NetScaler Solutions

http://docs.citrix.com/content/docs/en-us/netscaler/11-1/solutions.html
May 13, 2016

NetScaler Solutions

NetScaler solutions simplify the task of setting up frequently deployed configurations. Check this space from time to time for additional solutions.

This section includes the following solutions:

- Setting Up NetScaler for XenApp/XenDesktop
- RISE Integration: NetScaler ADC and Cisco Nexus 7000 Series Switch
- Global Server Load Balancing (GSLB) Powered Zone Preference

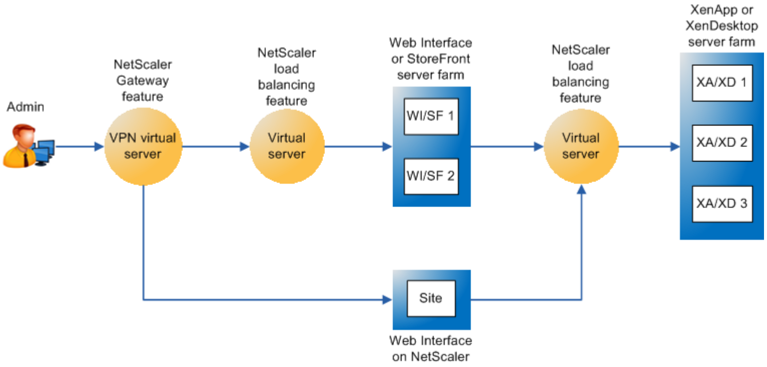
Setting Up NetScaler for XenApp/XenDesktop

A NetScaler appliance can provide load balanced, secure remote access to your XenApp/XenDesktop applications. You can use the NetScaler load balancing feature to distribute traffic across the XenApp/XenDesktop servers, and the NetScaler Gateway feature to provide secure remote access to the servers. NetScaler can also accelerate and optimize the traffic flow and offer visibility features that are useful for XenApp/XenDesktop deployments.

The configurations that are required to be performed on the NetScaler are consolidated in a wizard that simplifies the deployment. You can also apply the following preset configurations:

- Optimization settings such as TCP profiles, compression, caching, and SSL quantum settings.
- Security settings such as application firewall profiles and policies.
- Visibility settings such as HDX Insight policies.

Figure 1. NetScaler Appliance in XenApp/XenDesktop Setup


Admin
NetScaler Gateway feature
VPN virtual server
NetScaler load balancing feature
Virtual server
Web Interface or StoreFront server farm
WI/SF 1
WI/SF 2
NetScaler load balancing feature
Virtual server
XenApp or XenDesktop server farm
XA/XD 1
XA/XD 2
XA/XD 3
Site
Web Interface on NetScaler

The above figure shows the components involved in this deployment:

- **NetScaler Gateway.** Provides the URL for user access, and provides security by authenticating the users.
- **NetScaler load balancing virtual server.** Load balances the traffic for the Web Interface or StoreFront servers. You can also deploy a load balancing virtual server in front of the XenApp/XenDesktop servers to load balance key components such as XML Broker and Desktop Delivery Controller (DDC) server.
- **Web Interface or StoreFront or Web Interface on NetScaler.** Provides the interface through which you can access the applications.

  Note: Web Interface on NetScaler (WIonNS) is a customization of the Web Interface product, hosted on the NetScaler appliance.
- **XenApp/XenDesktop.** Provides the applications that your users want to access.

Prerequisites

Before using the wizard, make sure of the following:

- XenApp/XenDesktop servers are configured and available.
- Web Interface, StoreFront, or Web Interface on NetScaler servers are configured and available.
- You have a working knowledge of NetScaler Gateway, NetScaler, XenApp, XenDesktop, and StoreFront/Web Interface/Web Interface on NetScaler. For more information, see "Citrix eDocs."

To set up the NetScaler for XenApp/XenDesktop by using the wizard

1. Log on to the NetScaler appliance and, on the Configuration tab, navigate to Traffic Management > Load Balancing.
2. In the details pane, under XenApp/XenDesktop, click Set Up NetScaler for XenApp/XenDesktop.
   Note: If the setup exists on the NetScaler, click the Edit link corresponding to each of the section that you want to modify.
3. Select the XenApp/XenDesktop deployment type.
   Note: The wizard supports only the single-hop deployment of XenApp/XenDesktop.

