Integrating Citrix NetScaler ADCs with Cisco Application Centric Infrastructure

Citrix NetScaler 10.5
September 9, 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CITRIX Citrix and other Citrix product names referenced herein are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other product names, company names, marks, logos, and symbols are trademarks of their respective owners.

Contents

Introduction

As businesses quickly move to make the datacenter more agile, the application centric automation and virtualization of both hardware and software infrastructure become increasingly important. Cisco Application Centric Infrastructure (ACI) supplies the critical link between business-based requirements for applications and the infrastructure that supports them. The Citrix NetScaler ADC connects infrastructure and applications and makes their configuration available to the Cisco Application Policy Infrastructure (APIC) through integration.

Citrix NetScaler and Cisco ACI enable datacenter and cloud administrators to holistically control L2–L7 network services in a unified manner, through seamless insertion and automation of best-in-class NetScaler services into next-generation datacenters built on Cisco's ACI Architectures. NetScaler leverages the Cisco Application Policy Infrastructure Controller (APIC) to programmatically automate network provisioning and control on the basis of application requirements and policies for both datacenter and enterprise environments.

Cisco APIC addresses the two main requirements for achieving the application centric data center vision:

- Policy-based automation framework
- Policy-based service insertion technology

Policy-Based Automation Framework

A policy-based automation framework enables the Cisco APIC to dynamically provision and configure resources according to application requirements. As a result, core services such as firewalls and Layer 4 through 7 services can be consumed by applications, and these services can be made ready to use in a single automated step.

Being application centric, the APIC allows the creation of application profiles, which define the Layer 4 through 7 services consumed by a given datacenter-tenant application. Citrix NetScaler provides L4-L7 services such as load balancing, application acceleration, and application security.

Integration between the Cisco APIC controller and the NetScaler ADC is achieved through a NetScaler device package. Imported by the APIC controller, the device package enables REST-based API integration and allows the APIC controller to perform detailed feature-level configuration of the NetScaler.

Policy-Based Service Insertion

The Cisco APIC solution automates the steps of routing network traffic to the correct services on the basis of application policies. L4-L7 resources can be dynamically provisioned and configured according to application requirements on a per tenant basis.

The Cisco APIC offers a graphical drag and drop GUI for easy creation of L4-L7 Service Graphs that specify network traffic routing. Any of the L4-L7 ADC features available in the NetScaler device package can be included in a Service Graph definition, allowing comprehensive NetScaler integration with the Cisco APIC.

Policy-based service insertion automates the steps of routing network traffic to the correct services as specified by application policies. The automated addition, removal, and reordering of services allows administrators to quickly change the resources allocated to an application, without the need to rewire and reconfigure the network or relocate the services. For example, if a business decides to use load balancing feature found in a modern ADC, administrators can simply redefine the policy for the services that should be used for the related applications. The Cisco APIC can dynamically distribute new policies to the infrastructure and service nodes in minutes, without requiring manual changes to the network.

Once created, a Service Graph can be assigned to an Application Profile and contracted to a data center tenant, thereby defining the network traffic flow for that specific application and tenant.

Benefits of Using Citrix NetScaler ADCs in Cisco ACI

The unique Cisco ACI and Citrix NetScaler joint solution improves data center operations and application deployment, using the Cisco APIC as the central policy-control and management station, and Cisco ACI service-insertion technology to direct traffic to the appropriate service nodes.

The main benefits include:

- **Central point of network control with ADC service policy coordination and automation**: The Cisco APIC acts as a point of configuration management and automation for NetScaler ADCs (both MPX appliances and VPX virtual appliances), tightly coordinates the ADC service delivery with the network automation, and provides end-to-end telemetry and visibility of service-aware applications and tenants.
- **Scalable and elastic architecture for NetScaler ADCs**: Cisco ACI defines a policy-based service insertion mechanism for both physical and virtual ADC appliances, providing full lifecycle service management based on workload instantiation and decommissioning.
- **Investment protection**: Cisco ACI and Cisco APIC are fully compatible with existing ADC networks, preserving existing service operation models and using open standards protocols.

