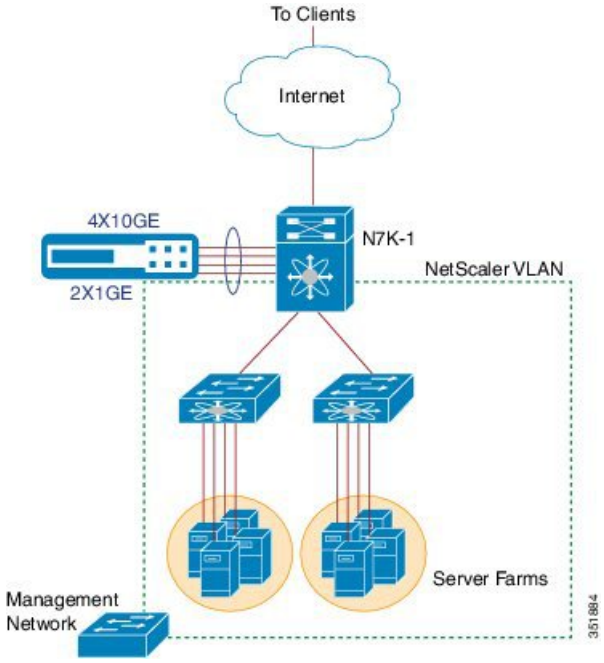
When the RISE service appliance receives a start notification, the appliance stops all control plane communication with the switch until after the switch sends a stop notification. The appliance uses the hitful and hitless status in the start and stop notifications to determine whether the data plane is operational.

One-Arm Mode Deployment

The recommended RISE deployment is a one-arm mode NetScaler deployment with all of the appliance ports bundled as a port channel connected to the Cisco Nexus Series switches.

In the one-arm mode (see figure below), the Citrix Netscaler Application Delivery Controller (ADC) appliance is configured with a VLAN that handles both client and server requests.

Figure 1: One-Arm Deployment



High Availability

This section describes the basic redundancy deployments that support the Cisco Remote Integrated Service Engine (RISE) runtime message handling between a service appliance and the Cisco Nexus 7000 Series switch. A high availability, redundant deployment uses a maximum of two appliances (peers) to support seamless switchover of flows in case one of the appliances becomes unresponsive.

When the redundancy involves multiple Cisco Nexus 7000 Series switches, the switches are considered to be both in active state (one as primary and the other as secondary). When two RISE-enabled appliances are connected to two Cisco Nexus 7000 Series switches (dedicated), the active appliance is connected to one Cisco Nexus 7000 Series chassis and the standby appliance is connected to the second chassis. This deployment ensures that even if one of the switches goes down, there is minimal disruption in the traffic.

NetScaler high availability can be used in conjunction with vPC. vPC is used when an Nexus switch fails, and NetScaler high availability is there for when a NetScaler fails. A NetScaler HA failover should only be triggered if one of the NetScalers actually stops functioning. If a Nexus switch fails and there is no vPC it causes the downstream NetScaler to "fail", but only because it lost connection to its HA peer.

Virtualization

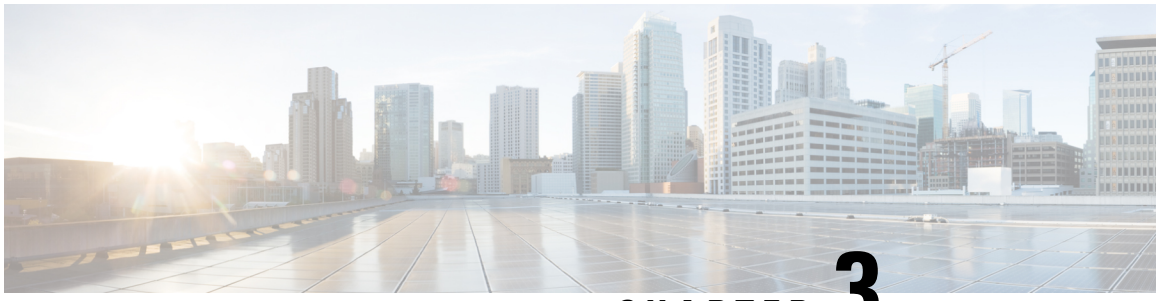
When the Cisco Nexus Series switch and the appliance are deployed in a RISE integration, the virtual device context (VDC) on the switch collapses multiple logical networks within a single physical infrastructure.

The appliance creates virtual contexts on the single physical appliance that is connected to the VDCs on the switch.

- The RISE-enabled appliance appears as a RISE slot within each of the VDCs for which it is a service context. The appliance does not appear in VDCs that are not associated with the RISE service context.
- The appliance has one RISE control channel per RISE instance.
- The service VLAN groups maintain the mapping of all of the data VLANs for each RISE instance.

The VDC ID is part of the discovery and bootstrap payload and the appliance is aware of the VDCs for each VLAN with which it is associated. The Cisco Nexus Series switch supports 32 RISE instances per VDC.

Multiple appliances can be connected to a single VDC. When two different appliances are connected to the same VDC, the RISE control VLAN need not be unique because the appliances can share the same RISE control VLAN. One or more appliances can also be connected to different VDCs on the same switch. In a multiple VDC deployment, all of the ports for an appliance are connected to its respective VDC and the VLANs for each appliance do not overlap.



CHAPTER 3

Preparing for RISE Integration

This chapter describes how to install and connect the appliances and the Cisco Nexus 7000 Series switches before deploying the Remote Integrated Service Engine (RISE) features.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “New and Changed Information” section or the "Feature History" table.

Information About Preparing for RISE Integration

This section includes the following topics:

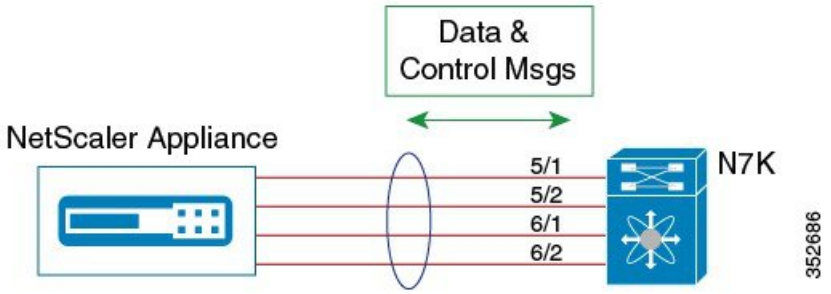
Connection Modes

You can connect the Citrix NetScaler Application Delivery Controller (ADC) appliance to the Cisco Nexus Series switch in one of the following ways:

Direct Connect Mode for a Standalone Switch

In a direct mode deployment, the service appliance is attached to a single Nexus Series switch. The switch can be standalone device or a VPC peer (recommended deployment). The following figure shows the topology for a direct mode deployment for a standalone Cisco Nexus switch.

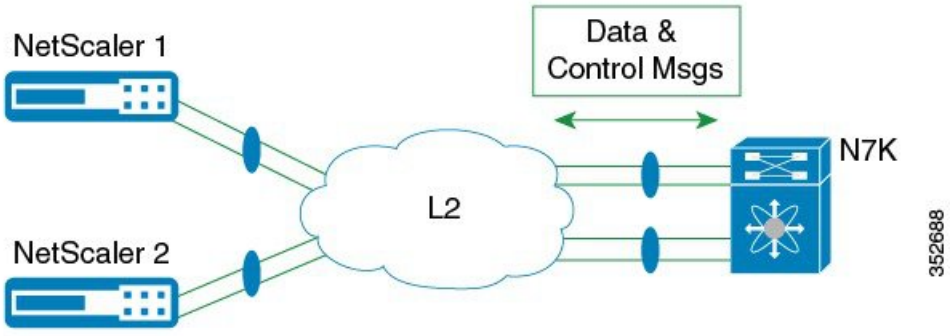
Figure 2: Direct Connect Mode for the Appliance and a Standalone Switch



Indirect Connect Mode

In an indirect mode deployment, a virtual service appliance is connected to a Cisco Nexus Series switch through a switched Layer 2 network. The topology in the following figure is for an indirect mode deployment.

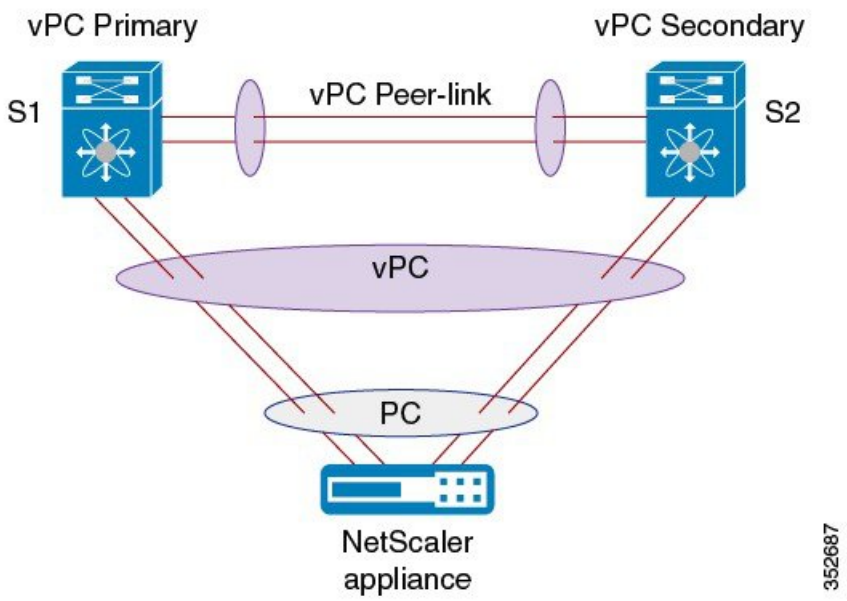
Figure 3: Indirect Connect Mode Through a Layer 2 Network



Virtual Port Channel (vPC) Connect Mode (Recommended Deployment Mode)

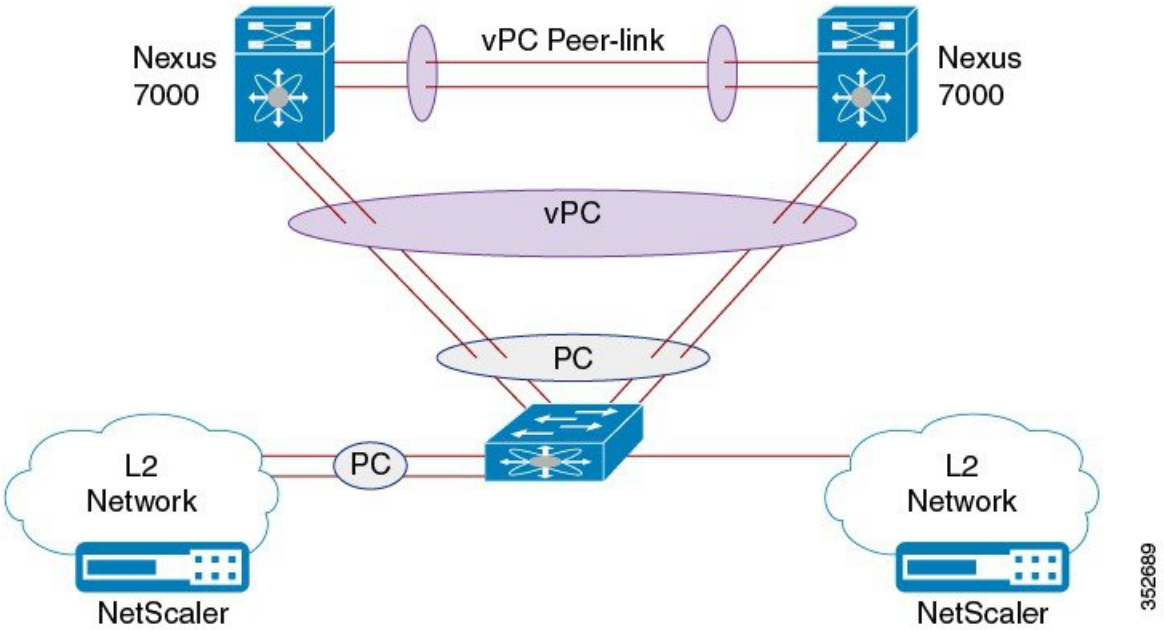
In a virtual port channel (vPC) direct mode deployment, the service appliance is attached to a single Nexus Series switch that is a vPC peer. The following figure shows the topology for a vPC direct mode deployment.

Figure 4: vPC Direct Connect Mode for Connecting to vPC Peer Switches



In a vPC indirect mode deployment, the service appliance is indirectly attached to a Cisco Nexus vPC peer through a Layer 2 network. The following figure shows the topology for a vPC indirect mode deployment.

Figure 5: vPC Indirect Connect Mode for Connecting to vPC Peer Switches



Guidelines and Limitations for Preparing for the RISE Integration

Cisco Remote Integration Services Engine (RISE) for Citrix NetScaler Application Delivery Controller (ADC) appliances and Cisco Nexus Series switches has the following guidelines and limitations:

-
- For the Citrix Application Delivery Controller (ADC) appliance in a RISE integration, the NetScaler 10.1.e or later software release is required.
- In RISE mode, the Citrix Application Delivery Controller (ADC) appliance always uses one link for both the data and control traffic (typically the port channel link).

Preparing for Cisco RISE with Citrix Application Delivery Controller (ADC)

This chapter describes how to prepare for integrating the Cisco Remote Integrated Services Engine (RISE) with Citrix Application Delivery Controller (ADC) appliance connected to the Cisco Nexus 7000 Series switches.

This section includes the following topics:

Installing the Cisco Nexus 7000 Series Switch

Perform the following steps to install and configure your Cisco Nexus switch before configuring the Remote Integrated Service Engine (RISE) feature for Cisco Nexus 7000 Series switches and service appliances:

Step 1 Install the Cisco Nexus 7000 Series switches and perform the basic setup such as applying the required licenses. For switch hardware installation instructions, see the *Cisco Nexus 7000 Series Hardware Installation and Reference Guide*.

Step 2 Install the appropriate Cisco NX-OS release software in your environment and create the basic configuration of the Cisco Nexus 7000 Series switches, which includes, but is not limited, to the following tasks:

a) Configure the physical Ethernet interfaces or a port channel for connecting to the service appliance and to allow control and data VLANs.
b) Configure the switch virtual interfaces (SVIs) for RISE control and data VLANs.
c) Configure the service VLAN groups.
d) Enable the RISE feature to allow for RISE integration.