4. Select the product (StoreFront, Web Interface, or Web Interface on NetScaler) that in your deployment provides the interface for access to the XenApp/XenDesktop applications.
5. Set up secure remote access.
    a. In the NetScaler Gateway Settings section, specify the details for the VPN virtual server.
    b. In the Certificate section, choose an existing certificate or install a new certificate.
    c. In the Authentication Settings section, configure the primary authentication mechanism to be used and specify the server details. You can also configure secondary authentication to provide two-factor authentication. Note: While configuring the primary authentication mechanism, you can select the Load Balancing check box to distribute traffic among authentication servers. In the address field that appears, specify the IP address to assign to the load balancing virtual server.
6. Set up the interface used to access the applications. In the Web Interface, StoreFront, or Web Interface on NetScaler section, do the following:
    a. Specify the details of the server that provides the interface for accessing the applications.
    b. Select the Load Balancing check box to distribute load among the servers. In the address field that appears, specify the IP address to assign to the load balancing virtual server. Note: If Web Interface on NetScaler is selected in this wizard, but it is not installed on the NetScaler appliance, you are prompted to upload the TAR and JRE files. For more information, see "Installing the Web Interface."
7. Specify the XenApp/XenDesktop server(s) from which the applications are to be accessed. In the Xen Farm section, do the following:
    a. Provide details of the servers from which your users want to access applications.
    b. Select the Load Balancing check box to distribute load among the servers. In the address field that appears, specify the IP address to assign to the load balancing virtual server.
8. Configure optimization, security, and visibility on the NetScaler appliance.
    - In the Optimization section, click Apply. The following configurations are executed internally:

      ```
      TCP Profile
      > set vpn vserver ag_vsvr1 -tcpProfileName nstcp_default_XA_XD_profile
      > set servicegroup WI_servicegroup -tcpProfileName nstcp_default_XA_XD_prof
      > set servicegroup SF_servicegroup -tcpProfileName nstcp_default_XA_XD_prof
      > set servicegroup XA_Primary_Broker_servicegroup -tcpProfileName nstcp_def
      > set servicegroup XA_Secondary_Broker_servicegroup -tcpProfileName nstcp_d
      > set servicegroup XD_servicegroup -tcpProfileName nstcp_default_XA_XD_prof

      Compression
      > enable ns feature cmp
      > set servicegroup WI_servicegroup -cmp on
      > set servicegroup SF_servicegroup -cmp on
      > set servicegroup XA_Primary_Broker_servicegroup -cmp on
      > set servicegroup XA_Secondary_Broker_servicegroup -cmp on
      > set servicegroup XD_servicegroup -cmp on

      Caching
      > enable ns feature IC
      > add cache contentgroup cache_group_XA-XD
      > set cache parameter -memLimit 100
      > add cache policy cache_pol1 -rule TRUE -action CACHE -storeInGroup cache_
      > bind cache global XA_XD_10.102.87.108_cachepol -priority 10 -gotoPriority

      SSL quantum settings
      > set ssl parameter -quantumSize 4 -sslTriggerTimeout 10 -encryptTriggerPkt
      ```

    - In the Security section, click Apply.

      Note: The security settings are not applicable for this release.

    - In the Visibility section, click Apply. The following configurations are executed internally:

      ```
      > enable feature Appflow
      > set vpn vserver ag_vsvr1 -appflowLog ENABLED
      ```

      Note: Make sure that the appliance is added to the NetScaler Insight Center appliance.
9. Click Done to complete the configuration.

RISE Integration: NetScaler ADC and Cisco Nexus 7000 Series Switch

Application-delivery solutions that use service modules or switches have required complex configurations and changes in the networking stack. Cisco Remote Integrated Service Engine (RISE) technology can logically integrate a Citrix NetScaler application delivery controller (ADC) with a Cisco Nexus 7000 Series switch as a virtual service module. The integration eliminates the complexities and limitations of traditional inline and one-arm mode configurations. The NetScaler functionality is available as a centralized resource that can be leveraged across the application infrastructure supported by the Cisco Nexus 7000 series switch. The RISE integration provides a service module's streamlined deployment and simplified configuration and operation, and the complete NetScaler application-delivery capabilities that can accelerate application performance for all users.

