NetScaler MAS 11.1

Feb 07, 2017

Overview

Single Server Deployment

Installing NetScaler MAS on Citrix XenServer
Installing NetScaler MAS on Microsoft Hyper-V
Installing NetScaler MAS on VMWare ESXi
Installing NetScaler MAS on Linux-KVM Server

Migrate from Single Server to HA Deployment

OpenStack Integration

Prerequisites

Pre-configuration Tasks in NetScaler MAS and OpenStack
Configuring LBaaS V1 using Horizon
Configuring LBaaS V2 using Command Line
Manual Provisioning of NetScaler VPX Instance on OpenStack
Integrating NetScaler MAS with OpenStack Heat Services
Configuring Layer 7 Content Switching
Shared VLAN Support for Administrative Partitions
Trial Licensing Workflow Enhancement
Service Package Isolation Policies
Flexible Policy-Based Device Allotment

NSX Integration

Configuration Jobs: Record and Play
Configuration Jobs: Replicate Configuration
Get Configuration Advice
Web Insight
Cache Insight
System Settings

Licensing

High Availability Deployment

How-to Articles

Instance Management
Configuration Management
Event Management
Certificate Management
Change Management
Application Management
Analytics
Authentication
NetScaler MAS System

StyleBooks

How to Use StyleBooks Shipped with NetScaler MAS
How to Create Your Own StyleBooks
How to Use User-Defined StyleBooks in NetScaler MAS
How to Use API to Create Configurations from StyleBooks
How to Enable Analytics and Configure Alarms on a Virtual Server Defined in a StyleBook
How to Create a StyleBook to Upload SSL Certificate and Certificate Key Files to NetScaler Instances
How to Use Microsoft Exchange StyleBook in Business Enterprises
How to Use Microsoft Skype for Business StyleBook in Business Enterprises

StyleBooks Grammar

Multi-Tenancy

Manage Admin Partitions

Monitor Globally Distributed Data Centers

Audit Configuration Changes

Network Reporting
Gateway Insight
Security Insight
WAN Insight
Managing NetScaler SD-WAN WO using NetScaler MAS
FAQs

Oct 02, 2017

This section provides the frequently asked questions on the following NetScaler MAS features. Click a feature name in the table below to view the list of FAQs for that feature.

<table>
<thead>
<tr>
<th>Analytics</th>
<th>Authentication</th>
<th>Configuration Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Management</td>
<td>Event Management</td>
<td>Instance Management</td>
</tr>
<tr>
<td>Stylebook</td>
<td>System Management</td>
<td></td>
</tr>
</tbody>
</table>

### Analytics

**How do I enable NetScaler MAS to monitor web-application and virtual-desktop traffic?**

Navigate to **Infrastructure > Instances**, and select the NetScaler instance on which you want to enable analytics. Select **Enable/Disable Insight** from the **Action** drop-down list. In the **Configure Insight** page that opens, select all the virtual servers on which you want to enable analytics, and click **Enable AppFlow**. For more details, see **How to Enable Analytics on Instances**.

**After I add the NetScaler instances, does NetScaler MAS automatically start collecting analytical information?**

No. You must first enable analytics on the virtual servers hosted in NetScaler instances that are managed by NetScaler MAS. For more details, see **How to Enable Analytics on Instances**.

**Should I access the individual NetScaler appliance for enabling analytics?**

No. All configuration is done from the NetScaler MAS user interface, which lists the virtual servers hosted on the specific NetScaler instance. For more details, see **How to Enable Analytics on Instances**.

**What are the types of virtual servers that can be listed on a NetScaler instance to enable analytics?**

Currently, the NetScaler MAS user interface lists the following virtual servers for enabling analytics:

- Load balancing virtual server
- Content switching virtual server
- VPN virtual server
- Cache redirection virtual server

**How do I attach an additional disk to NetScaler MAS?**

To attach an additional disk to NetScaler MAS:

1. Shut down the NetScaler MAS virtual machine.
2. In the hypervisor, attach an additional disk of the required disk size to NetScaler MAS virtual machine.
For example, for a NetScaler MAS virtual machine of 120 GB, if you want to increase its disk space to 200 GB, you then need to attach a disk space of 200 GB instead of 80 GB. Newly attached 200 GB of disk space will be used to store Database data, NetScaler MAS log files. The existing 120 GB disk space will be used to store core files, Operating system log files, and so on.

3. Start the NetScaler MAS virtual machine.

Authentication

What is load balancing of authentication requests?

The authentication-server load balancing feature enables NetScaler MAS to load balance the authentication requests that are directed to the external authentication servers. Load balancing the authentication servers ensures that the authentication load is split across multiple authentication servers and thus avoid an authentication server from being overloaded. You can create an authentication service to connect with and get user information from your existing external authentication server using the authentication protocols like LDAP, RADIUS, or TACACS.

Why do we need to cascade external authentication servers?

Cascaded external authentication servers provide uninterrupted authentication processing, allowing access to legitimate users if an authentication server fails. There is no limitation on which types of authentication servers you can cascade. You can have all RADIUS servers, or all LDAP servers, or a combination of RADIUS and LDAP servers.

How many external authentication servers can I cascade?

You can cascade up to 32 external authentication servers in NetScaler MAS.

Do I have an alternative when external authentication fails?

There could be a situation when external authentication completely fails, even when you have cascaded a number of servers. For example, the external servers could become unreachable, or a new user's credentials might not have been entered in any of the the external authentication servers. To prevent locking users out in such a situation, you can enable fallback local authentication. For more details, see Fallback Local Authentication.

What is fallback local authentication?

Fallback local authentication is an option to authenticate your users locally when external authentication fails. If external authentication fails, NetScaler MAS accesses the local user database to authenticate your users.

In NetScaler MAS, navigate to System > Authentication > Authentication Configuration. On this page, you can add multiple external authentication servers in a cascade, and you can select the Enable fallback local authentication option.

What is extraction of external user groups?

If you have added external servers for authenticating the users, you can import (extract) existing user groups into NetScaler MAS. You have to import user groups once and provide a group permission to a user group rather than importing individual users and giving them individual permissions. You do not have to recreate the users on NetScaler MAS.

Why do we need to assign group permissions?

When you are using the load balancing feature of NetScaler, you can integrate NetScaler MAS with external
authentication servers, and import user group information from the authentication servers. Log in to NetScaler MAS and manually create same group information in NetScaler MAS and assign permission to those groups. The user and user group permission is managed in NetScaler MAS and not in the external server. The users have different role-based access permissions on the external servers. Configure the same permissions for the users in NetScaler MAS also. Instead of configuring permissions individually for each user, you can configure a group-level permission so that the user-group members can access specific services on the load balanced virtual servers. The typical permissions that you can assign are permissions to manage NetScaler instances, NetScaler SDX instances, virtual servers, and so on, so that the users of that group can manage only those instances or virtual servers. You can later edit the permissions given to the users at the group level. You can even remove one or more user groups; other group users still function on NetScaler MAS.

Configuration Management

Can I perform configuration across multiple NetScaler instances simultaneously using NetScaler MAS?

Yes, you can use configuration jobs to perform configuration across multiple NetScaler instances.

What are configuration jobs on NetScaler MAS?

A job is a set of configuration commands that you can create and run on one or more managed instances. You can create jobs to make configuration changes across instances, replicate configurations on multiple instances on your network, and record-and-play configuration tasks using the NetScaler MAS GUI. You can also convert the recorded tasks into CLI commands.

You can use the Configuration Jobs feature of NetScaler MAS to create a configuration job, send email notifications, and check execution logs of the jobs created.

Can I schedule jobs using built-in templates in NetScaler MAS?

Yes, you can schedule a job by using the built-in template option. A job is a set of configuration commands that you can run on one or more managed instances. For example, you can use the built-in template option to schedule a job to configure syslog servers. You can choose to execute the job immediately, or schedule the job to be executed later.

You can save the configuration of a job that was previously created, and run the job again after modifying the commands, the parameters, the configuration source, and targeted instances. This is useful when the same set of commands has to be executed on a different instance, or when the job encounters an error and stops further execution.

Certificate Management

Does the deletion of SSL certificates from NetScaler MAS lead to deletion of certificates from NetScaler instances?

No

Event Management

How can I keep track of all the events that have been generated on my managed NetScaler instances using
NetScaler MAS?

As a network administrator, you can view details such as configuration changes, log on conditions, hardware failures, threshold violations, and entity state changes on your NetScaler instances, along with events and their severity on specific instances. You can use the NetScaler MAS events dashboard to view reports generated for critical event severity details on all your NetScaler instances.

What are event rules?

Using NetScaler MAS, you can configure rules to monitor specific events. Event Rules make it easier to monitor a large number of events generated across your NetScaler infrastructure.

You can filter a set of events by configuring rules with specific conditions and assigning actions to the rules. When the events generated meet the filter criteria in the rule, the action associated with the rule is executed.

The conditions for which you can create filters are severity, NetScaler instances, category, and failure objects. The actions you can assign to the events are sending an email notifications, forwarding SNMP traps from managed NetScaler instances to the NetScaler MAS, and sending an SMS notification.

Instance Management

What are data centers in NetScaler MAS?

A NetScaler MAS data center is a logical grouping of the NetScaler instances in a specific geographical location. Each server can monitor and manage several NetScaler instances within a data center. You can use the NetScaler MAS server to manage data such as syslog, application traffic flow, and SNMP traps from the managed instances. For more details on configuring data centers, see How to Configure Data Centers for Geomaps in NetScaler MAS.

What are the different Citrix Appliances that are supported by NetScaler MAS?

Instances are the Citrix appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler MAS. You must add these instances to the NetScaler MAS server. You can add the following Citrix appliances and virtual appliances to NetScaler MAS:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway
- NetScaler SD-WAN WO
- NetScaler SD-WAN EE

You can add instances either while setting up the NetScaler MAS server for the first time or at a later time.

What is an instance profile?

An instance profile is used by NetScaler MAS to access a particular instance.

An instance profile contains the user name and password for access to one or more instances. A default profile is available for each instance type. For example, the ns-root-profile is the default profile for NetScaler instances. It contains the
default NetScaler administrator credentials. When you change the credentials required for access to instances, you can define custom instance profiles for those instances.

**Can we add unlimited SD-WAN instances in NetScaler MAS? Can NetScaler MAS handle all scalar and vector counters for SD-WAN?**

Currently, there is no license limit on SD-WAN instances that can be added to NetScaler MAS. NetScaler MAS has a set of built-in reports that internally polls both scalar and vector counters.

**Can NetScaler MAS be installed on NetScaler SDX?**

No

**Stylebooks**

**Can stylebooks be used to configure different NetScaler instances running on different versions of the NetScaler software?**

Yes, you can use stylebooks to configure different NetScaler instances running on different versions if there is no discrepancy between the commands across different versions.

**When a stylebook is used to configure multiple NetScaler instances at the same time, and configuration of one NetScaler instance fails, what happens?**

If applying the configuration to a NetScaler instance fails, the configuration is not applied not any more instances, and already-applied configurations are rolled back.

**Do NetScaler backups made through NetScaler MAS include configurations applied through Stylebooks?**

Yes

**System Management**

**Can I assign a host name to my NetScaler MAS server?**

Yes, you can assign a host name to identify your NetScaler MAS server. To assign a host name, navigate to **System > System Administration > System Settings**, and click **Change Hostname**.

The host name is displayed on the Universal license for NetScaler MAS. For more information, see **How to Assign a Host Name to a NetScaler MAS Server**.

**Can I back up and restore my NetScaler MAS configuration?**

Yes, you can back up configuration files (NTP files and SSL certificates), system data, infrastructure and application data, and all your SNMP settings. If your NetScaler MAS ever becomes unstable, you can use the backed up files to restore your NetScaler MAS to a stable state.

To back up and restore your NetScaler MAS’s configuration, navigate to **System > Advanced Settings > Backup Files**, and click **Back Up** or **Restore** as the case may be. For more information, see **How to Back Up and Restore Configuration**.
NetScaler MAS.

Citrix recommends that you use this feature before performing an upgrade or for precautionary reasons.

What are Thresholds and Alerts on NetScaler MAS?

You can set thresholds and alerts to monitor the state of a NetScaler instance and monitor entities on managed instances. When the value of a counter exceeds the threshold, NetScaler MAS generates an alert to signify a performance-related issue. When the counter value returns to the clear value specified in the threshold, the event is cleared.

Can I generate a technical support file for NetScaler MAS?

Yes. Citrix recommends that you generate an archive of NetScaler MAS data and statistics before contacting technical support for debugging an issue. The archive is a TAR file that you can send to the technical support team.

You can generate a technical support file that contains debug logs, duration for which debug logs were collected, and distinct and diverse logs from the NetScaler MAS database.

To configure and send a technical support file, navigate to System > Diagnostics > Technical Support, and then, click Generate Technical Support File. For more information, see How to Generate a Tech Support File for NetScaler MAS.

What is syslog purging?

Syslog is a standard protocol for logging. Syslog enables isolation of the system that generates information and the system that stores the information. You can consolidate logging information and derive insights from the collected data. You can also configure syslog to log different types of events.

To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. You can specify the number of days after which all Generic Syslog data, AppFirewall data, and NetScaler Gateway data will be deleted from NetScaler MAS.

Can I configure NTP server on NetScaler MAS?

You can configure a Network Time Protocol (NTP) server in NetScaler MAS to synchronize the NetScaler MAS clock with the NTP server. Configuring an NTP server ensures that the NetScaler MAS clock has the same date and time settings as the other servers on the network.

To configure an NTP server, navigate to System > NTP Servers, and then click Add. For more information, see How to Configure NTP Server on NetScaler MAS.

From which version is the NetScaler MAS active-passive HA deployment supported?

The NetScaler MAS active-passive HA deployment mode is supported from NetScaler MAS version 11.1 build 54.14.

I had a NetScaler MAS active-active HA setup and had configured a NetScaler appliance with load balancing virtual server on it for unified GUI access. How do I update this configuration?

After you upgrade the NetScaler MAS HA pair to active-passive mode, you have to run the following command on the NetScaler appliance to update the load balancing configuration:

```
add lb monitor MAS_Monitor TCP-ECV -send "GET /mas_health HTTP/1.1\r\nAccept-Encoding: identity\r\nUser-Agent: NetScaler-Monitor\r\nConnection: close\r\n\" -recv "{"statuscode":0,
```
Can I configure load balancing of the NetScaler MAS HA pair on a NetScaler Instance using port 443?

No, you cannot configure load balancing of the NetScaler MAS HA pair on a NetScaler Instance using port 443.

When you configure the http-ecv and https-ecv monitors on NetScaler, it does not monitor the NetScaler MAS HA nodes correctly.

Can a NetScaler MAS server backup file be used to restore the configuration of another NetScaler MAS server?

Yes

After NetScaler MAS backs up a NetScaler instance, can that backup file be used to restore the configuration of another NetScaler instance through NetScaler MAS?

Yes. Download the NetScaler MAS backup file, upload it into another NetScaler instance's backup repository, and restore that instance. Make sure that the network information and authentication information do not conflict. For example, check for IP-address or port conflicts, mismatched password profiles. Also make sure that the restored VPX instance has the same NSIP address and NetScaler license as the one that was backed up.

Before restoring an instance in a high availability pair, make sure the IP addresses and state (primary or secondary) stored in the backup file match those of the original HA configuration. Also verify that the new primary and secondary have the same type of NetScaler license.

Can we force NetScaler MAS to use a SNIP address to communicate with the NetScaler instances, instead of using the NSIP address of the NetScaler MAS server?

Yes, you can add a SNIP address (with management enabled) in NetScaler MAS for communication with NetScaler instances.

When I back up NetScaler Instances in NetScaler MAS, is the result a full back-up or a basic back-up?

Backups of NetScaler instances by NetScaler MAS are full backups.

Is there a troubleshooting guide for NetScaler MAS?

Yes. See https://support.citrix.com/article/CTX224502.

How are NetScaler instances managed when a NetScaler MAS HA failover occurs?

If the heartbeat and SSH based check fails, the primary node is considered to be down and the secondary node takes over as the primary node. All the NetScaler instances are updated with the latest primary node details as their SNMP trap destination by default.

The new primary (active) NetScaler MAS node checks to determine whether the previously active node was configured as AppFlow collector or syslog server, if it was, the new primary adds the AppFlow collector or syslog server details to the information sent to the instances.

For syslog it replaces the old server details.

What happens when the NetScaler MAS HA node that went down comes back up?

After returning to service, the NetScaler MAS node remains passive unless the active node fails over.
How are NetScaler instances distributed across NetScaler MAS HA nodes?

All the NetScaler instances are managed by the primary NetScaler MAS node.

How are virtual server licenses managed in case of NetScaler MAS HA failover?

If the NetScaler MAS primary node on which vServer licenses are applied goes down, the new primary node manages the vServer licenses for a grace period of 30 days. The licenses have to be reapplied on the new primary by the end of the grace period. For alternatives, contact Citrix support.

Is a load balancer mandatory for a NetScaler MAS HA setup?

No, but if there is no load balancer, NetScaler MAS nodes must be accessed through their own IP addresses. The passive node is marked with the tag “Passive,” and Citrix recommends not to create any configurations on the passive node.

Does NetScaler MAS support an external database?

No

Can a NetScaler instance that is being managed by NetScaler MAS be used as a Load balancer for NetScaler MAS HA?

Yes

What data is synchronized between NetScaler MAS HA nodes?

Complete NetScaler MAS database is synchronized, and the following folders are synchronized:

- /var/mps/tenants/root/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/
- /var/mps/sdwanww_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/
- /var/mps/ssl_keys/
- /mpsconfig/ssl/
- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/
Release Notes

May 02, 2018

NetScaler Management and Analytics System (MAS) is a centralized network and application management, analytics, and orchestration solution. NetScaler MAS simplifies operations by providing administrators with enterprise-wide visibility and automating management jobs that need to be executed across multiple instances. It also provides real-time analytics data to help administrators identify and address application performance and security issues across the infrastructure.

The release notes describe the new features, enhancements to existing features, and the known issues in a build. The release notes for the 11.1 release includes the following sections:

- **What’s New**: The new features and enhancements to existing features released in a build.
- **Known Issues**: The issues that exist in a build, and their workarounds, wherever applicable.
- **Fixed Issues**: The issues addressed in a build.

To view the complete release notes document, click the following link.

<table>
<thead>
<tr>
<th>Release Notes for Build 48.10 of NetScaler MAS 11.1 Release</th>
<th>Published: August 11, 2016</th>
<th>Release Notes Version: 1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Notes for Build 49.16 of NetScaler MAS 11.1 Release</td>
<td>Published: September 28, 2016</td>
<td>Release Notes Version: 1.0</td>
</tr>
<tr>
<td>Release Notes for Build 50.10 of NetScaler MAS 11.1 Release</td>
<td>Published: October 28, 2016</td>
<td>Release Notes Version: 1.0</td>
</tr>
<tr>
<td>Release Notes for Build 51.26 of NetScaler MAS 11.1 Release</td>
<td>Published: February 03, 2017</td>
<td>Release Notes Version: 1.0</td>
</tr>
<tr>
<td>Release Notes for Build 52.15 of NetScaler MAS 11.1 Release</td>
<td>Published: March 17, 2017</td>
<td>Release Notes Version: 1.0</td>
</tr>
<tr>
<td>Release Notes for Build 53.11 of NetScaler MAS 11.1 Release</td>
<td>Published: April 12, 2017</td>
<td>Release Notes Version: 1.0</td>
</tr>
<tr>
<td>Release Notes for Build 54.14 of NetScaler MAS 11.1 Release</td>
<td>Published: June 29, 2017</td>
<td>Release Notes Version: 1.0</td>
</tr>
<tr>
<td>Release Notes for Build 55.10 of NetScaler MAS 11.1 Release</td>
<td>Published: August 09, 2017</td>
<td>Release Notes Version: 1.0</td>
</tr>
<tr>
<td>Release Notes for Build 56.15 of NetScaler MAS 11.1 Release</td>
<td>Published: November 17, 2017</td>
<td>Release Notes Version: 1.0</td>
</tr>
<tr>
<td>Release Notes for Build 57.11 of NetScaler MAS 11.1 Release</td>
<td>Published: January 25, 2018</td>
<td>Release Notes Version: 1.0</td>
</tr>
<tr>
<td>Release Notes for Build 58.13 of NetScaler MAS 11.1 Release</td>
<td>Published: May 02, 2018</td>
<td>Release Notes Version: 1.0</td>
</tr>
</tbody>
</table>
Note

These release notes do not document security related fixes. For a list of security related fixes and advisories, see the Citrix security bulletin.
### Overview

NetScaler Management and Analytics System (MAS) is a centralized management solution that simplifies operations by providing administrators with enterprise-wide visibility and automating management jobs that need to be executed across multiple instances. You can manage and monitor Citrix application networking products that include Citrix NetScaler MPX, Citrix NetScaler VPX, Citrix NetScaler Gateway, Citrix NetScaler SDX, Citrix NetScaler CPX, and Citrix NetScaler SD-WAN. You can use NetScaler MAS to manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console.

NetScaler MAS, a virtual appliance that runs on Citrix XenServer, VMware ESXi, and Linux KVM also addresses the application visibility challenge by collecting detailed information about web-application and virtual-desktop traffic, such as flow, user-session-level information, web page performance data, and database information flowing through the NetScaler appliances, NetScaler Gateway appliances, or NetScaler SD-WAN appliances at your site and providing actionable reports. It enables IT administrators to troubleshoot as well as proactively monitor customer issues in matter of minutes.

### Features

NetScaler MAS provides the following features:

<table>
<thead>
<tr>
<th>Features</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Applications</strong></td>
<td></td>
</tr>
<tr>
<td>Application Monitoring</td>
<td>Enables you to monitor the applications in your deployment based on the virtual server status.</td>
</tr>
<tr>
<td>Application Groups</td>
<td>Enables you to define applications based on the collection of virtual servers in NetScaler MAS. You can create an application group of Load Balancing, Content Switching, and GSLB virtual servers.</td>
</tr>
<tr>
<td>Application Configuration</td>
<td>Enables you to optimize your applications based on pre-defined configuration templates.</td>
</tr>
<tr>
<td><strong>Infrastructure</strong></td>
<td></td>
</tr>
<tr>
<td>Instances</td>
<td>Enables you to manage the NetScaler ADC, NetScaler Gateway, and NetScaler SD-WAN instances.</td>
</tr>
<tr>
<td><strong>Note:</strong> Currently NetScaler MAS supports only the WAN Optimization functionality for NetScaler SD-WAN instances.</td>
<td></td>
</tr>
<tr>
<td>Instance Groups</td>
<td>Enables you to group your instances as follows:</td>
</tr>
</tbody>
</table>
- Static Group: Allow you to define a device group that you can use in different tasks such as, Configuration Jobs and so on.
- Private IP-block: Enables you to group your instances based on geographical locations.

<table>
<thead>
<tr>
<th>Events</th>
<th>Provides the status of the instances managed in NetScaler MAS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Certificates</td>
<td>Provides certificate management.</td>
</tr>
<tr>
<td>Configuration Jobs</td>
<td>Enable you to configure instances in multiple ways.</td>
</tr>
<tr>
<td>Configuration Audit</td>
<td>Enables you to monitor and identify anomaly across the configurations in your instances.</td>
</tr>
<tr>
<td></td>
<td>- Configuration Advice: Allows you to identify configuration anomaly.</td>
</tr>
<tr>
<td></td>
<td>- Audit template: Allows you to monitor the changes across a specific configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Insight</td>
</tr>
<tr>
<td>HDX Insight</td>
</tr>
<tr>
<td>Gateway Insight</td>
</tr>
<tr>
<td>Security Insight</td>
</tr>
<tr>
<td>Network Reporting</td>
</tr>
<tr>
<td>Orchestration</td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Cloud Orchestration</td>
</tr>
<tr>
<td>Container Orchestration</td>
</tr>
</tbody>
</table>
The NetScaler MAS database is integrated with the server, and the server manages all the key processes, such as data collection, NITRO calls. In its data store, the server stores an inventory of instance details, such as host name, software version, running and saved configuration, certificate details, entities configured on the instance, and so on. A single server deployment is suitable if you want to process small amounts of traffic or store data for a limited time.

Currently, NetScaler MAS supports two types of NetScaler MAS server deployments: single server and high availability.

This document includes the following information:

- NetScaler MAS Architecture
- How NetScaler MAS Communicates with Managed Instances
- How NetScaler MAS Discovers Instances

### NetScaler MAS Architecture

The following image shows the different subsystems within NetScaler MAS and how communication happens between the NetScaler MAS server and managed instances.

![NetScaler MAS Architecture Diagram](https://docs.citrix.com)

The Service subsystem in NetScaler MAS acts as a web server that handles HTTP(s) requests and responses that are sent to subsystems within NetScaler MAS from the GUI or API, using ports 80 and 443. These requests are sent to the subsystems over the message bus (Message Processing System) by using the IPC (Inter-process Communication) mechanism. A request is sent to the Control subsystem, which either processes the information or sends it to the
appropriate subsystem. Each of the other subsystems—Inventory, Stylebooks, Data Collector, Configuration, AppFlow Decoder, AppFlow Analytics, Performance, Events, Entities, SLA Manager, Provisioner, and Journal—has a specific role.

Instance plug-ins are shared libraries that are unique to each instance type supported by NetScaler MAS. Information is transferred between NetScaler MAS and managed instances by using NITRO calls, or through the SNMP, Secure Shell (SSH), or Secure Copy (SCP) protocol. This information is then processed and stored in the internal database (Data Store).

How NetScaler MAS Communicates with Managed Instances

NetScaler MAS polls managed instances to collect information. The following list describes the various kinds of polling that occur between NetScaler MAS and managed instances, the protocols used to collect this information, and whether the polling intervals can be configured on the NetScaler MAS server.

- **Instance Polling.** By default, every minute, NetScaler MAS polls managed NetScaler instances to collect statistical information such as state, HTTP requests per second, CPU usage, memory usage, and throughput. This data collection uses NITRO calls. An instance is pinged if the NITRO call fails. This polling interval is not configurable.

- **Inventory Polling.** Every 30 minutes, inventory such as build version, system information, licensed features, and modes is collected from managed instances and updated in the NetScaler MAS database. This communication between NetScaler MAS and managed instances uses NITRO calls (nsconfig, version, route, stat, nsversion, nsnode and so on) and the Secure Shell (SSH) protocol. You can also rediscover instances if you want to collect inventory on a need basis. This polling interval is not configurable.

- **Performance Data Collection.** By default, every 5 minutes, performance data collection for network reporting is done by using NITRO calls. This retrieves instance statistics such as counter information and aggregates them on the basis of per minute, per hour, per day, or per week. You can view this aggregated data in pre-defined reports. This polling interval is not configurable.