Supported Citrix NetScaler Platforms

Cisco APIC is capable of orchestrating services deployed on the following Citrix NetScaler ADC form factors:

- Citrix NetScaler VPX instances running release 10.1
- Citrix NetScaler MPX appliances running release 10.1
- Citrix NetScaler NS1000V (a virtual NetScaler appliance sold and supported by Cisco)

Supported and Unsupported Citrix NetScaler Features

Citrix has introduced a new notion of function-definition, which includes the complete configuration details of a particular feature, such as Load Balancing. Cisco APIC mandates feature definitions. These definitions are easy to use and they simplify configuration. The entire NetScaler features set is included in the various functions definitions, although not all features are currently supported.

Cisco APIC supports following functions definitions:

- Load Balancing
- SSL Offload

Cisco APIC does not yet support the following functions definitions, although they appear in Cisco APIC user interface:

- AAA
- Application Firewall
- Cache Redirection
- Compression
- Content Accelerator
- Content Switching

- DataStream
- Domain Name Service
- Global Server Load Balancing
- Integrated Caching
- SSL VPN

Prerequisites and Points to Consider for Integrating NetScaler ADCs in Cisco ACI

The following are the prerequisites and points to consider before integrating NetScaler ADCs in Cisco ACI:

- The administrator should have conceptual knowledge of Cisco ACI components and Citrix NetScaler ADCs.
    - For more information about Cisco ACI and its components, see the product documentation at http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
    - For more information about the Citrix NetScaler ADCs, see the Citrix NetScaler product documentation at http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler-wrapper-con.html.
- All the required components of Cisco ACI, including Cisco APIC in the datacenter, must be set up and configured. For more information about Cisco ACI and its components, see the product documentation at http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
- The NetScaler ADCs must be deployed in the datacenter and have network connectivity with Cisco ACI. For more information about Citrix NetScaler ADCs, see the Citrix NetScaler product documentation at http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler-wrapper-con.html.
- NetScaler features are configured through function definitions in APIC, so it is important for the administrator to be cautious while providing the data. The administrator has to ensure the following:
    - Provide mandatory data for all the required entities for a given function.
    - Once configured, do not change attributes that cannot be modified (for example, serviceType of lbvserver in the load balancing function).
    - You must be familiar with all the required parameters for a given object, such as lbvserver. For an object that has a composite key, mere providing a unique name is not sufficient to create the object.
    - Bindings cannot be modified. To change a binding, the administrator must remove the existing binding and create a new one.
- The following NetScaler feature configurations are out-of-band. They cannot be performed through Cisco APIC:
    - High Availability configuration

    - Management access, including Subnet IP address (SNIP), VLAN, Interfaces, and NetScaler management IP address (NSIP) bindings
    - SSL Certificates
    - System user accounts and role-back-access (RBA) policies
- Citrix NetScaler SDX configuration is not supported through APIC.

Steps for Integrating NetScaler ADCs with Cisco ACI

Integrating the deployed NetScaler ADCs with Cisco ACI in your datacenter involves the following tasks:

1. **Configure the NetScaler ADCs for Management Access**: In this step, the administrator configures the management IP address (NSIP), management VLAN (NSVLAN, VLAN of NSIP), and specifies the default gateway on the deployed NetScaler ADCs, which are to be integrated with Cisco ACI. These configurations are made through the user interfaces of the NetScaler ADCs. For more information, see the Citrix NetScaler product documentation at http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler-wrapper-con.html.
2. **Download the NetScaler ADC Device package**. A NetScaler device package provides the APIC with information about NetScaler ADCs, including what NetScaler ADCs are and what they are capable of.
   A NetScaler device package is a zip file containing the following parts:
    - **Device Model**. An XML file that contains the following:
        - Device properties (for example, model and NetScaler software version)
        - Functions provided by NetScaler ADCs (for example, load balancing).
        - Configuration parameters of each function
        - Device configuration parameters
    - **Device script**. A Python script that integrates the APIC and the NetScaler ADC. The APIC events are mapped to function calls defined in the device script.
    - **Functional profile**. A profile of parameters with default values that are specified by Citrix. The administrator can configure a function to use these default values.
    - **Device-level configuration parameters**. A configuration file specifying the values of the parameters that are required by a NetScaler ADC. The configuration can be shared by one or more of the graphs that use the NetScaler ADC.