Installing the Citrix Netscaler Application Delivery Controller (ADC) Appliance

Perform the following steps to install and configure your Citrix NetScaler Application Delivery Controller (ADC) appliances before configuring the Remote Integrated Service Engine (RISE) feature for Cisco Nexus Series switches and Citrix NetScaler Application Delivery Controller (ADC) appliances.

Note For installation and configuration information, see the Installing the Netscaler Hardware.

The Citrix Application Delivery Controller (ADC) appliance is typically mounted in a rack and all models ship with rack-rail hardware. Installation can include the following tasks:

Step 1 Unpack the appliance—The hardware accessories for your particular appliance, such as cables, adapters, and rail kit, can vary depending on the hardware platform that you ordered. Unpack the box that contains your new appliance on a sturdy table with plenty of space and inspect the contents.

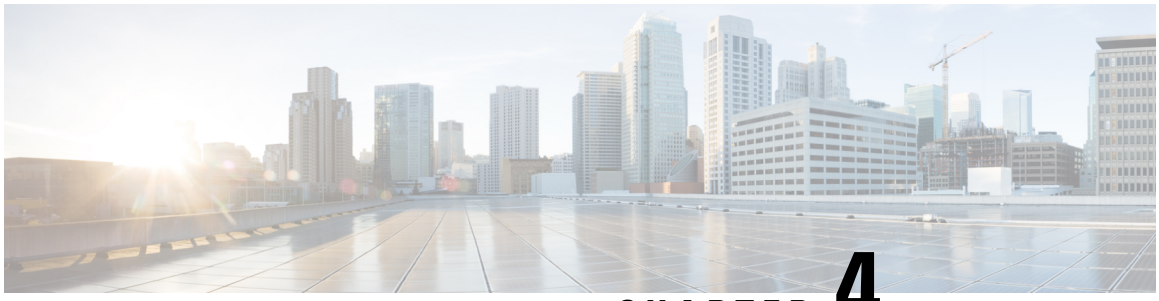
Step 2 Mount the appliance in the rack—Most appliances can be installed in standard server racks that conform to EIA-310-D specification. The appliances ship with a set of rails that you must install before you mount the appliance. The only tools that you need for installing an appliance are a Phillips screwdriver and a flathead screwdriver.

Step 3 Install your 1 G SFP transceivers—A Small Form-Factor Pluggable (SFP) is a compact transceiver that can operate at speeds of up to 1 gigabit per second and is available in both copper and fiber types. Inserting a 1 G SFP copper transceiver converts the 1 G SFP port to a 1000BASE-T port. Inserting a 1 G SFP fiber transceiver converts the 1 G SFP port to a 1000BASE-X port. Auto-negotiation is enabled by default on the 1 G SFP port into which you insert your 1 G SFP transceiver. As soon as a link between the port and the network is established, the speed and mode are matched on both ends of the cable.

Step 4 Install your XFP and 10 G SFP+ transceivers—A 10 Gigabit Small Form-Factor Pluggable (XFP or SFP+) is a compact optical transceiver that can operate at speeds of up to 10 gigabits per second. The MPX 15000 and MPX 17000 appliances use XFP transceivers and the MPX 8200/8400/8600, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 17500/19500/21500, and MPX 17550/19550/20550/21550 appliances use 10 G SFP+ transceivers.

What to do next

After the appliance is securely mounted on the rack, you are ready to connect the cables. Ethernet cables and the optional console cable are connected first. Connect the power cable last.



CHAPTER 4

Configuring RISE

This chapter describes how to configure the Remote Integrated Service Engine (RISE) feature on the Cisco Nexus Series switches and the Cisco NetScaler Application Delivery Controller (ADC) appliance. The Cisco NX-OS software supports the Cisco Nexus Series switches, which includes the Cisco Nexus Series switches. You can find detailed information about supported hardware in the *Cisco Nexus Series Hardware Installation and Reference Guide*.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Prerequisites for Configuring RISE

The RISE feature has the following prerequisites:

- Cable and power up the NetScaler Application Delivery Controller (ADC) appliance. See the “Preparing for RISE Integration” chapter for information on connecting the Cisco NetScaler Application Delivery Controller (ADC) appliance.
- For direct connect mode, create an interface or port channel on the Cisco Nexus Series switch and add all relevant management and data VLANs for the NetScaler Application Delivery Controller (ADC) appliance. See the *Cisco Nexus Series NX-OS Interfaces Configuration Guide*or information.
- For indirect connect mode, the RISE-enabled appliance must be configured with IP connectivity to the Cisco Nexus switch with Layer 2 adjacency.

Guidelines and Limitations

This section includes the following topics:

Guidelines and Limitations for Configuring RISE

RISE has the following guidelines and limitations:

- When configuring a route-map or prefix-list that contains RHI routes to be redistributed via OSPF, ensure that the prefix-list is created with the **le** option. For example, the command form **ip prefix-list list1 seq 10 permit 10.16.4.0/24 le 32** ensures that all RHI routes in the range 10.16.4.1/32 to 10.16.4.254/32 are redistributed via OSPF without the need to create a prefix-list for each RHI route in the 10.16.4.0/24 subnet. This action should be performed on the Nexus 7000 Series switch after creating an active RISE service.
- Auto-discovery, bootstrap, and auto port configuration are supported only in the direct connect and vPC direct connect modes. In indirect connect mode, manual configuration is required at each end on the Cisco Nexus Series switches and the Citrix NetScaler Application Delivery Controller (ADC) appliance in order to establish control channel connectivity and for the discovery and bootstrap process to occur.
- When the Citrix NetScaler Application Delivery Controller (ADC) appliance is indirectly connected to the Cisco Nexus Series switch, the service or management VLAN on the Citrix NetScaler Application Delivery Controller (ADC) appliance must establish the TCP RISE control channel with the Cisco Nexus Series switches.
- You can create up to 32 RISE services. However, the number of active RISE services that are supported is limited by the Cisco NX-OS software.
- Multiple instances of RISE services are supported per VDC.
- VLANs cannot be shared across virtual device contexts (VDCs) in a RISE deployment.
- After the RISE service is enabled on the Cisco Nexus Series switch, a service vlan-group must be created and associated to the RISE service to specify the data VLANs to be used on the Citrix NetScaler Application Delivery Controller (ADC) appliance.

- Control Plane Policing (CoPP) limits the number of packets that can be handled by a Cisco Nexus Series switch at one time. CoPP policies for RISE ports 8000 and 8001 are enabled by default as part of the (default) CoPP profiles.

Default Settings for RISE

The following table lists the default settings for RISE:

Table 1: Default RISE Parameters on the Cisco Nexus Series Switch

Parameter	Default
RISE mode	Disabled
CoPP	CoPP policies for RISE ports 8000 and 8001 are enabled by default.

Accessing the Switch and Appliance Interfaces

This section provides information on how to access the command-line interface (CLI) for the Cisco Nexus Series Series switch and the CLI and GUI for the Citrix NetScaler Application Delivery Controller (ADC) appliance. The switch and appliance interfaces enable you to perform many administrative tasks, including configuring the RISE feature.

Before logging into the interfaces, ensure that you have completed the installation process outlined in the "Preparing for RISE Integration" chapter.

This section includes the following topics:

Accessing the Cisco Nexus Series Switch

After the Cisco Nexus Series switch boots up, you can access the command-line interface (CLI). See the *Cisco Nexus Series NX-OS Fundamentals Configuration Guide* for more information on using the CLI.

To log onto the CLI through the console port, follow these steps:

Step 1 Use the switch's IP address to establish a Telnet or SSH connection from your PC to the switch.

Step 2 When the login prompt appears, enter your *login ID* and *password* to access the switch CLI.

Accessing the Citrix Netscaler Application Delivery Controller (ADC) Appliance

A Citrix NetScaler appliance has both a command line interface (CLI) and a graphical user interface (GUI). The GUI includes a configuration utility for configuring the appliance and a Dashboard for monitoring Netscaler performance. For initial access, all appliances ship with the default NetScaler IP address (NSIP) of 192.168.100.1 and default subnet mask of 255.255.0.0. You can assign a new NSIP and an associated subnet mask during initial configuration.

Note If you are using the direct connect mode to connect the appliance to the Cisco Nexus switch, you are not required to access the Citrix Netscaler Application Delivery Controller (ADC) appliance to configure RISE. For direct connect mode, the IP address and VLAN for management are pushed from the Cisco Nexus switch as part of RISE simplified provisioning.

The following table summarizes the available access methods.

Table 2: Methods for Accessing the Citrix Netscaler Appliance

Access Method	Port	Default IP Address Required?
CLI	Console	No
CLI and GUI	Ethernet	Yes

Using the Netscaler CLI

You can access the CLI either locally by connecting a workstation to the console port or remotely by connecting through Secure Shell (SSH) from any workstation on the same network.

Note To access Citrix eDocs, see the Citrix eDocs listing page for NetScaler 10.1 at http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler10-1-wrapper-con.html.

This section includes the following topics:

Logging onto the CLI Using the Console Port

The appliance has a console port for connecting to a computer workstation. To log on to the appliance, you need a serial crossover cable and a workstation with a terminal emulation program.

To log onto the CLI through the console port, follow these steps:

Step 1 Connect the console port to a serial port on the workstation, as described in the Citrix eDoc, *Connecting the Console Cable*.

Step 2 On the workstation, start HyperTerminal or any other terminal emulation program. If the logon prompt does not appear, you might need to press **Enter** one or more times to display the prompt.

Step 3 Log on using the administrator credentials. The command prompt (>) is displayed on the workstation monitor.

Logging into the Appliance CLI Using SSH

The SSH protocol is the recommended remote access method for accessing the command-line interface (CLI) of an appliance remotely from any workstation on the same network. You can use either SSH version 1 (SSH1) or SSH version 2 (SSH2). To verify that the SSH client is installed properly, use it to connect to any device on your network that accepts SSH connections.

To log onto the CLI using SSH, follow these steps:

Step 1 On your workstation, start the SSH client.

Step 2 For initial configuration, use the default NetScaler IP (NSIP) address, which is 192.168.100.1. For subsequent access, use the NSIP that was assigned during initial configuration. Select either SSH1 or SSH2 as the protocol. For information on initial configurations, see the Citrix eDoc. To access Citrix eDocs, see the Citrix eDocs listing page for NetScaler 10.1 at http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler10-1-wrapper-con.html.

Step 3 Log on by using the administrator credentials. For initial configuration, use **nsroot** as both the username and password. For example:

```
login as: nsroot
Using keyboard-interactive authentication.
Password:
Last login: Tue Jun 16 10:37:28 2009 from 10.102.29.9
 Done
>
```

Using the Netscaler GUI

The graphical user interface (GUI) includes a configuration utility and a statistical utility, called the Dashboard, either of which you access through a workstation connected to an Ethernet port on the appliance. If your computer does not have a supported Java plug-in installed, the utility prompts you to download and install the plug-in the first time you log on. If automatic installation fails, you can install the plug-in separately before you attempt to log on to the configuration utility or Dashboard.

Note Your workstation must have a supported web browser and version 1.6 or above of the Java applet plug-in installed to access the configuration utility and Dashboard.

Using the NetScaler Configuration Utility

After you log on to the configuration utility, you can configure the appliance through a graphical interface that includes context-sensitive help.

If your computer does not have a supported Java plug-in installed, the first time you log on to the appliance, the configuration utility prompts you to download and install the plug-in.

Note Before installing the Java 2 Runtime Environment, make sure that you have installed the full set of required operating system patches needed for the current Java release.

To log onto the configuration utility, follow these steps:

Step 1 Open your web browser and enter the NetScaler IP (NSIP) address as an HTTP address. If you have not set up the initial configuration, enter the default NSIP address (http://192.168.100.1). The Citrix Logon page appears.

Note If you have two Citrix NetScaler appliances in a high availability setup, make sure that you do not access the GUI by entering the IP address of the secondary Citrix NetScaler appliance. If you do so and use the GUI to configure the secondary appliance, your configuration changes are not applied to the primary appliance.

Step 2 In the User Name text box, enter nsroot.

Step 3 In the Password text box, type the *administrative password* that you assigned to the nsroot account during the initial configuration.

Step 4 For Deployment Type, choose **NetScaler ADC**.

Step 5 In the Start in list, click **Configuration**, and then click **Login**. The Configuration Utility page appears.

Note If your workstation does not already have a supported version of the Java runtime plug-in installed, the NetScaler prompts you to download the Java Plug-in. After the download is complete, the configuration utility page appears.

Using the Statistical Utility

The Dashboard is a browser-based application that displays charts and tables on which you can monitor NetScaler performance.

To log onto Dashboard, follow these steps:

Step 1 Open your web browser and enter the NetScaler appliance's NSIP address as an HTTP address (http://<NSIP>). The Citrix Logon page appears.

Step 2 In the User Name text box, enter **nsroot**.

Step 3 In the Password text box, enter the *administrative password* that you assigned to the nsroot account during the initial configuration.

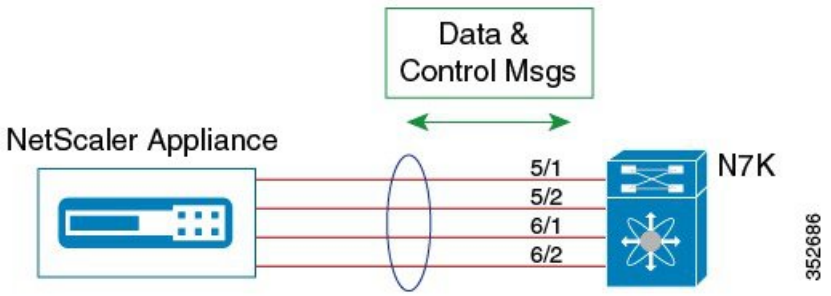
Step 4 In the Start in list, choose **Dashboard** and then choose **Login**.

For more information, see the Citrix eDoc, Accessing a Citrix NetScaler. To access Citrix eDocs, see the Citrix eDocs listing page for NetScaler 10.1 at http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler10-1-wrapper-con.html.