- **Instance Backup Polling.** Every 12 hours, NetScaler MAS backs up the current state of your managed NetScaler instances. This backup is done by using NITRO calls, Secure Shell (SSH) and Secure Copy (SCP) protocols. You can configure this polling interval by navigating to **System > System Administration > Policy Administration > Instance Backup Settings**.

- **Configuration Audits Polling.** Every 10 hours, auditing is performed to look for configuration changes that occur on NetScaler instances (for example, running vs. saved configuration). This enables you to see the difference between various revisions of NetScaler configuration files (ns.conf) and across various NetScaler version changes. NetScaler MAS collects configuration audits by using the Secure Shell (SSH) and Secure Copy (SCP) protocols. Running and saved configuration for auditing can be collected on demand by using NITRO calls. You can configure this polling interval for configuration audits by navigating to **Infrastructure > Configuration Audit** and clicking on the graph representing the NetScaler Configuration status. On the **Audit Reports** page, in the **Action** drop-down list, select **Configure Polling Interval**.
SSL Certificates Polling. Every 24 hours, NetScaler MAS polls SSL certificates by using NITRO calls and the Secure Copy (SCP) protocol. You can configure this polling interval for SSL certificates by navigating to Infrastructure > SSL Dashboard and clicking on the graph representing NetScaler SSL certificates. On the SSL Certificates page, in the Action drop-down list, click Configure Polling Interval.

Entity Polling. Every 30 minutes, entities are polled by NetScaler MAS by using NITRO calls. An entity is either a policy, virtual server, service, or action attached to a NetScaler instance. While this poling interval is configurable, you cannot set it to less than 10 minutes. To configure it, navigate to Applications > Dashboard > Settings > Configure Polling Interval for Entities. You can also poll the entities configuration when required by navigating to Applications > Dashboard > Load Balancing, select the appropriate entities, and click Poll Now.
Analytics. By default, every minute, the decoder collects and decodes the data received from all managed NetScaler instances and writes it to the internal database. This polling interval is not configurable.

In addition to polling, events generated by managed NetScaler instances are received by NetScaler MAS through SNMP traps sent to the instances. For example, an event is generated when there is a system failure or change in configuration.

During instance backup, SSL files, CA certificate files, NetScaler templates, database information, and so on are downloaded to NetScaler MAS. During a configuration audit, ns.conf files are downloaded and stored in the file system. All information collected from managed NetScaler instances are stored internally within the database.

How NetScaler MAS Discovers Instances

When you add an instance to NetScaler MAS, it implicitly adds itself as a trap destination for the instance and collects inventory of the instance.

The following diagram describes how NetScaler MAS implicitly discovers and adds instances.

As shown in the diagram, the following steps are performed implicitly by NetScaler MAS.

1) NetScaler MAS sends an Internet Control Message Protocol (ICMP) ping to locate the instance. Then, it uses the instance profile details to log on to the instance. Using a NetScaler NITRO call, NetScaler MAS retrieves the license
information of the instance. On the basis of the licensing information received, it determines whether the instance is a NetScaler instance and the type of NetScaler platform (for example, NetScaler MPX, NetScaler VPX, NetScaler SDX, or NetScaler Gateway). On successful detection of the NetScaler instance, it is added to the NetScaler MAS internal database.

For NetScaler SD-WAN instances, NetScaler MAS does not detect the instance by using licensing information. Instead, after locating the instance by using ICMP ping, it sends a NITRO request to the instance to check for the instance type and version.

This step might fail if the instance profile does not include the correct credentials. For NetScaler MPX, VPX, SDX, and NetScaler Gateway instances, this step might also fail if the licenses are not applied to the instance.

2) NetScaler MAS adds its IP address to the list of trap destinations on the instance. This allows NetScaler MAS to receive traps generated on the NetScaler instance.

This step might fail if the number of trap destinations on the instance exceeds the maximum limit of trap destinations. The maximum limit on NetScaler instances is 20.

For SD-WAN instances, NetScaler MAS adds its IP address as the SNMP manager on the instance.

3) NetScaler MAS collects inventory from the instance by sending a NITRO request. It collects instance details such as host name, software version, running and saved configuration, certificate details, entities configured on the instance, and so on.

This step might fail because of network or firewall issues.

For more information about adding instances, see Adding an Instance to NetScaler MAS.
Licensing

Aug 28, 2017

A NetScaler Management and Analytics System (NetScaler MAS) requires a verified NetScaler MAS license to manage and monitor Citrix NetScaler instances.

Instances

You can add any number of NetScaler instances in NetScaler MAS. But if you want to monitor and manage the virtual servers configured on the added instances, you might have to upgrade your licenses on NetScaler MAS.

Virtual Server Limitation

NetScaler MAS, by default can manage and monitor 30 virtual servers configured on your NetScaler instances.

<table>
<thead>
<tr>
<th>Licenses</th>
<th>System Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Licenses</td>
<td></td>
</tr>
<tr>
<td>Allowed Virtual Servers</td>
<td>Total Managed Virtual Servers</td>
</tr>
<tr>
<td>30</td>
<td>30</td>
</tr>
</tbody>
</table>

Licenses for additional virtual servers are available in virtual server packs of 10. You can obtain a valid license and add the licenses on the NetScaler MAS appliances through the NetScaler MAS GUI.

High Availability

Licenses are node locked to the Netscaler MAS servers, which means that you have to use a specific NetScaler MAS server's IP address for all the license-related operations on a high availability pair. When licensing, select a NetScaler MAS server that will be in charge of licensing, and apply all future licenses on that server.

Note: You need only one license file for installing the licenses to the NetScaler MAS high availability pair.

When fail-over occurs, the other node will maintain the licensing for a grace period of 30 days.

Orchestration

The Orchestration module is independent of licensing and is always available.

Upgrading the Virtual Server Licenses

You can upgrade the licensing on NetScaler MAS to monitor and manage more virtual servers hosted on the NetScaler appliances.

To upgrade your appliance licenses

1. In a web browser, type the IP address of the NetScaler Management and Analytics System (for example, http://192.168.100.1).

2. In User Name and Password, enter the administrator credentials.

3. On the Configuration tab, navigate to Infrastructure > Licenses > Settings.
4. In the details pane, go to License Files, and select one of the following options:

- **Upload license files from a local computer** - If a license is already present on your local computer, click **Browse** and select the license file (.lic) that you want to use to allocate your licenses. Click **Finish**.

- **Use License Activation Code** - Citrix emails the LAC for the license that you purchased. Enter the LAC in the text box and then click **Get Licenses**.

**Note**

If you select this option, the NetScaler Management and Analytics System must be connected to the Internet, or a proxy server must be available.

4. You can add more licenses from the License Settings page at any time.

**Verification**

You can verify the licenses installed on your NetScaler MAS by navigating to Infrastructure > Licenses > System
Licensing the Virtual Servers

You can select the virtual servers to manage and monitor through MAS. Earlier, NetScaler MAS randomly allocated licenses to the virtual servers discovered in NetScaler MAS.

If the total number of virtual servers hosted by the discovered NetScaler Instances is lower than the number of installed Virtual server licenses, NetScaler MAS licenses all the virtual servers.

Points to Note

- By default, NetScaler MAS automatically licenses the virtual servers randomly after each virtual server poll cycle.
- If the total number of virtual servers discovered in your NetScaler MAS is lower than the number of installed virtual server licenses, NetScaler MAS, by default, licenses all the virtual servers.
- To select the virtual servers manually, or to restrict licensing to limited virtual servers, you have to first disable auto licensing the virtual servers, and then select the virtual servers you want to manage.
- NetScaler MAS donot license the non-addressable virtual servers. to manage them, you need to manually license them.

To manage licensed virtual servers

1. Log on to NetScaler MAS using a supported web browser.
2. Navigate to Networks > Licenses > System Licenses.

The dashboard displays the virtual server licenses available, the managed virtual servers along with the virtual server type.

3. In the License Settings section, disable Auto-select Virtual servers.

4. Click Select Virtual Servers.

5. In the Choose Virtual Servers screen, select the type of virtual servers by clicking the relevant tab.
6. Select the virtual servers to be licensed from the available list.

7. Click **Next** to move to the other virtual servers' tab, or click **Save and Exit** to license the selected virtual servers.

---

**Expiry Checks for Virtual Server Licenses**

You can now view the status of and set alerts for virtual server license expiry in NetScaler MAS.

**To view the status of the licenses**

1. Navigate to **Infrastructure > Licenses > System Licenses**.

2. In the **License Expiry Information** section, you can find the details of the licenses that are going to expire:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Count</th>
<th>Day to expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No items</td>
<td></td>
</tr>
</tbody>
</table>

- **Feature**: Type of license that is going to expire.
- **Count**: Number of virtual servers or instances that will be affected.
● **Days to expiry:** Number of days remaining before expiry.

**To configure the notification settings of licenses**

1. Navigate to **Infrastructure > Licenses > Settings.**

2. In the **Notification Settings** section, click the pencil icon and edit the parameters.

![Notification Settings](image)

- **Email profile:** Email profile or distribution list for sending notifications when licenses reach threshold, or going to expire.
- **SMS Profile:** SMS profile or distribution list for sending notifications when licenses reach threshold, or going to expire.
- **Alert Threshold:** Set percentage of pooled licenses to notify administrators by Email or SMS.
- **License Expiry Threshold:** Number of days before the number of licenses determined by Alert Threshold expire.
Before You Begin

Before you install NetScaler MAS, you must understand the software requirements, browser requirements, port information, license information, and limitations.

This topic includes the following details:

- NetScaler MAS Features Supported by NetScaler Versions
- NetScaler MAS Features Supported by CloudBridge and NetScaler SD-WAN WO Versions
- NetScaler MAS Features Supported by XenApp and XenDesktop Versions
- Thin Clients Supported for HDX Insight
- Inter-Operability Matrix of NetScaler SD-WAN Platform Editions and NetScaler MAS Features
- Thin Clients Supported for NetScaler SD-WAN
- Operating Systems and Receiver Versions
- Supported Browsers
- Ports
- NetScaler Instance License Information Required for NetScaler MAS Analytics
- Limitation

### NetScaler MAS Features Supported by NetScaler Versions

NetScaler MAS is compatible with the following products.

<table>
<thead>
<tr>
<th>NetScaler MAS Feature</th>
<th>NetScaler Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>StyleBooks</td>
<td>10.5 and later</td>
</tr>
<tr>
<td>OpenStack/CloudStack Support</td>
<td>• 10.5 and later</td>
</tr>
<tr>
<td></td>
<td>• 11.0 and later - If a partition is required</td>
</tr>
<tr>
<td></td>
<td>• 11.1 and later - If partition on shared virtual LAN is required</td>
</tr>
<tr>
<td>NSX Support</td>
<td>11.1 Build 47.14 and later (VPX)</td>
</tr>
<tr>
<td>Mesos/Marathon Support</td>
<td>10.5 and later</td>
</tr>
<tr>
<td>Backup/Restore</td>
<td>• 10.1 and later</td>
</tr>
<tr>
<td></td>
<td>• For SDX 11.0 and later</td>
</tr>
<tr>
<td>Monitoring/Reporting &amp; Configuration using Jobs</td>
<td>10.1 and later</td>
</tr>
<tr>
<td>Analytics</td>
<td></td>
</tr>
<tr>
<td>Web Insight</td>
<td>10.1 and later</td>
</tr>
</tbody>
</table>
### NetScaler MAS Features Supported by CloudBridge and NetScaler SD-WAN WO Versions

<table>
<thead>
<tr>
<th>NetScaler MAS Feature</th>
<th>CloudBridge / NetScaler SD-WAN WANOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring/Reporting &amp; Configuration using Jobs</td>
<td>CloudBridge 7.4.0 and later</td>
</tr>
<tr>
<td>Analytics</td>
<td></td>
</tr>
<tr>
<td>HDX Insight</td>
<td>CloudBridge 7.4.0 and later</td>
</tr>
<tr>
<td>WAN Insight</td>
<td>CloudBridge 7.4.0 and later</td>
</tr>
</tbody>
</table>

### NetScaler MAS Features Supported by XenApp and XenDesktop Versions

<table>
<thead>
<tr>
<th>NetScaler MAS Feature</th>
<th>XenApp / XenDesktop Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDX Insight</td>
<td>XenAPP 6.5, build 6682 with HRP01</td>
</tr>
<tr>
<td>HDX Insight</td>
<td>XenDesktop 7.0, build 3018</td>
</tr>
</tbody>
</table>

### Note


NetScaler MAS can generate reports for applications that are published on XenApp or XenDesktop and accessed through Citrix Receiver. However, this capability depends on the operating system on which Receiver is installed. Currently, a NetScaler ADC does not parse ICA traffic for applications or desktops that are accessed through Citrix Receiver running on IOS, or Android operating systems.

**Thin Clients Supported for HDX Insight**

The following Thin Clients support HDX Insight for NetScaler MAS:

- WYSE Windows based Thin Clients
- WYSE Linux based Thin Clients
- WYSE ThinOS based Thin Clients
- 10Zig Ubuntu based Thin Clients
Inter-Operability Matrix of NetScaler SD-WAN Platform Editions and NetScaler MAS Features

<table>
<thead>
<tr>
<th>Platform Editions</th>
<th>Discovery</th>
<th>Configuration</th>
<th>Monitoring</th>
<th>Reporting</th>
<th>Event Management (SNMP Traps)</th>
<th>HDX Insight and WAN Insight Analytics</th>
<th>Multi-Hop Insight</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler SD-WAN WANOP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NetScaler SD-WAN Enterprise</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Thin Clients Supported for NetScaler SD-WAN

NetScaler MAS supports the following thin clients for monitoring NetScaler SD-WAN deployments:

- Dell Wyse WTOS Model R10L Rx0L Thin Client
- NComputing N400
- Dell Wyse WTOS Model CX0 C00X Xenith
- Dell Wyse WTOS Model TX0 T00X Xenith2
- Dell Wyse WTOS Model CX0 C10LE
- Dell Wyse WTOS Model R00LX Rx0L HDX Thin Client
- Dell Wyse Enhanced Suse Linux Enterprise, Model Dx0D, D50D
- Dell Wyse ZX0 290D7 (WES7) Thin Client

Operating Systems and Receiver Versions

The following table lists the operating systems supported by NetScaler MAS, and the Citrix Receiver versions currently supported with each system:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Receiver Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>4.0 Standard Edition</td>
</tr>
<tr>
<td>Linux</td>
<td>13.0.265571 and later</td>
</tr>
<tr>
<td>Mac</td>
<td>11.8, build 238301 and later</td>
</tr>
<tr>
<td>HTML5</td>
<td>1.5*</td>
</tr>
<tr>
<td>ChromeApp</td>
<td>1.5*</td>
</tr>
</tbody>
</table>

* Applicable with CloudBridge release 7.4 and later.

Supported Browsers

The following table lists the web browsers supported by NetScaler MAS:
<table>
<thead>
<tr>
<th>Web Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>11.0 and later</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>Chrome 19 and later</td>
</tr>
<tr>
<td>Safari</td>
<td>Safari 5.1.1 and later</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Firefox 3.6.25 and later</td>
</tr>
</tbody>
</table>

**Ports**

NetScaler MAS uses the NetScaler ADC's NetScaler IP (NSIP) address to communicate with the ADC. For communication purposes, the following ports must be open between the NetScaler ADC and NetScaler MAS.

<table>
<thead>
<tr>
<th>Type</th>
<th>Port</th>
<th>Details</th>
</tr>
</thead>
</table>
| TCP  | 80/443 | - For NITRO communication from NetScaler MAS to NetScaler or CloudBridge instance.  
|      |        |   - 443 - For NITRO communication between NetScaler MAS servers in high availability mode. |
| TCP  | 22     | - For SSH communication from NetScaler MAS to NetScaler or CloudBridge instance.  
<p>|      |        |   - For synchronization between NetScaler MAS servers deployed in high availability mode. |
| UDP  | 4739   | For AppFlow communication from NetScaler or CloudBridge instance to NetScaler MAS. |
| ICMP | No reserved port | To detect network reachability between NetScaler MAS and NetScaler instances, SD WAN instances, or the secondary NetScaler MAS server deployed in high availability mode. |
| SNMP | 161, 162 | To receive SNMP events from NetScaler instance to NetScaler MAS. |
| Syslog | 514     | To receive syslog messages in NetScaler MAS from NetScaler or CloudBridge instance. |
| TCP  | 25     | To send SMTP notifications from NetScaler MAS to users. |
| TCP  | 389/636 | Default port for authentication protocol. For communication between NetScaler MAS and LDAP external authentication server. |
| UDP  | 123    | Default NTP server port for synchronizing with multiple time sources. |
| RADIUS | 1812   | Default port for authentication protocol. For communication between NetScaler MAS and RADIUS external authentication server. |
| TACACS | 49     | Default port for authentication protocol. For communication between NetScaler MAS and TACACS external authentication server. |
| TCP  | 5557   | For logstream communication from NetScaler to NetScaler MAS. |</p>
<table>
<thead>
<tr>
<th>Type</th>
<th>Port</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>27000</td>
<td>License port for communication between NetScaler MAS license server and CPX instance.</td>
</tr>
<tr>
<td>TCP</td>
<td>7279</td>
<td>Citrix vendor daemon port</td>
</tr>
</tbody>
</table>

### NetScaler Instance License Information Required for NetScaler MAS Analytics

The data collected by NetScaler MAS depends on the version and licenses of the NetScaler instances being monitored.

### HDX Insight

HDX Insight reports are displayed only for NetScaler Platinum and Enterprise appliances running release 10.1, 10.5, 11.0, and 11.1.

<table>
<thead>
<tr>
<th>License/Duration</th>
<th>5 minutes</th>
<th>1 Hour</th>
<th>1 Day</th>
<th>1 Week</th>
<th>&gt; 1 Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Enterprise</td>
<td>✔</td>
<td>✔</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Platinum</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

### Limitation

NetScaler MAS supports IPv6 address to access the GUI for Management purposes only.
Single Server Deployment

Jun 26, 2016

In a NetScaler MAS single server deployment, the database is integrated with the server and a single server processes all the traffic.

To manage and monitor applications and the network infrastructure, you first install NetScaler MAS on one of the hypervisors and then add instances to the NetScaler MAS inventory. To view syslog, SNMP, and analytics data on NetScaler MAS, you have to configure these on each instance.

NetScaler MAS is a virtual appliance that must be deployed either on a Citrix XenServer server, VMware ESX server, or Microsoft Hyper-V.

This document includes the following details:

- Installing NetScaler MAS on Citrix XenServer
- Installing NetScaler MAS on Microsoft Hyper-V
- Installing NetScaler MAS on VMware ESXi
- Installing NetScaler MAS on Linux-KVM
Installing NetScaler MAS on Citrix XenServer

Sep 04, 2017

To install NetScaler MAS on Citrix XenServer, you must first download the NetScaler MAS .xva image file to your local computer. You must then use Citrix XenCenter to perform the NetScaler MAS installation.

Prerequisites

Before installing NetScaler MAS, verify that the following requirements have been met:

- XenServer version 5.6 or later is installed on hardware that meets the minimum requirements.
- XenCenter is installed on a management workstation that meets the minimum requirements. You have to use XenCenter to install NetScaler MAS on XenServer.
- You have downloaded the NetScaler MAS .XVA image file.

XenServer Requirements for NetScaler MAS

The following table lists the virtual computing resources that XenServer must provide for each NetScaler MAS virtual appliance.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>32 GB&lt;br&gt;Note: The default value is 8 GB. Citrix recommends that you increase the default value to 32 GB for better performance.</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>8 CPUs&lt;br&gt;Note: The default is 2 CPUs. Citrix recommends that you increase the default value to 8 CPUs for better performance.</td>
</tr>
<tr>
<td>Storage space</td>
<td>The default value is 120 GB. Actual storage requirement will depend on NetScaler MAS sizing estimation. If your NetScaler MAS storage requirement exceeds 120 GB, you have to attach an additional disk. Note that you can add only one additional disk. Citrix recommends you to estimate storage and attach additional disk at the time of initial deployment. For more information, see How to Attach an Additional Disk to NetScaler MAS.</td>
</tr>
<tr>
<td>Virtual Network Interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>1 Gbps or 100 Mbps</td>
</tr>
</tbody>
</table>

XenCenter System Requirements

XenCenter is a Windows client application. It cannot run on the same machine as the XenServer host. The following table describes the minimum system requirements.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>Requirement</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows 7, Windows XP, Windows Server 2003, or Windows Vista</td>
</tr>
<tr>
<td>.NET framework</td>
<td>Version 2.0 or later</td>
</tr>
<tr>
<td>CPU</td>
<td>750 megahertz (MHz), Recommended: 1 gigahertz (GHz) or faster</td>
</tr>
<tr>
<td>RAM</td>
<td>1 GB, Recommended: 2 GB</td>
</tr>
<tr>
<td>Network Interface Card</td>
<td>100 megabits per second (Mbps) or faster NIC</td>
</tr>
</tbody>
</table>

Installing NetScaler Management and Analytics System

1. Import the XVA image file to your XenServer, and from the **Console** tab configure the initial network configuration options, as shown in the figure below.

![NetScaler MAS initial network configuration](image)

2. After specifying the required IP addresses, select the deployment type as **NetScaler MAS Server**. If you do not select any option, by default, it is deployed as a server.

3. Type **Yes** to deploy NetScaler MAS as a standalone deployment.

4. Type **Yes** to restart the NetScaler MAS server.

**Note**

After you install NetScaler MAS, you can update the initial configuration settings at a later time.

To update the initial configuration in the NetScaler MAS, type **networkconfig** in the NetScaler MAS console. The console displays the NetScaler MAS initial network configuration options. You can then update the following parameters on the
console:

- Host name of NetScaler MAS
- NetScaler MAS IPv4 address
- Netmask
- Gateway IPv4 address
- DNS IPv4 address

Verification

After the server is installed, you can access the graphical user interface (GUI) by typing the IP address of the NetScaler MAS server in the address bar of your browser. The default administrator credentials to log on to the server are nsroot/nsroot.

The browser displays the NetScaler MAS configuration utility.
Installing NetScaler MAS on Microsoft Hyper-V

Sep 04, 2017

To install NetScaler MAS on Microsoft Hyper-V, you must first download the NetScaler MAS image file to your local computer. Also, make sure that your system has the hardware virtualization extensions, and verify that the CPU virtualization extensions are available.

Prerequisites

Before installing the NetScaler MAS virtual appliance, verify that the following requirements have been met:

- Microsoft Hyper-V version 6.2 or later is installed on hardware that meets the minimum requirements.
- Install Microsoft Hyper-V Manager on a management workstation that meets the minimum system requirements.
- You have downloaded the NetScaler MAS image file.

**Microsoft Hyper-V Requirements for NetScaler MAS**

The following table lists the virtual computing resources that Microsoft Hyper-V must provide for each NetScaler MAS virtual appliance.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>32 GB&lt;br&gt;Note: The default value is 8 GB. Citrix recommends that you increase the default value to 32 GB for better performance.</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>8 CPUs&lt;br&gt;Note: The default is 2 CPUs. Citrix recommends that you increase the default value to 8 CPUs for better performance.</td>
</tr>
<tr>
<td>Storage space</td>
<td>The default value is 120 GB. Actual storage requirement will depend on NetScaler MAS sizing estimation. If your NetScaler MAS storage requirement exceeds 120 GB, you have to attach an additional disk. Note that you can add only one additional disk. Citrix recommends you to estimate storage and attach additional disk at the time of initial deployment. For more information, see <a href="#">How to Attach an Additional Disk to NetScaler MAS</a>.</td>
</tr>
<tr>
<td>Virtual Network Interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>1 Gbps or 100 Mbps</td>
</tr>
</tbody>
</table>

**Microsoft Hyper-V System Requirements**

Microsoft Hyper-V is a Windows client application. The following table describes the minimum system requirements.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td>Component</td>
<td>Requirement</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>CPU</td>
<td>750 megahertz (MHz), Recommended: 1 gigahertz (GHz) or faster</td>
</tr>
<tr>
<td>RAM</td>
<td>1 GB, Recommended: 2 GB</td>
</tr>
<tr>
<td>Network Interface Card</td>
<td>100 megabits per second (Mbps) or faster NIC</td>
</tr>
</tbody>
</table>

Installing NetScaler Management and Analytics System

The number of NetScaler MAS server that you can install depends on the memory available on the Hyper-V server.

To install NetScaler MAS

1. Start Hyper-V Manager client on your workstation.
2. On the Action menu, click Import Virtual Machine.
3. Import the Hyper-V image, and do the following:
   a. In the Import Virtual Machine dialog box, in Locate Folder section, browse to the folder in which you saved the NetScaler MAS Hyper-V image, select the folder, and click Next.
   b. In the Select virtual machine section, select the appropriate virtual machine name.
   c. In the Choose Import Type section, select Copy the virtual machine (create a new unique ID) option and click Next.
   d. In the Choose Destination section, you can specify the folders to store the virtual machine files.

Note

By default the wizard imports the virtual machine files to default Hyper-V folders on your local host.
e. In the **Choose Storage Folders** section, you can select the location in which you want to store the virtual hard disks, and then click **Next**.

f. You can verify the Virtual Machine details in the summary pane, click **Finish**.
The NetScaler MAS Hyper-V image appears in the right pane.

4. Right-click the NetScaler MAS Hyper-V image, and then click **Settings**.

5. In the left pane of the dialog box that appears, navigate to **Hardware > VM_Bus Network Adaptor**, and in the right pane, from the Network drop-down list, select the appropriate network.
6. Click **Apply**, and then click **OK**.
7. Right-click the NetScaler MAS Hyper-V image and click **Connect**.
8. On the Console window, click **Start** button.
9. Configure the initial network configuration options, as shown in the figure below.

10. After specifying the required IP addresses, select the deployment type as NetScaler MAS server. If you do not select any option, by default, it will be deployed as a server.
11. Type Yes to deploy NetScaler MAS as a standalone deployment.

12. Type Yes to restart the NetScaler MAS server.

**Note**

After you install NetScaler MAS, you can update the initial configuration settings at a later time.

To update the initial configuration in the NetScaler MAS, type `networkconfig` in the NetScaler MAS console. The console displays the NetScaler MAS initial network configuration options. You can then update the following parameters on the console:

- Host name of NetScaler MAS
- NetScaler MAS IPv4 address
- Netmask
- Gateway IPv4 address
- DNS IPv4 address

**Verification**

After the server is installed, you can access the graphical user interface (GUI) by typing the IP address of the NetScaler MAS server in the address bar of your browser. The default administrator credentials to log on to the server are nsroot/nsroot.