   The administrator downloads the NetScaler device package from the location provided by Citrix.

3. **Import the NetScaler Device Package into Cisco ACI**. In this step, the administrator imports the downloaded device package into Cisco APIC in your datacenter, so that the APIC has the necessary information about the NetScaler ADCs and their capabilities. For more information on importing device packages into Cisco APIC in your datacenter, see the product documentation at http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/products-installation-and-configuration-guides-list.html.

4. **Register the required NetScaler ADCs with Cisco ACI**. In this task, the administrator registers the required NetScaler ADCs, which are deployed in the datacenter, to Cisco APIC. After the NetScaler ADCs are registered, the administrator configures various features, and then manages and monitors them through Cisco APIC. For more information on registering devices with Cisco APIC, see the product documentation at http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/products-installation-and-configuration-guides-list.html.

Deployment Modes of NetScaler ADCs in Cisco ACI

A NetScaler ADC resides between the clients and the servers, so that client requests and server responses pass through it. In a typical installation, virtual servers configured on the ADC provide connection points that clients use to access the applications behind the ADC. In this case, the ADC owns public IP addresses that are associated with its virtual servers, while the real servers are isolated in a private network. It is also possible to operate the ADC in a transparent mode as an L2 bridge or L3 router, or even to combine aspects of these and other modes.

A NetScaler appliance logically residing between clients and servers can be deployed in either of two modes:

- Inline
- Anywhere

Inline Mode

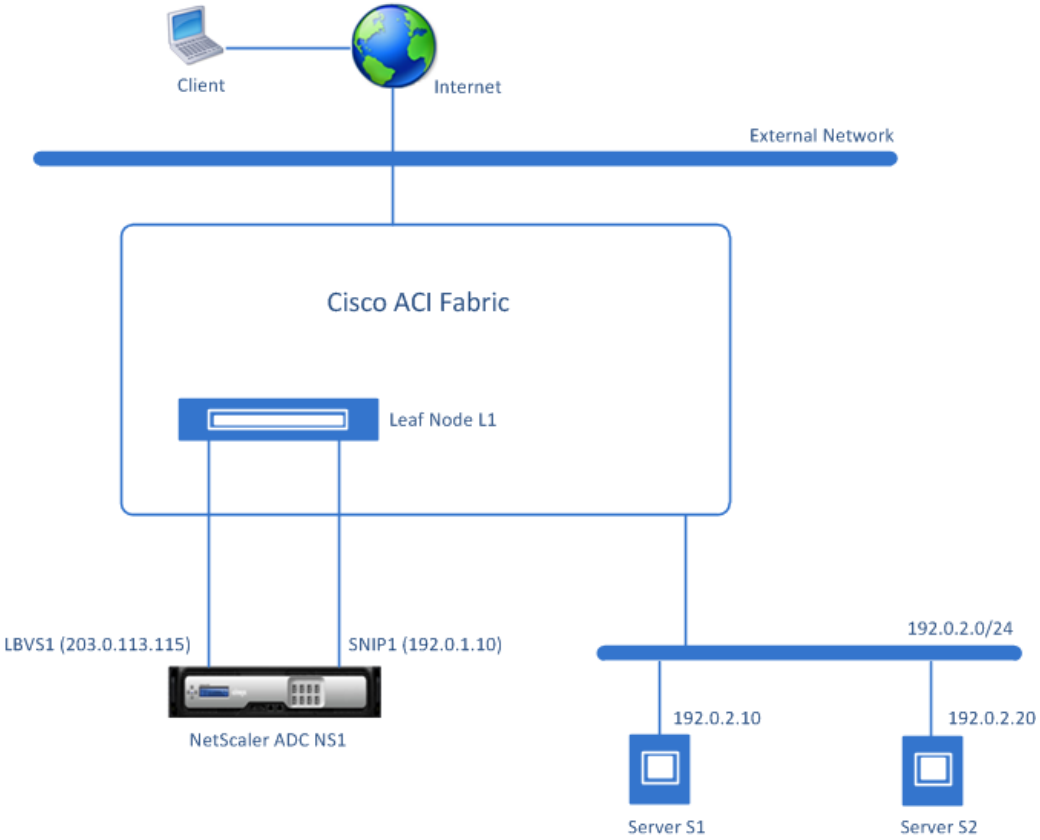
In inline mode, multiple network interfaces of the NetScaler ADC are connected to a leaf node of the Cisco ACI fabric, and the NetScaler ADC is logically placed between the clients and the servers. The appliance has a separate network interface for client networks and a separate network interface for server networks. It is possible for the servers to be in a public network and the clients to directly access the servers through the appliance, with the appliance transparently applying the L4-L7 features. Usually, virtual servers are configured to provide an abstraction of the real servers. Traffic from clients pass through the ADC to access a load balanced server. Client requests at the fabric are forwarded to the NetScaler ADC, and the NetScaler ADC uses the configured load balancing method to select the server.