An ADC deployed in an inline mode can create a bottleneck in the data center. Today, data-center traffic can handle traffic in the terms of terabytes per second, but the ADC capacity can scale up only to gigabytes per second range. The NetScaler ADC, with the new capability to integrate with Cisco Nexus 7000 switch using RISE, can be deployed in a one-arm mode and can provide ADC capabilities to data-center traffic with minimal configuration and maintenance overhead.

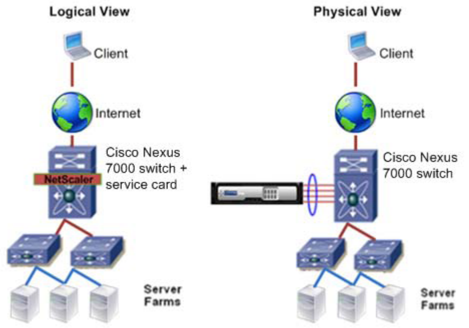
A one-arm mode deployment uses Source NAT (SNAT) and Policy Based Routing (PBR) to send only the necessary traffic through the ADC. With SNAT, the servers do not have visibility of client IP addresses. PBR resolves this issue, but it requires complex, manual configuration and is prone to errors. The Automatic Policy Based Routing (APBR) feature in RISE eliminates the need for Source NAT or manual PBR configuration in a one-arm mode design.

For more information about RISE functionality and other features, see Cisco Remote Integrated Service Engine for Citrix NetScaler Appliances and Cisco Nexus 7000 Series Switches Configuration Guide.

Understanding RISE

Cisco RISE technology logically integrates a Citrix NetScaler ADC with a Cisco Nexus 7000 Series switch as a virtual service module. After you connect the NetScaler ADC and the Cisco Nexus 7000 series switch, an initial handshake is performed and a control channel is established between the two devices to exchange port-channel information. The following figure shows the RISE deployment:

Figure 1. RISE Deployment



Because the NetScaler ADC appears to be a virtual module in the switch, client traffic that reaches the Cisco Nexus 7000 series switch is intelligently routed to the NetScaler ADC and then to the servers. The return traffic flows to the ADC through the Cisco switch, and then back to the client.

The interface or port-channel that connects the NetScaler ADC and Cisco Nexus 7000 series switch is a single trunk carrying both control and data VLANs. The control VLAN is used for all control channel communication, and the data VLAN is used for communicating data traffic.

For more information, see Cisco RISE Integration Overview.

This document includes the following:

- RISE Functionality
- RISE Network Topologies
- RISE Connection Modes

RISE Functionality

Updated: 2014-05-19

The feature integration that RISE enables between the NetScaler ADC and the Cisco Nexus 7000 Series switch provides the following functionalities:

- Plug and play auto-provisioning

  RISE provides a plug and play auto-provisioning feature. You can directly connect the NetScaler ADC to the Cisco Nexus 7000 series switch.
- Discovery and bootstrapping

  The discovery and bootstrap mechanism enables the Cisco Nexus 7000 Series switch to perform the initial setup of NetScaler automatically by exchanging information such as NSIP and VLANs to set up a RISE channel, which transmits control and data packets. For details, see Discovery and Bootstrap.
- Health Monitoring

  The NetScaler ADC uses its health monitoring feature to track and support server health by sending health probes to verify server responses. The Intelligent Services Control Manager (iSCM) on the Cisco Nexus 7000 Series switch and the Intelligent Services Control Client (iSCC) on the NetScaler ADC 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. For details, see Health Monitoring.
- APBR

Automatic Policy Based Routing (APBR) automatically routes the return traffic from the servers to the NetScaler ADC, preserving the client IP addresses. The automatic policy based routes are defined on the Cisco Nexus 7000 series switch. When the return traffic from the server reaches the Cisco Nexus 7000 series switch, the APBR policies defined on the switch route the traffic to the NetScaler ADC, which in turn routes the traffic to the client.

Note:

APBR can function only if USIP is enabled on the NetScaler ADC.

APBR can be deployed in a VPC mode or a non-VPC mode. For more details on VPC mode, see Cisco VPC.

For details on configuring APBR, see Configuring Auto Policy-Based Routing.