Configuring Cisco RISE in a Direct Mode Deployment

In a direct mode deployment, the service appliance, such as Citrix Netscaler Application Delivery Controller (ADC) appliance, is attached to a single Nexus Series switch. The switch can be standalone device or a VPC peer (recommended deployment). The following figure shows the topology for a direct mode deployment for a standalone Cisco Nexus switch.

Figure 6: Direct Connect Mode for the Appliance and a Standalone Switch



Note This task describes how to configure a standalone Cisco Nexus switch in a direct mode deployment. After configuring the Cisco Remote Integrated Services Engine (RISE) on the Cisco Nexus Series switch, the appliance that is directly connected to the standalone switch is automatically configured for RISE mode and all of its ports are in operation mode. No configuration is required on the appliance in a direct mode deployment.

To configure a switch that is a vPC peer in a direct mode deployment, see the "Configuring RISE in a vPC Mode Deployment" section.

Before you begin

- To enable auto-discovery of the appliance by the switches, use the **no shutdown** command to ensure that the physical ports are up by default.
- Interconnect the ports on the appliance with the standalone or port channel of the switch.
- Ensure that all of the switch ports to which the appliance is connected are dedicated to the appliance.
- Make sure that you are in the correct VDC on the Cisco Nexus switch. To switch VDCs, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature rise**	Enables the RISE feature on the Cisco Nexus Series switch.
Step 3	switch(config)# **service vlan-group** *group-number vlan-range*	Creates a VLAN group for the NetScaler appliance data VLANs on the Cisco Nexus Series switch. The range for the VLAN group is from 1 to 32, and the range for the configured VLANs is from 1 to 3967. You can enter the vlan-range using a comma (,), a dash (-), and the numbers.
Step 4	switch(config)# **service type rise name** *service-name* **mode direct**	Creates a RISE service instance, enters the RISE configuration mode on the Cisco Nexus Series switch, and specifies that the appliance is directly connected to the switch in order to establish RISE connectivity. You can enter up to 31 alphanumeric characters for the name of the RISE service instance.
Step 5	switch(config-rise)# **vlan** *vlan-id*	Assigns a VLAN to the Netscaler Application Delivery Controller (ADC) appliance that is directly connected to the Cisco Nexus Series switch. • The range is from 1 to 4094. • This VLAN controls message communication with the supervisor over the RISE port channel. The same VLAN can be used for the Netscaler Application

	Command or Action	Purpose
		Delivery Controller (ADC) appliance management VLAN. • The VLAN ID and SVI interface must be created before the RISE channel can be established. The IP address of the SVI interface is the supervisor IP address for Cisco Netscaler Application Delivery Controller (ADC) appliance to communicate with and send the control messages.
Step 6	switch(config-rise)# **ip** *ip-address netmask*	Specifies the IP address of the Citrix Netscaler Application Delivery Controller (ADC) appliance that is directly connected to the Cisco Nexus Series switch. This IP address controls message communication with the supervisor over the RISE port channel. The same IP address can be used for the management IP address of NetScaler appliance.
Step 7	switch(config-rise)# **vlan group** *vlan-group*	Specifies the RISE VLAN group to be used by Citrix Netscaler Application Delivery Controller (ADC) appliance. The range is from 1 to 32. **Note** The trunk-allowed VLANs on the port channel must include all of the VLANs in the VLAN group as well as the VLAN for the RISE control message.
Step 8	Use one of the following: • switch(config-rise)# **ethernet** *slot/port* • switch(config-rise)# **port-channel** *channel-number*	Creates an interface for sending out RISE discovery packets. • The range for the slot argument is from 1 to 253. The range for the port argument is from 1 to 128. • The range for the channel-number argument is from 1 to 4096.
Step 9	switch(config-rise)# **no shutdown**	Launches the auto-discovery and bootstrap configuration process. The NetScaler ADC appliance port channel is created with the RISE IP address set at the Citrix Netscaler Application Delivery Controller (ADC) appliance. **Note** The Cisco Nexus Series switches associates the Netscaler Application Delivery Controller (ADC) appliance serial number with the virtual slot number for this Cisco Netscaler Application Delivery Controller (ADC) appliance.

	Command or Action	Purpose
		Note Discovery does not start if any required information (such as the port, RISE VLAN, RISE IP address, or switch virtual interface [SVI] of the RISE VLAN) is not provided. If the discovery times out, the virtual module is shown in the inactive state. The **show rise detail** command on the switch displays the reason for discovery failure.
Step 10	(Optional) switch(config-rise)# **show module service**	Displays the status of the RISE service module on the Cisco Nexus Series switch. If the RISE service module is operational, the status that is displayed is "active."

Step 11	(Optional) switch(config-rise)# **attach rise** {**slot** *slot-number* | **name** *name*}	Connects the Cisco Nexus Series switch to the RISE service module and generates a RISE session from the switch, which allows Telnet access.
		• The slot number range varies based on the valid slot numbers for a particular VDC. The Cisco Nexus Series switch supports 32 RISE instances per VDC. The slot number range is as follows:
		  • From 300 to 331 for VDC 1
		  • From 332 to 363 for VDC 2
		  • From 364 to 395 for VDC 3
		  • From 396 to 427 for VDC 4
		• You can enter up to 32 alphanumeric characters for the RISE service module name.
		• After you enter the password, you can access the Citrix Netscaler Application Delivery Controller (ADC) appliance to configure it.

Step 12	switch(config-rise)# **show rise**	Displays the RISE configuration status on the Cisco Nexus Series switch. If RISE is configured on the switch, the state that is displayed is "active."

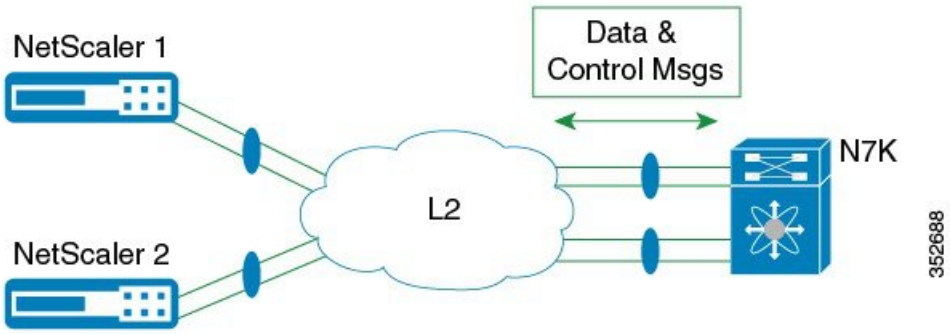
What to do next

Note After configuring RISE on the Cisco Nexus Series switch, the Citrix Netscaler Application Delivery Controller (ADC) appliance that is directly connected to the switch is automatically configured for RISE mode and all of its ports are in operation mode. No further configuration is required to deploy RISE on the Citrix Netscaler Application Delivery Controller (ADC) appliance.

Configuring RISE in an Indirect Mode Deployment

In an indirect mode deployment, a virtual service appliance, such as Citrix NetScaler Application Delivery Controller (ADC) appliance, is connected to a Cisco Nexus Series switch through a switched Layer 2 network. The topology in the following figure is for an indirect mode deployment.

Figure 7: Indirect Connect Mode Through a Layer 2 Network



This section includes the following topics:

Configuring RISE on the Cisco Nexus Switch

Before you begin

- Enable and configure the Cisco Nexus switches as vPC peers. See the *Cisco Nexus Series NX-OS Interfaces Configuration Guide* for information. The following parameters must be the same on both Cisco Nexus switches:
  - The vPC ID
  - The name of the RISE service instance
  - The vPC number of the port channel
  - The IP address of the Netscaler appliance
  - The number and range of the VLAN group for the Citrix NetScaler Application Delivery Controller (ADC) appliance.
- Make sure that you are in the correct VDC on the Cisco Nexus switch. To switch VDCs, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **feature rise**	Enables the RISE feature on the Cisco Nexus Series switch.
Step 3	switch(config)# **service vlan-group** *group-number vlan-range*	Creates a VLAN group for the Citrix NetScaler Application Delivery Controller (ADC) appliance data VLANs on the Cisco Nexus Series switch. The range for the VLAN group is from 1 to 32, and the range for the configured VLANs is from 1 to 3967. You can enter the vlan-range using a comma (,), a dash (-), and the numbers.
Step 4	switch(config)# **service type rise name** *service-name* **mode indirect**	Creates a RISE service instance, enters the RISE configuration mode on the Cisco Nexus Series switch, and specifies that the appliance is indirectly connected to the switch in order to establish RISE connectivity. You can enter up to 31 alphanumeric characters for the name of the RISE service instance.
Step 5	switch(config-rise)# **vlan** *vlan-id*	Assigns a VLAN to the Citrix NetScaler Application Delivery Controller (ADC) appliance that is directly connected to the Cisco Nexus Series switch. • The range is from 1 to 4094. • This VLAN controls message communication with the supervisor over the RISE port channel. The same VLAN can be used for the Citrix NetScaler Application Delivery Controller (ADC) appliance management VLAN. • The VLAN ID and SVI interface must be created before the RISE channel can be established. The IP address of the SVI interface is the supervisor IP address for Citrix NetScaler Application Delivery Controller (ADC) appliance to communicate with and send the control messages.
Step 6	switch(config-rise)# **ip** *ip-address netmask*	Specifies the IP address of the Citrix NetScaler Application Delivery Controller (ADC) appliance that is directly connected to the Cisco Nexus Series switch. This IP address controls message communication with the supervisor over the RISE port channel. The same IP address can be used for the management IP address of NetScaler appliance.
Step 7	switch(config-rise)# **vlan group** *vlan-group*	Specifies the RISE VLAN group to be used by Citrix NetScaler Application Delivery Controller (ADC) appliance. The range is from 1 to 32.

	Command or Action	Purpose
		Note The trunk-allowed VLANs on the port channel must include all of the VLANs in the VLAN group as well as the VLAN for the RISE control VLAN message.
Step 8	switch(config-rise)# **no shutdown**	Launches the auto-discovery and bootstrap configuration process. The Citrix NetScaler Application Delivery Controller (ADC) appliance port channel is created with the RISE IP address set at the Citrix NetScaler Application Delivery Controller (ADC) appliance. **Note** The Cisco Nexus Series switches associates the NetScaler appliance serial number with the virtual slot number for this Citrix NetScaler Application Delivery Controller (ADC) appliance. **Note** Discovery does not start if any required information (such as the port, RISE VLAN, RISE IP address, or switch virtual interface [SVI] of the RISE VLAN) is not provided. If the discovery times out, the virtual module is shown in the inactive state. The show rise command on the switch displays the reason for discovery failure.
Step 9	(Optional) switch(config-rise)# **show module service**	Displays the status of the RISE service module on the Cisco Nexus Series switch. If the RISE service module is operational, the status that is displayed is “active.”

Step 10	(Optional) switch(config-rise)# **attach rise** {**slot** *slot-number* | **name** *name*}	Connects the Cisco Nexus Series switch to the RISE service module and generates a RISE session from the switch, which allows Telnet access.
		• The slot number range varies based on the valid slot numbers for a particular VDC. The Cisco Nexus Series switch supports 32 RISE instances per VDC. The slot number range is as follows:
		  • From 300 to 331 for VDC 1
		  • From 332 to 363 for VDC 2
		  • From 364 to 395 for VDC 3
		  • From 396 to 427 for VDC 4
		• You can enter up to 32 alphanumeric characters for the RISE service module name.
		• After you enter the password, you can access the Citrix NetScaler Application Delivery Controller (ADC) appliance to configure it.

	Command or Action	Purpose
Step 11	switch(config-rise)# **show rise**	Displays the RISE configuration status on the Cisco Nexus Series switch. If RISE is configured on the switch, the state that is displayed is “active.”

Configuring NSIP on the Appliance

The NetScaler management IP address (NSIP) is the IP address for management and general system access to the Citrix NetScaler Application Delivery Controller (ADC) appliance and for high availability (HA) communication.

Configuring NSIP Using the CLI

You can configure the NSIP on your appliance by using either the configuration prompts or the command-line interface (CLI).

Note To prevent an attacker from impeding your ability to send packets to the appliance, choose a nonroutable IP address on your organization's LAN as your appliance IP address.

Before you begin

Ensure that a port channel is configured on the appliance and that the appliance's physical ports are mapped to this port channel.

Perform one of the following tasks:

Option	Description
config ns	Displays prompts for configuring the NSIP.
set ns config -ipaddress *address* **-netmask** *netmask* **add ns ip** *ip-address netmask* **-type** *type* **add route** *network netmask gateway* **save ns config** **reboot**	Configures the NSIP using the CLI.

Example:

The following example shows how to configure the NSIP using the CLI:

```
set ns config -ipaddress 10.102.29.60 -netmask 255.255.255.0
save ns
```

Configuring NSIP Using the Configuration Utility

Before you begin

- Create a port channel on the Citrix NetScaler Application Delivery Controller (ADC) appliance and map its physical ports to this port channel.

Step 1 Navigate to **System > Settings**.

Step 2 In the details pane, under Settings, click **Change NSIP Settings**.

Step 3 In the Configure NSIP Settings dialog box, set the parameters. For a description of a parameter, hover the mouse cursor over the corresponding field.

Step 4 Under Interfaces, choose the interfaces from the Available Interfaces list and click **Add** to move them to the Configured Interfaces list.

Step 5 Click **OK**. In the Warning dialog box, click **OK**. The configuration takes effect after the Citrix NetScaler Application Delivery Controller (ADC) appliance is restarted.

Configuring a NSVLAN on Citrix NetScaler Application Delivery Controller (ADC) Appliance

The NSVLAN is a VLAN to which the NetScaler management IP (NSIP) address's subnet is bound. The NSIP subnet is available only on interfaces that are associated with NSVLAN. By default, NSVLAN is VLAN1, but you can designate a different VLAN as NSVLAN. If you designate a different VLAN as an NSVLAN, you must reboot the Citrix NetScaler Application Delivery Controller (ADC) appliance for the change to take effect. After the reboot, NSIP subnet traffic is restricted to the new NSVLAN.

Perform only one of the following tasks:

Configuring NSVLAN Using the CLI

Enter the following commands prompt to configure NSVLAN using the CLI:

Before you begin

- Create a port channel on the Citrix NetScaler Application Delivery Controller (ADC) appliance and map its physical ports to this port channel.
- Configure the NS IP address (NSIP) on the appliance.