The browser displays the NetScaler MAS configuration utility.
Installing NetScaler MAS on VMWare ESXi

Sep 04, 2017
To install NetScaler MAS virtual appliances on VMware ESXi, use VMware vSphere client.

Prerequisites

Before you begin installing a virtual appliance, verify that the following requirements:

- Install VMware ESXi version 4.1 or later hardware that meets the minimum requirements.
- Install VMware Client on a management workstation that meets the minimum system requirements.
- Install VMware OVF Tool (required for VMware ESXi version 4.1) on a management workstation that meets the minimum system requirements.
- Download the NetScaler MAS set up files.

Note

VMotion is not support on NetScaler MAS.

VMware ESXi Hardware Requirements

The following table lists the virtual computing resources that you need on your VMware ESXi server to install a NetScaler MAS virtual appliance.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>32 GB &lt;br&gt; <strong>Note</strong>: The default value is 8 GB. Citrix recommends that you increase the default value to 32 GB for better performance.</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>8 CPUs &lt;br&gt; <strong>Note</strong>: The default is 2 CPUs. Citrix recommends that you increase the default value to 8 CPUs for better performance.</td>
</tr>
<tr>
<td>Storage space</td>
<td>The default value is 120 GB. Actual storage requirement will depend on NetScaler MAS sizing estimation. If your NetScaler MAS storage requirement exceeds 120 GB, you have to attach an additional disk. Note that you can add only one additional disk. Citrix recommends you to estimate storage and attach additional disk at the time of initial deployment. For more information, see How to Attach an Additional Disk to NetScaler MAS.</td>
</tr>
<tr>
<td>Virtual Network Interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>1 Gbps or 100 Mbps</td>
</tr>
</tbody>
</table>

To install NetScaler MAS

1. Start the VMware vSphere client on your workstation.
2. In the IP address / Name text box, type the IP address of the VMware ESXi server that you want to connect to.
3. In the User Name and Password text boxes, type the administrator credentials, and then click Login.
4. On the File menu, click Deploy OVF Template.
5. In the Deploy OVF Template dialog box, in Deploy from a file or URL, browse to the location where you saved the NetScaler MAS setup files, select the .ovf file, and click Next.

**Note**

If a warning message appears with the following text: The operating system identifier is not supported on the selected host, check to see if the VMware server supports FreeBSD operating system. Click Yes.

6. On the OVF Template Details page, click Next.
7. Type a name for the NetScaler MAS virtual appliance, and then click Next.
8. Specify the Disk Format by selecting either Thin provisioned format or Thick provisioned format.

**Note**

Citrix recommends that you select Thick provisioned format.

9. Click Finish to start the installation process.
10. You are now ready to start the NetScaler MAS virtual appliance.

11. In the navigation pane, select the virtual appliance that you just installed and, from the **Inventory** menu, select **Virtual Machine**, and then select **Upgrade Virtual Hardware**. In the Confirm Virtual Machine dialog box, click **Yes**.
12. In the Inventory menu, select **Virtual Machine**, and then select **Edit Settings**.

13. In the **Virtual Machine Properties** dialog box, on the **Hardware** tab, click **Memory**, and then in the right pane specify the **Memory Size** as 8 GB.

14. Click **CPUs**, and then in the right pane, specify the CPUs as 4. Click **OK**.

15. Add an additional disk as per your requirement.
16. In the navigation pane, select the virtual appliance that you just installed and, from the **Inventory** menu, select **Virtual Machine**, select **Power**, and then select **Power On**.

17. Select the **Console** tab to display the NetScaler MAS Initial Network Configuration options for specifying the host name, IPv4 address, subnet mask (Netmask), and Gateway IP address for the NetScaler MAS virtual appliance.
18. After completing the initial configuration, select the NetScaler MAS Server option to start the virtual appliance as a server.

19. Type **Yes** to deploy NetScaler MAS as a standalone deployment.

20. Type **Yes** to restart the NetScaler MAS server.

**Note**

After you install NetScaler MAS, you can update the initial configuration settings at a later time.

To update the initial configuration in the NetScaler MAS, type `networkconfig` in the NetScaler MAS console. The console
displays the NetScaler MAS initial network configuration options. You can then update the following parameters on the console:

- Host name of NetScaler MAS
- NetScaler MAS IPv4 address
- Netmask
- Gateway IPv4 address
- DNS IPv4 address

Verification

After the server is installed, you can access the graphical user interface (GUI) by typing the IP address of the NetScaler MAS server in the address bar of your browser. The default administrator credentials to log on to the server are nsroot/nsroot.

The browser displays the NetScaler MAS configuration utility.
Installing NetScaler MAS on Linux-KVM Server

Aug 30, 2017

Virtualization platforms on which the Citrix NetScaler Management and Analytics System (MAS) can be provisioned include Linux-KVM.

Before you install NetScaler MAS on Linux-KVM, make sure that your system has the hardware virtualization extensions, and verify that the CPU virtualization extensions are available. Verify that `virsh` (a command-line tool for managing virtual machines) is available on the hypervisor.

Use your administrator credentials to log on to Citrix.com website, access the latest NetScaler MAS setup files, and download them onto your computer. Then, install the NetScaler MAS on your Linux-KVM platform and configure it for your network.

**Prerequisites**

Before installing the NetScaler MAS virtual appliance, verify that Linux-KVM version 3.6.11-4 and later is installed on hardware that meets the minimum requirements.

**Hardware Requirements**

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>A 64-bit x86 processor with the hardware virtualization features that are included in the AMD-V and Intel VT-x processors. Provide at least 2 CPU cores to host Linux-KVM. Note: To test whether your CPU supports Linux host, enter the following command at the host Linux shell prompt: `egrep '^flags.* (vmx</td>
</tr>
<tr>
<td>Memory (RAM)</td>
<td>Minimum 4 GB for the host Linux kernel. Add additional memory as required by the VMs.</td>
</tr>
<tr>
<td>Hard Disk</td>
<td>Calculate the space for Host Linux kernel and VM requirements. A single NetScaler MAS VM requires 120 GB of disk space.</td>
</tr>
</tbody>
</table>

**Note**

The memory and hard disk requirements specified above are for deploying NetScaler MAS on the OpenStack platform, considering that there are no other virtual machines running on the host. The hardware requirements for OpenStack depends on the number of virtual machines running on it.

**Software Requirements**

Citrix recommends newer kernels, such as the 64-bit version of the 3.6.11-4 kernel or later.

**Guest Virtual Machine Hardware Requirements**

NetScaler virtual machine and NetScaler MAS support only IDE hard disk type.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>32 GB</td>
</tr>
<tr>
<td><strong>Note</strong>: The default value is 8 GB. Citrix recommends that you increase the default value to 32 GB for better performance.</td>
<td></td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>8 CPUs</td>
</tr>
<tr>
<td><strong>Note</strong>: The default is 2 CPUs. Citrix recommends that you increase the default value to 8 CPUs for better performance.</td>
<td></td>
</tr>
<tr>
<td>Storage Space</td>
<td>The default value is 120 GB. Actual storage requirement will depend on NetScaler MAS sizing estimation. If your NetScaler MAS storage requirement exceeds 120 GB, you have to attach an additional disk. Note that you can add only one additional disk. Citrix recommends you to estimate storage and attach additional disk at the time of initial deployment. For more information, see <a href="https://docs.citrix.com">How to Attach an Additional Disk to NetScaler MAS</a>.</td>
</tr>
<tr>
<td>Virtual Network Interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>3Gbps or 100 Mbps</td>
</tr>
</tbody>
</table>

**Networking Requirements**

NetScaler MAS supports only one virtIO para-virtualized network interface. This interface should be connected to the management network of the Linux-KVM host, so that the NetScaler MAS and Linux-KVM can communicate.
Downloading NetScaler Management and Analytics System Setup Files

To download the NetScaler Management and Analytics System setup files from www.citrix.com:

1. Open a web browser and type www.citrix.com in the address bar.
2. Click Log In, enter your login credentials, and then again click Log In.
3. Navigate to the Downloads section.
4. From the Downloads drop-down list, select NetScaler ADC.
5. On the NetScaler ADC page, select the release. For example, select Release 11.1.
6. Click Components to expand it, and click NetScaler Management and Analytics System.
7. Scroll down to the list of available builds, and then select a build. For example, select NetScaler MAS Image for Linux-KVM, 11.1-Build 44.5.
8. Click Download File, accept the end-user license agreement, and download the compressed image file to any folder on your local machine.

Installing the NetScaler Management and Analytics System on Linux-KVM

1. Using SSH, log on to the KVM host.
2. At the CLI prompt, by using any of the file transfer programs, copy the image to a folder on the server.
3. Navigate to the directory where you have saved the downloaded image.
4. Perform these at the command line:
   a. List the files in the directory verify the presence of the image file.
   b. Use the tar command to untar the NetScaler Management and Analytics System image file. The unzipped package contains the following components:
      1. A domain XML file that specifies the NetScaler MAS attributes
      2. A text file that specifies the check sum of the domain disk image
      3. A domain disk image

Example

```
tar -xfvz MAS-KVM.tgz

MAS-KVM.xml
MAS-KVM.qcow2
checksum.txt
```

Example

```
root@ubuntu:/mnt/build# tar xvzf MAS-KVM-11.1-50.10.tgz
MAS-KVM.xml
checksum.txt
```

- Create a copy of MAS-KVM.xml as MAS1-KVM.xml, as a backup option. Open the MAS1-KVM.xml file by using the vi editor.
- Edit MAS1-KVM.xml for the following networking attributes:
  - name - Specify the name.
  - mac - Specify the MAC address.
  - source file - Specify the absolute disk-image source path. The file path has to be absolute.

Note

The domain name and the MAC address must be unique.

```
Example
```

iv. mode - Specify the mode.
v. model type - Set to virtIO.
vi. source dev - Specify the interface.
Define the VM attributes in the MAS1-KVM.xml file by using the following command:

```bash
virsh define <FileName>.xml
```

Start the NetScaler MAS by entering the following command:

```bash
virsh start [<DomainName> | <DomainUUID>]
```

Start the NetScaler MAS:

```bash
virsh start MAS
```

You can connect to the NetScaler MAS virtual machine by using the following command:

```bash
virsh console <DomainName>
```

Example

```
root@ubuntu:~/mas-build# virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml
```

```
root@ubuntu:~/mas-build# virsh start MAS
Domain MAS started
```

```
root@ubuntu:~/mas-build# virsh console MAS
Connected to domain MAS
Escape character is ^]`
```

Configuring the NetScaler Management and Analytics System
**Note**

On some Linux KVM hosts, FreeBSD guests fail to restart properly if they have more than one CPU. When the NetScaler MAS virtual appliance is restarted, the NetScaler MAS CLI and GUI become unresponsive. For details, see [https://bugs.launchpad.net/qemu/+bug/1329956](https://bugs.launchpad.net/qemu/+bug/1329956).

To avoid the NetScaler MAS CLI and GUI from becoming unresponsive when the NetScaler MAS virtual appliance is restarted, shut down all the virtual machines on the KVM host, and perform the following on the KVM host:

1. Remove the kvm_intel module using the following command:
   
   `rmmod kvm_intel`

2. Disable APICv and reload kvm_intel module using the following command:
   
   `modprobe kvm_intel enable_apicv=N`

3. Start the virtual machines on the KVM host.

After installing the NetScaler MAS, allow about ten minutes for the services to become available, and then log on to the NetScaler MAS.

1. At the command line, use the default system administrator credentials to log on to the system
   - Username: nsroot
   - Password: nsroot

**Note**

After logging on for the first time, you should change the administrative password. Then, configure the MAS to function in your network. You can change the password from the NetScaler MAS user interface. From the NetScaler MAS home page, navigate to System > User Administration > Users. Select the user and click Edit, and then update the password in the Password field.

2. At the prompt, type:
   
   `shell`

3. Type `networkconfig` to enter the NetScaler MAS initial network configuration menu. Configure the management IP address.

4. To complete the initial network configuration of NetScaler MAS, follow the prompts. The console displays the NetScaler MAS initial network configuration options for setting the following parameters for the NetScaler MAS. The host name is populated by default.
   a. Enter 2 to update NetScaler MAS IPv4 address - management IP address at which you access a NetScaler MAS
   b. Enter 3 to update Netmask - subnet mask associated with the Management IP address
   c. Enter 4 to update Gateway IPv4 address - default gateway IP address for the subnet of the Management IP address of the NetScaler MAS
   d. Enter 7 to save and quit - saves your configuration changes and exits the system

5. Execute the deployment script by typing the command at the shell prompt:
   
   `deployment_type.py`

6. In the deployment screen that appears, select the deployment type as NetScaler MAS server.

7. Type Yes to deploy NetScaler MAS as a standalone deployment.

8. Type Yes to restart the NetScaler MAS server.

9. After NetScaler MAS server restarts, log on to NetScaler MAS by using the default administrator credentials as nsroot/nsroot through the command line or the GUI.

You can later access the NetScaler MAS by typing the IP address of the NetScaler MAS server in the address bar of your browser. The default administrator credentials to log on to the server are nsroot/nsroot.
A high availability (HA) deployment of two NetScaler MAS servers can provide uninterrupted operation in any transaction. An HA pair of NetScaler MAS servers is in active-passive mode. When two NetScaler MAS servers are configured in active-passive mode, both servers have the same configuration. This active-passive deployment type is ideal for disaster recovery.

In this type of active-passive deployment, one NetScaler MAS server is configured as the primary node and the other as the secondary node. If, for any reason, the primary node goes down, the secondary node takes over.

The secondary node listens to the heartbeat messages that the primary node sends through the NetScaler MAS database. If the secondary node does not receive the heartbeats for a specific period of time, the secondary node performs an SSH based check of NetScaler MAS processes on the primary node. If the heartbeat and SSH based check fails, the primary node is considered to be down and the secondary node takes over as the primary node (a process called failover). The whole process requires about 15-20 seconds, depending on hardware infrastructure and network.

A failover occurs if one of the following conditions is encountered:

- Primary server loses connectivity in the LAN.
- Primary server encounters a critical software issue.
- Primary server encounters a hardware issue, such as power failure.
- The administrator manually forces the primary server to shut down and the secondary server takes over.

The following figure shows a high availability deployment of two NetScaler MAS servers in active-passive mode.

When configuring your NetScaler MAS deployment in HA mode, installing both the server nodes in the same subnet is recommended.
Points to Note

- The upgrade process changes the active-active HA setup to an active-passive HA setup.
- You can access an HA node from the GUI by entering either the primary or secondary IP address. You can see the marking as "Passive" for the secondary node. If you have configured load balancing in NetScaler MAS with unified access, you can enter the load balancing virtual server IP address to view and manage your NetScaler MAS HA setup.
- Although you can make configuration changes on both the primary and secondary nodes, making them only on the active (primary) node is strongly recommended.
- In a high availability setup, all configuration files are synchronized automatically from the primary node to the secondary node at an interval of one minute. Database synchronization happens instantly and is taken care by the backup and disaster recovery (BDR) software.
- In a high availability setup, all system settings configuration done on the primary node propagates automatically to the secondary. For all other commands, the database synchronization takes care the propagation from the primary to secondary and you need not run these commands separately.
- As part of the upgrade process, all configurations are updated such that all NetScaler instances are now managed by the active node. This is applicable to all configurations such as SNMP, Syslog, Analytics, and so on.
- After you upgrade the NetScaler MAS to active-passive mode, some NetScaler instances will still continue to send traffic to the passive node for approximately 5 minutes. As a result, the incoming traffic will be lost for that duration.
- If you had configured a load balancing virtual server for unified management access of your NetScaler MAS servers, after you upgrade the NetScaler MAS HA pair to active-passive mode you have to run the following command on the NetScaler appliance to update the load balancing configuration:

```
add lb monitor MAS_Monitor TCP-ECV -send "GET /mas_health HTTP/1.1\nAccept-Encoding: identity\nUser-Agent: NetScaler-Monitor\nConnection: close\n\n" -recv "{"statuscode":0, "is_passive":0}" -LRTM DISABLED
```

- In a high availability setup, the heartbeat messages set up through Nitro commands and Database synchronization.
- NetScaler MAS does not support forced synchronization. You cannot force the synchronization from either the primary or the secondary node.
- Automatic HA synchronization is enabled by default. You cannot enable or disable automatic HA synchronization after you deploy the HA pair.
- In a high availability setup, you must open the following ports in both the NetScaler MAS servers:
  - For ICMP (ping) – (No reserved port) To detect network reachability.
  - For NITRO communications (TCP) - Port 443.
  - For synchronization - Port 22.
  - For Database synchronization - Port 5454.
- You cannot use Nitro calls to force the primary to stay primary and the secondary to stay secondary.
- It is recommended not to configure HA nodes in different subnets in NetScaler MAS.
- When upgrading from active-active to active-passive, always use the same software version and build number on both the primary and the secondary server.
- Always use the GUI to perform the NetScaler MAS upgrade.
- In a high availability setup, when you initiate the upgrade on either of the nodes via GUI, the other node is automatically upgraded. However, always using the primary node for the upgrade is recommended.
- After completion of the upgrade process, either node can act as a primary node. No data is lost during the upgrade.
- You can gracefully shutdown a node in HA setup so that DB gracefully shuts down. At the command prompt, type shutdown –p now to shut down the node.
A hard reboot should not be performed in a high availability setup.

- It is highly recommended to deploy the NetScaler MAS HA nodes in the same datacenter.
- NetScaler MAS HA and NetScaler MAS single server nodes can manage and monitor NetScaler instances that are deployed in different datacentres having latency less than or equal to 150ms.
- The latency between two NetScaler MAS HA nodes deployed in different data centers is less than or equal to 10 ms.

Recommended Precautions:

- Back up the NetScaler MAS server before you upgrade.
- When upgrading NetScaler MAS servers in a high availability setup, do not make any configuration changes on either of the nodes.

Warning

Do not refresh your browser until the upgrade process is successfully completed. It might take a few minutes for the upgrade process to finish.

Prerequisites

Before you set up HA for NetScaler MAS, note the following requirements:

- The NetScaler MAS active-passive HA deployment mode is supported from NetScaler MAS version 11.1 build 54.14.
- In an HA setup, both nodes must run the same version of NetScaler MAS System software.
- You have to have downloaded the NetScaler Management and Analytics System image file.

For production use of the NetScaler Management and Analytics System, Citrix recommends that you set CPU priority (in virtual machine properties) to the highest level, to improve scheduling behavior and network latency.

The following table lists the minimum requirements for the virtual computing resources that XenServer, VMWare ESX, or Microsoft Hyper-V must provide for each component of this deployment.

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>32 GB</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The default value is 8 GB. Citrix recommends that you increase the default value to 32 GB for better performance.</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>8 CPUs</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The default is 2 CPUs. Citrix recommends that you increase the default value to 8 CPUs for better performance.</td>
</tr>
</tbody>
</table>
Storage space

The default value is 120 GB. Actual storage requirement will depend on NetScaler MAS sizing estimation.

If your NetScaler MAS storage requirement exceeds 120 GB, you have to attach an additional disk. Note that you can add only one additional disk.

Citrix recommends you to estimate storage and attach additional disk at the time of initial deployment.

For more information, see How to Attach an Additional Disk to NetScaler MAS.

<table>
<thead>
<tr>
<th>Virtual Network Interfaces</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hypervisor Requirements</th>
<th>XenServer</th>
<th>6.2, 6.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMWare ESX</td>
<td>5.5, 6.0</td>
<td></td>
</tr>
<tr>
<td>Microsoft Hyper-V</td>
<td>2012 R2</td>
<td></td>
</tr>
<tr>
<td>Linux - KVM</td>
<td>Ubuntu, Fedora</td>
<td></td>
</tr>
</tbody>
</table>

Installing NetScaler MAS in HA Mode

Obtain the NetScaler MAS image file from the Citrix download site. Installing a NetScaler MAS in HA mode involves the following steps:

1. Provisioning the first server node
2. Provisioning the second server node
3. Deploying the two server nodes in HA mode

Provisioning the First Server Node

To begin provisioning the NetScaler MAS HA setup, install the first NetScaler MAS server. Use the image file that you downloaded from the Citrix download site.

1. Import the image file to your hypervisor, and then from the Console tab configure the initial network configuration
2. After specifying the required IP addresses, select the deployment type as **NetScaler MAS Server**. If you do not select any option, by default, it’ll be deployed as a server.

3. The deployment console prompts you to select the server deployment (as Standalone). Enter **No** to confirm the deployment as HA pair.

4. The console prompts you to select the (first server node). Enter **Yes** to confirm the node as the first server node.

5. The console prompts you to restart the server. Enter **Yes** to restart.

**Provisioning the Second Server Node**

After provisioning the first NetScaler MAS server, provision the second server. On your hypervisor, use the same image file
that you used to install the first server, or obtain that same version of the image from the Citrix download site.

1. Import the image file to your hypervisor, and then from the **Console** tab configure the initial network configuration options as explained on the following screen:

```
NetScaler MAS initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([ ]).
Selecting the listed number allows the address to be changed.

1. NetScaler MAS Host Name [HA-2]:
2. NetScaler MAS IPv4 address [10.102.29.53]:
3. Netmask [255.255.255.0]:
4. Gateway IPv4 address [10.102.29.1]:
5. DNS IPv4 Address [127.0.0.2]:
6. Cancel and quit.
7. Save and quit.
```

Select a menu item from 1 to 7 [?]?

2. After specifying the required IP addresses, select the deployment type as **NetScaler MAS server**. If you do not select any option, by default, it will be deployed as a server.

```
Network configuration is completed successfully.
NetScaler MAS Deployment Configuration.
The following menu enables you to select the components of your NetScaler MAS deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as NetScaler MAS Server.

1. NetScaler MAS Server.
3. Telemetry Node.
4. Cancel and exit.
```

Select an option from 1 to 4 [1]:

3. The deployment console prompts you to select the server deployment (as Standalone). Enter **No** to confirm the deployment as HA pair.

```
Select an option from 1 to 4 [1]: 1
Selected Option 1. NetScaler MAS Server.
NetScaler MAS Standalone deployment [yes/no]: no
```

4. The console then prompts you to select the (first server node). Enter **NO** to confirm the node as the second server node.

```
Select an option from 1 to 4 [1]: 1
Selected Option 1. NetScaler MAS Server.
NetScaler MAS Standalone deployment [yes/no]: no
First Server Node for NetScaler MAS [yes/no]: no
```

5. Enter the first server's IP address and password, and reboot the node when the console prompts.
Deploying the two servers in HA mode

To complete the installation process of the two server nodes as an HA pair, you have to deploy these nodes from the GUI of the first server node that you configured. Internal communication between the two servers starts when you deploy the first server node.

1. In a web browser, type the IP address of the first NetScaler MAS server node (for example, http://10.102.29.52).
2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. Select the deployment type as **Two Servers deployed in High Availability Mode**, and click **Next**.
4. On the **System** tab, navigate to **Deployment** and click **Deploy**.
5. A confirmation message appears. Click **Yes**.

After you deploy the NetScaler MAS in HA mode, either the first server node or the second server node can be an active node. The active node is identified by the **star** symbol as shown in the following figure, which shows the node at 10.102.29.53 as the active node. The other node acts as a passive node and is ready to take over as soon as the active node becomes unavailable.
Configuring Load Balancing of the NetScaler MAS HA Pair on a NetScaler Instance

You can configure the NetScaler MAS in HA mode with unified GUI access. Both the primary and secondary servers must be connected to a load balancing virtual server hosted in a NetScaler instance. The load balancing virtual server sends the requests to the primary NetScaler MAS server. The primary node accepts connections and manages all the devices. All the communications like AppFlow, SNMP, LogStream, Syslog, and so on are managed by the primary node.

You can access an HA node through its IP address or through the load balancing virtual server's IP address. If you use the load balancing virtual server's IP address, the GUI of the active node appears. The service state of the passive node is shown as down.

![Deployment Diagram](image-url)
To configure load balancing of the NetScaler MAS HA pair by using the NetScaler command line

1. On a workstation or laptop, open an SSH connection to the instance by using an SSH client, such as PuTTY.

2. Log on to the NetScaler instance. In **User Name** and **Password**, type the administrator credentials. The defaults are `nsroot` and `nsroot`, respectively.

3. At the command prompt, type:

   ```
   add lb vserver <Load Balancer name> HTTP <Vserver_ip> 80 -persistenceType SOURCEIP
   add server <MAS Server 1 name> < MAS Server 1_ip>
   add server <MAS Server 2 name> < MAS Server 2_ip>
   add service <Service 1 name> <MAS Server 1 name> HTTP 80 -maxReq 1
   add service <Service 2 name> <MAS Server 2 name> HTTP 80 -maxReq 1
   add lb monitor MAS_Monitor TCP-ECV -send "GET /mas_health HTTP/1.1\nAccept-Encoding: identity\nUser-Agent: NetScaler-Monitor\nConnection: close\n\" -recv "{\"statuscode\":0, \"is_passive\":0}" -LRTM DISABLED
   bind service <Service 1 name> -monitorName <Monitor name>
   bind service <Service 2 name> -monitorName <Monitor name>
   ```

To configure the NetScaler MAS HA pair by using the NetScaler GUI
1. In a web browser, type the IP address of the **NetScaler instance** (for example, http://192.168.100.1).

2. In the **User Name** and **Password** fields, enter the administrator credentials.

3. On the **Configuration** tab, navigate to **Traffic Management > Load Balancing > Virtual Servers** and select **Add**.

4. Enter the name and IP address for the load balancing virtual server in the **Name** and **IP Address** fields, respectively. **Note:** The IP address you enter becomes the load balancing virtual server's virtual IP (VIP) address and can be used to access the HA pair once the configuration is complete.

5. In the **Protocol** field, choose the communication protocol for the load balancing virtual server.

6. In the **Port** field, enter the virtual server's port number. Then, click **OK**.

7. Click **Persistence** and select **SourceIP** as the persistence type.

8. To add load balancing services for the NetScaler MAS HA pair, select the **Services and Service Groups** tab, and then select **Load Balancing Virtual Server Service Binding** to add new services.

   Alternatively, to add a load balancing service, navigate to **Traffic Management > Load Balancing > Services**, and click **Add**.

9. To set a threshold limit for a service, navigate to **Traffic Management > Load Balancing > Services**. On the Services page, click the service you want to modify. On the **Load Balancing Service** page, click **Thresholds & Timesouts** under the **Advanced Settings** section on the right of the page. Under **Threshold**, enter 1 as the value for Max Requests and
10. Add the services for the first and second NetScaler MAS by clicking the plus sign (+) and clicking **Bind**.
11. Bind a monitor to each service by navigating to Configuration > Traffic Management > Load Balancing > Services and selecting the monitor type as tcp-ecv for each of the two services.