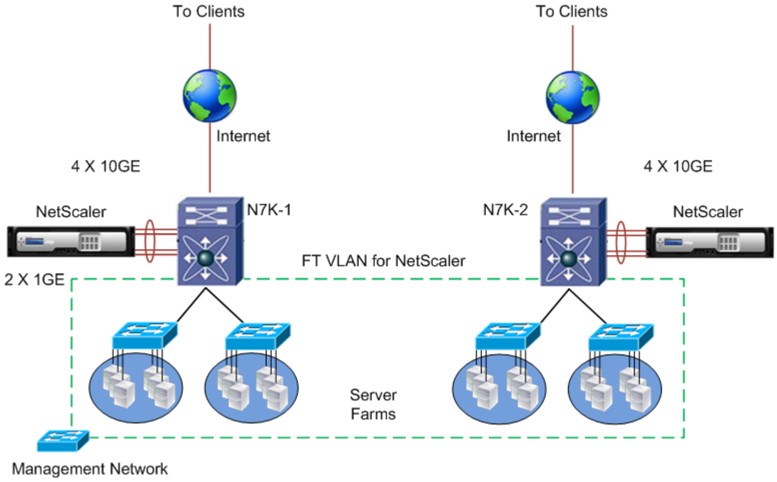
RISE Network Topologies

Updated: 2014-05-19

RISE can be deployed in any of the following modes:

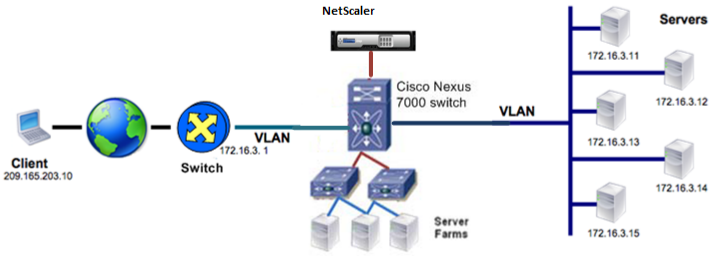
- One-Arm modeâ€” The NetScaler ADC's ports are bundled as a port channel connected to the Cisco Nexus 7000 Series switch. In one-arm mode, the ADC is configured with a VLAN that handles both client and server requests.

  Figure 2. One-Arm Mode



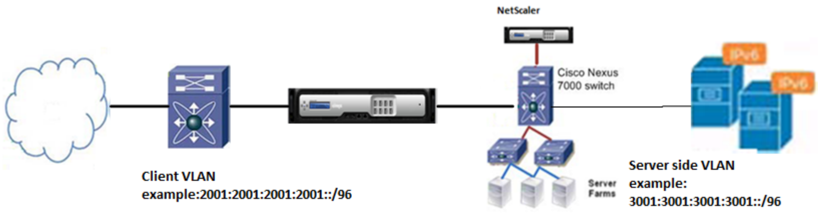
- Bridged modeâ€” In bridged mode, the NetScaler ADC bridges traffic between two VLANs in the same IP subnet. The VLAN facing the WAN is the client VLAN. The VLAN facing the data center is the server VLAN. A bridge group virtual interface (BVI) joins the two VLANs into one bridge group.

  Figure 3. Bridged Mode



- Routed modeâ€”In routed mode, the NetScaler ADC is the next hop in the network, typically with the client-side VLAN and the server-side VLAN in different IP subnets or in different IP networks.

  Figure 4. Routed Mode



RISE Connection Modes

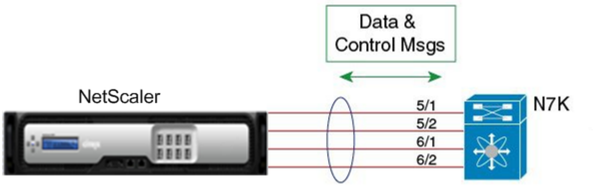
Updated: 2014-05-27

You can connect the Citrix NetScaler appliance to the Cisco Nexus 7000 Series switch in one of the following ways:

Direct Connect Mode for a Standalone Switch

In a direct mode deployment, the NetScaler ADC is attached to a single Nexus 7000 Series switch. The switch can be standalone device or a vPC peer.

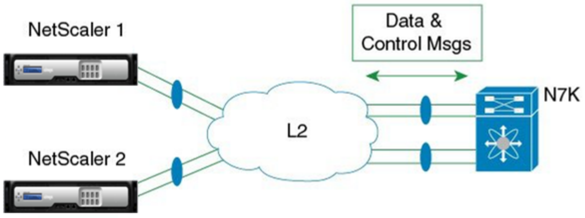
Figure 5. Direct Connect Mode



Indirect Connect Mode

In an indirect mode deployment, a virtual NetScaler ADC is connected to a Cisco Nexus 7000 Series switch through a switched layer 2 network.