Step 1 **set ns config - nsvlan** *positive_integer* **- ifnum** *interface_name ...* [**-tagged** (**YES** | **NO**)]

Note You must reboot the appliance for the configuration to take effect.

```
set ns config -nsvlan 300 -ifnum 1/1 1/2 1/3 -tagged NO
save config
```

Step 2 (Optional) **show ns config**

```
set ns config -nsvlan 300 -ifnum 1/1 1/2 1/3 -tagged NO
save config
```

Step 3 (Optional) **unset ns config -nsvlan**

Restores the default configuration.

Configuring NSVLAN Using the Configuration Utility

Before you begin

- Create a port channel on the Citrix NetScaler Application Delivery Controller (ADC) appliance and map its physical ports to this port channel.
- Configure the NetScaler IP address (NSIP) on the appliance.

Step 1 Navigate to **System > Settings**.

Step 2 In the details pane, under Settings, click **Change NSVLAN Settings**.

Step 3 In the Configure NSVLAN Settings dialog box, set the parameters. For a description of a parameter, hover the mouse cursor over the corresponding field.

Step 4 Under Interfaces, choose the interfaces from the Available Interfaces list and click **Add** to move them to the Configured Interfaces list.

Step 5 Click **OK**. In the Warning dialog box, click **OK**. The configuration takes effect after the Citrix NetScaler Application Delivery Controller (ADC) appliance is restarted.

Configuring RISE in vPC Mode (Recommended Deployment Mode)

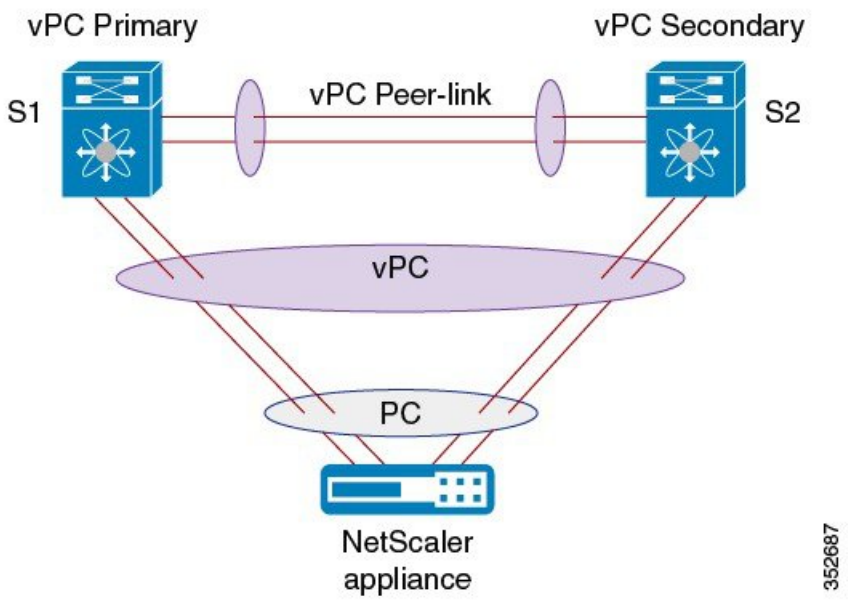
In a virtual port channel (vPC) deployment, two service appliances, such a Citrix NetScaler Application Delivery Controller (ADC) appliance, are each connected to separate Cisco Nexus Series switches that are in vPC mode through a peer link. This is the recommended topology for deploying the RISE feature on a Cisco Nexus switch and a Citrix NetScaler Application Delivery Controller (ADC) appliance.

This section includes the following topics:

Configuring RISE in a vPC Direct Mode Deployment

In an direct mode deployment, the service appliance, such as appliance, is attached to a single Nexus Series switch. The switch can be standalone device or a VPC peer (recommended deployment). The following figure shows the topologies for a vPC direct mode deployment.

Figure 8: vPC Direct Connect Mode for Connecting to vPC Peer Switches



Note This task describes how to configure a vPC peer switch in a direct mode deployment. After configuring RISE on the Cisco Nexus Series switch, the Citrix NetScaler Application Delivery Controller (ADC) appliance that is directly connected to the switch is automatically configured for RISE mode and all of its ports are in operation mode. No configuration is required on the Citrix NetScaler appliance in a direct mode deployment.

Repeat these steps to configure each vPC peer switch to which an appliance is connected.

Before you begin

- Enable and configure the Cisco Nexus switches as vPC peers. See the *Cisco Nexus Series NX-OS Interfaces Configuration Guide* for information. The following parameters must be the same on both Cisco Nexus switches:
  - The vPC ID
  - The name of the RISE service instance
  - The vPC number of the port channel
  - The IP address of the appliance
  - The number and range of the VLAN group for the ADC appliance
- Make sure that you are in the correct VDC on the Cisco Nexus switch. To switch VDCs, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature rise**	Enables the RISE feature on the Cisco Nexus Series switch.
Step 3	switch(config)# **service vlan-group** *group-number vlan-range*	Creates a VLAN group for the NetScaler appliance data VLANs on the Cisco Nexus Series switch. The range for the VLAN group is from 1 to 32, and the range for the configured VLANs is from 1 to 3967. You can enter the vlan-range using a comma (,), a dash (-), and the numbers.
Step 4	switch(config)# **service type rise name** *service-name* **mode vpc**	Creates a RISE service instance, enters the RISE configuration mode on the Cisco Nexus Series switch, and specifies that the appliance is directly connected to the switch in order to establish RISE connectivity. You can enter up to 31 alphanumeric characters for the name of the RISE service instance.
Step 5	switch(config-rise)# **vlan** *vlan-id*	Assigns a VLAN to the NetScaler appliance that is directly connected to the Cisco Nexus Series switch. • The range is from 1 to 4094. • This VLAN controls message communication with the supervisor over the RISE port channel. The same VLAN can be used for the Citrix Netscaler Application Delivery Controller (ADC) appliance management VLAN. • The VLAN ID and SVI interface must be created before the RISE channel can be established. The IP address of the SVI interface is the supervisor IP address for Citrix NetScaler Application Delivery Controller (ADC) appliance to communicate with and send the control messages.
Step 6	switch(config-rise)# **ip** *ip-address netmask*	Specifies the IP address of the Citrix NetScaler Application Delivery Controller (ADC) appliance that is directly connected to the Cisco Nexus 7000 Series switch. This IP address controls message communication with the supervisor over the RISE port channel. The same IP address can be used for the management IP address of Citrix Netscaler Application Delivery Controller (ADC) appliance.
Step 7	switch(config-rise)# **vlan group** *vlan-group*	Specifies the RISE VLAN group to be used by Citrix NetScaler Application Delivery Controller (ADC) appliance.

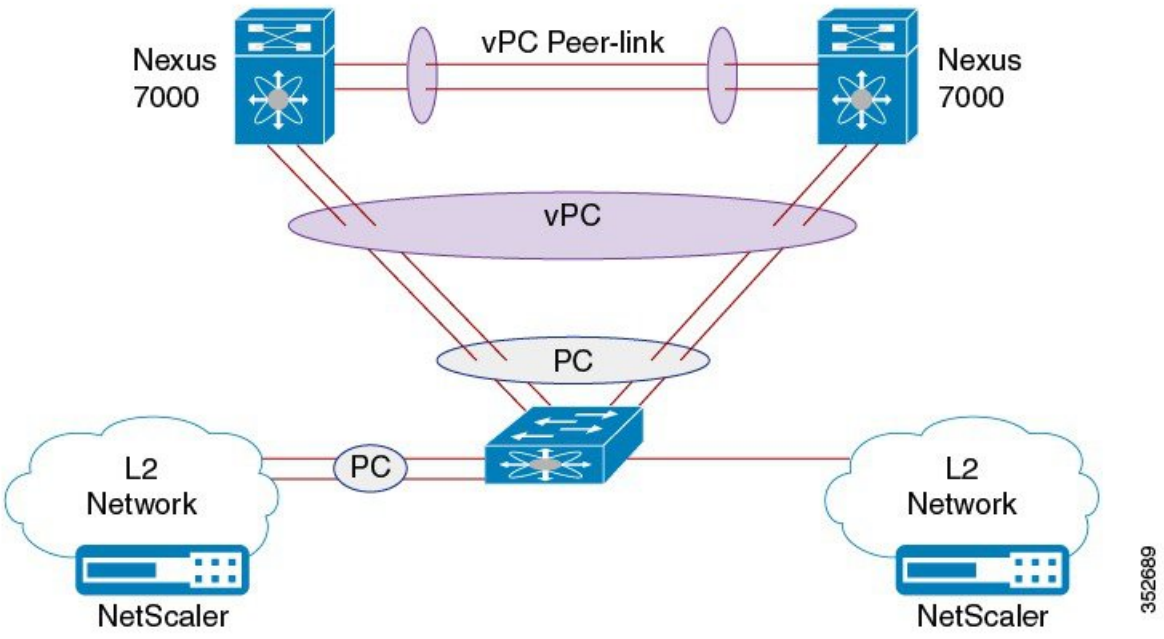
	Command or Action	Purpose
		The range is from 1 to 32. **Note** The trunk-allowed VLANs on the port channel must include all of the VLANs in the VLAN group as well as the VLAN for the RISE control message.
Step 8	Use one of the following: • switch(config-rise)# **ethernet** *slot/port* • switch(config-rise)# **port-channel** *channel-number*	Creates an interface for sending out RISE discovery packets. • The range for the slot argument is from 1 to 253. The range for the port argument is from 1 to 128. • The range for the channel-number argument is from 1 to 4096.
Step 9	switch(config-rise)# **no shutdown**	Launches the auto-discovery and bootstrap configuration process. The Citrix NetScaler Application Delivery Controller (ADC) appliance port channel is created with the RISE IP address set at the Citrix NetScaler Application Delivery Controller (ADC) appliance. **Note** The Cisco Nexus Series switches associates the NetScaler appliance serial number with the virtual slot number for this Citrix Netscaler Application Delivery Controller (ADC) appliance. **Note** Discovery does not start if any required information (such as the port, RISE VLAN, RISE IP address, or switch virtual interface [SVI] of the RISE VLAN) is not provided. If the discovery times out, the virtual module is shown in the inactive state. The show rise command on the switch displays the reason for discovery failure.
Step 10	(Optional) switch(config-rise)# **show module service**	Displays the status of the RISE service module on the Cisco Nexus Series switch. If the RISE service module is operational, the status that is displayed is “active.”
Step 11	(Optional) switch(config-rise)# **attach rise** {**slot** *slot-number* | **name** *name*}	Connects the Cisco Nexus Series switch to the RISE service module and generates a RISE session from the switch, which allows Telnet access. • The slot number range varies based on the valid slot numbers for a particular VDC. The Cisco Nexus Series switch supports 32 RISE instances per VDC. The slot number range is as follows: • From 300 to 331 for VDC 1 • From 332 to 363 for VDC 2

	Command or Action	Purpose
		• From 364 to 395 for VDC 3 • From 396 to 427 for VDC 4 • You can enter up to 32 alphanumeric characters for the RISE service module name. • After you enter the password, you can access the Citrix NetScaler Application Delivery Controller (ADC) appliance to configure it.
Step 12	switch(config-rise)# **show rise**	Displays the RISE configuration status on the Cisco Nexus Series switch. If RISE is configured on the switch, the state that is displayed is "active."

Configuring RISE in a vPC Indirect Mode Deployment

In a vPC indirect mode deployment, the service appliance, such as Citrix NetScaler Citrix Netscaler Application Delivery Controller (ADC) appliance, is indirectly attached to a Cisco Nexus vPC peer through a Layer 2 network. The following figure shows the topology for a vPC indirect mode deployment.

Figure 9: vPC Indirect Connect Mode for Connecting to vPC Perr Switches



This section includes the following topics:

Configuring RISE on the Cisco Nexus Switch

Before you begin

- Enable and configure the Cisco Nexus switches as vPC peers. See the *Cisco Nexus Series NX-OS Interfaces Configuration Guide* for information. The following parameters must be the same on both Cisco Nexus switches:
  - The vPC ID
  - The name of the RISE service instance
  - The vPC number of the port channel
  - The IP address of the Netscaler appliance
  - The number and range of the VLAN group for the Citrix NetScaler Application Delivery Controller (ADC) appliance.
- Make sure that you are in the correct VDC on the Cisco Nexus switch. To switch VDCs, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature rise**	Enables the RISE feature on the Cisco Nexus Series switch.
Step 3	switch(config)# **service vlan-group** *group-number vlan-range*	Creates a VLAN group for the Citrix NetScaler Application Delivery Controller (ADC) appliance data VLANs on the Cisco Nexus Series switch. The range for the VLAN group is from 1 to 32, and the range for the configured VLANs is from 1 to 3967. You can enter the vlan-range using a comma (,), a dash (-), and the numbers.
Step 4	switch(config)# **service type rise name** *service-name* **mode indirect**	Creates a RISE service instance, enters the RISE configuration mode on the Cisco Nexus Series switch, and specifies that the appliance is indirectly connected to the switch in order to establish RISE connectivity. You can enter up to 31 alphanumeric characters for the name of the RISE service instance.
Step 5	switch(config-rise)# **vlan** *vlan-id*	Assigns a VLAN to the Citrix NetScaler Application Delivery Controller (ADC) appliance that is directly connected to the Cisco Nexus Series switch. • The range is from 1 to 4094. • This VLAN controls message communication with the supervisor over the RISE port channel. The same VLAN can be used for the Citrix NetScaler

	Command or Action	Purpose
		Application Delivery Controller (ADC) appliance management VLAN. • The VLAN ID and SVI interface must be created before the RISE channel can be established. The IP address of the SVI interface is the supervisor IP address for Citrix NetScaler Application Delivery Controller (ADC) appliance to communicate with and send the control messages.
Step 6	switch(config-rise)# **ip** *ip-address netmask*	Specifies the IP address of the Citrix NetScaler Application Delivery Controller (ADC) appliance that is directly connected to the Cisco Nexus Series switch. This IP address controls message communication with the supervisor over the RISE port channel. The same IP address can be used for the management IP address of NetScaler appliance.
Step 7	switch(config-rise)# **vlan group** *vlan-group*	Specifies the RISE VLAN group to be used by Citrix NetScaler Application Delivery Controller (ADC) appliance. The range is from 1 to 32. **Note** The trunk-allowed VLANs on the port channel must include all of the VLANs in the VLAN group as well as the VLAN for the RISE control VLAN message.
Step 8	switch(config-rise)# **no shutdown**	Launches the auto-discovery and bootstrap configuration process. The Citrix NetScaler Application Delivery Controller (ADC) appliance port channel is created with the RISE IP address set at the Citrix NetScaler Application Delivery Controller (ADC) appliance. **Note** The Cisco Nexus Series switches associates the NetScaler appliance serial number with the virtual slot number for this Citrix NetScaler Application Delivery Controller (ADC) appliance. **Note** Discovery does not start if any required information (such as the port, RISE VLAN, RISE IP address, or switch virtual interface [SVI] of the RISE VLAN) is not provided. If the discovery times out, the virtual module is shown in the inactive state. The show rise command on the switch displays the reason for discovery failure.