Disabling HA on a NetScaler MAS HA pair

You can disable high availability on a NetScaler MAS HA pair and convert the nodes to stand-alone NetScaler MAS servers. In the GUI, you can select one of the NetScaler MAS servers to retain all the data, and remove the other server node from the HA configuration.

To disable High Availability via GUI:

1. In a web browser, type the IP address of the NetScaler MAS server node that you want to retain the data (for example, http://10.102.29.53).
2. In the User Name and Password fields, enter the administrator credentials.
3. On the System tab, navigate to Deployment and click Break HA.
The other server node restarts, and the node on which you issue the command goes out of service for a while. You can remove the other load balancing virtual server and replace its VIP address in all the configurations in which it was used.

When the server node that you remove from the HA configuration restarts, all its configurations and settings are deleted. You have to access its console to choose a deployment type. The following screen on the console appears automatically.

```
Network configuration is completed successfully.
NetScaler MAS Deployment Configuration.
The following menu enables you to select the components of your NetScaler MAS deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as NetScaler MAS Server.

-----------------------
Cancelling or quitting this menu will deploy NetScaler MAS as a server. If you wish you change the deployment, please run this script at /tmp/deployment_type.py again.

1. NetScaler MAS Server.
3. Telemetry Node.
4. Cancel and exit.

Select an option from 1 to 4 [4]:
```

Select the deployment type as **NetScaler MAS Server** to start the deployment process again.

**Note**

When breaking HA, data on the node where you initiate **Break HA** is retained. You can break HA from either the primary or the secondary node, but doing so from primary node avoids losing data that has not been synced to the secondary node.
Redeploying High Availability on a NetScaler MAS

After you break the HA in NetScaler MAS to a standalone deployment, you can redeploy the HA in NetScaler MAS. Redeploying HA is similar to the first-time deployment of HA.

To redeploy HA in NetScaler MAS

1. On a workstation or laptop, open an SSH connection to the appliance by using an SSH client. Log in to the appliance using `nsrecover` as the user name and enter the password that you have set. Run the `deployment_type.py` script in the secondary node.

   **Note:** After breaking the HA, you cannot log in to the secondary node console using `nsroot` as the user name, since the secondary node is down.

2. Alternately, you can also log in to the hypervisor console and run the `deployment_type.py` script in the secondary node.

3. In the GUI, access the primary node of the HA pair. Navigate to **System > Deployment** and then click the **Deploy** button. The system reboots and the HA pair is established.

   **Important**

   If you use an external SNMP server in a NetScaler MAS HA setup, you have to configure SNMP requests to be sent to individual nodes. You will not get responses if the SNMP server is configured to send requests to the load balancing virtual server's IP address.
How to Use Database Recovery Script to Recover Inaccessible NetScaler MAS Servers

Jun 18, 2017

The maximum size of the NetScaler MAS database depends on the system database model, and is not the same on all systems. If the size of your database exceeds the threshold, the database becomes inaccessible, which might cause your NetScaler MAS server to not respond. In such cases, you can use the following procedures to connect to the file system, delete a few components, and make the database accessible. You can then perform recovery operations. This operation takes approximately an hour to 90-minutes.

The NetScaler MAS recovery script helps you delete some data from the database by prompting you to navigate from one component to another, without affecting the core system files, or the settings of the NetScaler MAS. Files such as the upgrade images, backup files (instance and NetScaler MAS server), Analytics reports, perf reports can be deleted using this operation.

This document includes the following:

- How to Use NetScaler MAS Database Recovery Script for a NetScaler MAS Standalone Deployment
- How to Use NetScaler MAS Database Recovery Script for a NetScaler MAS High Availability Deployment

How to Use NetScaler MAS Database Recovery Script for a NetScaler MAS Standalone Deployment

Use the following procedure in a single server NetScaler MAS deployment to connect to the file system, delete a few components, and make the database accessible, and then perform the recovery operations.

1. Using a SSH client or your hypervisor's console, log on to NetScaler MAS and type the following command:

   `/mps/mas_recovery/mas_recovery.py`

2. When the screen displays a caution message for stopping a few MAS processes, press the y key.

   The following screen appears while the system determines which components of the database you can delete without affecting the system's core files.
3. When a screen similar to the following example appears, decide which components to delete, and then press the y key.

4. When prompted to delete database components, specify the components as described on the screen. For example:
5. When prompted to delete file-system components, specify the components as described on the screen. For example:

6. When confirmation prompt appears, press the y key to stop all NetScaler MAS processes and initiate cleanup of the selected components, or press n to return to the Filesystem components selection screen.
7. Wait for about 30 minutes for internal DB operations to complete after NetScaler MAS has restarted. You should then be able to connect to NetScaler MAS database. If not, run the recovery script again to free up more space. When NetScaler MAS is up and running, it should work as expected.

How to Use NetScaler MAS Database Recovery Script for a NetScaler MAS High Availability Deployment

The database system for NetScaler MAS servers in a high availability deployment will be in continuous synchronization mode. You need to replicate the procedure to use the recovery script individually on both the NetScaler MAS servers. You also need to break the high availability pair and reconfigure it once the recovery operations are done. This operation approximately takes two hours.

Use the following procedure to connect to the file system, delete a few components, and make the database accessible, and then perform recovery operations.

1. Using a SSH client or your hypervisor's console, log on to NetScaler MAS.

2. Run the NetScaler MAS recovery script (/mps/mas_recovery/mas_recovery.py) individually on node 1 and node 2.

```
Last login: Tue Jun 13 18:44:16 2017 from 10.252.242.167
> shell
bash-2.05b# /mps/mas_recovery/mas_recovery.py
```

Note

Ensure that you Restart both nodes.

3. When the screen displays a caution message for stopping a few MAS processes, press the y key.
The following screen appears while the system determines which components of the database you can delete without affecting the system's core files.

```
Checking whether DB is accessible...
DB is accessible.
Please wait. Gathering data. This will take some time.
```

4. When a screen similar to the following example appears, decide which components to delete, and then press the y key.

```
<table>
<thead>
<tr>
<th>DB component</th>
<th>Current size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perf Reports</td>
<td>860.59 MB</td>
</tr>
<tr>
<td>Analytics</td>
<td>37.54 MB</td>
</tr>
<tr>
<td>Device Events</td>
<td>14.48 MB</td>
</tr>
<tr>
<td>App Health Summary</td>
<td>5.70 MB</td>
</tr>
<tr>
<td>App Counter Data</td>
<td>4.61 MB</td>
</tr>
<tr>
<td>App Summary</td>
<td>4.29 MB</td>
</tr>
<tr>
<td>Device Syslogs</td>
<td>56.00 KB</td>
</tr>
<tr>
<td>Filesystem component</td>
<td>Current size</td>
</tr>
<tr>
<td>MAS Images</td>
<td>7.43 GB</td>
</tr>
<tr>
<td>Device Backup</td>
<td>54.67 MB</td>
</tr>
<tr>
<td>MAS Backup</td>
<td>48.88 MB</td>
</tr>
<tr>
<td>Core Files</td>
<td>373.58 KB</td>
</tr>
<tr>
<td>ESXi NSVX Images</td>
<td>0.00 B</td>
</tr>
<tr>
<td>SDX Images</td>
<td>0.00 B</td>
</tr>
<tr>
<td>NetScaler Images</td>
<td>0.00 B</td>
</tr>
<tr>
<td>Techsupport Bundles</td>
<td>0.00 B</td>
</tr>
<tr>
<td>Docker NSCPX images</td>
<td>0.00 B</td>
</tr>
</tbody>
</table>
```

5. When prompted to delete database components, do not specify any of the listed components, select Continue without selecting. For example:
6. When prompted to delete file-system components, specify the components as described on the screen. For example:

7. Once the nodes are up, wait for about 30 minutes for internal database operations to complete.

8. The database should now be up on both nodes.

9. Log on to any one of the NetScaler MAS servers using a supported web browser.

10. Navigate to System > Deployment, and click Break HA.

11. Using a SSH client or your hypervisor's console, log on to NetScaler MAS.

12. Run the NetScaler MAS recovery script (/mps/mas_recovery/mas_recovery.py) individually on node 1 and node 2, and delete the database components. For example:
Note

Make sure that you delete the **same** database components on both the NetScaler MAS servers, and restart both the nodes.

13. Let the two nodes run for at least 45 minutes, and then recreate the HA pair by running the deployment script (deployment_type.py) on the console of each node.
Migrate a Single Server Deployment to a High Availability Deployment

Jul 13, 2017

You can upgrade your NetScaler MAS single server to a high availability (HA) deployment of two NetScaler MAS servers. An HA pair of NetScaler MAS servers is in active-passive mode, and both the servers will have the same configuration. This active-passive deployment type is ideal for disaster recovery.

In this type of active-passive deployment, one NetScaler MAS server is configured as the primary node and the other as the secondary node. If, for any reason, the primary node goes down, the secondary node takes over.

To migrate a NetScaler MAS single server to a high availability (HA) pair, you need to provision a new NetScaler MAS server node, configure it to the existing NetScaler MAS single server, and deploy them as a HA pair.

Migrating a NetScaler MAS single server to an HA mode involves the following steps:

1. Modifying the existing server node
2. Provisioning the second server node
3. Deploying the two nodes in HA mode
4. Configuring the HA pair (optional)

Modifying the Existing MAS Server Node

To migrate the NetScaler MAS from single server to HA mode, you have to change the initial deployment type of the server node to HA mode.

1. On a workstation or laptop, open the console of the existing NetScaler MAS server node.
2. Log on to NetScaler MAS. The default credentials are nsroot and nsroot.
3. In the shell prompt, type `deployment_type.py` and press enter.

4. Select the deployment type as NetScaler MAS server. If you do not select any option, by default, it’s deployed as a server.

   ```bash
   $ python deployment_type.py
   ```

   NetScaler MAS Deployment Configuration.
The following menu enables you to select the components of your NetScaler MAS deployment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as NetScaler MAS Server.

   1. NetScaler MAS Server.
   3. Telemetry Node.
   4. Cancel and exit.

   Select an option from 1 to 4 [4]: 1

5. The deployment console prompts you to select the server deployment (as Standalone). Enter `No` to confirm the deployment as HA pair.

   ```text
   Select an option from 1 to 4 [4]: 1
   Selected Option 1. NetScaler MAS Server.
   NetScaler MAS Standalone deployment [yes/no]: no
   ```

6. The console prompts you to select the (first server node). Enter `Yes` to confirm the node as the first server node.

   ```text
   Select an option from 1 to 4 [4]: 1
   Selected Option 1. NetScaler MAS Server.
   NetScaler MAS Standalone deployment [yes/no]: no
   First Server Mode for NetScaler MAS [yes/no]: yes
   ```

7. The console prompts you to restart the server. Enter `Yes` to restart.

   ```text
   First Server Mode for NetScaler MAS [yes/no]: yes
   Restart the system for the configuration to take effect. Do you want to restart? [yes/no]: yes
   ```

Provisioning the Second Server Node

You have to provision the second server on your hypervisor. Use the same image file that you used to install the first server, or obtain an image file of the same version from the Citrix download site.

1. Import the image file to your hypervisor, and then from the **Console** tab configure the initial network configuration options as explained on the following screen:
2. After specifying the required IP addresses, select the deployment type as NetScaler MAS server. If you do not select any option, by default, it’ll be deployed as a server.

3. The deployment console prompts you to select the server deployment (as Standalone). Enter No to confirm the deployment as HA pair.

4. The console then prompts you to select the (first server node). Enter NO to confirm the node as the second server node.

5. Enter the first server's IP address and password, and reboot the node when prompted by the console.

Deploying the two servers in HA mode
To complete the installation process of the two server nodes as an HA pair, you have to deploy these nodes from the GUI of the previously existing MAS server node. Internal communication between the two servers starts when you deploy the two server nodes.

1. In a web browser, type the IP address of the previously existing NetScaler MAS server node (for example, http://10.102.29.56).
2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. On the **System** tab, navigate to **Deployment** and click **Deploy**.

4. A confirmation message appears. Click **Yes**.

After you deploy the NetScaler MAS in HA mode, either the first server node or the second server node can be an active node. The active node is identified by the **star** symbol as shown in the following figure, which shows the node at 10.102.29.53 as the active node. The other node acts as a passive node and is ready to take over as soon as the active node becomes unavailable.
Configuring Load Balancing of the NetScaler MAS HA Pair on a NetScaler Instance

You can configure the NetScaler MAS in HA mode with unified GUI access. Both the primary and secondary servers must be connected to a load balancing virtual server hosted in a NetScaler instance. The load balancing virtual server sends the requests to the primary NetScaler MAS server. The primary node accepts connections and manages all the devices.

You can access an HA node through its IP address or through the load balancing virtual server's IP address. If you use the load balancing virtual server's IP address, the GUI of the active node appears. The service state of the passive node is shown as down.

To configure the NetScaler MAS HA pair by using the command line interface:

1. On a workstation or laptop, open an SSH connection to the NetScaler appliance by using an SSH client, such as PuTTY.
2. Log on to the appliance. In **User Name** and **Password**, type the administrator credentials. The defaults are **nsroot** and **nsroot**, respectively.
3. At the command prompt, type:
add lb vserver <Load Balancer name> HTTP <Vserver_ip> 80 -persistenceType SOURCEIP

add server <NMAS Server 1 name> < NMAS Server 1_ip>

add server <NMAS Server 2 name> < NMAS Server 2_ip>

add service <Service 1 name> <NMAS Server 1 name> HTTP 80 -maxReq 1

add service <Service 2 name> <NMAS Server 2 name> HTTP 80 -maxReq 1

add lb monitor MAS_Monitor TCP-ECV -send "GET /mas_health HTTP/1.1\r\nAccept-Encoding: identity\r\nUser-Agent: NetScaler-Monitor\r\nConnection: close\r\n\r\n" -recv "{"statuscode":0, "is_passive":0}" -LRTM DISABLED

bind service <Service 1 name> -monitorName <Monitor name>

bind service <Service 2 name> -monitorName <Monitor name>

bind lb vserver <Load Balancer name> <Service 1 name>

bind lb vserver <Load Balancer name> <Service 2 name>

To configure the NetScaler MAS HA pair by using the NetScaler GUI:

1. In a web browser, type the IP address of the NetScaler appliance (for example, http://192.168.100.1).
2. In the User Name and Password fields, enter the administrator credentials.
3. On the Configuration tab, navigate to Traffic Management > Load Balancing > Virtual Servers and select Add.
4. Enter the name and IP address for the load balancing virtual server in the Name and IP Address fields, respectively.

Note
The IP address you enter becomes the load balancing virtual server's virtual IP (VIP) address and can be used to access the HA pair once the configuration is complete.
5. In the **Protocol** field, choose the communication protocol for the load balancing virtual server.
6. In the **Port** field, enter the virtual server's port number. Then, click **OK**.
7. Click **Persistence** and select **SourceIP** as the persistence type.
8. To add load balancing services for the NetScaler MAS in HA pair, select the **Services and Service Groups** tab, and then select **Load Balancing Virtual Server Service Binding** to add new services.

Alternatively, to add a load balancing service, navigate to **Traffic Management > Load Balancing > Services**, and click **Add**.

9. Add the services for the first and second NetScaler MAS by clicking +, and click **Bind**.
10. Bind monitor to each service by navigating to Configuration > Traffic Management > Load Balancing > Services, edit both the services select the monitor type as tcp-ecv.

**Important**: If you use an external SNMP server in a NetScaler MAS HA setup, you have to configure SNMP requests to be sent to individual nodes. You will not get responses if the SNMP server is configured to send requests to the load balancing virtual server’s IP address.
Migrating from NetScaler Insight Center to NetScaler MAS

Apr 04, 2017

You can now migrate your NetScaler Insight Center deployment to NetScaler MAS without losing the existing configuration, settings, or data. With NetScaler MAS you can not only view the various analytics generated by the NetScaler instances associated with an application, but can also manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console.

**Note**
Migration is currently supported only on NetScaler Insight Center Standalone instances.

**Prerequisites**
Before migrating the NetScaler Insight Center virtual appliance to NetScaler MAS, verify that the following requirements have been met:

- NetScaler Insight Center 11.1 Build 47.14 or later is installed.
- You have downloaded the NetScaler MAS 11.1 49.X .tgz image file.

**Hardware Requirement:**

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td></td>
<td>Note: Citrix recommends that you use <strong>32 GB</strong> for better performance.</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Note: Citrix recommends 8 CPUs for better performance.</td>
</tr>
<tr>
<td>Storage space</td>
<td>120 GB</td>
</tr>
<tr>
<td></td>
<td>Note: Citrix recommends that you use 500 GB for better performance.</td>
</tr>
<tr>
<td>Virtual Network Interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>1 Gbps or 100 Mbps</td>
</tr>
<tr>
<td>Hypervisor Requirements</td>
<td>XenServer</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td>VMWare ESX</td>
</tr>
<tr>
<td></td>
<td>Microsoft Hyper-V</td>
</tr>
<tr>
<td></td>
<td>Linux - KVM</td>
</tr>
</tbody>
</table>

Installation Procedure

To migrate NetScaler Insight Center to NetScaler MAS

1. Log on to shell prompt of NetScaler Insight Center.

2. Download the NetScaler MAS build to the `/var/mps/mps_images` folder.

3. Untar the TGZ file by using the `tar -zxvf build-mas-11.1-49.X.tgz` command.

```
bash-2.05b# ./installmas
installmas: [2850]: VERSION mas-11.1-49.4.gz
install version (11.1-49.4) kernel (mas-11.1-49.4.gz)
installmas: [2850]: install version (11.1-49.4) kernel (mas-11.1-49.4.gz)
There may be a pause of up to 3 minutes while data is written to the flash.
Do not interrupt the installation process once it has begun.
Installation will proceed in 5 seconds, CTRL-C to abort
```

4. Install NetScaler MAS by using the `/installmas` command.
After the migration, all the NetScaler instances that were discovered in the NetScaler Insight Center inventory appear in the **Infrastructure > Instances** section of NetScaler MAS. However, for the first time you need to manually poll the virtual servers hosted in the discovered appliances.

**Note**

In NetScaler MAS, by default, there is no licensing cost to manage and monitor 30 virtual servers created within the discovered NetScaler instances. To monitor and manage more than 30 virtual servers, install the required MAS licenses. For more details, see [NetScaler MAS Licensing](https://docs.citrix.com).
Adding an Instance to NetScaler MAS

Jan 17, 2017

Instances are Citrix appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler MAS. You must add instances to the NetScaler MAS server if you want to manage and monitor these instances. You can add the following Citrix appliances and virtual appliances to NetScaler MAS:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway
- NetScaler SD-WAN WO
- NetScaler SD-WAN EE

You can add instances either while setting up the NetScaler MAS server for the first time or at a later time.

Note

NetScaler MAS uses the NetScaler IP (NSIP) address of the NetScaler instances for communication. For information about the ports that must be open between the NetScaler instances and NetScaler MAS, see Ports.

For NetScaler SD-WAN WO and NetScaler SD-WAN EE instances, NetScaler MAS uses the mangagement IP address of the instances for communication.

This document includes the following information:

- How NetScaler MAS Discovers and Adds Instances
- How to Add Instances to NetScaler MAS

How NetScaler MAS Discovers and Adds Instances

When you add an instance to the NetScaler MAS server, the server implicitly adds itself as a trap destination for the instance and collects inventory of the instance.

The following diagram describes how NetScaler MAS implicitly discovers and adds instances.
As shown in the diagram, the following steps are performed implicitly by NetScaler MAS.

1) The NetScaler MAS server sends an Internet Control Message Protocol (ICMP) ping to locate the instance. Then, it uses the instance profile details to log on to the instance. Using a NetScaler NITRO call, NetScaler MAS retrieves the license information of the instance. On the basis of the licensing information, it determines whether the instance is a NetScaler instance and the type of NetScaler platform (for example, NetScaler MPX, NetScaler VPX, NetScaler SDX, or NetScaler Gateway). On successful detection of the NetScaler instance, it is added to the NetScaler MAS server's database.

For NetScaler SD-WAN instances, NetScaler MAS does not detect the instance by using licensing information. Instead, after locating the instance by using ICMP ping, it sends a NITRO request to the instance to check for the instance type and version.

This step might fail if the instance profile does not include the correct credentials. For NetScaler MPX, NetScaler VPX, NetScaler SDX, and NetScaler Gateway instances, this step might also fail if the licenses are not applied to the instance.

2) NetScaler MAS adds its IP address to the list of trap destinations on the instance. This allows the NetScaler MAS server to receive traps generated on the NetScaler instance.

This step might fail if the number of trap destinations on the NetScaler instance exceeds the maximum limit of trap destinations. The maximum limit on NetScaler instances is 20.

For NetScaler SD-WAN instances, NetScaler MAS adds its IP address as the SNMP manager on the instance.

3) NetScaler MAS collects inventory from the instance by sending a NITRO request. It collects instance details such as host name, software version, running and saved configuration, certificate details, entities configured on the instance, and so on.

This step might fail because of network or firewall issues.

How to Add Instances to NetScaler MAS

You can add instances either while setting up the NetScaler MAS server for the first time or at a later time.

To add instances, you must specify either the host name or IP address of each NetScaler instance, or a range of IP addresses.
For SD-WAN instances, specify the IP address of each instance, or a range of IP addresses. Note that NetScaler MAS supports only NetScaler SD-WAN WO and NetScaler SD-WAN EE editions.

You must then specify an instance profile that NetScaler MAS can use to access the instance.

This instance profile contains the user name and password of the instance(s) that you want to add to NetScaler MAS. For each instance type, a default profile is available. For example, the ns-root-profile is the default profile for NetScaler instances. This profile is defined by the default NetScaler administrator credentials. If you have changed the default admin credentials of your instances, you can define custom instance profiles for those instances. If you change the credentials of an instance after the instance is discovered, you must edit the instance profile or create a new profile, and then rediscover the instance.

**Note**

- To add NetScaler instances configured in a cluster, you must specify either the cluster IP address or any one of the individual nodes in the cluster setup. However, on NetScaler MAS, the cluster is represented by the cluster IP address only.
- For NetScaler instances set up as an HA pair, when you add one instance, the other instance in the pair is automatically added.

If two NetScaler MAS servers are set up in high availability mode, when an instance is added, load balancing comes into effect and the instances are distributed across the two NetScaler MAS server nodes by using the round-robin method.

**To add an instance to NetScaler MAS**

1) In a web browser, type the IP address of the NetScaler Management and Analytics System (for example, http://192.168.100.1).

2) In the User Name and Password fields, enter the administrator credentials. The default administrator credentials are nsroot/nsroot.
3) Navigate to **Infrastructure > Dashboard** and click **All Instances**. On the **Instances** page, click **New** at the top right corner of the page. On the **Add Instances** page, from **Instance Type**, select the type of instance you want to add, and then follow the instructions in step 4.

Alternatively, navigate to **Infrastructure > Instances**. Under **Instances**, select the type of instance you want to add (for example, NetScaler VPX) and click **Add**.

4) Select one of the following options:

- **Enter Device IP address** - For NetScaler instances, specify either the host name or IP address of each instance, or a range of IP addresses. For SD-WAN instances, specify the IP address of each instance, or a range of IP addresses.
- **Import from file** - From your local system, upload a text file that contains the IP addresses of all the instances you want to add.

5) From **Profile Name**, select the appropriate instance profile, or create a new profile by clicking the + icon.

**Note**

For NetScaler CPX instances, you must specify the **HTTP**, **HTTPS**, **SSH**, and **SNMP** port details of the host. You can also specify the range of ports that were published by the host in the **Start Port** and **Number of ports** field. Also, if your NetScaler CPX IP address is reachable from the NetScaler MAS server, select the **Routable** checkbox. If your NetScaler CPX IP address is reachable through the host, uncheck the **Routable** checkbox and specify the host's IP address.

6) Click **OK** to initiate the process of adding instances to NetScaler MAS.
Note

If you want to rediscover an instance, navigate to **Infrastructure > Instances > NetScaler <Instance Type>**, select the instance you want to rediscover, and then from the **Action** drop-down list, click **Rediscover**.
Upgrading NetScaler MAS

Oct 18, 2016

Each NetScaler MAS release offers new and updated features with increased functionality. Citrix recommends you upgrade NetScaler MAS to the latest release to avail of the new features and bug fixes. A comprehensive list of enhancements, known issues, and bug fixes is included in the release notes accompanying the release announcement. It is also important to understand the licensing framework and types of licenses before you start to upgrade. For NetScaler MAS licensing information, see Licensing.

After the upgrade operation is started, NetScaler MAS restarts and the existing connections are terminated and reconnected when the upgrade is completed successfully. The existing configuration is preserved, but NetScaler MAS does not process any data until the upgrade is successfully completed.

For NetScaler MAS servers in high availability mode, you can upgrade either by accessing the first node or the second node or the load balancing virtual server IP address. Both the NetScaler MAS servers will automatically upgrade to the latest build once you initiate the upgrade process in either of the servers.

Note the following recommended precautions:

- Back up the NetScaler MAS server before you upgrade.
- After the upgrade, you might have to reestablish connections between the NetScaler MAS and the monitored instances. A confirmation prompt warns you that connections can fail if you proceed.
- For NetScaler MAS servers in high availability pair, when upgrading, do not make any configuration changes from either of the nodes.

Warning

You should not refresh the browser until the upgrade process is successfully completed. It might take a few minutes for the upgrade process to finish.

To upgrade NetScaler MAS

1. In a web browser, type the IP address of the NetScaler MAS server.
   Note: For NetScaler MAS servers in High Availability mode, type the IP address of either of the NetScaler MAS servers in the HA pair, or the load balancing virtual server IP address.

2. In the User Name and Password fields, enter the administrator credentials.

3. Navigate to System > System Administrations. Under the System Administration sub-heading, click Upgrade NetScaler MAS.

4. On the Upgrade NetScaler MAS page, upload a new image file by selecting either Local (your local machine) or Appliance (the build file must be present on the NetScaler MAS virtual appliance).
5. Click **OK**. Upgrade process starts along with the following message.

![Initialization message](image)
How-to Articles

Jun 19, 2017

NetScaler MAS "How-to Articles" are simple, relevant, and easy to implement articles on the features of NetScaler MAS. These articles contain information about some of the popular NetScaler MAS features such as instance management, application management, StyleBooks, certificate management, and Analytics.

Click a feature name in the table below to view the list of how-to articles for that feature.