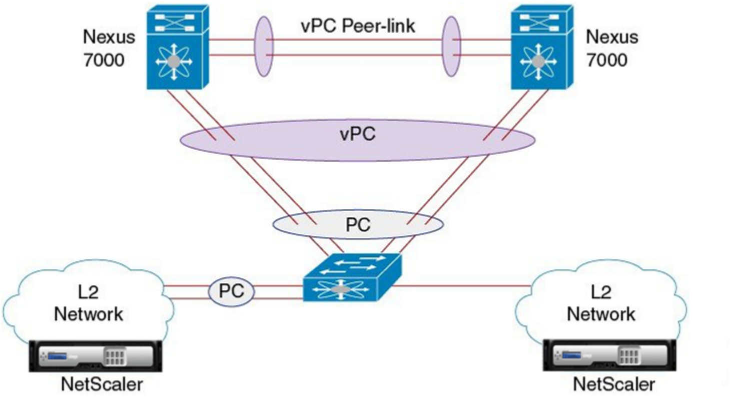
Figure 6. Indirect Connect Mode



Virtual Port Channel (vPC) Connect Mode

In a virtual port channel (vPC) direct mode deployment, the NetScaler ADC is attached to a single Nexus 7000 Series switch that is a vPC peer.

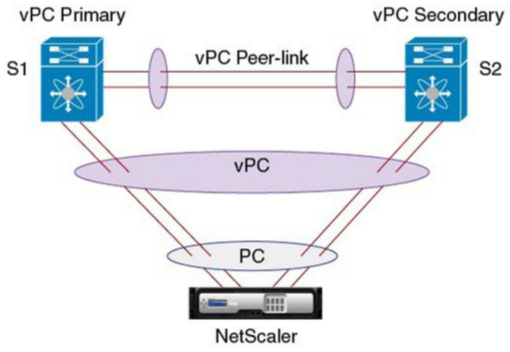
Figure 7. Virtual Port Channel (vPC) Connect Mode



vPC Indirect Connect Mode

In a vPC indirect mode deployment, the NetScaler ADC is indirectly attached to a Cisco Nexus vPC peer through a layer 2 network.

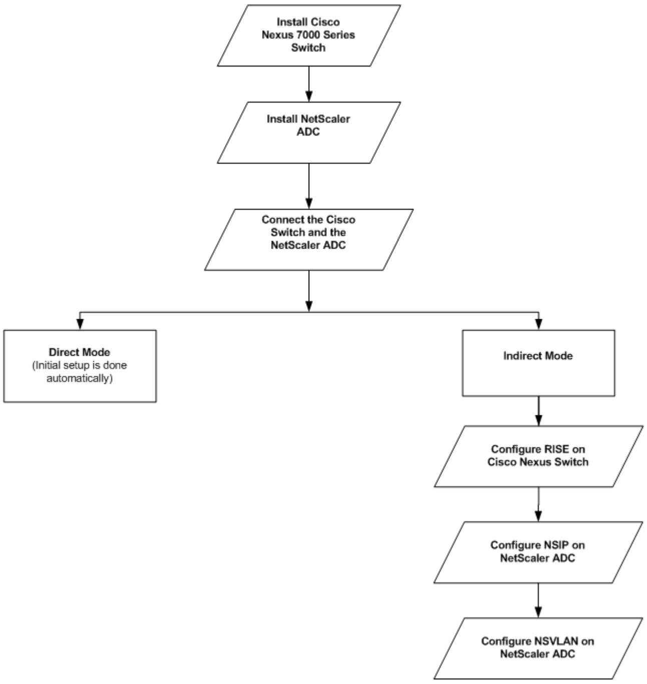
Figure 8. vPC Indirect Connect Mode



For more information on connection modes, see Connection Modes.

Getting Started with RISE

To begin using the RISE features, first install the Cisco Nexus 7000 series switch and the NetScaler ADC. Then, connect the NetScaler ADC to the Cisco Nexus 7000 switch either directly or indirectly. If you plan to connect the NetScaler ADC directly to the Cisco Nexus 7000 switch, the initial setup is done automatically by the auto-discovery feature. The following figure explains the flow of steps in the configuration of RISE.