	Command or Action	Purpose
Step 9	(Optional) switch(config-rise)# **show module service**	Displays the status of the RISE service module on the Cisco Nexus Series switch. If the RISE service module is operational, the status that is displayed is “active.”

Step 10	(Optional) switch(config-rise)# **attach rise** {**slot** *slot-number* | **name** *name*}	Connects the Cisco Nexus Series switch to the RISE service module and generates a RISE session from the switch, which allows Telnet access.
		• The slot number range varies based on the valid slot numbers for a particular VDC. The Cisco Nexus Series switch supports 32 RISE instances per VDC. The slot number range is as follows:
		  • From 300 to 331 for VDC 1
		  • From 332 to 363 for VDC 2
		  • From 364 to 395 for VDC 3
		  • From 396 to 427 for VDC 4
		• You can enter up to 32 alphanumeric characters for the RISE service module name.
		• After you enter the password, you can access the Citrix NetScaler Application Delivery Controller (ADC) appliance to configure it.

Step 11	switch(config-rise)# **show rise**	Displays the RISE configuration status on the Cisco Nexus Series switch. If RISE is configured on the switch, the state that is displayed is “active.”

Configuring NSIP on the Appliance

The NetScaler management IP address (NSIP) is the IP address for management and general system access to the Citrix NetScaler Application Delivery Controller (ADC) appliance and for high availability (HA) communication.

Configuring NSIP Using the CLI

You can configure the NSIP on your appliance by using either the configuration prompts or the command-line interface (CLI).

Note To prevent an attacker from impeding your ability to send packets to the appliance, choose a nonroutable IP address on your organization's LAN as your appliance IP address.

Before you begin

Ensure that a port channel is configured on the appliance and that the appliance's physical ports are mapped to this port channel.

Perform one of the following tasks:

Option	Description
config ns	Displays prompts for configuring the NSIP.
set ns config -ipaddress *address* **-netmask** *netmask* **add ns ip** *ip-address netmask* **-type** *type* **add route** *network netmask gateway* **save ns config** **reboot**	Configures the NSIP using the CLI.

Example:

The following example shows how to configure the NSIP using the CLI:

```
set ns config -ipaddress 10.102.29.60 -netmask 255.255.255.0
save ns
```

Configuring NSIP Using the Configuration Utility

Before you begin

- Create a port channel on the Citrix NetScaler Application Delivery Controller (ADC) appliance and map its physical ports to this port channel.

Step 1 Navigate to **System > Settings**.

Step 2 In the details pane, under Settings, click **Change NSIP Settings**.

Step 3 In the Configure NSIP Settings dialog box, set the parameters. For a description of a parameter, hover the mouse cursor over the corresponding field.

Step 4 Under Interfaces, choose the interfaces from the Available Interfaces list and click **Add** to move them to the Configured Interfaces list.

Step 5 Click **OK**. In the Warning dialog box, click **OK**. The configuration takes effect after the Citrix NetScaler Application Delivery Controller (ADC) appliance is restarted.

Configuring a NSVLAN on Citrix NetScaler Application Delivery Controller (ADC) Appliance

The NSVLAN is a VLAN to which the NetScaler management IP (NSIP) address's subnet is bound. The NSIP subnet is available only on interfaces that are associated with NSVLAN. By default, NSVLAN is VLAN1, but you can designate a different VLAN as NSVLAN. If you designate a different VLAN as an NSVLAN, you must reboot the Citrix NetScaler Application Delivery Controller (ADC) appliance for the change to take effect. After the reboot, NSIP subnet traffic is restricted to the new NSVLAN.

Perform only one of the following tasks:

Configuring NSVLAN Using the CLI

Enter the following commands prompt to configure NSVLAN using the CLI:

Before you begin

- Create a port channel on the Citrix NetScaler Application Delivery Controller (ADC) appliance and map its physical ports to this port channel.
- Configure the NS IP address (NSIP) on the appliance.

Step 1 **set ns config - nsvlan** *positive_integer* **- ifnum** *interface_name ...* [**-tagged** (**YES** | **NO**)]

Note You must reboot the appliance for the configuration to take effect.

```
set ns config -nsvlan 300 -ifnum 1/1 1/2 1/3 -tagged NO
save config
```

Step 2 (Optional) **show ns config**

```
set ns config -nsvlan 300 -ifnum 1/1 1/2 1/3 -tagged NO
save config
```

Step 3 (Optional) **unset ns config -nsvlan**

Restores the default configuration.

Configuring NSVLAN Using the Configuration Utility

Before you begin

- Create a port channel on the Citrix NetScaler Application Delivery Controller (ADC) appliance and map its physical ports to this port channel.
- Configure the NetScaler IP address (NSIP) on the appliance.

Step 1 Navigate to **System > Settings**.

Step 2 In the details pane, under Settings, click **Change NSVLAN Settings**.

Step 3 In the Configure NSVLAN Settings dialog box, set the parameters. For a description of a parameter, hover the mouse cursor over the corresponding field.

Step 4 Under Interfaces, choose the interfaces from the Available Interfaces list and click **Add** to move them to the Configured Interfaces list.

Step 5 Click **OK**. In the Warning dialog box, click **OK**. The configuration takes effect after the Citrix NetScaler Application Delivery Controller (ADC) appliance is restarted.

Route Health Injection

Route Health Injection (RHI)) allows NetScaler to advertise the VIPs to upstream and downstream routers. The NetScaler uses health probes together. When a VIP becomes unavailable, NetScaler withdraws the RHI information.

Once the Service Card (SC) Engine on the Cisco Nexus 7000 Series switch receives the RHI advertised messages from the Intelligent Service Card Client (ISCC) residing on the NetScaler appliance, the switch updates its routing tables to reflect the new route in the RHI message.

Use the **show routing** command on the switch to display the route automatically inserted for the VIP.

Service Card Engine

The Service Card (SC) Engine handles tasks related to the initialization and flow of Remote Health Injection (RHI) messages.

During the SC Engine initialization, the SC Engine registers with the Universal Routing information Base (URIB) as a URIB client so that it can access the routing database. After registration is successful, the SC Engine can add routes received from NetScaler to the routing database.

When the ISCC receives an RHI message from NetScaler, it sends a TLV and encrypted message to SC Engine containing the RHI payload and RISE headers. SC Engine transport decrypts and processes the RHI message. Each RHI message contains a common header with RHI opcode and a RHI request payload. The message header also contains the number of RHI entries contained in the RHI request payload.

The SC Engine also checks the status of the SVI for the VLAN sent by NetScaler. It obtains the interface number for the SVI and call the URIB APIs to add, delete, or delete all routes. The other parameters sent in the URIB API are present in the RHI request payload received by the SC Engine. All routes are added as static routes to the VRF that this SVI is associated with.

Intelligent Service Card Client

The Intelligent Service Card Client (ISCC) is the SDK component on NetScaler The Route Health Injection (RHI) message is a pass-through message for the ISCC. The ISCC copies the payload from NetScaler into the RHI message payload directed towards the Service Card (SC) Engine.

The SC Engine sends an acknowledgment when its processes the RHI message, then the ISCC transparently sends the acknowledgment to NetScaler. NetScaler is responsible for starting a timer and handling the failure if it does not receive an acknowledgment in time.

Universal Routing Information Base

The Universal Routing Information Base (URIB) hosts APIs to add, delete and modify routes on the Supervisor. The details of route modification are transparent to the SC Engine.

Verifying the RISE Configuration

To display the RISE configuration on the Cisco Nexus Series switch, perform one of the following tasks.

Note For detailed information about the fields in the output from these commands, see the "Cisco NX-OS RISE Commands" chapter.

Command	Purpose
show module service	Displays the status of the RISE service module on the Cisco Nexus Series switch.
show rise [**detail**]	Displays the RISE configuration status on the Cisco Nexus Series switch.
show rise vlan-group	Displays VLAN group information for the NetScaler appliance data VLANs on the Cisco Nexus Series switch.
show running-config services	Displays the RISE running configuration on the Cisco Nexus Series switch.
show tech-support services [**detail**]	Displays troubleshooting information for RISE on the Cisco Nexus Series switch.

The following example is partial sample output from the **show rise** command:

```
switch# show rise
Name           Slot Vdc Rise-Ip         State        Interface
                 Id  Id
-------------- ---- --- --------------- ------------ ---------
mpx205a        332   2   10.90.14.216    active       Po2051
```

The following example is partial sample output from the **show rise detail** command:

```
swicth# show rise detail

RISE module name: mpx205a
  State: active
  Admin state: Enabled
  Interface: Po2051
  RISE Channel connectivity via interface Po2051
  Mode: vpc
  Slot id: 332
  Service token: 0x2
  Serial number: MH8C02AM50
  SUP IP: 10.90.14.138
  RISE IP: 10.90.14.216
  VDC id: 2
  VLAN: 99
  VLAN group: 20
  VLAN list: 99-101
  Data Interface: N/A
```

To display the RISE configuration on the Citrix Netscaler Application Delivery Controller (ADC) appliance, perform one of the following:

Command	Purpose
show rise apbrsvc	Displays the RISE configuration status on the Citrix Netscaler Application Delivery Controller (ADC) appliance.

The following example is sample output from the **show rise profile** command:

```
mpx24> show rise profile

1)      Service Name   : mpx4
        Status         : Active
        Mode           : vPC-Direct
        Device Id      : FOC1824R00P
        Slot Number    : 300
        VDC Id         : 1
        vPC Id         : 510
        SUP IP         : 172.16.0.2
        VLAN           : 301
        VLAN Group     : 1
        ISSU           : None
        Interface      : LA/1 : 10/3 10/4
2)      Service Name   : mpx4
        Status         : Active
        Mode           : vPC-Direct
        Device Id      : FOC1751R0QV
        Slot Number    : 300
        VDC Id         : 1
        vPC Id         : 510
        SUP IP         : 172.16.0.3
        VLAN           : 301
        VLAN Group     : 1
        ISSU           : None
        Interface      : LA/1 : 10/7 10/8


 Done
```

Verifying the SC Engine Configuration

To display the SC Engine configuration on the Cisco Nexus Series switch, perform one of the following tasks.

Note For detailed information about the fields in the output from these commands, see the “Cisco NX-OS RISE Commands” chapter.

Command	Purpose
show system internal SC_Engine rise version	Displays the version of each service and version of SC_Engine on the Cisco Nexus Series switch.

Command	Purpose
show system internal SC_Engine pkt-stats	Displays all the statistics of the SC_Engine packet at RX/TX on a rise socket on the Cisco Nexus Series switch.
show system internal SC_Engine mem-stats	Displays VLAN group information for the NetScaler appliance data VLANs on the Cisco Nexus Series switch.
show system internal SC_Engine event-history debugs[**detail**]	Displays the RISE running configuration on the Cisco Nexus Series switch.
show system internal SC_Engine event-history-errors	Displays troubleshooting information for RISE on the Cisco Nexus Series switch.
show system internal SC_Engine event-history-all	Displays profile information for RISE on the Cisco Nexus Series switch.
show system internal SC_Engine event-history warnings	Displays profile information for RISE on the Cisco Nexus Series switch.

The following example is partial sample output from the **show system internal SC_Engine rise version** command:

```
switch#  show system internal SC_Engine rise version
Name       Version
-------  ---------
SC_Engine  2.1
MPX        2.1
Emu        2.1
VPX        2.1
```