<table>
<thead>
<tr>
<th>Instance Management</th>
<th>Configuration Management</th>
<th>Certificate Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Management</td>
<td>StyleBooks</td>
<td>Analytics</td>
</tr>
<tr>
<td>Event Management</td>
<td>Authentication</td>
<td>NetScaler MAS System</td>
</tr>
</tbody>
</table>

Instance Management

How to Add Instances to NetScaler MAS
How to Create Instance Groups on NetScaler MAS
How to Configure Data Centers for Geomaps in NetScaler MAS
How to Force a Failover to the Secondary NetScaler Instance by Using NetScaler MAS
How to Force a Secondary NetScaler Instance to Stay Secondary by Using NetScaler MAS
How to Back Up and Restore an Instance using NetScaler MAS

Configuration Management

How to Upgrade NetScaler SDX Instances by Using NetScaler MAS
How to Schedule Jobs Created by Using Built-in Templates in NetScaler MAS
How to Reschedule Jobs That Were Configured by Using Built-in Templates in NetScaler MAS
How to Reuse Executed Configuration Jobs
How to Upgrade NetScaler Instances using NetScaler MAS
How to Create a Configuration Job on NetScaler MAS
How to Use Variables in Configuration Jobs on NetScaler MAS
How to Use Configuration Templates to Create Audit Templates on NetScaler MAS
How to Create Configuration Jobs from Corrective Commands on NetScaler MAS
How to Replicate Running and Saved Configuration Commands from One NetScaler Instance to Another on NetScaler MAS
How to Create Configuration Jobs for NetScaler SD-WAN WO Instances in NetScaler MAS
Certificate Management

- How to Configure an Enterprise Policy on NetScaler MAS
- How to Install SSL Certificates on a NetScaler Instance from NetScaler MAS
- How to Update an Installed Certificate from NetScaler MAS
- How to Link and Unlink SSL Certificates by Using NetScaler MAS
- How to Create a Certificate Signing Request (CSR) by Using NetScaler MAS
- How to Set Up Notifications for SSL Certificate Expiry from NetScaler MAS
- How to Use the SSL Dashboard to Monitor Certificates from NetScaler MAS

Application Management

- How to Search for Entities in NetScaler MAS
- How to Disable Entities in NetScaler MAS
- How to View the Effective State of a Virtual Server on NetScaler MAS
- How to Create an Application Definition in NetScaler MAS
- How to Create Load Balancing Support through Application Dashboard in NetScaler MAS

StyleBooks

- How to Use StyleBooks Shipped with NetScaler MAS
- How to Create Your Own StyleBooks
- How to Use User-Defined StyleBooks in NetScaler MAS
- How to Use API to Create Configurations from StyleBooks
- How to Enable Analytics and Configure Alarms on a Virtual Server Defined in a StyleBook
- How to Create a StyleBook to Upload SSL Certificate and Certificate Key Files to NetScaler MAS
- How to Use Microsoft Exchange StyleBook for Business Enterprises
- How to Use Microsoft Skype for Business StyleBook for Business Enterprises

Analytics

- How to Enable Analytics on Instances
- How to Configure Adaptive Thresholds
- How to Configure SLA Management
- How to Configure Database Summarization for Analytics
How to Create Thresholds and Alerts Using NetScaler MAS
How to Disable URL Data Collection for Analytics from NetScaler MAS
How to View Network Reports for NetScaler SD-WAN WO Instances

Event Management
How to Set Event Age for Events on NetScaler MAS
How to Schedule an Event Filter by Using NetScaler MAS
How to Set Repeated Email Notifications for Events from NetScaler MAS
How to Suppress Events by Using NetScaler MAS
How to Use the Events Dashboard to Monitor Events
How to Set Multiple Event Rules Notifications in NetScaler MAS
How to Modify the Reported Severity of Events that Occur on NetScaler Instances
How to View the Events Summary in NetScaler MAS
How to View Event Reports for NetScaler SD-WAN WO Instances
How to Display Event Severities and Skews of SNMP Traps on the Infrastructure Dashboard of NetScaler MAS

Authentication
How to Cascade External Authentication Servers
How to Add RADIUS Authentication Servers
How to Add LDAP Authentication Servers
How to Add TACACS Authentication Servers
How to Extract Authentication Server Group in NetScaler MAS
How to Enable Fallback Local Authentication

NetScaler MAS System
How to Use Database Recovery Script to Recover Inaccessible NetScaler MAS Servers
How to Upgrade NetScaler MAS
How to Generate a Tech Support File for NetScaler MAS
How to Back up and Restore your NetScaler MAS Server in a Single-Server Deployment
How to Back Up and Restore a NetScaler MAS Configuration in an HA Pair
How to Enable Shell Access for Non-Default Users in NetScaler MAS
How to Configure NTP Server on NetScaler MAS
How to Configure SSL Settings for NetScaler MAS
How to Configure Syslog Purging Interval for MAS
How to View Auditing Information of NetScaler MAS
How to Configure System Notification Settings of NetScaler MAS
How to Monitor CPU, Memory, and Disk Usage of NetScaler MAS
How to Configure a Cipher Group for NetScaler MAS
How to Create SNMP Traps, Managers, and Users on NetScaler MAS
How to Assign a Host Name to a NetScaler MAS Server
How to Add Instances to NetScaler MAS

Jan 17, 2017

Instances are Citrix appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler MAS. You must add instances to the NetScaler MAS server if you want to manage and monitor these instances. You can add the following Citrix appliances and virtual appliances to NetScaler MAS:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway
- NetScaler SD-WAN WO
- NetScaler SD-WAN EE

You can add instances either while setting up the NetScaler MAS server for the first time or at a later time.

**Note**

NetScaler MAS uses the NetScaler IP (NSIP) address of the NetScaler instances for communication. For information about the ports that must be open between the NetScaler instances and NetScaler MAS, see Ports.

For NetScaler SD-WAN WO and NetScaler SD-WAN EE instances, NetScaler MAS uses the management IP address of the instances for communication.

How NetScaler MAS Discovers and Adds Instances

When you add an instance to the NetScaler MAS server, the server implicitly adds itself as a trap destination for the instance and collects inventory of the instance.

The following diagram describes how NetScaler MAS implicitly discovers and adds instances.

![Diagram showing how NetScaler MAS discovers and adds instances](image-url)
As shown in the diagram, the following steps are performed implicitly by NetScaler MAS.

1) The NetScaler MAS server sends an Internet Control Message Protocol (ICMP) ping to locate the instance. Then, it uses the instance profile details to log on to the instance. Using a NetScaler NITRO call, NetScaler MAS retrieves the license information of the instance. On the basis of the licensing information, it determines whether the instance is a NetScaler instance and the type of NetScaler platform (for example, NetScaler MPX, NetScaler VPX, NetScaler SDX, or NetScaler Gateway). On successful detection of the NetScaler instance, it is added to the NetScaler MAS server’s database.

For NetScaler SD-WAN instances, NetScaler MAS does not detect the instance by using licensing information. Instead, after locating the instance by using ICMP ping, it sends a NITRO request to the instance to check for the instance type and version.

This step might fail if the instance profile does not include the correct credentials. For NetScaler MPX, NetScaler VPX, NetScaler SDX, and NetScaler Gateway instances, this step might also fail if the licenses are not applied to the instance.

2) NetScaler MAS adds its IP address to the list of trap destinations on the instance. This allows the NetScaler MAS server to receive traps generated on the NetScaler instance.

This step might fail if the number of trap destinations on the NetScaler instance exceeds the maximum limit of trap destinations. The maximum limit on NetScaler instances is 20.

For SD-WAN instances, NetScaler MAS adds its IP address as the SNMP manager on the instance.

3) NetScaler MAS collects inventory from the instance by sending a NITRO request. It collects instance details such as host name, software version, running and saved configuration, certificate details, entities configured on the instance, and so on.

This step might fail because of network or firewall issues.

How to Add Instances to NetScaler MAS

You can add instances either while setting up the NetScaler MAS server for the first time or at a later time.

To add instances, you must specify either the host name or IP address of each instance, or a range of IP addresses.

For SD-WAN instances, specify the IP address of each instance, or a range of IP addresses. Note that NetScaler MAS supports only NetScaler SD-WAN WO and NetScaler SD-WAN EE editions.

You must then specify an instance profile that NetScaler MAS can use to access the instance.

This instance profile contains the user name and password of the instance(s) that you want to add to NetScaler MAS. For each instance type, a default profile is available. For example, the ns-root-profile is the default profile for NetScaler instances. This profile is defined by the default NetScaler administrator credentials. If you have changed the default admin credentials of your instances, you can define custom instance profiles for those instances. If you change the credentials of an instance after the instance is discovered, you must edit the instance profile or create a new profile, and then rediscover the instance.

Note

- To add NetScaler instances configured in a cluster, you must specify either the cluster IP address or any one of the individual nodes in the cluster setup. However, on NetScaler MAS, the cluster is represented by the cluster IP address only.
For NetScaler instances set up as an HA pair, when you add one instance, the other instance in the pair is automatically added.

If two NetScaler MAS servers are set up in high availability mode, when an instance is added, load balancing comes into effect and the instances are distributed across the two NetScaler MAS server nodes by using the round-robin method.

To add an instance to NetScaler MAS

1) Log on to the NetScaler MAS server.
2) Navigate to Infrastructure > Dashboard and click All Instances. On the Instances page, click New at the top right corner of the page. On the Add Instances page, from Instance Type, select the type of instance you want to add, and then follow the instructions in step 3. Alternatively, navigate to Infrastructure > Instances. Under Instances, select the type of instance you want to add (for example, NetScaler VPX) and click Add.
3) Select one of the following options:
   - **Enter Device IP address** - For NetScaler instances, specify either the host name or IP address of each instance, or a range of IP addresses. For SD-WAN instances, specify the IP address of each instance, or a range of IP addresses.
   - **Import from file** - From your local system, upload a text file that contains the IP addresses of all the instances you want to add.
4) From Profile Name, select the appropriate instance profile, or create a new profile by clicking the + icon.

**Note**

For NetScaler CPX instances, you must specify the **HTTP**, **HTTPS**, **SSH**, and **SNMP** port details of the host. You can also specify the range of ports that were published by the host in the **Start Port** and **Number of ports** field. Also, if your NetScaler CPX IP address is reachable from the NetScaler MAS server, select the **Routable** checkbox. If your NetScaler CPX IP address is reachable through the host, uncheck the **Routable** checkbox and specify the host's IP address.

5) Click **OK** to initiate the process of adding instances to NetScaler MAS.

**Note**

If you want to rediscover an instance, navigate to Infrastructure > Instances > NetScaler <Instance Type>, select the instance you want to rediscover, and then from the Action drop-down list, click Rediscover.
How to Configure Data Centers for Geomaps in NetScaler MAS

Nov 21, 2016

A NetScaler MAS data center is a logical grouping of the NetScaler instances in a specific geographical location. You can have several NetScaler instances within a data center that can be monitored and managed by the NetScaler MAS server. You can use the NetScaler MAS server to manage data such as syslog, appflow, and SNMP etc from the managed instances.

In addition to the server node, configure an IP block for your data center by specifying the lowest and highest IP addresses in a group of addresses assigned to instances at the data center. Multiple IP blocks can be associated with a data center.

Before configuring a data center, you must create IP blocks, so that NetScaler MAS can recognize which data center an instance belongs to when it is added to the NetScaler MAS server. For example, if the instance's IP address falls within the range of an IP block associated with Data Center 1, the instance being added to NetScaler MAS is known to be located in Data Center 1.

To create an IP block

1. Navigate to Infrastructure > Data Centers > IP Blocks, and then click Add.
2. In Configure IP Blocks, specify the name of the IP block and the starting and ending IP addresses in the IP block. Then, specify the country, region, and city. You might have to specify the latitude and longitude of the city if it is not already saved in the geo database.
3. Click Create to finish.

To configure a data center

1. Navigate to Infrastructure > Data Centers, and then click Add.
2. In Configure Data Center, specify the name of the data center.
3. From the list of available IP blocks, select one or more blocks to associate with the data center.
4. Click Create.
For more information on adding NetScaler instances to NetScaler MAS, see Adding an Instance to NetScaler MAS.
How to Force a Failover to the Secondary NetScaler Instance by Using NetScaler MAS

Jun 29, 2016

You might want to force a failover if, for example, you need to replace or upgrade the primary NetScaler instance. You can force failover from either the primary instance or the secondary instance. When you force a failover on the primary instance, the primary becomes the secondary and the secondary becomes the primary. Forced failover is only possible when the primary instance can determine that the secondary instance is UP.

A forced failover is not propagated or synchronized. To view the synchronization status after a forced failover, you can view the status of the instance.

A forced failover fails in any of the following circumstances:

- You force failover on a standalone system.
- The secondary instance is disabled or inactive. If the secondary instance is in an inactive state, you must wait for its state to be UP to force a failover.
- The secondary instance is configured to remain secondary.

The NetScaler instance displays a warning message if it detects a potential issue when you run the force failover command. The message includes the information that triggered the warning, and requests confirmation before proceeding.

You can force a failover on a primary instance or on a secondary instance.

To force a failover to the secondary NetScaler instance using NetScaler MAS

1. In NetScaler MAS, navigate to **Infrastructure > Dashboard > Instances**, and then select an instance under an instance type (NetScaler VPX).
2. Select instances in an HA setup from the instances listed under the selected instance type.
3. From the **Action** drop-down, select **Force Failover**.
4. Click **Yes** to confirm the force failover action.
NetScaler VPX

- Add
- Edit
- Delete
- Dashboard
- View Backup

**Profiles**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.102.62.204-10.102</td>
<td>Select Action, Create Cluster, Reboot</td>
</tr>
<tr>
<td>10.102.40.150-10.102</td>
<td>Force Failover, Stay Secondary, Events, Ping, TraceRoute, Rediscover, Enable/Disable Insight, Unmanage, Annotate, Configure SNMP, Configure Syslog</td>
</tr>
<tr>
<td>10.102.40.80</td>
<td></td>
</tr>
<tr>
<td>10.102.163.4</td>
<td></td>
</tr>
</tbody>
</table>
How to Force a Secondary NetScaler Instance to Stay Secondary by Using NetScaler MAS

Jun 29, 2016

In an HA setup, the secondary node can be forced to stay secondary regardless of the state of the primary node.

For example, suppose that the primary node needs to be upgraded and the process takes a few seconds. During the upgrade, the primary node might go down for a few seconds, but you do not want the secondary node to take over; you want it to remain the secondary node even if it detects a failure in the primary node.

When you force the secondary node to stay secondary, it will remain secondary even if the primary node goes down. Also, when you force the status of a node in an HA pair to stay secondary, it does not participate in HA state machine transitions. The status of the node is displayed as STAYSECONDARY.

Forcing the node to stay secondary works on both standalone and secondary nodes. On a standalone node, you must use this option before you can add a node to create an HA pair. When you add the new node, the existing node continues to function as the primary node, and the new node becomes the secondary node.

**Note**

When you force a system to remain secondary, the forcing process is not propagated or synchronized. It affects only the node on which you run the command.

To configure a secondary NetScaler instance to stay secondary by using NetScaler MAS

1. In NetScaler MAS, navigate to **Infrastructure > Dashboard > Instances**, and then select an instance under an instance type (NetScaler VPX).
2. Select instances in an HA setup from the instances listed under the selected instance type.
3. From the **Action** drop-down, select **Stay Secondary**.
4. Click **Yes** to confirm the execution of the “Stay Secondary” action.
NetScaler VPX

![NetScaler VPX interface screenshot]

- **Add**
- **Edit**
- **Delete**
- **Dashboard**
- **View Backup**

### IP Address
- 10.102.62.204-10.102.62.206
- 10.102.40.150-10.102.40.152
- 10.102.40.80

- Select Action
  - Create Cluster
  - Reboot
  - Force Failover
  - Stay Secondary
- **Events**
- **Ping**
- **TraceRoute**
- **Rediscover**
- **Enable/Disable Insight**
- **Unmanage**
How to Create Instance Groups on NetScaler MAS

Jun 30, 2016
To create an instance group, you must first add all your NetScaler instances to NetScaler MAS. After you have added the instances successfully, create instance groups based on their device family. By creating a group of instances, you can simultaneously perform actions such as upgrade, backup, and restore on all instances that have been grouped, instead of performing them on each instance separately.

To create an instance group using NetScaler MAS
1. In NetScaler MAS, navigate to **Infrastructure > Instance Groups**, and then click **Add**.
2. Give a name to your instance group and select the device family from the drop-down menu.
3. Move the instances from the available table to the configured table to add them to your instance group.
4. Click **Create**.
How to Back Up and Restore an Instance using NetScaler MAS

Jun 30, 2016

You can back up the current state of a NetScaler instance. At a later time, if the instance becomes unstable, you can use the backed up files to restore the instance to the stable state. Use this feature before performing an upgrade or for precautionary reasons.

To back up an instance by using NetScaler MAS

1. In NetScaler MAS, navigate to **Infrastructure > Instances**. Under **Instances**, select the type of instance (NetScaler VPX) to view a list of instances of that type.
2. Select the instance that you want to back up, and then click **View Backup**.
3. On the **Backup Files** page, click **Back Up**.
4. You can choose to encrypt your backup file for additional security.
5. Click **Continue**.

To restore an instance using NetScaler MAS

1. Navigate to **Infrastructure > Instances**, select the instance that you want to restore, and then click **View Backup**.
2. On the **Backup Files** page, select the backup file that you want to restore, and then click **Restore**.
How to Upgrade NetScaler SDX Instances by Using NetScaler MAS

Jun 29, 2016
You can perform a single-bundle upgrade of your NetScaler SDX instances running NetScaler release 11.0 and later. To perform a single-bundle upgrade, you use a built-in task in NetScaler MAS. With this built-in task, you can upgrade the NetScaler SDX Management Service, XenServer hypervisor, and the supplemental packs and hotfixes for XenServer hypervisor.

To upgrade NetScaler SDX instances using NetScaler MAS

1. In NetScaler MAS, navigate to Infrastructure > Configuration Jobs > Maintenance Tasks, and then execute the UpgradeNSSDX built-in task to upgrade your NetScaler SDX instances.
2. On the Upgrade NetScaler SDX Appliance(s) page, from the Software Image drop-down menu, select either Local (your local machine) or Appliance (the single bundle image file must be present on NetScaler MAS).
3. Click Add Instances. In the displayed list, select the NetScaler instances or instance groups that you want to upgrade.
4. Click OK. You can monitor the progress of the NetScaler SDX upgrade through a task log. To view the task log, click the Execution Summary button.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UpgradeNetScaler</td>
<td>Upgrade NetScaler.</td>
</tr>
<tr>
<td>UpgradeCloudBridgeWANOpt</td>
<td>Upgrade CloudBridge WAN Opt.</td>
</tr>
<tr>
<td>UpgradeNSSDX</td>
<td>Upgrade NetScaler SDX.</td>
</tr>
<tr>
<td>ConfigureHAPair</td>
<td>Configure HA Pair of NetScaler Instances.</td>
</tr>
<tr>
<td>ConvertHAtoCluster</td>
<td>Convert HA Pair of Instances to 2 Node Cluster.</td>
</tr>
</tbody>
</table>
How to Schedule Jobs Created by Using Built-in Templates in NetScaler MAS

Dec 27, 2016

You can schedule a job by using the built-in template option. A job is a set of configuration commands that you can run on one or more managed instances. For example, you can use the built-in template option to schedule a job to configure syslog servers. You can also, choose to execute the job immediately or schedule the job to be executed at a later stage.

To schedule a job by using built-in templates in NetScaler MAS

1. In NetScaler MAS, navigate to Infrastructure > Configuration Jobs, and then click Create Job.

2. On the Create Job page, on the Select Configuration tab, specify the Job Name and select the Instance Type from the drop-down list.

3. Select Inbuilt Template from the Configuration Source drop-down list. Drag and drop the NSConfigureSyslogServer command to the right pane, and then click Next.

4. On the Select Instances tab, click Add Instances, select the instances on which you want to run the job, and then click OK.

5. Click Next. On the Specify Variable Values tab, select one of the following options to specify variables for your instances:

   - Variable values from an input file - Download an input file to enter values for the variables that you have defined in your commands, and then upload the file to the NetScaler MAS server.
   - Common variable values for all instances – Specify the syslog server IP address and port.

6. On the Job Preview tab, you can evaluate and verify the commands to be run on each instance or instance group.

7. Click Next.
8. On the **Execute** tab, set the following conditions:

- **On Command Failure** - If a command fails, you can either choose to ignore the errors and continue to execute the job or stop further execution of the job. Choose the action that you want to execute from the drop-down list.
- **Execution Mode** - You can either execute the job now or schedule to execute the job at a later time. If you want to schedule the job at a later time, you must specify the execution frequency settings for that job. Choose the schedule you want the job to follow from the drop-down list.

9. You can also execute a job on a set of instances sequentially or in parallel by selecting the required method under **Execution Settings**. If a job execution fails on any instance, it does not continue on the remaining instances.

10. Click **Finish**.
How to Reschedule Jobs That Were Configured by Using Built-in Templates in NetScaler MAS

Sep 29, 2016

You can reschedule a job that you scheduled by using built-in templates in NetScaler MAS. For example, you can change the action that NetScaler MAS must take if a command fails. If you had previously opted to ignore an error and continue, you can change it to roll back all successful commands if a command fails.

To reschedule a job that was configured by using built-in templates in NetScaler MAS

1. In NetScaler MAS, navigate to Infrastructure > Configuration Jobs.
2. Select the job you want to edit, add or remove instances, specify variable values, and then change execution actions and settings.
3. Click Finish to reschedule the job.

Note

You can also select the job and click Execute again to run the job without modifying any source, instance, and commands. This is useful when you have to run the same set of commands on same instances. Sometimes, the job may encounter a transient error from the server side, and you may have to run the job again.
How to Reuse Executed Configuration Jobs

Sep 29, 2016

Configuration jobs allows you to create a set of configuration commands that you can run on one or more managed instances. You can also run the same set of saved configuration jobs after modifying the commands, the parameters, the configuration source, and instances in the job. This is useful when the same set of commands have to be executed on a different instance, or when the job encounters an error and stops further execution.

NetScaler MAS provides a function to execute the completed jobs again. With this function, jobs that are executed completely can be run again without changing the job name.

**Note**: You can re-execute only those jobs that are executed when the mode of execution is “Now”.

**To edit completed jobs**

1. From NetScaler MAS home page navigate to **Infrastructure > Configuration Jobs**.
2. In **Jobs** page, select a job that shows the Execution Summary as Completed, and click **Edit**. You can also edit a scheduled configuration job.
3. In **Configure Job** page, you can see that the Job Name and the Instance type are non-editable. You can modify other fields like configuration source, add instances, edit variable values, and set execution settings.
4. Click **Finish** to run the configuration job again.

**Note**
You can also select the job and click Execute again to run the job without modifying any source, instance, and commands. This is useful when you have to run the same set of commands on same instances. Sometimes, the job may encounter a transient error from the server side, and you may have to run the job again.
## Jobs

<table>
<thead>
<tr>
<th>Action</th>
<th>Name</th>
<th>Exec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Action</td>
<td>ns-config-syslog</td>
<td>Execute Again</td>
</tr>
<tr>
<td>Execution Hist</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Completed**
  - Started by nsroot
  - on Sep 16 1:04 PM

- **Created on:** Sep 16 1:04 PM
- **Created by:** nsroot
How to Upgrade NetScaler Instances using NetScaler MAS

Dec 16, 2016

You can use NetScaler MAS to upgrade one or more NetScaler instances. Before upgrading an instance, make sure that you have uploaded the correct build and documentation files to the NetScaler instances. Also, it is recommended that you understand the licensing framework and types of licenses before you upgrade any instances.

To upgrade a NetScaler instance using NetScaler MAS

1. In NetScaler MAS, navigate to Infrastructure > Configuration Jobs > Maintenance Tasks, and then execute the UpgradeNetScaler built-in task to upgrade the NetScaler instance.

2. On the Upgrade NetScaler Appliance(s) page, from the Software Image drop-down menu, select either Local (your local machine) or Appliance (the certificate file must be present on the NetScaler MAS virtual appliance).

3. Click Add Instances. In the displayed list, select the NetScaler instances or instance groups that you want to upgrade.

Note

- To upgrade NetScaler instances in high availability mode, you have to select the IP addresses of the primary and secondary instances.
- To upgrade NetScaler instances in cluster mode, select the cluster IP address.

4. Click OK. You can monitor the progress of the NetScaler instance upgrade through a task log. To view the task log, click the Execution Summary button.
How to Create a Configuration Job on NetScaler MAS

Dec 27, 2016

A job is a set of configuration commands that you can create and run on one or more multiple managed instances. You can create jobs to make configuration changes across instances, replicate configurations on multiple instances on your network, and record-and-play configuration tasks using the NetScaler MAS GUI and convert it into CLI commands.

You can use the Configuration Jobs feature of NetScaler MAS to create a configuration job, send email notifications, and check execution logs of the jobs created.

To create a configuration job on NetScaler MAS

1. Navigate to the Infrastructure > Configuration Jobs.
2. Click Add to create a job.
3. After selecting the required custom job parameters such as the name of the job, the configuration type, adding instances it must be run on, the variables for the instances.
4. In the Execute tab, choose to either execute your job now or schedule to execute the job at a later time. Also, you must also select what action NetScaler MAS should take if the command fails.

To send email notification for a job

An email notification is now sent every time a job is executed or scheduled. The notification will cover details such as the success or failure of the job along with the relevant details.

After creating a job, in the Execute tab, select the Email checkbox under the Receive Execution Report Through section. Choose an email distribution list from the drop-down list. You can also create an email distribution list by clicking the + icon and specifying email server details.

To view execution summary details
Navigate to **Infrastructure > Configuration Jobs**. Select a job and click **Details**. Click Execution Summary to see the status of the instance on that executed the job, the commands executed on the job, the start and end time of the job, and the instance user's name.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Status</th>
<th>Commands</th>
<th>Start Time</th>
<th>End Time</th>
<th>Instance User</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.102.29.191</td>
<td>Completed</td>
<td>3/3</td>
<td>Sep 16 1:04 PM</td>
<td>Sep 16 1:04 PM</td>
<td>nsroot</td>
</tr>
</tbody>
</table>
How to Use Variables in Configuration Jobs on NetScaler MAS

May 18, 2017
A configuration job is a set of configuration commands that you can execute on one or more managed instances. When you execute the same configuration on multiple instances, you might want to use different values for the parameters used in your configuration. You can define variables that enable you to assign different values for these parameters or execute a job across multiple instances.