Install Cisco Nexus 7000 Series Switch
Install NetScaler ADC
Connect the Cisco Switch and the NetScaler ADC
Direct Mode (Initial setup is done automatically)
Indirect Mode
Configure RISE on Cisco Nexus Switch
Configure NSIP on NetScaler ADC
Configure NSVLAN on NetScaler ADC

This document includes the following:

- Installing the Cisco Nexus Switch and the NetScaler ADC
- Accessing the Cisco Nexus Switch and the NetScaler ADC
- Configuring RISE
- Configuring High Availability

Installing the Cisco Nexus Switch and the NetScaler ADC

Updated: 2014-05-26

You need to first install the Cisco Nexus 7000 series switch, and then install the NetScaler ADC.

Installing Cisco Nexus 7000 Series Switch

To install the Cisco Nexus 7000 Series Switch, see Installing Cisco Nexus 7000 Series Switch.

Installing NetScaler ADC

To install the NetScaler ADC, see Installing NetScaler ADC.

To install a virtual NetScaler ADC appliance, see Installing NetScaler Virtual Appliances on XenServer or Installing NetScaler Virtual Appliances on VMware ESX.

Accessing the Cisco Nexus Switch and the NetScaler ADC

Updated: 2014-05-26

After you have completed the installation process, you can access the Cisco Nexus Series 7000 switch through the command-line interface (CLI) and the Citrix NetScaler appliance through the graphical user interface (GUI) or the CLI. To perform administrative tasks and also, to configure RISE, you need to access the Cisco switch and the NetScaler ADC.

Accessing the Cisco Nexus Series 7000 Switch

After installing the Cisco Nexus 7000 series switch, you can access it using the command line interface. To access the Cisco Nexus 7000 Series Switch, see Accessing the Cisco Nexus 7000 series switch.

Accessing the NetScaler ADC

A 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 statistical utility, called Dashboard. 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 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.
For information about the procedures to access through CLI and GUI, see Using the Command Line Interface and Using Graphical User Interface.

Configuring RISE

Updated: 2015-03-18

After you install the Cisco Nexus 7000 series switch and the NetScaler ADC, configure the appliance to work in direct mode, indirect mode, VPC direct mode, or VPC indirect mode.

Direct Mode

The NetScaler ADC which 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 appliance in a direct mode deployment. For details on configuring RISE in direct mode, see Configuring RISE in Direct Mode.

Indirect Mode

For indirect mode deployment, configure RISE on Cisco Nexus switch, and then configure NSIP and NSVLAN on NetScaler ADC.

- Configuring RISE on Cisco Nexus Switch
- Configuring NSIP on NetScaler ADC
- Configuring NSVLAN on NetScaler ADC

If the direct mode is disabled. all Layer 2 (L2) discovery messages are dropped and L2 RISE discovery does not take place. While, if the direct mode is enabled, the L2 discovery messages are parsed. If L2 RISE discovery messages are successfully parsed, the Indirect Mode is automatically enabled.

If indirect mode is disabled, NetScaler RISE daemon does not listen on TCP ports 8000 and 8001. As a result, RISE heartbeats stop and RISE profiles go down. While, if indirect mode is enabled, NetScaler RISE daemon starts listening on TCP ports 8000 and 8001. As a result, RISE heartbeats may be exchanged and RISE profiles may come up.

The default setting for RISE is direct attach mode as enabled and indirect mode as disabled. With these settings, the direct attach mode works. However, indirect mode will not work. If you want to deploy NetScaler in an indirect mode setting with N7K then use the following setting:

```
set rise param -indirectMode ENABLED
```

With active RISE profiles in direct mode, you must consider the followings points:

1. The set rise param -directMode DISABLED command displays a warning message; Warning: Disabling direct mode with one or more active RISE profile(s) on DIRECT ATTACH mode may cause corresponding RISE profile(s) to not come UP on reboot
2. The set rise param -indirectMode DISABLED displays a warning message; Warning: Disabling indirect mode will cause any active RISE profile(s) to go down

However, if the direct mode is enabled, and NetScaler starts receiving L2 RISE discovery messages, it automatically turns the indirect mode as enabled. Otherwise, RISE direct mode does not work.