Consider an example of a load balancing setup in Cisco ACI fabric that uses a NetScaler ADC NS1 deployed in inline mode. NetScaler NS1 is connected to leaf node L1 of the Cisco ACI fabric. A load balancing virtual server LBVS1 on NetScaler ADC NS1 is used to load balance servers S1 and S2 in the Cisco ACI fabric. Servers S1 and S2 belong to same subnet, 192.0.2.0/24.

NetScaler NS1 is connected to L1 through two interfaces. The first link is dedicated for client side connections and the second link is dedicated for server side connections.

A subnet IP (SNIP) address SNIP1 (192.0.1.10) is configured on NS1 for enabling the NS1 to communicate with servers S1 and S2. LBVS1 is accessible through the first link.

NS1 advertises routes for LBVS1 and SNIP1 using routing protocols to Cisco ACI fabric. Similarly, the fabric advertises routes for S1 and S2 to NS1. Services SVC-S1 and SVC-S2 on NS1 represent servers S1 and S2, respectively.



Following is the traffic flow in this example:

1. Client CL1 sends a request packet to LBVS1. The request packet has:
    - Source IP = IP address of the client
    - Destination IP = IP address of LBVS1 (203.0.113.15)
2. LBVS1 of NS1 receives the request packet.
3. LBVS1's load balancing algorithm selects server S2.
4. NS1 opens a connection between SNIP1 and S2, and then sends the request packet from SNIP1 to S2. The request packet has:
    - Source IP address = SNIP1 (192.0.1.10)
    - Destination IP address = IP address of S2 (192.0.2.20)
5. S2’s response reaches CL1 through NS1.