For example, consider a basic load balancing configuration where you add a load balancing virtual server, add two services, and bind the services to the virtual server. Now, you might want to have the same configuration on two instances but with different values for the virtual server and services names and IP addresses. You can use the configuration jobs feature to achieve this by using variables to define the names and IP addresses of the virtual server and services.

In this example, the following commands and variables are used:

```plaintext
add lb vserver servername HTTP ipaddress portnumber
add service servicename1 ipaddress1 HTTP 80
add service servicename2 ipaddress2 HTTP 80
bind lb vserver servername servicename1
bind lb vserver servername servicename2
```

To create a configuration job by defining variables in NetScaler MAS

1. Navigate to Infrastructure > Configuration Jobs.
2. Click Add to create a job.
3. On the Create Job page, select the custom job parameters such as the name of the job, the instance type, and the configuration type.
4. In the Configuration Editor, type in the commands to add a load balancing virtual server, two services, and bind the services to the virtual server. Select the values that you want to convert to a variable, and then click Convert to Variable. For example, select the IP address of the load balancing server ipaddress, and click Convert to Variable as shown in the image below.
5. Once you see dollar signs enclose the variable's value, click on the variable to further specify the details of the variable such as name, display name, and type. You can also click the Advanced option if you want to further specify a default value for your variable. Click Save and then, click Next.

Type in the rest of your commands and define all the variables.
6. Select the instances you want to run the configuration job on.

7. In the **Specify Variable Values** tab, select the **Variable Values from an Input File** option and then click **Download Input Key File**. In our example, you will need to specify the server name on each instance, the IP addresses of the server and services, port numbers, and the service names. Save the file and upload it. If your values aren't defined accurately, the system might throw an error.

8. The input key file is downloaded to your local system and you can edit it by specifying the variable values for each NetScaler instance you've selected previously and click **Upload** to upload the input key file to NetScaler MAS. Click **Next**.

9. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

10. In the **Execute** tab, you can choose to execute your job now or schedule it to be executed at a later time. You can also choose what action NetScaler MAS should take if the command fails and if you'd like to send an Email notification regarding the success or failure of the job along with other details.
After configuring your jobs and executing it, you can see the job details by navigating to **Infrastructure > Configuration Jobs** and select the job you just configured. Click on **Details** and then, click on **Variable Details** to see the list of variables added to your job.
How to Use Configuration Templates to Create Audit Templates on NetScaler MAS

Dec 27, 2016

You can now use configuration commands that were previously saved as configuration templates to create Audit Templates that can be applied to specific NetScaler instances. While creating an audit template, you can drag and drop previously saved configuration templates into the Commands field, and edit the template to suit your requirements. You can then apply the audit template to specific NetScaler instances. NetScaler MAS compares these instances with the audit template and reports any mismatch. This process helps you identify errors and rectify them in a timely manner.

You can create configuration templates while creating a new job and saving a set of configuration commands as a template. When you save these templates on the Create Jobs page, they are automatically displayed on the Create Template page.

For example, consider a basic load balancing configuration for which you add a load balancing virtual server, add two services, and bind the services to the virtual server.

This example uses the following commands:

- `add lb vserver servername HTTP ipaddress portnumber`
- `add service servicename1 ipaddress1 HTTP 80`
- `add service servicename2 ipaddress2 HTTP 80`
- `bind lb vserver servername servicename1`
- `bind lb vserver servername servicename2`

To save a configuration template in NetScaler MAS

1. Navigate to Infrastructure > Configuration Jobs, and click Create Job.
2. On the Create Job page, specify the job name and the instance type.
3. Choose Configuration Template as the Configuration Source and, in the Commands field, enter commands such as those in the above example.
4. Select the Save as Configuration Template checkbox and specify a name for your template. You can choose to overwrite other templates that exist with the same name.
5. Click Save.
To use a configuration template to create an audit template in NetScaler MAS

1. Navigate to **Infrastructure > Configuration Audit > Audit Templates**, and click **Add**.
2. On the **Create Template** page, specify a name for the template name, and enter a description.
3. From the **Configuration Source** list, select **Configuration Template**, and then drag and drop the template into the Commands field in the right pane. You can also edit the configuration and save the template with a different name. Click **Next**.
4. On the **Select Instances** tab, click **Add Instances** and add the instances on which you want to run the configuration. Click **OK**.
5. Click **Finish**.
The audit template appears in the Audit Templates list and is run every 12 hours against the configurations of the specified instances.
How to Create Configuration Jobs from Corrective Commands on NetScaler MAS

Dec 27, 2016

You can create audit templates with specific configurations that you want running on certain NetScaler instances. NetScaler MAS compares these instances with the audit template and reports any mismatch in the configurations. If you change the configuration of some instances, you can use the NetScaler MAS corrective commands feature to create an audit template with the modified and corrected configuration commands for specific NetScaler instances.

When there is a difference a configuration commands being run on an instance and the command that is saved, a Diff Exists status message appears on the Audit Report page. Clicking the Diff Exists link takes you to the Configuration Diff page, where you can view the corrective command and create a job to be run on that specific instance.

To create a configuration job from corrective commands on NetScaler MAS

1. Navigate to Infrastructure > Configuration Audit.

2. On the Configuration Audit page, click on any graph to access the Audit Reports page.

3. Click the Diff Exists link for the instance for which you want to correct the configuration commands. The Configuration Diff page appears, listing the differences between the Saved Configuration, Running Configuration, and Correction Configuration for that instance.

4. Click Create Job to go to the Create Job page, on which the corrective commands pre-populated. For instructions on how to create a configuration job, see How to Create a Configuration Job on NetScaler MAS.
How to Replicate Running and Saved Configuration Commands from One NetScaler Instance to Another on NetScaler MAS

Dec 27, 2016
You can now replicate a NetScaler instance’s configuration on other instances. When you configure a job in NetScaler MAS, select an instance as the Configuration Source and choose the selected instance’s running or saved configuration.

For example, when you select Running Configuration and click Extract, NetScaler MAS sends a request to the selected NetScaler instance to locate the running configuration, and displays it as a template. You can drag and drop the template into the Commands field in the right-hand pane. You can modify commands, parameters, and the instances.

To replicate running and saved configuration commands of one instance to another instance on NetScaler MAS

1. Navigate to Infrastructure > Configuration Jobs, and click Create Job.

2. Specify the job name and the type of instance. For example, specify NetScaler Running Config1 as your job’s name and the instance type as NetScaler.

3. Select Instance as the Configuration Source, select the source instance whose configuration you want to replicate on other instances.

4. You will see the following three options:
   - Running Configuration
   - Saved Configuration
   - Configuration by time duration

5. Choose Running Configuration, and click Extract. The number of running configuration commands executed on that instance is displayed.
6. Drag and drop the commands in the **Commands** field in the right pane.

7. You can edit the commands in the Commands field. For example, if the commands extracted are to set up a NetScaler instance which includes adding partitions, setting up load balancing, binding the load balancing server to services, and so on. You may want to edit your commands, to set up your new NetScaler instances without partitions. So, to remove partitions, manually delete commands related to the creation of partitions and click **Next**.

8. Click **Add Instances** and add the instances on which you want to apply the running configuration commands. Click **OK** and then, click **Next**.

9. If you have specified variables in the commands, on the **Specify Variable Values** tab, click **Download Input Key File**. In the downloaded file, specify values for the variables, and then upload the file to NetScaler MAS.

10. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

11. In the **Execute** tab, you can choose to execute your job now or schedule it to be executed at a later time. You can also choose what action NetScaler MAS should take it the command fails and if you'd like to send an Email notification regarding the success or failure of the job along with other details.
How to Create Configuration Jobs for SD-WAN WO Instances in NetScaler MAS

Jan 24, 2017

A job is a set of configuration commands that you can create and schedule on one or more managed instances. For NetScaler SD-WAN WAN optimization (WO) instances, you can use the following options to create jobs:

- **Configuration Template**: You can use the configuration editor to type in CLI commands, save the configuration as a template, and use it to configure jobs.

- **Inbuilt Template**: You can choose from a list of configuration templates. These templates provide the syntaxes of the CLI commands and allow you to specify values for the variables. The inbuilt templates are listed, with their descriptions in the table below.

- **File**: You can upload a configuration file from your local machine and create jobs.

Once a job is created, you can choose to execute the job immediately or schedule the job to be executed later. You can also set the execution frequency.

<table>
<thead>
<tr>
<th>Inbuilt Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnableCloudBridgeWANOpt</td>
<td>Enables traffic through the NetScaler SD-WAN WO appliance.</td>
</tr>
<tr>
<td>DisableCloudBridgeWANOpt</td>
<td>Disables the traffic through NetScaler SD-WAN WO appliance.</td>
</tr>
<tr>
<td>RestartCloudBridgeWANOpt</td>
<td>Restarts NetScaler SD-WAN WO appliance.</td>
</tr>
<tr>
<td>RestoreConfig</td>
<td>Restores the configuration of NetScaler SD-WAN WO appliance.</td>
</tr>
<tr>
<td>AddLink</td>
<td>Creating or defining links enable the SD-WAN WO appliance to prevent congestion and loss on the links and to perform traffic shaping. You can define the maximum bandwidth sent or received over the link and also specify it is LAN side or WAN side traffic.</td>
</tr>
<tr>
<td>ConfigureBandwidth</td>
<td>Sets the bandwidth limits and other bandwidth management settings.</td>
</tr>
<tr>
<td>AddUser</td>
<td>Adds a new user, for whom you can assign privileges.</td>
</tr>
<tr>
<td>AddUserAdvancedPlatform</td>
<td>Adds a new user enables you to assign privileges not available in the AddUser template.</td>
</tr>
<tr>
<td>AddService-class</td>
<td>Creates a service class for NetScaler SD-WAN WO appliance with one or more service class filters and enables it.</td>
</tr>
<tr>
<td>SetApplication</td>
<td>Sets the application classifier definition.</td>
</tr>
<tr>
<td>AddorRemoveVideoCachingPorts</td>
<td>Adds or removes the port number at which the video source can send or receive data. The default port is 80.</td>
</tr>
<tr>
<td>RemoveVideoCachingSource</td>
<td>Removes one or more video caching source. Specify the video source IP address or domain name.</td>
</tr>
<tr>
<td><strong>Inbuilt Template</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VideoCachingState</td>
<td>Enables or disables the video caching feature on NetScaler SD-WAN WO appliances.</td>
</tr>
<tr>
<td>ClearVideoCaching</td>
<td>Clears either the video cache or the video caching statistics.</td>
</tr>
<tr>
<td>SetVideoCaching</td>
<td>Sets the maximum size for cached objects. An object larger than this limit is not cached. By default, the maximum caching object size is 100 MB.</td>
</tr>
<tr>
<td>AddVideoCachingSource</td>
<td>Adds the IP address or the domain name of the video source. Includes options to enable or disable video caching for that source.</td>
</tr>
<tr>
<td>ConfigureRemoteLicenseServer</td>
<td>Configures the centralized license server. Specify the license server model, IP address and port number.</td>
</tr>
<tr>
<td>ConfigureLocalLicenseServer</td>
<td>Sets the license server location as local.</td>
</tr>
<tr>
<td>InstallCACert</td>
<td>Installs CA certificates on NetScaler SD-WAN WO appliance. Specify the certificate name, file name and the keystore password.</td>
</tr>
<tr>
<td>InstallCombinedCerKey</td>
<td>Installs a combined SSL certificate-key pair file.</td>
</tr>
<tr>
<td>InstallSeperateCertKey</td>
<td>Installs SSL certificate and key as separate files.</td>
</tr>
<tr>
<td>EnableWCCP</td>
<td>Enables WCCP deployment mode.</td>
</tr>
<tr>
<td>AddWCCPServiceGroup</td>
<td>Adds a new WCCP service-group definition for NetScaler SD-WAN WO appliance.</td>
</tr>
<tr>
<td>DisableWCCP</td>
<td>Disables the WCCP deployment mode.</td>
</tr>
<tr>
<td>AddTrafficShapingPolicy</td>
<td>Creates a traffic shaping policy for the NetScaler SD-WAN appliance. The policy controls the network bandwidth.</td>
</tr>
<tr>
<td>SetTrafficShapingPolicy</td>
<td>Modifies the traffic shaping policy for NetScaler SD-WAN WO appliance. The policy controls the network bandwidth.</td>
</tr>
<tr>
<td>AddVideoPrePopulation</td>
<td>Creates a video pre-population entry, which enables you to download and cache a video in advance. You can also specify when to cache a video.</td>
</tr>
<tr>
<td>UpdateVideoPrePopulation</td>
<td>Modifies a video prepopulation entry, which specifies when to cache a video.</td>
</tr>
<tr>
<td>AddVideoPrePopulationNow</td>
<td>Configures video prepopulation, enabling you to download and cache a video immediately. You can control how you want to download and cache videos from the URL(s).</td>
</tr>
<tr>
<td>VideoPrePopulationState</td>
<td>Changes, starts, updates, or removes video pre-population.</td>
</tr>
<tr>
<td>ConfigureSyslogServer</td>
<td>Sets the IP address and the port number of the syslog server.</td>
</tr>
<tr>
<td>ConfigureAlert</td>
<td>Configures alert level.</td>
</tr>
</tbody>
</table>

**To create a configuration job for NetScaler SD-WAN WO instances:**

1. In NetScaler MAS, navigate to **Networks > Configuration Jobs**, and then click **Create Job**.

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved.
2. On the **Create Job** page, under the **Select Configuration** tab, specify the **Job Name**.

3. In the **Instance Type** field, select **NetScaler SD-WAN WO**.

4. In the **Configuration Source** drop-down list, select an option to create a job.

   **Note**

   Select **Save as Configuration Template** and specify a name to save the configuration as a template and reuse it.

5. Click **Next**, and then on the **Select Instances** tab, click **Add Instances**. Select the instances on which you want to run the job, and then click **OK**.

6. Click **Next**, and then on the **Specify Variable Values** tab, select one of the following options to specify variables for your instances:

   * **Variable values from an input file**: Click **Download Input Key** File to download an input file. In the input file, enter values for the variables that you have defined in your commands, and then upload the file to the NetScaler MAS server.

   * **Common variable values for all instances**: Enter values for the variables. The variables vary depending on the selected template.
7. Click Next, on the Job Preview tab, you can evaluate and verify the commands to be executed as a job.

8. Click Next, on the Execute tab, set the following conditions:

* **On Command Failure:** What to do if a command fails: ignore the errors and continue the job, or stop further execution of the job. Choose an action from the drop-down list.

* **Execution Mode:** Execute the job immediately, or schedule execution for a later time. If you schedule execution for a later time, you must specify the execution frequency settings for the job. Choose the schedule you want the job to follow from the Execution Frequency drop-down list.
9. Under **Execution Settings**, select to execute the job sequentially (one after the other), or in parallel (at the same time).

10. To have a job execution report emailed to a list of recipients, select the **Email** checkbox in the **Receive Execution Report Through** section. From the drop-down list that appears, choose an email distribution list. To create an email distribution list, click the + icon and enter the email addresses of the recipients, and email server details.

11. Click **Finish**.
How to Set Event Age for Events on NetScaler MAS

Jun 29, 2016

You can set the Event Age option to specify the time interval (in seconds) after which NetScaler MAS refreshes an event rule.

For example, if you use NetScaler MAS to monitor and manage various NetScaler appliances, and you want to be notified by email every time any of your virtual servers goes down for 15 seconds or longer, you can create an event rule with the necessary filters and set the rule's event age to 15 seconds. Then, every time a virtual server remains down for 15 or more seconds, you will receive an email notification with details such as entity name, status change, and time.

To set event age in NetScaler MAS

1. In the NetScaler MAS, navigate to Infrastructure > Events > Rules, and click Add.
2. On the Create Rule page, set the rule parameters.
3. Specify the event age in seconds.
How to Schedule an Event Filter by Using NetScaler MAS

Jun 29, 2016

After creating a filter for your rule, if you do not want the NetScaler MAS server to send a notification every time the event generated satisfies the filter criteria, you can schedule the filter to trigger only at specific time intervals such as daily, weekly, or monthly.

For example, if you have scheduled a system maintenance activity for different applications on your instances at different times, the instances might generate multiple alarms.

If you have configured a filter for these alarms and enabled email notifications for these filters, the server sends a large number of email notifications when NetScaler MAS receives these traps. If you want the server to send these email notifications during a specific time period only, you can do so by scheduling a filter.

To schedule a filter using NetScaler MAS

1. In the NetScaler MAS, navigate to Infrastructure > Events > Rules.
2. Select the rule you want to schedule a filter for, and click View Schedule.
3. On the Scheduled Rule page, click Schedule and specify the following parameters:
   - **Enable Rule** – Select this checkbox to enable the scheduled event rule.
   - **Recurrence** - Interval at which to schedule the rule.
   - **Scheduled Time Interval (Hours)** – Hour(s), at which to schedule the rule (use the 24 hour format).
4. Click Schedule.
How to Set Repeated Email Notifications for Events from NetScaler MAS

Jun 29, 2016

To ensure that all critical events are addressed and no important email notifications are missed, you can opt to send repeated email notifications for event rules that meet the criteria you've selected. For example, if you've created an event rule for instances that involve disk failures, and you want to be notified until the issue is resolved, you can opt to receive repeated email notifications about those events.

These email notifications are sent repeatedly, at pre-defined intervals, until the recipient acknowledges having seen the notification or the event rule is cleared.

To set repeated email notifications from NetScaler MAS

1. In NetScaler MAS, navigate to Infrastructure > Events > Rules, and click Add to create a rule.
2. On the Create Rule page, set the rule parameters.
3. Under Event Rule Actions, click Add Action. Then, select Send e-mail action from the Action Type drop-down list and select an Email Distribution List.
4. Select the Repeat Email Notification until the event is cleared check box.

![Add Event Action](image_url)
How to Suppress Events by Using NetScaler MAS

Jun 29, 2016
You can suppress or drop events for a specific time period using the suppress event action on NetScaler MAS.

To suppress events using NetScaler MAS

1. In NetScaler MAS, navigate to Infrastructure > Events > Rules.
2. Specify all the parameters required to create a rule.
3. Under Event Rule Actions, click Add Action to assign notification actions for the event.
4. On the Add Event Action page, select Suppress Action from the Action Type drop-down.
5. Click OK.
How to Use the Events Dashboard to Monitor Events

Jun 30, 2016
As a network administrator, you can view details such as configuration changes, login conditions, hardware failures, threshold violations, and entity state changes on your NetScaler instances, along with events and their severity on specific instances. You can use the NetScaler MAS's events dashboard to view reports generated for critical event severity details on all your NetScaler instances.

To view the details on the events dashboard

Navigate to **Infrastructure > Events > Reports**.

The Top 10 Devices graph on the dashboard displays a report of the top 10 instances by the number of events generated on them. You can click on an instance on the graph to view further details of the event’s severity.

You can view more details by navigating to the NetScaler instance (**Infrastructure > Events > Reports > NetScaler instance**) to view the following:

- Top 10 devices by hardware failure
- Top 10 devices by configuration change
- Top 10 devices by authentication failure

- Top 10 devices by entity state changes
Top 10 devices by threshold violation
How to Set Multiple Event Rules Notifications in NetScaler MAS

Sep 30, 2016

You can configure rules to monitor specific events. Rules make it easier to monitor a large number of events generated across your NetScaler infrastructure.

You can filter a set of events by configuring rules with specific conditions and assigning actions to the rules. When the events generated meet the filter criteria in the rule, the action associated with the rule is executed. The conditions for which you can create filters are: severity, NetScaler instances, category, and failure objects.

You can assign the following actions to the events:

- **Send e-mail Action**: Sends an email for the events that match the filter criteria.
- **Send Trap Action**: Sends or forwards SNMP traps to an external trap destination
- **Send SMS Action**: Sends a Short Message Service (SMS) message for each event that matches the filter criteria.

To add event rules and set event rule actions

1. Navigate to **Infrastructure > Events > Rules**, and click **Add**.
2. On the **Create Rule** page, set the following parameters:
   - **Name**—Name of the event rule.
   - **Enabled**—Enable the event rule.
   - **Event Age**—Enter the time interval (in seconds) after which you want NetScaler MAS to refresh the event rule.
   - **Severity**—Severity of the events for which you want to add the event rule.
   - **Instances**—IP addresses of the NetScaler instances for which you want to define the event rule.
   - **Category**—Category or categories of the events generated by the NetScaler instances.
   - **Failure Objects**—Entity instances or counters for which an event has been generated. You can now use the wildcard character search for failure objects by entering an asterisk (*) in the **Add** field above the Failed Objects parameter.
3. Under **Event Rule Actions**, click **Add Action** to assign notification actions for the event. Select an **Action Type** and the **Distribution List** from the drop-down menu. The action types are:
   - **Mail Profile**—Mail server and mail profile details. An email is triggered when the events meet the defined filter criteria.
   - **Trap Profile**—Trap destination and trap profile details. Trap messages are send to specific trap listeners when events meet the defined filter criteria.
   - **SMS Profile**—SMS server and SMS profile details. An SMS message is triggered when the events meet the defined filter criteria.
   - **Suppress Action** - Suppresses or drops the events for a specific time period.
4. Click **OK**.
5. Click **Create** to create the event rule.
How to Modify the Reported Severity of Events that Occur on NetScaler Instances

Dec 27, 2016
You can manage the reporting of events generated on all your devices, so that you can view event details regarding a particular event on a particular instance and view reports on the basis of event severity. You can create event rules that use the default severity settings, and you can change the severity settings. You can configure severity for both generic and enterprise-specific events.

You can define the following levels of severity: Critical, Major, Minor, Warning, and Clear.

To modify event severity

1. Navigate to Infrastructure > Events > Event Settings.
2. Click the tab for the instance that you want to modify. Then, select the event from the list and click Configure Severity.
3. In Configure Event Severity, select the severity level from the drop-down list.
4. Click OK.
How to View Events Summary in NetScaler MAS

May 30, 2017

You can now view an Events Summary page to monitor the events and traps received on your NetScaler MAS server. Navigate to Infrastructure > Events. The Events Summary page displays the following information in a tabular format:

- **Summary of all the events received by NetScaler MAS.** The events are listed by category, and the different severities are displayed in different columns: Critical, Major, Minor, Warning, Clear, and Information. For example, a Critical event would occur when a NetScaler instance goes down and stops sending information to the NetScaler MAS server. During the event, a notification is sent to an administrator, explaining the reason why the instance is down, the time for which it had been down, and so on. The event is then recorded on the Events Summary page, on which you can view a summary and access the details of the event.

- **Number of traps received for each category.** The number of traps received, categorized by severity. By default, each trap sent from NetScaler instances to NetScaler MAS has an assigned severity, but as the network administrator, you can specify its severity in the NetScaler MAS GUI.

If you click on a category type or a trap severity number, you are taken to the Events page, on which filters such as the Category and Severity are preselected. This page displays more information about the event, such as the NetScaler instance’s IP address and host name, date on which the trap was received, category, and the message notification.
How to Display Event Severities and Skews of SNMP Traps on the Infrastructure Dashboard of NetScaler MAS

Dec 27, 2016

When you create an event and its settings in NetScaler MAS, you can view the event immediately on the Event Summary page. Similarly, you can view and monitor the health, up time, models, and the versions of all NetScaler instances added to your NetScaler MAS server in minute detail on the Infrastructure Dashboard.

On the Infrastructure dashboard, you can now mask irrelevant values so that you can more easily view and monitor information such as event by severities, health, up time, models, and version of NetScaler instances in minute detail.

For example, events with a Critical severity level might occur rarely. However, when these critical events do occur on your network, you might want to further investigate, troubleshoot, and monitor where and when the event occurred. If you select all severity levels except Critical, the graph displays only the occurrences of critical events. Also, by clicking on the graph, you are taken to the Severity based events page, where you can see all details regarding when a critical event occurred for the duration that you've selected: the instance source, the date, category, and message notification sent when the critical event occurred.

Similarly, you can view the health of a NetScaler VPX instance on the Dashboard. You can mask the time during which the instance was up and running, and display only the times the instance was out of service. By clicking on the graph, you are taken to that instance’s page, where the out of service filter is already applied, and see details such as host name, the number of HTTP requests it received per second, CPU usage, and so on. You can also select the instance and see that particular NetScaler instance's dashboard for more details.

To select specific events by severity in NetScaler MAS

1. Log on to NetScaler MAS, using your administrator credentials.
2. Navigate to Infrastructure > Dashboard.
3. From the drop-down in the upper-right corner of the page, select the duration for which you want to see events by severity.
4. The **Events by Severity** donut chart displays a visual representation of the events by their severity.

5. You can mask irrelevant severities to more easily view and monitor your chosen severity. Below the **Events by Severity** donut chart you can see the types of events that are represented in the chart. When you select any one of them, the chart displays only those events. For example, to view only critical issues, select “Critical,” and unselect the other event types.

6. Click the graph to display the **Severity based events** page, which shows the following details for the event selected severity for the selected duration:
   - Instance Source
   - Data of the event
   - Category of events generated by the NetScaler instance
   - Message notification sent
How to Set Up Notifications for SSL Certificate Expiry from NetScaler MAS

Jun 29, 2016

As a security administrator, you can set up notifications to inform you when certificates are about to expire and to include information about which NetScaler instances use those certificates. By enabling notifications, you can renew your SSL certificates on time.

To set up notifications from NetScaler MAS

1. In NetScaler MAS, navigate to **Infrastructure > SSL Certificates**.
2. On the **SSL Certificates** page, click **Settings**.
3. On the **Certificate Settings** page, click the **Edit** icon.
4. In the **Notification Settings** section, specify when you want to send the notification in terms of number of days prior to the expiration date.
5. Choose the type of notification you want to send. Select the notification type and the distribution list from the drop-down menu. The notification types are as follows:
   - **Email** – Specify a mail server and profile details. An email is triggered when your certificates are about to expire.
   - **SMS** – Specify a Short Message Service (SMS) server and profile details. An SMS message is triggered when your certificates are about to expire.
6. Click **Save**.

![Notification Settings](image)
How to Install SSL Certificates on a NetScaler Instance from NetScaler MAS

Jun 29, 2016
Before installing SSL certificates on NetScaler instances, ensure that the certificates are issued by trusted CAs. Also, make sure that the key strength of the certificate keys is 2048 bits or higher and that the keys are signed by using secure signature algorithms.