The following example is partial sample output from the **show system internal SC_Engine pkt-stats** command:

```
switch# show system internal SC_Engine packet-stats
Service name: MPX
--------------------------------  --------  --------
Opcode                            Tx        Rx
--------------------------------  --------  --------
RISE_OPC_SVC_RHI                  0         0
RISE_OPC_SVC_RHI_BULK             0         0
RISE_OPC_SVC_APBR                 0         0
RISE_OPC_SVC_APBR_BULK            0         0
RISE_OPC_SVC_DISCOVERY            57869     57869
RISE_OPC_SVC_BOOTSTRAP_CONFIRM    57869     0
RISE_OPC_SVC_PORT_STATUS          0         0
RISE_OPC_SVC_ISSU                 0         0
RISE_OPC_SVC_VLAN_GROUP           0         0
RISE_OPC_SVC_SYS_INFO             0         0
RISE_OPC_SVC_DELETE               0         0
RISE_OPC_SVC_BULK                 0         0
RISE_OPC_CP_SLOT_DOWN             0         0
RISE_OPC_SUP_IP_CONFIG            0         0
RISE_OPC_RISE_IP_CONFIG           0         0
RISE_OPC_SVC_DIRECT_DISCOVERY     2         2
RISE_OPC_SVC_DIRECT_BOOTSTRAP_CO  2         2
RISE_OPC_SVC_DIRECT_BOOTSTRAP_4_  0         0
RISE_OPC_SVC_DIRECT_PORTS_START   2         2
RISE_OPC_SVC_DIRECT_PORTS_END     2         2
```

```
RISE_OPC_SVC_PURGE                0         0
RISE_OPC_SVC_PBR_ENABLE           0         0
RISE_OPC_SVC_PBR_DISABLE          0         0
--------------------------------  --------  --------
                          Total:  115746    57877

Service name: Emu
--------------------------------  --------  --------
Opcode                            Tx        Rx
--------------------------------  --------  --------
RISE_OPC_SVC_RHI                  0         0
RISE_OPC_SVC_RHI_BULK             0         0
RISE_OPC_SVC_APBR                 0         0
RISE_OPC_SVC_APBR_BULK            3         3
RISE_OPC_SVC_DISCOVERY            58895     58895
RISE_OPC_SVC_BOOTSTRAP_CONFIRM    58895     0
RISE_OPC_SVC_PORT_STATUS          0         0
RISE_OPC_SVC_ISSU                 0         0
RISE_OPC_SVC_VLAN_GROUP           0         0
RISE_OPC_SVC_SYS_INFO             0         0
RISE_OPC_SVC_DELETE               0         0
RISE_OPC_SVC_BULK                 0         0
RISE_OPC_CP_SLOT_DOWN             0         0
RISE_OPC_SUP_IP_CONFIG            0         0
RISE_OPC_RISE_IP_CONFIG           0         0
RISE_OPC_SVC_DIRECT_DISCOVERY     0         0
RISE_OPC_SVC_DIRECT_BOOTSTRAP_CO  0         0
RISE_OPC_SVC_DIRECT_BOOTSTRAP_4_  0         0
RISE_OPC_SVC_DIRECT_PORTS_START   0         0
RISE_OPC_SVC_DIRECT_PORTS_END     0         0
RISE_OPC_SVC_PURGE                0         0
RISE_OPC_SVC_PBR_ENABLE           0         0
RISE_OPC_SVC_PBR_DISABLE          0         0
--------------------------------  --------  --------
                          Total:  117793    58898

Service name: VPX
--------------------------------  --------  --------
Opcode                            Tx        Rx
--------------------------------  --------  --------
RISE_OPC_SVC_RHI                  0         0
RISE_OPC_SVC_RHI_BULK             0         0
RISE_OPC_SVC_APBR                 0         0
RISE_OPC_SVC_APBR_BULK            0         0
RISE_OPC_SVC_DISCOVERY            50588     50587
RISE_OPC_SVC_BOOTSTRAP_CONFIRM    50587     0
RISE_OPC_SVC_PORT_STATUS          0         0
RISE_OPC_SVC_ISSU                 0         0
RISE_OPC_SVC_VLAN_GROUP           0         0
RISE_OPC_SVC_SYS_INFO             0         0
RISE_OPC_SVC_DELETE               0         0
RISE_OPC_SVC_BULK                 0         0
RISE_OPC_CP_SLOT_DOWN             0         0
RISE_OPC_SUP_IP_CONFIG            0         0
RISE_OPC_RISE_IP_CONFIG           0         0
RISE_OPC_SVC_DIRECT_DISCOVERY     0         0
RISE_OPC_SVC_DIRECT_BOOTSTRAP_CO  0         0
RISE_OPC_SVC_DIRECT_BOOTSTRAP_4_  0         0
RISE_OPC_SVC_DIRECT_PORTS_START   0         0
RISE_OPC_SVC_DIRECT_PORTS_END     0         0
RISE_OPC_SVC_PURGE                0         0
RISE_OPC_SVC_PBR_ENABLE           0         0
RISE_OPC_SVC_PBR_DISABLE          0         0
--------------------------------  --------  --------
```

```
                        Total:  101175    50587       332   2   10.90.14.216    active
    Po2051
```

The following example is partial sample output from the **show system internal SC_Engine mem-stats** command:

```
switch#  show system internal SC_Engine mem-stats
Private Mem stats for UUID : Malloc track Library(103) Max types: 5
--------------------------------------------------------------------------------
Curr alloc: 1353 Curr alloc bytes: 96546(94k)


Private Mem stats for UUID : Non mtrack users(0) Max types: 130
--------------------------------------------------------------------------------
Curr alloc: 364 Curr alloc bytes: 39020(38k)


Private Mem stats for UUID : libsdwrap(115) Max types: 22
--------------------------------------------------------------------------------
Curr alloc: 34 Curr alloc bytes: 1149192(1122k)

...
```

The following example is partial sample output from the **show system internal SC_Engine event-history debugs**[**detail**] command:

```
switch# show system internal SC_Engine event-history debugs
1) Event:E_DEBUG, length:45, at 451405 usecs after Fri Nov 25 00:39:14 2011
    [104] SC_Engine_demux(1198):[FU_EVENT_CAT_MTS_MSG
]


2) Event:E_DEBUG, length:49, at 451400 usecs after Fri Nov 25 00:39:14 2011
    [104] SC_Engine_demux(1190):[Got a message event cat 1]


3) Event:E_DEBUG, length:49, at 451395 usecs after Fri Nov 25 00:39:14 2011
    [104] SC_Engine_demux(1189):[Got a message event cat 1]
```

The following example is partial sample output from the **show system internal SC_Engine event-history-errors** command:

```
switch# show system internal SC_Engine event-history-errors
1) Event:E_DEBUG, length:45, at 771310 usecs after Fri Nov 25 00:41:01 2011
    [104] SC_Engine_demux(1198):[FU_EVENT_CAT_MTS_MSG]
2) Event:E_DEBUG, length:49, at 771305 usecs after Fri Nov 25 00:41:01 2011
    [104] SC_Engine_demux(1190):[Got a message event cat 1]
3) Event:E_DEBUG, length:49, at 771301 usecs after Fri Nov 25 00:41:01 2011
    [104] SC_Engine_demux(1189):[Got a message event cat 1]
...
```

The following example is partial sample output from the **show system internal SC_Engine event-history-all** command:

```
switch# show system internal SC_Engine event-history-all
1) Event:E_DEBUG, length:45, at 341769 usecs after Tue Nov 29 21:25:32 2011
    [104] SC_Engine_demux(1198):[FU_EVENT_CAT_MTS_MSG]
2) Event:E_DEBUG, length:49, at 341764 usecs after Tue Nov 29 21:25:32 2011
    [104] SC_Engine_demux(1190):[Got a message event cat 1]
3) Event:E_DEBUG, length:49, at 341759 usecs after Tue Nov 29 21:25:32 2011
```

```
    [104] SC_Engine_demux(1189):[Got a message event cat 1]
```

The following example is partial sample output from the **show system internal SC_Engine event-history warnings** command:

```
switch# show system internal SC_Engine event-history warnings
1) Event:E_DEBUG, length:74, at 760859 usecs after Thu Nov 24 21:19:16 2011
    [103] SC_Engine_restore_pss_data(577):[(Error) 0x40480010 in pss2_move2location]
etc…
```

Monitoring Cisco RISE

Use the **show rise profile** command on the Citrix Netscaler Application Delivery Controller (ADC) appliance to display RISE statistics, as shown in the following example:

```
For vPC mode (direct):

mpx24> show rise profile
1)      Service Name   : mpx24
        Status         : Active
        Mode           : vPC-Direct
        Device Id      : FOC2865R92P
        Slot Number    : 300
        VDC Id         : 1
        vPC Id         : 510
        SUP IP         : 172.16.0.2
        VLAN           : 10
        VLAN Group     : 1
        ISSU           : None
        Interface      : LA/1 : 10/3 10/4

For Indirect mode (in vPC, only 1 out of 2 entries shown):

1) Service Name   : profile_301
 Status         : Active
 Mode           : Indirect
 Device Id      : N77-C7706:FXS1736Q96T
 Slot Number    : 332
 VDC Id         : 2
 vPC Id         : 0
 SUP IP         : 172.16.0.2
 VLAN           : 10
 VLAN Group     : 24
 ISSU           : None
 Interface      : N/A
```

Configuration Examples for RISE

Example: RISE Direct Mode Deployment

This example shows how to configure a RISE service on a standalone Cisco Nexus Series switch that is connected directly to a Citrix Netscaler Application Delivery Controller (ADC) appliance.

Note When the Citrix Netscaler Application Delivery Controller (ADC) appliance is directly connected to a standalone Cisco Nexus Series switch and the RISE control channel is configured on the Cisco Nexus Series switch, the Citrix Netscaler Application Delivery Controller (ADC) appliance is automatically configured for RISE mode and all of its ports are set to operation mode.

```
switch# configure terminal
switch(config)# port-channel 300
switch(config-if)# switchport trunk allowed vlan 20,30,40
switch(config-if)# no shut
switch(config)# ethernet 5/1-2
switch(config-if-range)# channel-group 100
switch(config)# ethernet 6/1-2
switch(config-if-range)# channel-group 100
switch(config)# service vlan-group 1 20,30,40
switch(config)# feature rise
switch(config)# service type rise name ns21 mode direct
switch(config-rise)# vlan 3
switch(config-rise)# ip 3.3.3.21 255.0.0.0
switch(config-rise)# vlan group 1
switch(config-rise)# port-channel 100
switch(config-rise)# no shutdown

switch(config-rise)# attach rise slot 300
Attaching to RISE 300 ...

Username:nsroot
Warning: Permanently added '3.3.3.21' (RSA) to the list of known hosts.
Password:
Last login: Fri Sep 27 14:58:44 2013 from 10.99.0.15
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
        The Regents of the University of California.  All rights reserved.

 Done
```

Example: RISE Indirect Mode Deployment

This example shows how to configure a RISE service on the Cisco Nexus Series switch that is connected to a Citrix Netscaler Application Delivery Controller (ADC) appliance through a Layer 2 network:

```
switch# configure terminal
switch(config)# port-channel 301
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport allowed vlan 10,20,30,40,50,60
switch(config)# ethernet 5/1-2
switch(config-if-range)# channel-group 100
switch(config-if-range)# no shutdown
switch(config)# ethernet 6/1-2
switch(config-if-range)# channel-group 100
switch(config-if-range)# no shutdown
switch(config)# service vlan-group 1 20,30,40
switch(config)# feature rise
switch(config)# service type rise name ns22 mode indirect
switch(config-rise)# vlan 10
switch(config-rise)# ip 3.3.3.22 255.0.0.0
switch(config-rise)# vlan group 22
switch(config-rise)# no shutdown
```

```
switch(config-rise)# show module service

switch(config-rise)# attach rise slot 301
rise_ent->rise_ip = 2010101
ipaddr 10.10.10.5
Attaching to RISE 301 ...
To exit type 'exit', to abort type '$.'
Telnet rlogin escape character is '$'.
Trying 10.10.10.5...
Connected to 10.10.10.5.
Escape character is '^]'.
```

The following sample output from **show** commands enables you to verify the configuration:

```
switch(config-rise)# show rise detail
RISE module name: ns22
  State: active
  Admin state: enabled
  Interface: N/A
  Mode: indirect
  Slot id: 301
  Service token: 0x1
  Serial number: HE2H81UJ47
  SUP IP: 3.101.0.10
  RISE IP: 10.10.10.5
  VDC id: 1
  VLAN: 10
  VLAN group: 22
  VLAN list: 122,221-224,231-234
```

Example: RISE vPC Direct Mode Deployment

You configure RISE on the Cisco Nexus switch vPC peer that are indirectly connected to the Citrix Netscaler Application Delivery Controller (ADC) appliance following the same steps that you use to configure an indirect mode deployment.

The following sample outputs show that the RISE device is active and operational and is connected using the vPC deployment mode:

```
switch# show rise
Name          Slot  Vdc  Rise-Ip         State        Interface
                Id  Id
------------- ---- --- --------------- ------------ ----------
mpx205a         332  2   10.90.14.216    active       Po2051

switch# show rise detail

RISE module name: mpx205a
  State: active
  Admin state: Enabled
  Interface: Po2051
  RISE Channel connectivity via interface Po2051
  Mode: vpc
  Slot id: 332 <== unique slot ID for the RISE device
  Service token: 0x2
  Serial number: MH8C02AM50
  SUP IP: 10.90.14.138
  RISE IP: 10.90.14.216
  VDC id: 2
  VLAN: 99
  VLAN group: 20
  VLAN list: 99-101
  Data Interface: N/A
```

Related Documents

Related Topic	Document Title
Commands on the Cisco Nexus Series switch	*Cisco Nexus Series NX-OS Fundamentals Configuration Guide*
CoPP	*Cisco Nexus Series NX-OS Security Configuration Guide*
Interfaces and vPCs	*Cisco Nexus Series NX-OS Interfaces Configuration Guide*
Policy-based routing	*Cisco Nexus Series NX-OS Unicast Routing Configuration Guide*
VDCs	*Cisco Nexus Series NX-OS Virtual Device Context Configuration Guide*
High availability and Cisco Nexus Series switches	*Cisco Nexus Series NX-OS High Availability and Redundancy Guide*

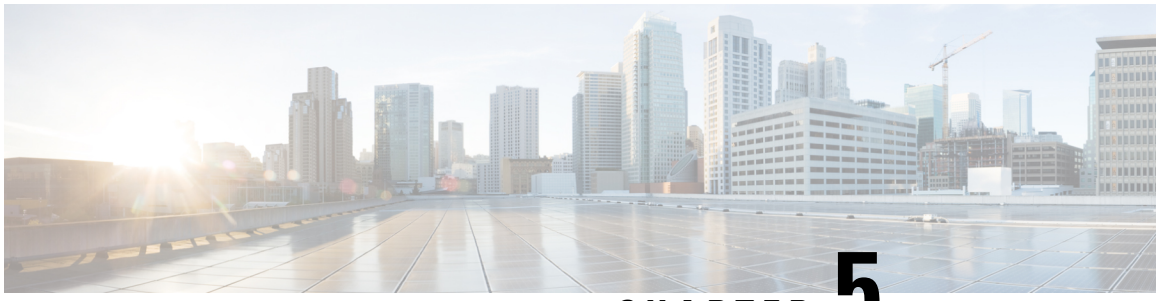
Feature History for RISE

The following table lists the feature history for this feature.

Table 3: Feature History for RISE

Feature Name	Release	Feature Information
RISE	Cisco NX-OS 8.0(1)	Replaced the keyword **ISCM** with the keyword **SC_ENGINE** in all commands.
Route Health Injection	Cisco NX-OS 7.2(0)D1(1)	Added the following enhancements: • Route health injection. • ISIM initialization and flow. • RHI with VPC. • Interface database. • ISCC. • URIB.
RISE vPC	Cisco NX-OS 6.2(8)	Added support for direct and indirect connect mode for a service appliance that is attached to a virtual port channel (vPC) peer through a Layer 2 network.