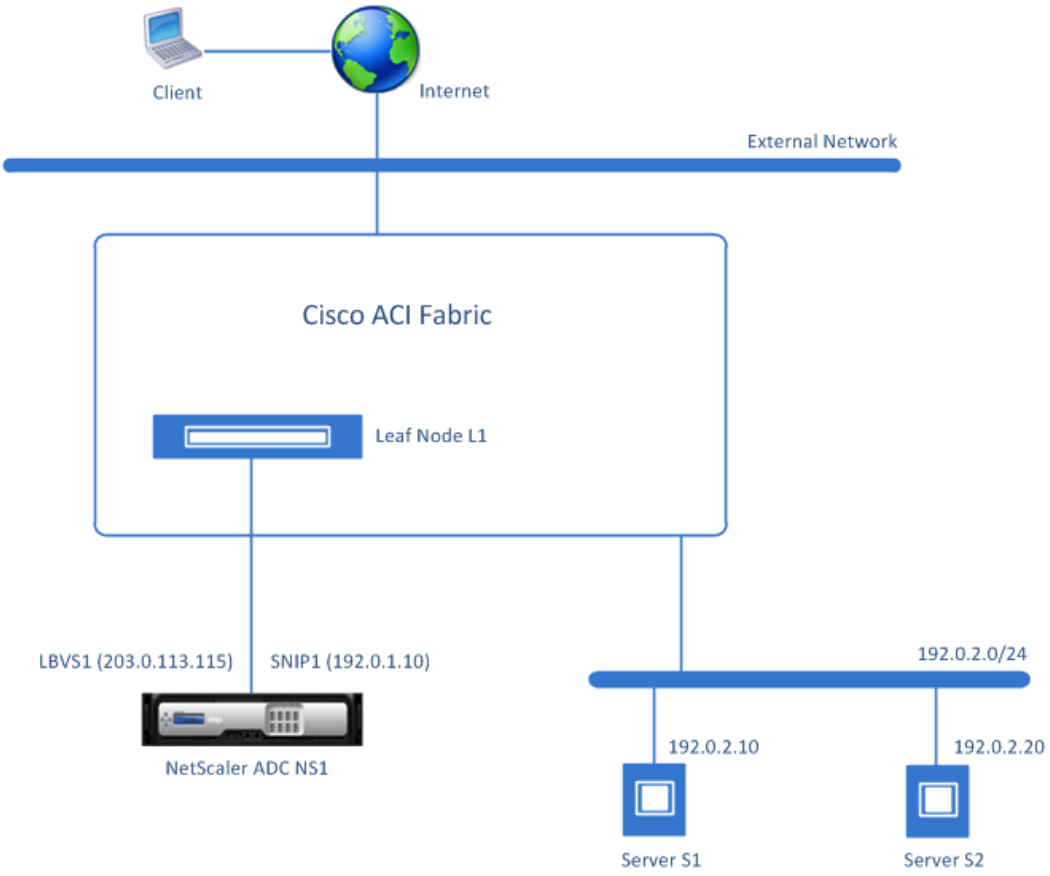
Anywhere Mode

In Anywhere mode, only one network interface of the ADC is connected to one of the leaf node of Cisco ACI fabric. Anywhere mode can simplify network changes needed for NetScaler ADC installation in some environments. Client requests received on the fabric are forwarded to the ADC, and the ADC uses the configured load balancing method to select the server.

Consider an example of a load balancing setup in Cisco ACI fabric that uses a NetScaler ADC NS1 deployed in Anywhere mode. NetScaler NS1 is connected to leaf node L1 of the Cisco ACI fabric. A load balancing virtual server LBVS1 on NetScaler ADC NS1 is used to load balance servers S1 and S2 in the Cisco ACI fabric. Servers S1 and S2 belong to same subnet, 192.0.2.0/24.

Only one interface of NetScaler ADC NS1 is connected to L1. SNIP address SNIP1 (192.0.1.10) is configured on NS1 and is used by NS1 to communicate with servers S1 and S2.

NS1 advertises routes for LBVS1 and SNIP1 using routing protocols to Cisco ACI fabric. Similarly, the fabric advertises routes for S1 and S2 to NS1. Services SVC-S1 and SVC-S2 on NS1 represent servers S1 and S2, respectively.



Following is the traffic flow in this example:

1. Client CL1 sends a request packet to LBVS1. The request packet has:
    - Source IP = IP address of the client
    - Destination IP = IP address of LBVS1 (203.0.113.15)
2. LBVS1 of NS1 receives the request packet.
3. LBVS1's load balancing algorithm selects server S2.
4. NS1 opens a connection between SNIP1 and S2, and then sends the request packet from SNIP1 to S2. The request packet has:
    - Source IP address = SNIP1 (192.0.1.10)
    - Destination IP address = IP address of S2 (192.0.2.20)
5. S2’s response reaches CL1 through NS1.