With active RISE profiles in Indirect Attach mode, the set rise param -indirectMode DISABLED command displays a warning message; Warning: Disabling indirect mode will cause any active RISE profile(s) to go down leading to RISE profiles on Indirect Attach going down.

vPC Direct Mode

The NetScaler ADC which 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 appliance in a direct mode deployment. For details on configuring RISE in direct mode, see Configuring RISE in vPC Direct Mode.

vPC Indirect Mode

In a vPC indirect mode deployment, the NetScaler ADC is indirectly attached to a Cisco Nexus vPC peer through a Layer 2 network.

- Configuring RISE on Cisco Nexus Switch
- Configuring NSIP on NetScaler ADC
- Configuring NSVLAN on NetScaler ADC

For details on configuring RISE in direct mode, see Configuring RISE in vPC Direct Mode.

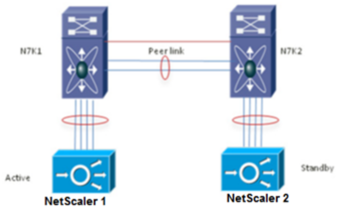
For information on configuring RISE, see Configuring RISE.

Configuring High Availability

Updated: 2014-05-26

In a High Availability setup, the RISE deployment uses a maximum of two NetScaler ADCs. If one ADC becomes unavailable, the traffic flow is seamlessly switched to the other ADC.

Figure 1. High Availability



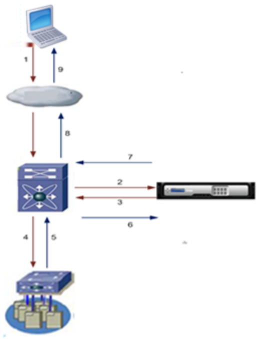
For information about high availability configuration, see High Availability.

Use Case: Configuring Auto Policy-Based Routing

Auto Policy-Based Routing (APBR) automatically routes the return traffic from the servers to the NetScaler ADC, preserving the client IP addresses. The automatic policy based routes are defined on the Cisco Nexus 7000 series switch. When the return traffic from the server reaches the Cisco Nexus 7000 series switch, the APBR policies defined on the switch route the traffic to the NetScaler ADC, which in turn routes the traffic to the client.

To understand the need for APBR, first consider a NAT based scenario in which a packet flows from the client to the server and from the server back to the client.

Figure 1. Packet Flow



1. Client initiates the traffic to the virtual IP (VIP) address.

   SRC_IP= Client IP; DST_IP= VIP
2. The Cisco Nexus switch forwards the packet to the NetScaler ADC.

   SRC_IP= Client IP; DST_IP= VIP
3. The ADC performs source NAT and destination NAT (Network Address Translation), changes the source IP and destination IP addresses, and sends the packet to the Cisco Nexus switch.

   SRC_IP= NAT_IP; DST_IP= RS_IP
4. The Cisco Nexus switch receives the packet and forwards it to a server.

   SRC_IP= NAT_IP; DST_IP= RS_IP
5. The server processes the packet and forwards it to the Cisco Nexus 7000 series switch.

   SRC_IP= RS_IP IP; DST_IP= NAT_IP
6. The Cisco Nexus switch forwards the packet to the NetScaler ADC.

   SRC_IP= RS_IP IP; DST_IP= NAT_IP
7. The NetScaler ADC changes the source IP address and forwards the packet to the Cisco Nexus 7000 series switch.

   SRC_IP= VIP; DST_IP= Client_IP
8. The Cisco Nexus 7000 series switch forwards the packet to the client.

   SRC_IP= VIP; DST_IP= Client_IP

   The client receives the packet. However, the client IP address is not visible to the server.

Now, consider a scenario in which policy based routing (PBR) directs packet flow.

1. Client initiates the traffic to the virtual IP (VIP) address.

   SRC_IP= Client IP; DST_IP= VIP
2. The Cisco Nexus switch forwards the packet to the NetScaler ADC.

   SRC_IP= Client IP; DST_IP= VIP
3. The ADC performs destination NAT (Network Address Translation), changes the destination IP, and then sends the packet to the Cisco Nexus switch.

   SRC_IP= Client IP; DST_IP= RS_IP
4. The Cisco Nexus switch receives the packet and forwards it to a server.

    SRC_IP= Client IP; DST_IP= RS_IP

5. The server processes the packet and forwards it to the Cisco Nexus 7000 series switch.

   SRC_IP= RS_IP IP; DST_IP= Client IP
6. The Cisco Nexus switch forwards the packet to the NetScaler ADC.