Feature Name	Release	Feature Information
RISE	Cisco NX-OS 6.2(2a)	This feature was introduced on the Cisco Nexus 7000 Series switches.
	Citrix Netscaler 10.1.e	This feature was introduced on the Citrix Netscaler Application Delivery Controller (ADC) appliance



CHAPTER 5

Configuring Auto Policy-Based Routing

This chapter describes how to configure the Auto Policy-Based Routing (PBR) feature on the Citrix NetScaler Application Delivery Controller (ADC) appliance to ensure that return traffic from the real server (RS) reaches the RISE appliance.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About Auto Policy-Based Routing

This section includes the following topics:

Auto Policy-Based Routing

Policy-Based Routing (PBR) allows the creation of policies or rules that can selectively alter the path that packets take within the network. PBR can be used to mark packets so that certain types of traffic are prioritized over the rest, sent to a different destination, or exit through a different physical interface on the router. Classification of interesting traffic is performed using access control lists (ACLs).

PBR rules ensure that return traffic from the real server (RS) reaches the Remote Integrated Service Engine (RISE) appliance. The control channel on the Cisco Nexus Series switch is used to automate the creation of PBR rules.

After the RISE appliance applies the required configuration, the appliance sends auto PBR (APBR) messages to the Cisco Nexus switch including a list of servers (IP addresses, ports, and protocol) and the next-hop IP address of the appliance.

The Cisco Nexus switch creates the PBR rules for the associated switch virtual interfaces (SVIs). For the local servers, the switch creates the ACLs and route maps.

Use Source IP Option

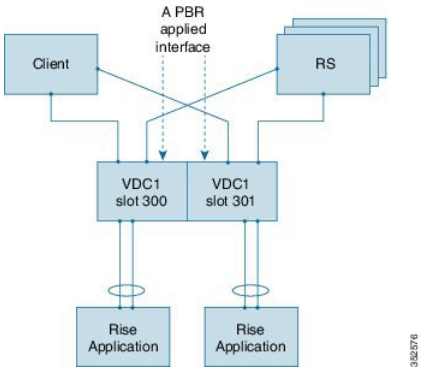
Auto policy-based routing (APBR) rules are configured on the Cisco Nexus switch by the Citrix NetScaler appliance only if the Use Source IP (USIP) option is enabled in the services or service groups on the Citrix NetScaler appliance. The rules are withdrawn when the USIP option is disabled. The USIP option can be configured locally or globally.

Appliance High Availability

High availability is supported for RISE appliances that share an APBR applied interface. Connect your appliances and Cisco Nexus switches using one of the following topologies to enable high availability:

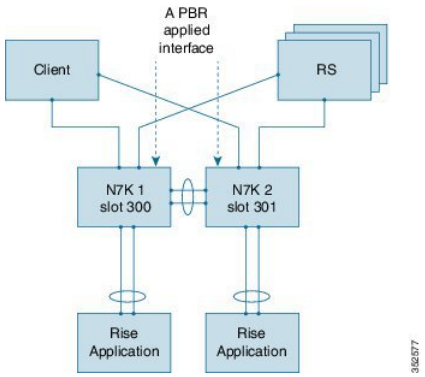
- Two appliances that are each connected to a different virtual device context (VDC) in the same Cisco Nexus Series switch.

Figure 10: Two Appliances, Two VDCs, One Switch



- Each appliance is connected to a different Cisco Nexus switch and each switch is in virtual port channel (vPC) mode through a peer link.

Figure 11: Two Appliances, Two vPC Peer Switches



- Two appliances are each connected to a different VDC in the same Cisco Nexus Series switch.

In each of the preceding topologies, one appliance is active and the other is in standby. Each connection acts as a separate service and is unaware of the other service. Each appliance sends APBR rules to the service in each VDC or in each switch, depending upon the topology. Each service sends the appropriate response to the appliance to which it is connected.

When a failover occurs, the standby appliance becomes the new active appliance. The old active appliance sends a PURGE message to the service. After the APBR purge is complete and the old active appliance receives a response, the appliance sends fresh APBR rules. Sending fresh rules ensures that the stale configuration does not remain on the old active appliance

Guidelines and Limitations for Auto Policy-Based Routing

Auto policy-based routing (APBR) has the following guidelines and limitations:

- The globally configured Use Source IP (USIP) takes precedence only when the user does not specify a local choice for the USIP option.
- If the USIP option is set on a service or service group by way of inheritance at the time you create either the service or group, the option is sticky on that service or group.
- If you modify a global property, such as USIP, after you create a service or service group, the global modification does not apply to either the service or group. However, you can modify a service or group locally by using the **set** commands.
- One RS cannot be connected through multiple VLAN interfaces. However, one or more RSs can be connected through the same interface on the Cisco Nexus device to which the APBR policy is applied.
- Multiple next-hop IP addresses for the same RS are not supported in RISE
- RISE does not support multiple services with the same RS IP address and port protocol. The only exception is as follows: Two identical services (with different service names) can be on the active and standby RISE-enabled appliance, pointing to the same APBR configuration.
- The virtual routing and forwarding (VRF) instance of the route to the RS must be the same as for the client VLAN switch virtual interface (SVI) to which the virtual IP (VIP) address is associated. The VRF does not need to be the default VRF.

- We do not recommend that you make any route changes on the egress interface to the RS. If you do make changes, see the troubleshooting information at http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler-wrapper-con.html.
- Equal Cost Multipath (ECMP) is not supported.

Default Settings for Auto Policy-Based Routing

The following table lists the default settings for the Use Source IP (USIP) option on the Citrix NetScaler Application Delivery Controller (ADC) appliance:

Table 4: Default APBR Parameters on the Citrix NetScaler Application Delivery Controller (ADC) Appliance

Parameter	Default
USIP	Disabled

Configuring Auto Policy-Based Routing

This section includes the following topics:

Enabling the RISE Feature and NS Modes

To manually enable the RISE feature and any RISE_APBR NS modes for publishing APBR rules, type the following commands at the command prompt:

Step 1 (Optional) > **enable feature RISE**

This step is only required if you did not enable RISE when you configured Cisco RISE with Citrix Netscaler. See the "Configuring Rise" chapter.

Enables the RISE feature on the appliance.

Step 2 > **enable ns mode RISE_APBR**

Enables the modes of type RISE_APBR on the Citrix Netscaler.

Enabling APBR on the Cisco Nexus Switch

You must enable the policy-based routing feature on the Cisco Nexus Series switch to support auto policy-based routing (APBR). The Citrix Netscaler Application Delivery Controller (ADC) appliance automatically adds the appropriate rules to the Cisco Nexus switch for APBR.

Before you begin

Make sure that you are in the correct VDC on the Cisco Nexus switch. To switch VDCs, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	switch# config term	Enters global configuration mode
Step 2	switch(config)# feature pbr	Enables policy-based routing (PBR) on the Cisco Nexus Series switch.
Step 3	switch(config)# exit	Exits the global configuration mode.

Configuring APBR on the Citrix NetScaler Application Delivery Controller (ADC) Appliance

This section includes the following topics:

Configuring NSIP on the Appliance

The NetScaler management IP address (NSIP) is the IP address for management and general system access to the Citrix NetScaler Application Delivery Controller (ADC) appliance and for high availability (HA) communication.

Configuring NSIP Using the CLI

You can configure the NSIP on your appliance by using either the configuration prompts or the command-line interface (CLI).

Note To prevent an attacker from impeding your ability to send packets to the appliance, choose a nonroutable IP address on your organization's LAN as your appliance IP address.

Before you begin

Ensure that a port channel is configured on the appliance and that the appliance's physical ports are mapped to this port channel.

Perform one of the following tasks:

Option	Description
config ns	Displays prompts for configuring the NSIP.
set ns config -ipaddress *address* **-netmask** *netmask* **add ns ip** *ip-address netmask* **-type** *type* **add route** *network netmask gateway*	Configures the NSIP using the CLI.

Option	Description
save ns config **reboot**	

Example:

The following example shows how to configure the NSIP using the CLI:

```
set ns config -ipaddress 10.102.29.60 -netmask 255.255.255.0
save ns
```

Configuring NSIP Using the Configuration Utility

Before you begin

- Create a port channel on the Citrix NetScaler Application Delivery Controller (ADC) appliance and map its physical ports to this port channel.

Step 1 Navigate to **System > Settings**.

Step 2 In the details pane, under Settings, click **Change NSIP Settings**.

Step 3 In the Configure NSIP Settings dialog box, set the parameters. For a description of a parameter, hover the mouse cursor over the corresponding field.

Step 4 Under Interfaces, choose the interfaces from the Available Interfaces list and click **Add** to move them to the Configured Interfaces list.

Step 5 Click **OK**. In the Warning dialog box, click **OK**. The configuration takes effect after the Citrix NetScaler Application Delivery Controller (ADC) appliance is restarted.

Configuring a NSVLAN on Citrix NetScaler Application Delivery Controller (ADC) Appliance

The NSVLAN is a VLAN to which the NetScaler management IP (NSIP) address's subnet is bound. The NSIP subnet is available only on interfaces that are associated with NSVLAN. By default, NSVLAN is VLAN1, but you can designate a different VLAN as NSVLAN. If you designate a different VLAN as an NSVLAN, you must reboot the Citrix NetScaler Application Delivery Controller (ADC) appliance for the change to take effect. After the reboot, NSIP subnet traffic is restricted to the new NSVLAN.

Perform only one of the following tasks:

Configuring NSVLAN Using the CLI

Enter the following commands prompt to configure NSVLAN using the CLI:

Before you begin

- Create a port channel on the Citrix NetScaler Application Delivery Controller (ADC) appliance and map its physical ports to this port channel.
- Configure the NS IP address (NSIP) on the appliance.

Step 1 **set ns config - nsvlan** *positive_integer* **- ifnum** *interface_name ...* [**-tagged** (**YES** | **NO**)]

Note You must reboot the appliance for the configuration to take effect.

```
set ns config -nsvlan 300 -ifnum 1/1 1/2 1/3 -tagged NO
save config
```

Step 2 (Optional) **show ns config**

```
set ns config -nsvlan 300 -ifnum 1/1 1/2 1/3 -tagged NO
save config
```

Step 3 (Optional) **unset ns config -nsvlan**

Restores the default configuration.

Configuring NSVLAN Using the Configuration Utility

Before you begin

- Create a port channel on the Citrix NetScaler Application Delivery Controller (ADC) appliance and map its physical ports to this port channel.
- Configure the NetScaler IP address (NSIP) on the appliance.

Step 1 Navigate to **System > Settings**.

Step 2 In the details pane, under Settings, click **Change NSVLAN Settings**.

Step 3 In the Configure NSVLAN Settings dialog box, set the parameters. For a description of a parameter, hover the mouse cursor over the corresponding field.

Step 4 Under Interfaces, choose the interfaces from the Available Interfaces list and click **Add** to move them to the Configured Interfaces list.

Step 5 Click **OK**. In the Warning dialog box, click **OK**. The configuration takes effect after the Citrix NetScaler Application Delivery Controller (ADC) appliance is restarted.

Enabling the USIP Option

APBR rules are configured on the Cisco Nexus Series switch by the Citrix Netscaler Application Delivery Controller (ADC) appliance when the Use Source IP (USIP) option is enabled. Perform only one of the following tasks to enable the USIP option on the Citrix Netscaler Application Delivery Controller (ADC) appliance:

Enabling the USIP Option for a Service

To create a service and enable and set the Use Source IP (USIP) option on that service, type the following commands at the command prompt:

Before you begin

Ensure that the NSIP and NSVLAN are configured on the Citrix Netscaler Application Delivery Controller (ADC) appliance.

Step 1 Use one of the following commands:

Option	Description
add service *service_name ipaddress protocol-type port_number* [**-usip** [**yes** | **no**]	Creates a service and enables the USIP option. The RISE appliance sends the server address, port, protocol, and the IP address of the next-hop interface and the VLAN to the Cisco Nexus switch. The *protocol-type* argument specifies a supported protocol including but not limited to the following keywords: **dns**, **http**, **ssl**, **tcp**, or **udp**. **Note** IPv6 addresses are not supported.
set service *service_name* [**-usip yes**]	Enables the USIP option on a previously configured service. **Note** This command is not required if you previously configured the specified service using the **add service** command with the **-usip** keyword

Example:

The following example shows how to create a service named svc12 and enable the USIP option on the service:

```
> add service svc12 192.168.12.23 http 80 -usip YES
```

Example:

The following example shows how to change a previously created service (svc12) to enable APBR:

```
> set service svc12 -usip YES
```

Step 2 (Optional) **unset service** *service-name*

Disables disable the USIP option on an already configured service and deletes the corresponding APBR route on the Cisco Nexus device

Example:

The following example shows how to disable the USIP option on the service and delete the corresponding APBR route on the Cisco Nexus device:

```
unset service svc12
```

Enabling the USIP Option for a Service Group

To create a service group and enable the Use Source IP (USIP) option on that group, enter the following commands at the command prompt:

Before you begin

Ensure that the NSIP and NSVLAN are configured on the Citrix Netscaler Application Delivery Controller (ADC) appliance.

Step 1 > **add serviceGroup** *service_name protocol-type port_number* [**-usip** [**yes** | **no**]

Creates a service group and enables the USIP option. The RISE appliance sends multiple APBR messages to the Cisco Nexus device.

The *protocol-type* argument specifies a supported protocol including but not limited to the following keywords: **dns**, **http**, **ssl**, **tcp**, or **udp**.

Note IPv6 addresses are not supported.

Example:

The following example shows how to create a service named svc12 and enable the USIP option on the service:

```
> add serviceGroup svc_grp_1 http 80 -usip YES
```

Step 2 > **bind serviceGroup** *service_group_name ipaddress port_number*

Associates an IP address and port to the service group being configured. Repeat this step for each member IP address and port.

Note IPv6 addresses are not supported.

Example:

The following example shows how to associate three IP addresses and ports to the group being configured.

```
> bind serviceGroup svc_grp_1 192.168.14.12 80
> bind serviceGroup svc_grp_1 192.168.14.13 80
> bind serviceGroup svc_grp_1 192.168.14.14 80
```

Step 3 Required: > **set serviceGroup** *service_name* [**-usip** [**yes**]

Sets the specified service and enables the USIP option.