To install an SSL certificate from NetScaler MAS

1. In NetScaler MAS, navigate to Infrastructure > SSL Certificates.
2. In the upper-right corner of the dashboard, click Install.
3. On the Install SSL Certificate on NetScaler Instance page, specify the following parameters:
   - **Certificate File** - Upload an SSL certificate file by selecting either Local (your local machine) or Appliance (the certificate file must be present on the NetScaler MAS virtual instance).
   - **Key File** - Upload the key file.
   - **Certificate Name** – Specify a name for the certificate key.
   - **Password** - Password to encrypt the private key. You can use this option to upload encrypted private keys.
   - **Instance IP Address** - Select the NetScaler instances on which you want to install your certificates.
4. To save the configuration for future use, select the Save Configuration check box.
5. Click OK.
Install SSL Certificate on NetScaler Instance

Certificate File*
Choose File ▼ default_ssl_cert

Key File
Choose File ▼ default_ssl_key

Certificate Name*
Test Certificate

Password
******

Save Configuration

Instance IP Address*

- 10.102.40.59-P4050_11
- 10.102.40.60-P4050_11
- 10.102.40.60-P4050_1
- 10.102.40.60-P4050_14
- 10.102.40.59-P4050_14
- 10.102.62.285

OK  Close
How to Update an Installed Certificate from NetScaler MAS

Jun 29, 2016

After you receive a renewed certificate from the certificate authority (CA), you can update existing certificates from NetScaler MAS without needing to log on to individual NetScaler instances.

To update an SSL certificate, key, or both from NetScaler MAS

1. In NetScaler MAS, navigate to Infrastructure > SSL Certificates.
2. Click any of the graphs to see the list of SSL certificates.
3. On the SSL Certificates page, select a certificate and click Update. Alternatively, click the SSL certificate to view its details, and then click Update in the upper-right corner of the SSL Certificate page.
4. On the Update SSL Certificate page, make the required modifications to the certificate, key, or both and click OK.
How to Link and Unlink SSL Certificates by Using NetScaler MAS

Mar 09, 2017

You create a certificate bundle by linking multiple certificates together. To link a certificate to another certificate, the issuer of the first certificate must match the domain of the second certificate. For example, if you want to link certificate A to certificate B, the “issuer” of certificate A must match the “domain” of certificate B.

To link one SSL certificate to another certificate using NetScaler MAS

1. In NetScaler MAS, navigate to Infrastructure > SSL Certificates.
2. Click any of the graphs to see the list of SSL certificates.
3. Select the certificate that you want to link, and then select Link from the Action drop-down list.
4. From the list of matched certificates, select the certificate to which you want to link, and then click OK.

Note

If a matching certificate is not found, the following message is displayed: No certificate found to link.

To unlink an SSL certificate using NetScaler MAS

1. In NetScaler MAS, navigate to Infrastructure > SSL Certificates.
2. Click any of the graphs to see the list of SSL certificates.
3. Choose either of the linked certificates that are linked, and then select Unlink from the Action drop-down list.
4. Click OK.

Note

If the selected certificate is not linked to another certificate, the following message is displayed: Certificate does not have any CA link.
How to Create a Certificate Signing Request (CSR) using NetScaler MAS

Jun 29, 2016

A Certificate Signing Request (CSR) is a block of encrypted text that is generated on the server on which the certificate will be used. It contains information that will be included in the certificate such as the name of your organization, common name (domain name), locality, and country.

To create a CSR using NetScaler MAS

1. In NetScaler MAS, navigate to **Infrastructure > SSL Certificate**.
2. Click any of the graphs to see the list of installed SSL certificates, and then select the certificate for which you want to create a CSR and select Create CSR from the Action drop-down.
3. On the **Create Certificate Signing Request (CSR)** page, specify a name for the CSR.
4. Do one of the following:
   - **Upload a key** - Select the **I have a Key** option. To upload your key file, select either **Local** (your local machine) or **Appliance** (the key file must be present on the NetScaler MAS virtual instance).
   - **Create a key** - Select the **I do not have a Key** option, and then specify parameters such as the encryption type, name, size in bits, and format.
5. Click **Continue**.
6. On the following page, provide additional details. If you want to create the CSR without changing the defaults, click **Continue**.

---

**Note**

Most fields have default values extracted from the subject of the selected certificate. The subject contains details such as the common name, organization name, state, and country.
How to Configure an Enterprise Policy on NetScaler MAS

Jun 29, 2016

You can configure an enterprise policy and add all trusted CAs, secure signature algorithms, and select the recommended key strength for your certificate keys in NetScaler MAS. If any of the certificates installed on your NetScaler instance have not been added to the enterprise policy, the SSL certificate dashboard displays the issuer of those certificates as Not Recommended.

Also, if the certificate key strength does not match the recommended key strength in the enterprise policy, the SSL certificate dashboard displays the strengths of those keys as Not Recommended.

To configure an enterprise policy on NetScaler MAS

1. In NetScaler MAS, navigate to Infrastructure > SSL Certificates, and then click Settings.
2. Click the Edit icon to add all trusted CAs, secure signature algorithms, and select the recommended key strength for your certificates and keys.
3. Click Save to save your enterprise policy.
How to Use the SSL Dashboard to Monitor Certificates from NetScaler MAS

Jan 06, 2017

You can use the SSL certificate dashboard in NetScaler MAS to view graphs that help you keep track of certificate issuers, key strengths, and signature algorithms. The SSL certificate dashboard also displays graphs that indicate the following:

- Number of days after which certificates expire
- Number of used and unused certificates
- Number of self-signed and CA-signed certificates
- Top 10 instances by number of certificates in use

To monitor SSL certificates in NetScaler MAS, navigate to Infrastructure > SSL Certificates.

The NetScaler MAS SSL Dashboard also shows the distribution of SSL protocols that are running on your virtual servers. As an administrator, you can specify the protocols that you want to monitor through the SSL policy. For more information, see Configuring SSL Policies. The protocols supported are SSLv2, SSLv3, TLS1.0, TLS1.1, and TLS1.2. The SSL protocols used on virtual servers appear in a bar chart format. Clicking on a specific protocol displays a list of virtual servers using that protocol.

A donut chart appears after Diffie-Hellman (DH) or Ephemeral RSA keys are enabled or disabled on the SSL dashboard. These keys enable secure communication with export clients even if the server certificate does not support export clients.
as in the case of a 1024-bit certificate. Clicking on the appropriate chart displays a list of the virtual servers on which DH or Ephemeral RSA keys are enabled.
Change Management

Jun 28, 2016
How to Disable Entities in NetScaler MAS

Jun 29, 2016
When you disable a service, you must specify the time in seconds after which, no new connections are established with that service and existing connections to that service are terminated.

You can also gracefully shut down the service before disabling the service. By gracefully shutting down the service, existing connections to the service are processed but no new connections are established.

To disable a service in NetScaler MAS

1. In the NetScaler MAS, navigate to Applications > Dashboard > Load Balancing > Services.
2. Select the service you want to shut down, and click Disable.
3. In the Disable Service page, specify a value in the Time in seconds field. You can also choose the check box to gracefully shut down the service here.
4. Click OK.

Note
You will be prompted by NetScaler MAS to confirm every time you want to disable a service or a virtual server.
How to Search for Entities in NetScaler MAS

Jun 29, 2016
You can search for entities in NetScaler MAS.

To search for entities in NetScaler MAS

1. In NetScaler MAS, navigate to Applications > Dashboard. Expand the feature name and click the type of entity. (For example, to look for a service, expand Load Balancing, and then click Services.)
2. In the upper-right corner, click Search.
3. From the drop-down list, select the field on which you want to perform the search, and then enter the text with which you want to filter the displayed entities.
4. Click Refine Search.
How to View the Effective State of a Virtual Server on NetScaler MAS

Jun 29, 2016
You can view the effective state of a virtual server in NetScaler MAS. The effective state of a load balancing virtual server indicates whether or not that virtual server can serve traffic. If a load balancing virtual server has a backup virtual server that is operational, the effective state of the load balancing virtual server in NetScaler MAS is UP.

In NetScaler MAS, navigate to Applications > Dashboard > Load Balancing > Virtual Servers.

Virtual Servers

<table>
<thead>
<tr>
<th>Instance Name</th>
<th>State</th>
<th>Effective State</th>
<th>Protocol</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.102.62.204</td>
<td>Up</td>
<td>Up</td>
<td>HTTP</td>
<td>vip1</td>
</tr>
<tr>
<td>10.102.62.204-p2</td>
<td>Up</td>
<td>Up</td>
<td>HTTP</td>
<td>vip1</td>
</tr>
<tr>
<td>CLTnode80 (10.102.40.80)</td>
<td>Out of Service</td>
<td>Down</td>
<td>HTTP</td>
<td>vip1-svcLAB_Dynasty_Rack72_testforlongV</td>
</tr>
<tr>
<td>CLTNode80 (10.102.40.80-10.102.40.80_P1_U2)</td>
<td>Down</td>
<td>Down</td>
<td>HTTP</td>
<td>OWA_vserver_2</td>
</tr>
</tbody>
</table>
How to Create an Application Definition in NetScaler MAS

May 22, 2017

You can define an application based on a collection of virtual servers in NetScaler MAS. You can create an application through either a static or dynamic configuration.

The two types of application definitions are as follows:

1. **Static Definition of Applications** - In a static definition, you select the virtual servers that you want to define in the application. You can define an application with load balancing, content switching, and GSLB virtual servers. This definition does not get updated when new virtual servers are configured on your NetScaler instance. You will need to manually update this list to include more virtual servers.

2. **Dynamic Definition of Applications** - In a dynamic definition, you use one of the two criteria listed below to define an application:
   - **Servers**: You specify the server or service IP address, server name, or the port of the backend server on which the applications are running. You can enter one IP address, a range of IP addresses, or a combination of both separated by commas. For example, you can enter 10.102.29.20, 10.102.43.10-60, 10.216.43.45.
   - **Virtual Servers**: You can specify either one of the following: the virtual server IP address, virtual server name, or the port of the backend server on which the applications are running. You can enter one IP address or a range of IP addresses or a combination of both separated by commas. For example, you can enter 10.102.29.20, 10.102.43.10-60, 10.216.43.45.

If you configure a virtual server that meets these conditions, the definition gets updated automatically when NetScaler MAS polls entities. To initiate a poll manually, click **Poll Now** located in the **Applications** tab.

1. In NetScaler MAS, navigate to **Applications** > **Dashboard**. Select the **Applications** tab, and click **New Application**.
2. Enter the name of the application.
3. In static method of defining applications, you select an existing virtual server. First, select a type of virtual server from the **Add Virtual Servers** drop-down list. The types of virtual servers supported on NetScaler MAS are as follows:
   - Load balancing virtual servers
   - Content switching virtual servers
   - GSLB virtual servers
   - NetScaler Gateway virtual servers
   - Cache redirection virtual servers
   - Authentication virtual servers

   Once you select the type of virtual server, select the virtual servers from the corresponding page that slides in and click **Select**. You can select multiple servers, and you can also select the entire list of virtual servers. The selected virtual servers are added to the application. Click **OK**. The corresponding NetScaler instances, load balancing services, and service groups are added to the application.

   **Note**: In the virtual servers selection page, you can set the page option to display a maximum of 250 servers per page. But,
NetScaler MAS allows you to select only 100 instances at a time to be added to an application. If the number of instances are more than 100, set the page option to display 100 instances, select all the instances in that page, and then click Select to add them to the application. Perform this for all subsequent pages.

4. In dynamic method of defining applications, you define a criteria for selecting the virtual servers. If you want to select an existing virtual server, Select Define Selection Criteria and dynamically add applications by one of the following three methods:

- Specifying the IP address of the virtual server on which the applications are running. You can enter one IP address or a range of IP addresses or a combination of both separated by commas.
- Specifying the name of the server on which the applications or services are running.

  Note: You can also search for server names by using wild card extensions. For example, ssl* will add all ssl virtual servers to the application.

- Specifying the port number at which the application is listening to on the selected server.

You can edit the name of the existing virtual servers by clicking the edit icon next to the name of the load balancing virtual server.

NetScaler MAS displays all applications created in small windows arranged vertically. These windows show the name of the application, and the number of virtual servers, services, service groups for each application in a single-line display.

You can directly enable or disable the bound services, and service groups from these windows. For example, when you click Load Balancing Services in MAS-HA application, all the services which are bound to this application will be listed. You can choose multiple objects to view the objects or services bound to the instance. You can enable or disable all the services for different virtual servers.

Click on the name of the application in each window to view all details. The statistics for each application are displayed in three tabs to the right - Dashboard, Services, and Configuration. These tabs allows you to configure the applications.
For more information on how to configure load balancing servers, see Create Load Balancing Support through Application Dashboard.
How to Create Load Balancing Support through Application Dashboard in NetScaler MAS

Dec 27, 2016

You might need to bind or unbind services on the load balancing virtual servers depending on the traffic that the load balancing virtual servers receive in your network. NetScaler MAS provides a simplified functionality of adding or removing services and service groups from the MAS GUI instead of performing these tasks from the NetScaler appliances itself.

To configure services in NetScaler MAS

In NetScaler MAS, navigate to Applications > Dashboards. In the right hand page, select Applications tab. The Applications page lists all the virtual servers added in the MAS. Select the required load balancing virtual server.

Note

You can also add new load balancing virtual servers by clicking New Application. Also, you can edit the name of the existing virtual servers by clicking the edit icon next to the name of the load balancing virtual server.

For more information on how to create an application definition in NetScaler MAS, see Creating an Application Definition in NetScaler MAS.

Each load balancing virtual server displays three tabs - Dashboard, Services, and Configuration.
transactions that the server has processed, the number of client connections, and the throughput of the server.

Services - The Services tab displays a snapshot of the services and service groups configured on the load balancing virtual server. The tab also displays the type of traffic configured for the virtual server and the port. Click the Services and Service Groups tables to quickly enable or disable them.

For example, if you want to disable services, click on Services and in the Bound Services page that opens, select the instance(s) to be disabled and click Disable.

Configuration - The Configuration tab displays all the parameters configured on the load balancing virtual server.

The Configuration tab has four sections:

- Services and Services Groups - Click on Load Balancing Virtual Server Service Bindings and Load Balancing Virtual Server ServiceGroup Bindings. Follow the steps to bind or unbind remove services and service groups from the load balancing virtual servers.
- Basic Settings - You can set or edit a few basic settings that you had provided while adding the load balancing virtual server to MAS. Click the edit icon to change the settings. You can only edit the IP address of the virtual server. Click More to change the redirection mode to determine where to forward the incoming traffic. The NetScaler appliance supports the following redirection modes:
  - IP-Based (the default)
  - MAC Based
  - IP Tunnel Based
- **TOS Id Based**

  You can also enable RHI to advertise the route of a VIP address.

- **Method** - You can modify the load balancing method and set the service request rate and type in this section. Click in the drop-down list. Click the edit icon to select the required method from the drop-down list.

- **Persistence** - You can modify the persistence settings here to maintain the states of connections on the servers represented by that virtual server. Click the edit icon to select the persistence type from the drop-down list and set the other related parameters.

  **Note:** Click **OK** to save all changes.

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Services</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Services and Service Groups</strong></td>
<td><strong>2 Load Balancing Virtual Server Service Bindings</strong></td>
<td><strong>1 Load Balancing Virtual Server ServiceGroup Binding</strong></td>
</tr>
<tr>
<td><strong>Basic Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>nmas-ha-lb</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>UP</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>10.102.29.192</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Traffic Domain</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Listen Priority</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Listen Policy Expression Range</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>Redirection Mode</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>RHI State</td>
<td>IP</td>
<td></td>
</tr>
<tr>
<td>AppFlow Logging</td>
<td>PASSIVE ENABLED</td>
<td></td>
</tr>
<tr>
<td><strong>Method</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load Balancing Method</td>
<td>ROUNDROBIN</td>
<td></td>
</tr>
<tr>
<td>Backup LB Method</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Service Startup Request Rate</td>
<td>PER_SECOND</td>
<td></td>
</tr>
<tr>
<td>New Service Request unit Increment Interval</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Persistence</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Persistence</td>
<td>SRCIPDESTIP</td>
<td></td>
</tr>
<tr>
<td>Timeout</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Persistence Mask</td>
<td>255.255.255.255</td>
<td></td>
</tr>
<tr>
<td>Persistence Mask Length</td>
<td>128</td>
<td></td>
</tr>
</tbody>
</table>

For more information on services and service groups, binding and unbinding services and service groups, see [http://docs.citrix.com/en-us/netscaler/11-1.html](http://docs.citrix.com/en-us/netscaler/11-1.html).
How to Enable Analytics on Instances

Jan 09, 2017

You can enable analytics for a specific virtual server on the selected instance, representing an application server, and monitor the traffic of that application server. Analytics provide statistics for the virtual server.

To enable Analytics on NetScaler MAS

1. In a web browser, type the IP address of the NetScaler Management and Analytics System (for example, http://192.168.100.1).

2. In User Name and Password, enter the administrator credentials.

3. Navigate to Infrastructure > Instances, and select the NetScaler instance you want to enable analytics.

4. From the Action drop-down, select Enable/Disable Insight.

5. Select the virtual servers, and click Enable AppFlow.

6. In the Enable AppFlow field, type true, and based on the analytics you want to enable, select Security Insight or Web Insight, or both.

7. Click Ok.
How to Configure Adaptive Thresholds

Jun 28, 2016

The adaptive threshold functionality sets the threshold value for the maximum number of hits on each URL. If the maximum number of hits on a URL is greater than the threshold value set for the URL, a syslog message is sent to an external syslog server. The threshold value interval can be in either days or weeks.

The threshold value is calculated as follows:

Threshold value = Max hits * Threshold multiplier

Where:

- Max hits is the maximum number of hits on a URL.
- Threshold multiplier is an integer value that you define (default: 2).

1. In NetScaler MAS, navigate to System > Analytics Settings > Adaptive Thresholds, and then click Add.
2. On the Create Adaptive Thresholds page, specify the following parameters:
   - Name - Threshold name
   - Entity - URL
   - Duration - Duration of the threshold (day or week)
   - Threshold Multiplier - A user-defined integer that is multiplied with the maximum hit count of the specified URL to obtain the adaptive threshold for the URL.
How to Configure SLA Management

Jun 29, 2016
Service Level Agreement Management feature will help you to manage SLA over Server Response Time, Hits/sec and Bandwidth usage across your Domain usage. Configuring SLA on various breaches eases you to monitor a large number of events generated across your NetScaler infrastructure.

You can configure SLA breach for the following:

- Server Response time
- SLA Breach Frequency for Bandwidth
- SLA Breach Frequency for Hits
- SLA Breach Frequency for Response Time

You can configure notifications for each SLA breach whenever your appliance encounters it. You can configure the notification type as Mail, SMS, or Syslog and configure distribution lists respectively.

1. Navigate to System > Analytics Settings > SLA Management.
2. From the list displayed, select the NetScaler IP address of an appliance on which you want to manage SLA.
3. Click Add, if you want to add a new SLA Group and add breach definitions to it. Alternatively, you can select a SLA group from the list if you already have added a SLA group.
4. In the SLA Group field, enter the name for the new SLA group.
5. Select the appropriate check boxes to enable or disable the SLA monitors.
6. Select the appropriate breach values for the selected options.
   - for example, Maximum Server Response Time (ms)* = 22 ms.
7. Select the notification type and the interval to notify from the Notification Type and Interval drop-downs appropriately.
8. You can select the distribution lists to send the notifications from the Mail/SMS/Syslog Distribution List drop-down.
9. Click Create, to create and add a SLA group to your NetScaler appliance.
How to Configure Database Summarization for Analytics

Jun 29, 2016
Configure Database Summarization in NetScaler MAS allows you to customize the duration for you want to store the historical data of your NetScaler analytics data. You can choose the following database summarization types for your analytics' historical data:

- Hours to persist minutely data
- Days to persist hourly data
- Days to persist daily data

1. Navigate to System > Analytics Settings > Database Summarization.
2. Click on the Insight type you want to configure the database summarization.

![Database Summarization Configuration](image)

3. Specify the duration for which you want to retain Insight data on NetScaler MAS.
For example, for Gateway Insight, you can store your analytics' minutely historical data for 2 hours, or hourly data for 1 day.
Gateway Insight

Configure the duration you want to persist the Gateway Insight data for on per summarization level.

Hours to persist minutely data
2

Days to persist hourly data
1

Days to persist daily data
31

[OK]  [Close]
How to Create Thresholds and Alerts Using NetScaler MAS

Jun 30, 2016

You can set thresholds and alerts to monitor the state of a NetScaler instance. You can set thresholds on counters and monitor instances and entities on managed instances.

When the value of a counter exceeds the threshold, NetScaler MAS generates an event to signify a performance-related issue. When the counter value matches the clear value specified in the threshold, the event is cleared, which means that the particular threshold has returned to its normal state.

You can also associate an action with the threshold. Actions include sending an alert, email, or SMS notification. When the threshold is breached, NetScaler MAS performs the action you define is taken automatically like enabling an alert and sending an email or SMS notification.

2. On the Create Thresholds and Alerts page, specify the following details:
   - **Name** – Name for configuring the threshold.
   - **Traffic Type** – Type of traffic for which you want to configure the threshold.
   - **Entity** – Category or resource type for which you want to configure the threshold.
   - **Reference Key** – Automatically generated value based on the selected traffic type and entity.
   - **Duration** - Interval for which you want to configure the threshold.
   - **Community** – Community string for each trap that is to be sent to the trap listener.
3. Optionally, configure actions such as alerts, emails notifications, and SMS notifications.
4. Click Create.
How to Disable URL Data Collection for Analytics from NetScaler MAS

Jun 30, 2016
You can disable URL data collection if you do not want URL reports to be displayed on the Web Insight node of the dashboard in NetScaler MAS.

1. In NetScaler MAS, navigate to System > Analytics Settings, and then click Configure Data Record Settings.
2. In the Web Insight URL Data Collection Settings section, if the Enable URL Data Collection option is checked, clear the check box.
3. Click OK.
How to Attach an Additional Disk to NetScaler MAS

Jan 11, 2017

To attach an additional disk to NetScaler MAS:

1. Shut down the NetScaler MAS virtual machine.

2. In the hypervisor, attach an additional disk of the required disk size to NetScaler MAS virtual machine.

For example, for a NetScaler MAS virtual machine of 120 GB, if you want to increase its disk space to 200 GB, you then need to attach a disk space of 200 GB instead of 80 GB. Newly attached 200 GB of disk space will be used to store Database data, NetScaler MAS log files. The existing 120 GB disk space will be used to store core files, Operating system log files, and so on.

3. Start the NetScaler MAS virtual machine.
How to Cascade External Authentication Servers

Jun 29, 2016

A NetScaler MAS supports a unified system of authentication, authorization, and accounting (AAA) protocols, including RADIUS, LDAP, and TACACS, in addition to supporting local servers for authenticating local users and groups. The unified support provides a common interface to authenticate and authorize all of the local and external AAA clients who are accessing the system. NetScaler MAS can authenticate users regardless of the actual protocols they communicate with the system.

Cascading external authentication servers provides a continuous non-failing process for authenticating and authorizing external users. If authentication fails on the first authentication server, NetScaler MAS attempts to authenticate the user by using the second external authentication server, and so on. To enable cascading authentication, you need to add the external authentication servers to NetScaler MAS. You can add any type of the supported external authentication servers (RADIUS, LDAP, and TACACS). For example, if you want to add four external authentication servers for cascading authentication, you can add two RADIUS servers, one LDAP server, and one TACACS server, or all servers can be of RADIUS type. You can configure up to 32 external authentication servers in NetScaler MAS.

1. In NetScaler MAS, navigate to System > Authentication > Authentication Summary.
2. On the Authentication page, under the Authentication heading, click Authentication Configuration.
3. On the Authentication Configuration page, select EXTERNAL from the Server Type drop-down list (only external servers can be cascaded).
4. Click Insert, and on the External Servers page, select one or multiple authentication servers that you would like to cascade.
5. Click OK to close the page.

The selected servers are displayed on the Authentication Servers page as shown in the figure below.

You can also specify the order of authentication by using the icon next to the server names to move servers up or down the list.
## Authentication Configuration

The appliance can authenticate users with local user accounts or by using an external authentication server.

### Server Type

- **EXTERNAL**

### External Servers

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Server Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>10.102.166.80</td>
</tr>
<tr>
<td>LDAP</td>
<td>_LDAP2</td>
</tr>
<tr>
<td>LDAP</td>
<td>_LDAP1</td>
</tr>
</tbody>
</table>

- Enable fallback local authentication

[View Image](https://docs.citrix.com)
How to Add RADIUS Authentication Servers

Jul 01, 2016

A RADIUS authentication server operates by using the User Datagram Protocol (UDP). The RADIUS server receives a user's connection request, authenticates the user, and then returns the configuration information needed by the system that delivers services to the user. The RADIUS server is connected to a network access server (NAS). When the NAS sends an Access-Request, the RADIUS server searches its database for the user name and other details. If the user name does not exist in the database, the RADIUS server immediately sends an Access-Reject message, or it can load a default profile on the MAS. In RADIUS, authentication and authorization are coupled together. If the user details are authenticated, the RADIUS server returns an Access-Accept response. It also sends a list of attribute-value pairs that describe the parameters to be used for that particular session.

1. In NetScaler MAS, navigate to System > Authentication > RADIUS.

2. On the RADIUS page, click Add.

3. On the Create RADIUS Server page, set the parameters, and click Create to add the server to the list of RADIUS authentication servers.

4. The following parameters are mandatory to create the RADIUS server:
   - Name – type the name of the RADIUS server
   - IP Address – type the IP address of the RADIUS server
   - Port – by default, port 1812 is used for RADIUS authentication messages. You can specify a different port number, if required.
   - Time-out (seconds) – type the number of seconds. This is the time that the NetScaler MAS system waits for a response from the RADIUS server.
   - Secret Key – type any alphanumeric expression. This is the key that is shared between the NetScaler MAS and the RADIUS server for communication.

5. Click Details to expand the section and set the additional parameters.
You can provide more optional details while adding a RADIUS server. Some of the additional parameters you can enter are NAS details, vendor information, attribute information, and type of password authentication.
How to Add LDAP Authentication Servers

Jul 01, 2016

The LDAP protocol that is integrated in NetScaler MAS along with RADIUS and TACACS authentication servers, allows the system to search for user credentials from the distributed directories and authenticate the users.

1. In NetScaler MAS, navigate to System > Authentication > LDAP.

2. On the LDAP page, click Add.

3. On the Create LDAP Server page, set the parameters and click Create to add the server to the list of LDAP authentication servers.

4. The following parameters are mandatory to create the LDAP server:

   - Name – type the name of the LDAP server.
   - IP Address – type the IP address of the LDAP server.
   - Security Type – select the type of communication required between the system and the LDAP server from the drop-down list. Apart from plaintext communication you can choose encrypted communication by selecting either Transport Layer Security (TLS) or SSL.
   - Port – by default, port 389 is used for LDAP authentication. You can specify a different port number, if required.
   - Server Type – select Active Directory (AD) or Novell Directory Service (NDS) as the type of LDAP server.
   - Time-out (seconds) – type the number of seconds. This is the time that the NetScaler MAS system waits for a response from the LDAP server.