   SRC_IP= RS_IP IP; DST_IP= Client IP
7. The NetScaler ADC changes the source IP address and forwards the packet to the Cisco Nexus 7000 series switch.

   SRC_IP= VIP; DST_IP= Client_IP
8. The Cisco Nexus 7000 series switch forwards the packet to the client.

   SRC_IP= VIP; DST_IP= Client_IP
9. The client receives the packet. The client IP address is visible to the server. However, PBR requires manual and complex configurations and is prone to errors.

To overcome these drawbacks, configure APBR rules on the RISE appliance. When APBR is configured, the packets flow as described in the following procedure:

1. Client initiates the traffic to the virtual IP (VIP) address.

   SRC_IP= Client IP; DST_IP= VIP
2. The Cisco Nexus switch forwards the packet to the NetScaler ADC.

   SRC_IP= Client IP; DST_IP= VIP
3. The ADC performs load balancing and changes the destination IP address to the appropriate server IP address and forwards the packet to the Cisco Nexus switch in an APBR message.

   SRC_IP= Client IP; DST_IP= RS_IP
4. The Cisco Nexus switch receives the packet and forwards it to a server by using a route map.

   SRC_IP= Client IP; DST_IP= RS_IP
5. The server processes the packet and forwards it to the Cisco Nexus 7000 series switch.

   SRC_IP= RS_IP IP; DST_IP= Client_IP
6. When the packet reaches the Nexus switch, the switch applies the APBR rules, sets the next hop IP address to that of the NetScaler ADC, and forwards the packet to the NetScaler ADC.

   SRC_IP= RS_IP IP; DST_IP= Client_IP
7. The NetScaler ADC changes the source IP address and forwards the packet to the Cisco Nexus 7000 series switch.

   SRC_IP= VIP; DST_IP= Client_IP
8. The Cisco Nexus 7000 series switch forwards the packet to the client.

   SRC_IP= VIP; DST_IP= Client_IP
9. The client receives the packet successfully.

Note: 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 APBR message control flow is explained below

1. After USIP is enabled in the services on Netscaler ADC, it publishes the IP address, port number and protocol details of the server to the Cisco Nexus 7000 series switch over the RISE control channel.
2. Using the IP address, port number and protocol details of the server, the Cisco Nexus 7000 series switch creates an APBR rule which consists of ACLs and route maps.
   Note:
   - For local servers, the switch creates ACLs and route maps.
   - For remote servers , the switch forwards the APBR messages to other Cisco Nexus 7000 series switches.
3. The RISE appliance then applies the APBR rules to the switch virtual interface on the Cisco Nexus 7000 series switch connected to server.

To configure the APBR functionality:

- Enable the feature on the Cisco Nexus switch

- Configure APBR on NetScaler ADC
    - Configure NSIP
    - Configure NSVLAN
    - Enable USIP option

For more information, see Configuring Auto Policy-Based Routing.

Global Server Load Balancing (GSLB) Powered Zone Preference

GSLB powered zone preference is a feature that integrates XenApp/XenDesktop, StoreFront, and NetScaler to provide clients access to the most optimized data center on the basis of the client location.

In a distributed XenApp/XenDesktop deployment, StoreFront might not select an optimal datacenter when multiple equivalent resources are available from multiple datacenters. In such cases, StoreFront randomly selects a datacenter. It can send the request to any of the XenApp/XenDesktop servers in any datacenter, regardless of proximity to the client making the request.

With this enhancement, the client IP address is examined when an HTTP request arrives at the NetScaler Gateway appliance, and the real client IP address is used to create the datacenter preference list that is forwarded to StoreFront. If the NetScaler appliance is configured to insert the zone preference header, StoreFront 3.5 or later can use the information provided by the appliance to reorder the list of delivery controllers and connect to an optimal delivery controller in the same zone as the client. StoreFront selects the optimal gateway VPN virtual server for the selected datacenter zone, adds this information to the ICA file with appropriate IP addresses, and sends it to the client. Storefront then tries to launch applications hosted on the preferred datacenter's delivery controllers before trying to contact equivalent controllers in other datacenters.

For more information about configuring this solution, click here.

For a video overview about GSLB powered zone preference solution, click https://www.youtube.com/watch?v=Y8DELum0Xp0.