Note The **-usip** keyword is not required on each service if you use the **add serviceGroup** command with the **-usip** keyword.

Example:

```
> set serviceGroup svc_grp_1
```

The following example shows how to disable the USIP option on all members of a service group and delete the corresponding APBR rules on the Cisco Nexus device:

```
unset serviceGroup svc_grp_1
```

Enabling the USIP Option Globally

To globally enable Use Source IP (USIP) on the Citrix Netscaler Application Delivery Controller (ADC) appliance and set the USIP option on all services and service groups, enter the following command at the command prompt

SUMMARY STEPS

1. > **enable ns mode usip**

DETAILED STEPS

> **enable ns mode usip**

Enables USIP on the Netscaler Application Delivery Controller (ADC) appliance. All subsequent added services are APBR services.

Example:

The following example shows how to enable USIP on the Citrix Netscaler Application Delivery Controller (ADC) appliance and then create a service for which the USIP option is set because the setting is inherited from the global configuration:

```
> enable ns mode USIP
 Done
> add service svc_gl 192.168.12.72 http 80
 Done
```

Verifying the Auto Policy-Based Routing Configuration

To display the auto policy-based routing (APBR) configuration on the Citrix NetScaler Application Delivery Controller (ADC) appliance, perform one of the following tasks on appliance:

Command	Purpose
show apbrSvc service	Displays information about the APBR service.
show apbrSvc -summary [**detail**]	Displays information about the APBR service.
show license	Displays information about the license that is loaded on the Citrix NetScaler Application Delivery Controller (ADC) appliance.
show rise apbrSvc	Displays the RISE running configuration on the Cisco Nexus Series switch.
show rise profile	Displays information about service profile.
show service *service-name*	Displays information about the specified service.

The following example is sample output from the **show apbrSvc** command on the Citrix Netscaler Application Delivery Controller (ADC) appliance. The same information is displayed by using the **show rise apbrsvc** command.

```
> show apbrSvc

1) Entity Name    : s1
   Entity Type    : Service
   Server IP      : 192.168.15.252
   Server Port    : 80
   Protocol       : HTTP
   Nexthop IP     : 192.168.4.100
   VLAN           : 4
2) Entity Name    : s2
```

```
   Entity Type    : Service
   Server IP      : 192.168.15.253
   Server Port    : 80
   Protocol       : HTTP
   Nexthop IP     : 192.168.4.100
   VLAN           : 4
3) Entity Name    : s3
   Entity Type    : Service
   Server IP      : 192.168.15.254
   Server Port    : 80
   Protocol       : HTTP
   Nexthop IP     : 192.168.4.100
   VLAN           : 4
4) Entity Name    : sg2
   Entity Type    : ServiceGroup
   Server IP      : 192.168.13.202
   Server Port    : 101
   Protocol       : HTTP
   Nexthop IP     : 192.168.4.100
   VLAN           : 4
5) Entity Name    : sg2
   Entity Type    : ServiceGroup
   Server IP      : 192.168.13.202
   Server Port    : 102
   Protocol       : HTTP
   Nexthop IP     : 192.168.4.100
   VLAN           : 4
 Done
```

The following example is sample output from the **show rise apbrsvc-summary** command:

```
> show rise apbrSvc -summary
-------------------------------------------------------------------------------
      EntityName IPAddress         Port  Protocol   NexthopIP         VLAN
-------------------------------------------------------------------------------
1     s1         192.168.15.252    80    HTTP       192.168.4.100     4
2     s2         192.168.15.253    80    HTTP       192.168.4.100     4
3     s3         192.168.15.254    80    HTTP       192.168.4.100     4
4     sg2        192.168.13.202    101   HTTP       192.168.4.100     4
5     sg2        192.168.13.202    102   HTTP       192.168.4.100     4
 Done
```

The following example is sample output from the **show service** command. This example shows that Use Source IP (USIP) is enabled on the service and that the APBR rules have been added to the service.

Note The following status messages for the APBR RISE code can be displayed in the output for this command:

- APBR rule successfully Added—The APBR rule was added on the Cisco Nexus device.
- APBR rule successfully Deleted—The APBR rule was deleted on the Cisco Nexus device.
- APBR rule fixed by Admin—The admin has fixed the discrepancy on the Cisco Nexus device.
- APBR rule not configured due to Timeout—The APBR rule was not configured even after retries.
- APBR rule not configured due to Lack of Memory—The APBR rule was not configured because there is not enough memory on the Netscaler appliance.
- APBR rule dispatch pending—The APBR rule is pending because it is waiting to be dispatched or it is waiting confirmation from the Cisco Nexus device.

```
> show service svc_grp_1

s1 (192.168.15.252:80) - HTTP
State: DOWN
Last state change was at Thu Apr  3 13:04:15 2014
Time since last state change: 0 days, 00:00:28.850
Server Name: 192.168.15.252
Server ID : None Monitor Threshold : 0
Max Conn: 0
Max Req: 0 Max Bandwidth: 0 kbits
Use Source IP: YES <===
Use Proxy Port: NO
Client Keepalive(CKA): YES
Access Down Service: NO
TCP Buffering(TCPB): YES
HTTP Compression(CMP): YES
Idle timeout: Client: 180 sec
Server: 360 sec
Client IP: DISABLED
Cacheable: NO
SC: OFF
SP: OFF
Down state flush: ENABLED
Appflow logging: ENABLED
TD: 0
RISE CODE:  APBR rule successfully Added <===
.
.
.
 Done
```

The following example is sample partial output from the **show rise profile** command:

```
> show rise profile

1) Service Name   : NS-rise
   Status         : Active
   Mode           : Indirect
   Device Id      : JAF1429CJLB
   Slot Number    : 300
   VDC Id         : 1
   vPC Id         : 0
   SUP IP         : 173.173.1.1
   VLAN           : 3
   VLAN Group     : 1
   ISSU           : None
   Interface      : N/A
```

To display the auto policy-based routing (APBR) configuration on the Cisco Nexus Series switch and verify that the APBR policy was added, perform one of the following tasks on the switch:

Command	Purpose
show access list dynamic	Displays information about the APBR service.
show rise [**detail**]	Displays information about the APBR service.
show route-map	Displays information about the license that is loaded on the Citrix Netscaler appliance.
show service rise auto-pbr ipv4 slot *slot*	Displays the RISE running configuration on the Cisco Nexus Series switch.

The following example displays dynamic access list matching the Real Server IP addresses:

```
switch# show access-lists dynamic

Example correct output:

IPV4 ACL _rise-system-acl-172.16.10.5-Vlan1010
        10 permit tcp 10.10.10.11/32 eq 80 any
        20 permit tcp 10.10.10.12/32 eq 80 any
IPV4 ACL _rise-system-acl-172.16.11.5-Vlan1011
        10 permit tcp 10.10.11.11/32 eq 50000 any
```

The following example is sample output from the **show rise** command:

```
switch# show rise

Name            Slot Vdc Rise-Ip         State        Interface
                  Id  Id
--------------- ---- --- --------------- ------------ ---------
MPX             300  1   10.175.1.11     active       Po10
Emu             301  1   100.0.1.4       active       N/A
VPX             302  1   100.0.1.6       active       N/A

APBR Configuration <===
rs ip           rs port protocol nhop ip         rs nhop  apbr state slot-id
--------------- ------- -------- --------------- -------- ---------- -------
100.0.1.1       33275   TCP      100.0.1.2       Vlan100  ADD FAIL   301
100.0.1.3       64301   TCP      100.0.1.4       Vlan100  ADD DONE   301
100.0.1.5       21743   TCP      100.0.1.6       Vlan100  ADD DONE   301
```

The following partial output from the **show rise detail** command includes all of the APBR entries that were automatically added to the Cisco Nexus Series switch:

```
switch# show rise detail

RISE module name: MPX
  State: active
  Admin state: enabled
  Interface: Po10
  Mode: direct
  Slot id: 300
  Service token: 0x6
  Serial number: AJSFH28FUF
  SUP IP: 10.175.1.99
  RISE IP: 10.175.1.11
  VDC id: 1
  VLAN: 175
  VLAN group: N/A
  VLAN list: N/A
  Data Interface: N/A

RISE module name: Emu
  State: active
  Admin state: enabled
  Interface: N/A
  Mode: indirect
  Slot id: 301
  Service token: 0x7
  Serial number: 123-SERIAL
  SUP IP: 100.0.1.1
  RISE IP: 100.0.1.4
  VDC id: 1
  VLAN: 100
  VLAN group: N/A
  VLAN list: N/A
```

```
  Data Interface: N/A

RISE module name: VPX
  State: active
  Admin state: enabled
  Interface: N/A
  Mode: indirect
  Slot id: 302
  Service token: 0x8
  Serial number: HE2H81UJ47
  SUP IP: 100.0.1.1
  RISE IP: 100.0.1.6
  VDC id: 1
  VLAN: 100
  VLAN group: N/A
  VLAN list: N/A
  Data Interface: N/A

APBR Configuration
rs ip           rs port protocol nhop ip         rs nhop  apbr state slot-id
--------------- ------- -------- --------------- -------- ---------- -------
100.0.1.1       33275   TCP      100.0.1.2       Vlan100  ADD FAIL   301
100.0.1.3       64301   TCP      100.0.1.4       Vlan100  ADD DONE   301
100.0.1.5       21743   TCP      100.0.1.6       Vlan100  ADD DONE   301
```

The following partial output from the **show service rise auto-pbr** command lists all APBR entries on the Cisco Nexus Series switch:

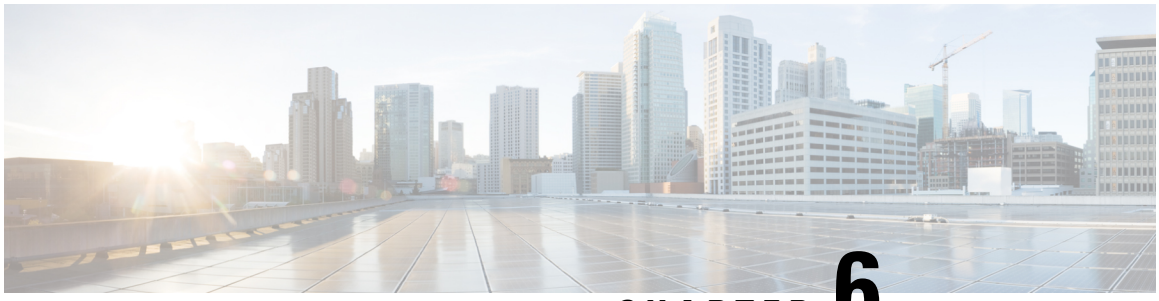
```
switch# show service rise ipv4 auto-pbr slot 301

APBR routes added by slot 301
rs ip            port    protocol  nhop ip          rs nexthop inf
---------------  ------  --------  ---------------  --------------
100.0.1.1        33275   TCP       100.0.1.2        Vlan100
100.0.1.3        64301   TCP       100.0.1.4        Vlan100
100.0.1.5        21743   TCP       100.0.1.6        Vlan100
```

Feature History for Auto Policy-Based Routing

The following table lists the feature history for this feature.

Table 5: Feature History for APBR

Feature Name	Release	Feature Information
Auto policy-based routing (APBR)	Cisco NX-OS 6.2(8)	Support for this feature was introduced on the Cisco Nexus 7000 Series switches.
Appliance high availability		
APBR on vPC		



CHAPTER 6

Troubleshooting RISE Integration

This chapter describes how to troubleshoot the Remote Integrated Service Engine (RISE) feature on the Cisco Nexus Series switches and the Cisco NetScaler Application Delivery Controller (ADC) appliance. The Cisco NX-OS software supports the Cisco Nexus Series switch. You can find detailed information about supported hardware in the *Cisco Nexus Series Hardware Installation and Reference Guide*.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “New and Changed Information” section or the "Feature History" table.

Troubleshooting the RISE Integration

This chapter includes the following topics:

Interpreting System Messages

For information on error and system messages for the Cisco Nexus 7000 Series switch, see the *Cisco MDS 9000 Family and Nexus 7000 Series NX-OS System Messages Reference*.

For information on system messages for the Citrix NetScaler Application Delivery Controller (ADC) appliance, see the Citrix eDocs, Log Message Reference.

Note To access Citrix eDocs, see the Citrix eDocs listing page for NetScaler 10.1 at http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler10-1-wrapper-con.html.

Troubleshooting the RISE Configuration on the Switch

Step 1 switch# **show rise detail**

```
switch# show rise detail

RISE module name: ns21
  State: inactive
inactive reason:     Control VLAN interface is not operational.

  Admin state: enabled
  Interface: N/A
  Mode: indirect
  Slot id: 300
  Service token: 0x0
  Serial number: HE2H81UJ47
  SUP IP: 3.101.0.10
  RISE IP: 3.3.3.21
  VDC id: 1
  VLAN: 3
  VLAN group: 21
  VLAN list: 121,222-224,231-234
```

Displays the detailed RISE configuration status on the Cisco Nexus Series switch. The output shows the state of the RISE service. If the service is inactive, the Inactive Reason field explains the reason for this state. The following reasons might appear in the Inactive Reason field in the output of the show rise detail command:

- Service table is full.
- Another service is already using this port.
- Error in bootstrap response.
- Timed out while waiting for bootstrap response
- Control VLAN interface is not operational.
- RISE interface is not operational.
- RISE interface does not have control VLAN as trunk member.
- Control VLAN interface does not have valid IP.
- RISE port channel has no member ports.
- RISE IP is already assigned to another service.

Step 2 switch# **show tech-support services**

Displays detailed troubleshooting information for RISE on the Cisco Nexus Series switch.

Troubleshooting the RISE Service on the Appliance

At the Citrix Netscaler Application Delivery Controller (ADC) CLI, enter the **show rise profile** command.

Displays RISE configuration status on the Citrix NetScaler Application Delivery Controller (ADC) appliance.

The output shows the state of the RISE service. The status field informs you whether the service is Inactive or Active. If the service is Inactive, it means that the RISE channel was not established or is no longer connected.

```
RISE-mpx> show rise profile

1)      ProfileName:  profile_331 IPAddress:  3.101.0.10
        Mode:  Direct             Status:  Active
        VdcId:  1                 SlotNumber:  331
        Vlan:  3                  VlanGroupId:  25
        Ifnum:  LA/1
 Done
```