You can provide more optional details while creating an LDAP server. You can also validate the LDAP certificate by checking the box and specifying the host name to be entered on the certificate. Some of the additional parameters you can add are Domain Nameserver (DN) details for queries against a directory service, default authentication group, group attributes, and other attributes.
How to Add TACACS Authentication Servers

Jun 29, 2016
TACACS, along with RADIUS and LDAP, handles remote authentication services for network access.

1. In NetScaler MAS, navigate to System > Authentication > TACACS.
2. On the TACACS page, click Add.
3. On the Create TACACS Server page, enter the following details:
   1. Name of the TACACS server
   2. IP address of the TACACS server
   3. Port and timeout in seconds
   4. Type the key that is shared by the system and the TACACS server for communication.
How to Extract Authentication Server Group in NetScaler MAS

Jul 01, 2016

NetScaler MAS allows you to extract the group of users existing on the external authentication server, and assign them permissions as their role demands and as per the NetScaler definitions. This has two advantages:

1. You do not have to create users on NetScaler MAS. Though the groups are extracted into the NetScaler MAS server, they are managed on the external servers from the NetScaler MAS rather than adding them on the system.

2. NetScaler MAS performs the authorization of users by assigning group permissions to access specific load balancer virtual servers, and for specific applications on the system. In future, when the particular authentication server is removed from the system, the groups and users will be automatically removed from the system.

1. In NetScaler MAS, navigate to System > User Administration > Groups.

2. Click Add to create a group.

3. On the Create System Group page, type the name of the group, set permissions either as admin or readonly. The other options that you can configure are session timeout, where you can set a timeout limit for the sessions logged in the users of that group, and you can also set the VM instances that can be accessed by the group members.

Note

Make sure that the name of the user group created on NetScaler MAS is exactly the same as that created on external authentication servers. If not, the system will not recognize the group and the group members will not be extracted into the system.
4. In the next screen, you can provide permissions to a particular NetScaler instance. This allows the users to access only that virtual appliance. But, the users can still create a new NetScaler instance in the system and manage that instance.

When you finish creating a group in the system, all the users in external authentication server are extracted into the system. You can check this by selecting the group and clicking Edit. The Users table in Create System Group displays the list of users connected with the group.

If the group name matches the group name on the external authentication server, the user inherits all of the authorization definitions when logged on to the system.
How to Enable Fallback Local Authentication

Nov 07, 2016

Fallback local authentication feature enables local authentication to take over if the external authentication fails. A user configured on both NetScaler MAS and on an external authentication server can log on to NetScaler MAS, even though the configured external authentication server is down or unreachable. For Fallback Local Authentication to work, make sure about these three factors:

- You should be able to access NetScaler MAS even after external authentication server goes down.
- You should be configured on both NetScaler MAS and the external authentication server.
- You should add at least one external server.

To enable Fallback Local Authentication, do the following:

1. In NetScaler MAS, navigate to System > Authentication > Authentication Configuration.

2. Select EXTERNAL from the Server Type* list.

   **Note**: If you select LOCAL from the list, authentication of users happens at the default local authentication server.

3. Click **Insert**, select an external server from the list of external servers displayed, and click **OK** to add the external server.

   **Note**: You should have already added the external servers before this step to make them appear in the list. For more information as to how to add external servers, see the following articles:

   - How to add Radius Servers
   - How to add LDAP Servers
   - How to add TACACS Servers

4. Select the **Enable fallback local authentication** option.
## Authentication Configuration

The appliance can authenticate users with local user accounts or by using an external authentication server.

**Server Type**

- EXTERNAL

### External Servers

<table>
<thead>
<tr>
<th></th>
<th>Server Type</th>
<th>Server Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>RADIUS</td>
<td>RADIUS R1</td>
</tr>
<tr>
<td>✓</td>
<td>RADIUS</td>
<td>RADIUS R2</td>
</tr>
</tbody>
</table>

- Enable fallback local authentication

[OK]  [Close]
How to Upgrade NetScaler MAS

Jun 29, 2016

Each NetScaler MAS release offers new and updated features with increased functionality. A comprehensive list of enhancements is listed in the release notes accompanying the release announcement. Take a moment to read the release notes before you upgrade the software. It is important to understand the licensing framework and types of licenses before you start to upgrade.

1. Navigate to System > System Administrations. Under the System Administration sub-heading, click Upgrade NetScaler MAS.
2. On the Upgrade NetScaler MAS page, upload a new image file by selecting either Local (your local machine) or Appliance (the certificate file must be present on the NetScaler MAS virtual appliance).
3. Click OK.
How to Generate a Tech Support File for NetScaler MAS

Jun 29, 2016

Citrix recommends that you generate an archive of NetScaler MAS data and statistics before contacting technical support for debugging an issue. The archive is a TAR file that you can send to the technical support team.

Note

For NetScaler MAS servers in an HA pair, you can generate a technical support file from either one of the servers. Citrix advises you to not use the load balancing virtual server IP address to generate the technical support file.

1. Navigate to System > Diagnostics > Technical Support, and then click Generate Technical Support File.

2. On the Generate Support File page, select the following options:

- **Collect Debug Logs** – Select this option to collect afdecoder logs.
- **Duration** – Enter the duration for which debug logs should be collected.
- **Collect Data Distribution** – Select this option to collect distinct and diverse logs from the database.

The archive file is created as a TAR file.

For example, the archive file that is created might be named NetScaler_MAS_<DDMMYY>.tar.gz.

3. Download the files and email them to the Citrix technical support team.
How to Configure NTP Server on NetScaler MAS

Jun 29, 2016

You can configure a Network Time Protocol (NTP) server in NetScaler MAS to synchronize its clock with the NTP server. Configuring an NTP server ensures that the NetScaler MAS clock has the same date and time settings as the other servers on the network.

1. Navigate to System > NTP Servers, and then click Add.
2. On the Create NTP Server page, enter the following details:
   - **Server Name/IP Address** – Enter the domain name or IP address of the NTP server. The name or IP address cannot be changed after you have added the NTP server.
   - **Minimum Poll Interval** – Specify the minimum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the minimum poll interval to be 64 seconds, which can be expressed as $2^6$, enter 6.
   - **Maximum Poll Interval** – Specify the maximum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the maximum poll interval to be 256 seconds, which can be expressed as $2^8$, enter 8.
   - **Key Identifier** - Enter the key identifier that can be used for symmetric key authentication with the NTP server. Do not add a key identifier if you choose to select Autokey.
   - **Autokey** - Select Autokey if you want to use public key authentication with the NTP server. Do not select if you want to add a key identifier.
   - **Preferred** – Select this option if you want to specify this NTP server as the preferred server for clock synchronization. This applies only if more than one server is configured.
3. Click Create.

Create NTP Server

1. Navigate to System > NTP Servers.
2. Click NTP Synchronization and select the Enable NTP Synchronization checkbox.
3. Click OK.
NTP Synchronization

Enable NTP Synchronization

OK Cancel
How to Configure SSL Settings for NetScaler MAS

Jun 29, 2016

SSL (Secure Socket layer) and TLS (Transport Layer Security) are commonly used security networking protocols that provide encrypted communication between users and servers. You can configure SSL settings on NetScaler MAS and specify the type of clients that connect to the system.

2. On the Configure SSL Settings page, review the current protocol settings and the cipher suites applied to the system.
3. To modify the protocol settings, navigate to Edit Settings > Protocol Settings and make the changes that you want.
4. To modify the applied cipher suites, navigate to Edit Settings > Cipher Suites and make the changes that you want.
5. Click OK, and then click Done.
How to Configure Syslog Purging Interval for MAS

Jun 29, 2016

Syslog is a standard protocol for logging. It has two components: the Syslog auditing module, which runs on the NetScaler instance, and the Syslog server, which can run either on the underlying FreeBSD operating system (OS) of the NetScaler instance or on a remote system. SYSLOG uses User Datagram Protocol (UDP) for data transfer.

Syslog enables isolation of the system that generates information and the system that stores the information. You can consolidate logging information and derive insights from the collected data. You can also configure syslog to log different types of events.

To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. You can specify the number of days after which the following syslog data will be deleted from NetScaler MAS:

- **Generic Syslog Data**
- **AppFirewall Data**
- **NetScaler Gateway Data**

You can also configure the NetScaler Gateway purge interval by syslog type. This purge interval takes precedence over the purge interval configured to retain NetScaler Gateway data.

1. Navigate to **System > Auditing**, and then click **Syslog Purge Settings**.
2. In **Configure Syslog Purge Settings** page, enter the following details:
   - **Retain Syslog Generic Data** – Specify the number of days for which NetScaler MAS retains generic syslog messages.
   - **Retain AppFirewall Data** – Specify the number of days for which NetScaler MAS retains AppFirewall syslog messages.
   - **Retain NetScaler Gateway Data** – Specify the number of days for which NetScaler MAS retains NetScaler Gateway syslog messages.
3. Select the **Configure NetScaler Gateway Purge Interval by Syslog Type** checkbox if you want this to take precedence over the purge settings interval configured to retain the NetScaler Gateway data.
4. Select one or more of the following options:
   - **Type** - The type of NetScaler Gateway syslog types generated on the devices, such as Login, Logout, Login failed, ICA proxy session start, and others. Select the type for which you want syslog data deleted from the NetScaler MAS server.
   - **Purge Interval (Days)** - The time interval between two successive purge operations performed on syslog data.
5. Click **OK**.
Configure Syslog Purge Settings

You can specify the number of days after which the following syslog data will be deleted from the NetScaler MPS server:

- NetScaler AppFiewal Citrix
  - Days
- NetScaler Gateway Citrix
  - Days
- NetScaler Gateway Citrix
  - Days
- [ ] Configure NetScaler Gateway purges interval by syslog type

OK Cancel
How to View Auditing Information of NetScaler MAS

Jun 29, 2016

Syslog is a standard protocol for logging. It has two components: the Syslog auditing module, which runs on the NetScaler instance, and the Syslog server, which can run either on the underlying FreeBSD operating system (OS) of the NetScaler instance or on a remote system. SYSLOG uses User Datagram Protocol (UDP) for data transfer.

Syslog enables isolation of the system that generates information and the system that stores the information. You can consolidate logging information and derive insights from the collected data. You can also configure syslog to log different types of events.

You can monitor the syslog messages that a NetScaler device generates if you configure the device to redirect syslog messages to NetScaler MAS. You can schedule a job to create syslog servers that generate different kinds of syslog data using the built-in templates feature in NetScaler MAS.

First, configure a syslog server to which the instance can send log information. Then, specify the date and time format for recording log messages.

1. Navigate to System > Auditing > Syslog Servers.
2. In the details pane, click Add.
3. On the Create Syslog Server page, enter the following values:
   - Name - Name for the syslog server.
   - IP Address - IP address of the syslog server.
   - Port - Syslog server port.
4. Choose the log levels (All, None, or Custom). Accordingly, select the severity levels.
5. Click Create.

1. Navigate to System > Auditing > Syslog Servers.
2. Select the syslog server, and then, click Syslog Parameters.
3. On the Configure Syslog Parameters page, specify the date and time format.
4. Click OK.

2. In the right pane, under Syslog Viewer, you can select the syslog file you want to view from the File drop-down option. Additionally, syslog files can be further filtered by module, event type, and severity.
3. Click Apply to generate the syslog messages.
How to Configure System Notification Settings of NetScaler MAS

Jun 29, 2016
You can send notifications to select groups of users for a number of system-related functions. You can set up a notification server in NetScaler MAS, and you can configure email and Short Message Service (SMS) gateway servers to send email and text notifications to users.

1. Navigate to System > Notifications > Settings, and then click Change Notification Settings.
2. On the Configure System Notification Settings page, enter the following details:
   - Category – Category or categories of events generated by NetScaler MAS.
   - Email – Choose an email distribution list from the drop-down list. You can also create an email distribution list by clicking the “+” icon and specifying email server details.
   - SMS (Text Message) – Choose an SMS distribution list from the drop-down list. You can also create an SMS distribution list by clicking the “+” icon and specifying SMS server details.
3. Click OK.
How to Monitor CPU, Memory, and Disk Usage of NetScaler MAS

Jun 29, 2016

You can use the information maintained in logs and statistics that are also displayed in reports to guide you to configure and maintain NetScaler MAS.

To monitor CPU, memory, and disk usage, navigate to **System > Statistics**.

You can view real-time CPU, memory, and disk utilization charts.

![Statistics](image-url)
How to Configure a Cipher Group for NetScaler MAS

Jun 29, 2016

A cipher group is a set of cipher suites that you bind to an SSL virtual server, service, or service group on the NetScaler instance. A cipher suite comprises a protocol, a key exchange (Kx) algorithm, an authentication (Au) algorithm, an encryption (Enc) algorithm, and a message authentication code (Mac) algorithm.

1. Navigate to System > Cipher Groups, and then click Add.
2. On the Create Cipher Group page, enter the following details:
   - **Group Name** - Name for the cipher group.
   - **Cipher Group Description** – Provide a description for your cipher group.
   - **Cipher Suites** – Click Add to select cipher suites from the Available list, and then move the selected (or all) cipher suites to the Configured list.
3. Click Create.

![Create Cipher Group](image)
How to Create SNMP Traps, Managers, and Users on NetScaler MAS

Jun 30, 2016

You can configure an SNMP agent on a Citrix NetScaler instance to generate asynchronous events called *traps*. Traps are generated whenever there are abnormal conditions on the NetScaler instance. The traps are then sent to a remote device called a *trap listener*, which then alerts you to the abnormal condition on the NetScaler instance.

Alternatively, you can query the SNMP agent for system-specific information from a remote device called an *SNMP manager*. The agent then searches the management information base (MIB) for requested data and sends the data to the SNMP manager.

1. Navigate to **System > SNMP > Trap Destinations**.
2. Under **SNMP Traps**, click **Add** to create a new SNMP trap, and then specify the following details:
   - **Version** – Select the SNMP version to use.
   - **Destination Server** - Name or IP address of the trap destination.
   - **Port** - Enter the trap destination's port. The port is set to 162 by default.
   - **Community** – Specify the community string to use when sending a trap to the trap listener.
3. Click **Create**.

1. Navigate to **System > SNMP > Managers**.
2. Under **SNMP Manager**, click **Add** to create a new SNMP manager community, and then specify the following details:
   - **SNMP Manager** - Enter the name or IP address of the SNMP manager.
   - **Community** – Specify the community string to use when sending traps to the trap listener.
3. Optionally, in **Netmask**, specify the subnet mask of the SNMP manager network.
4. Click **Create**.

1. Navigate to **System > SNMP > Users**.
2. Under **SNMP User**, click **Add**.
3. Enter the user name and assign a security level to the user from the drop-down list.
4. Based on the Security Level you've assigned to the user, you might need to provide additional authentication protocols, such as authentication protocols, privacy passwords, and assign SNMP views.
How to Back up and Restore your NetScaler MAS Server in a Single-Server Deployment

Jun 04, 2017

In a NetScaler MAS single-server deployment, you can take periodic backups of your NetScaler MAS server. You can either take a partial backup of the server that includes the configuration files, instance details, system data, and so on, or you can take a complete backup of the entire NetScaler MAS server. If your NetScaler MAS becomes unstable, you can use these backed up files to restore your server to a stable state. Citrix recommends that you back up your NetScaler MAS server's configuration before performing an upgrade or for precautionary reasons.

This document includes the following information:

- How to Take a Partial Backup of Your NetScaler MAS Server and Restore It
  - Backing Up the NetScaler MAS Configuration
  - Transferring a NetScaler MAS Backup File to an External System
  - Restoring NetScaler MAS Configuration from a Backup File
- How to Take a Complete Backup of your NetScaler MAS Server and Restore It
  - Deploying, Backing up, and Restoring your NetScaler MAS Server

In a partial backup process, you can back up the following components of your NetScaler MAS server:

- NetScaler MAS Configuration Files:
  - SNMP
  - Syslog server configuration files
  - NTP files
  - SSL certificates
  - Control Center files
- Configuration audit templates.
- System data stored on the database:
  - List of tenants and users created.
  - External authentication server configuration (LDAP, RADIUS, and others).
  - Configuration jobs and job templates created.
- Infrastructure and application data stored on the database:
  - Data from added and managed NetScaler instances.
  - Instance profile details, version details, instance group details, and so on.
  - A static application (group of virtual servers) created by the administrator.
- SNMP settings.

In this backup process, you cannot back up NetScaler instances, analytics data, events, and syslog messages.

Note

1. To backup and restore your NetScaler instances, see How to Back Up and Restore an Instance using NetScaler MAS.
2. To backup and restore your NetScaler instances in a high availability setup, see How to Back Up and Restore a NetScaler MAS Configuration in an HA Pair.
Backing Up the NetScaler MAS Configuration

By default, the NetScaler MAS server backs up the configuration every 24 hours (at 00.30 hours). You can also take a backup at a time of your choosing. You can further move a copy of the backed up file to another system.

The backup is stored as a compressed TAR file that can also be encrypted. By default, three backup files are retained in the server. To avoid issues due to non-availability of disk space, you can store a maximum of 10 backup files on your NetScaler MAS server. However, Citrix recommends that you store some copies of your backup files on the server or transfer the files to another system.

To back up a NetScaler MAS configuration

1. Navigate to System > Advanced Settings > Backup Files, and then click Back Up.
2. To encrypt the backup file, select the Password Protect file checkbox, and then provide a password to encrypt the file.

Transferring a NetScaler MAS Backup File to an External System

You can transfer a copy of the backup file to another system as a precautionary measure. When you want to restore the configuration, you have to first upload the file to the NetScaler MAS server and then perform the restore operation.

To transfer a NetScaler MAS backup file

1. Navigate to System > Advanced Settings > Backup Files.
2. Select the backup file that you want to move to another system, and then click Transfer.
3. On the Backup Files page, specify the following parameters:
   
   - **Server** - IP address of the system where you want to transfer the backed-up file.
   - **User Name and Password** - User credentials of the new system where the backed-up files are being copied.
- **Port** - Port number of the system the files are being transferred to.
- **Transfer Protocol** - Protocol being used to make the backup file transfer. You can select SCP, SFTP, or FTP protocols to transfer the backed-up file.
- **Directory Path** - The location where the backed-up file is being transferred to on the new system.

Alternatively, you can also set the external systems detail by navigating to **System > System Backup Settings**.

4. You can delete the backup file from NetScaler MAS after transfer by selecting the **Delete file from NetScaler Management and Analytics System after transfer** checkbox.

5. Click **OK** to make the transfer.

---

**Note**

To save a copy of the backup file in your local system, navigate to **System > Advanced Settings > Backup Files**, select the file you want to copy, and then click **Download**.

---

**Restoring the NetScaler MAS Configuration from a Backup File**

When you restore the NetScaler MAS configuration from a previously backed up file, the restore operation untars the backup file and then restores the configuration. The restore operation deletes the existing configuration and replaces it with the configuration in the backup file.

**Note**

The restore operation will not succeed if your backup file has been renamed or if the contents within the backup file have been modified.

---

**To restore a NetScaler MAS configuration from a backup file**

1. Navigate to **System > Advanced Settings > Backup Files**.
2. Select the backup file that you want to restore, and then click **Restore**.
3. On the confirmation dialog box, click **Yes**.
Note

To restore the configuration from a backup file stored in an external system, you have to upload the backup file to the NetScaler MAS server before performing the restore operation. To upload the file, navigate to System > Advanced Settings > Backup Files, and then click Upload.

To take a backup of your entire NetScaler MAS server, you have to set up a second NetScaler MAS server as the backup server. This backup server continuously archives the complete data of your primary NetScaler MAS server to ensure minimum loss of data in the event that your system becomes unstable.

In this complete backup process, you cannot back up the following components of your NetScaler MAS server:

- Files related to Orchestration
- MAS SSL certificates
- MAS SSL keys
- MAS NTP server configuration files
- MAS server SNMP configuration files
- MAS syslog configuration files
- MAS DNS configuration files
- MAS debug logs
- MAS licenses

The following diagram illustrates the architecture of this setup, and also how the backup process works.
A Write-Ahead Logging (WAL) archive folder is created on the backup NetScaler MAS server that continuously collects transaction logs from the WAL folder in the database of the primary NetScaler MAS server.

A transaction log stores every transaction made to database server. These logs are important in case of disaster recovery, and they must not be corrupted.

The entire database within the primary NetScaler MAS server is archived and transferred to the backup server during a scheduled time. By default, this is done once every 15 days. This method of transferring the entire NetScaler MAS server's database to a backup NetScaler MAS server is called 'base backup.' At any point of time, only one 'base backup' is retained on the backup NetScaler MAS server.

Important
- You can take complete backup of a NetScaler MAS server only if it is in a single-server deployment.
- You can register only one backup server with a primary NetScaler MAS server.
- While you can specify a time interval to retain data, it cannot exceed 30 days or be less than 5 days. By default, the backup retention period is 15 days. Assuming your backup retention period is 5 days, a new TAR file is created with transaction logs that have been collected in the WAL folder as a new backup file (base backup) every 5 days.

Deploying, Backing Up, and Restoring your NetScaler MAS Server

Before you back up and restore your primary NetScaler MAS server, you must install the primary and backup NetScaler MAS servers on a hypervisor, such as Citrix XenServer.

To deploy your NetScaler MAS servers

To deploy the primary NetScaler MAS server on Citrix XenServer, see Installing the NetScaler MAS on Citrix XenServer.

On the hypervisor's Console tab:
1. Enter your network configurations and specify the IP addresses of the primary and backup NetScaler MAS servers.
2. Select the deployment type as **Remote Backup Node**, and then type **Yes** to deploy as a standalone deployment, and **Yes** to restart the NetScaler MAS server.

![NetScaler MAS Deployment Configuration.](image)

To back up your primary NetScaler MAS server from the NetScaler MAS server's GUI

1. In a web browser, type the IP address of your primary NetScaler MAS server (for example, http://192.168.100.1).
2. In the **User Name** and **Password** fields, enter the administrator credentials. The default administrator credentials are `nsroot` and `nsroot`.
3. Navigate to **System > System Administration**. Under **Policy Administration**, select **Advanced Backup Settings**.
4. On the **Configure Advanced Backup Settings** page, click **Enable Remote Backups** to start the backup process.

**Note**

Make sure you have enough space on the backup VM, if you are going to retain the WAL logs for a long time. Collecting WAL logs over an indefinite period of time can cause space issues on the backup node.

You can follow the guidelines given below during upgrade of NetScaler MAS:

1. Disable the advanced backup on primary NetScaler MAS server, before upgrading.
2. Upgrade the primary NetScaler MAS server.
3. Upgrade the backup NetScaler MAS server and register it as remote server to the primary NetScaler MAS server.
4. Enable advanced backup on primary NetScaler MAS server.
To restore your NetScaler MAS server

1. On the hypervisor's console, find your backup NetScaler MAS server, and locate the remote backup script (pgsql_remote_backup.sh) at /mps/scripts/pgsql.
2. Run the following command to restore your NetScaler MAS server:

   `sh pgsql_restore_remote_backup.sh`
How to Enable Shell Access for Non-Default Users in NetScaler MAS

Jul 25, 2016
You can enable shell access for non-default users in NetScaler MAS. You can use this feature to enable and set up communication mode with instances.

**Note**
By default, shell access is disabled for non-default users.

1. In NetScaler MAS, navigate to **System > System Administration**.
2. In **System Settings**, click **Change System Settings**.
3. On the **Modify System Settings** page, configure the following parameters:
   - **Communication with instances** - Select the communication protocol.
   - **Secure Access** - Enable secure access for NetScaler MAS.
   - **Enable Session Timeout** - Specify the time period for which to retain an inactive session.
   - **Allow Basic Authentication** - Allow Management Service to accept credentials given using Basic Authentication Protocol.
   - **Enable nsrecover Login** - Enable nsrecover login on Management Service.
   - **Enable Certificate Download** - Enables you to download certificates from the added NetScaler.
   - **Enable Shell access for non-nsroot User** - Enable shell access for non-default users in NetScaler MAS.
4. Click **OK**.
How to Assign a Host Name to a NetScaler MAS Server

Jun 30, 2016
To identify a NetScaler MAS server, you can assign the server a host name. The host name is displayed on the Universal license for NetScaler MAS.

1. In NetScaler MAS, navigate to System > System Administration.
2. Under System Settings, click Change Hostname.
3. On the Configure Hostname page, enter a host name and click OK.
How to Back Up and Restore a NetScaler MAS Configuration in an HA Pair

Mar 30, 2017
You can back up the current configuration of a NetScaler MAS. In an HA deployment of NetScaler MAS, you can back up and restore the NetScaler MAS configuration from either one of the servers. If you are using a load balancing virtual server IP address to take the backup, the backup file can be stored on either server and must be checked manually.

If you restore when only one node is active, or when restoring if a fail over happens, the restore process fails to complete.

1. Navigate to System > Advanced Settings > Backup Files, and then click Back Up.
2. To encrypt the backup file, select the Password Protect file checkbox.

1. Navigate to System > Advanced Settings > Backup Files.
2. Select the backup file that you want to restore, and then click Restore.

Note

The time taken to restore two NetScaler MAS servers in HA mode depends on the number of network instances being managed by the NetScaler MAS servers.
Managing NetScaler SD-WAN WO using NetScaler MAS

Mar 20, 2017
This page provides quick access links to the topics that you can refer to set up NetScaler MAS and to manage your SD-WAN WO appliances using NetScaler MAS.

Overview

Architecture and Communication Process

Before You Begin

Single Server Deployment

High Availability Deployment

Migrate a Single Server Deployment to a High Availability Deployment

Migrating from NetScaler Insight Center to NetScaler MAS

How to Add Instances to NetScaler MAS

How to Create Instance Groups on NetScaler MAS

How to Back Up and Restore an Instance using NetScaler MAS

How to Create Configuration Jobs for NetScaler SD-WAN WO Instances in NetScaler MAS

How to Schedule Jobs Created by Using Built-in Templates in NetScaler MAS

How to Reschedule Jobs That Were Configured by Using Built-in Templates in NetScaler MAS

How to Reuse Executed Configuration Jobs

WAN Insight

HDX Insight

How to View Network Reports for NetScaler SD-WAN WO Instances

How to Configure Adaptive Thresholds
How to Configure Database Summarization for Analytics
How to Create Thresholds and Alerts Using NetScaler MAS

How to Set Event Age for Events on NetScaler MAS
How to Schedule an Event Filter by Using NetScaler MAS
How to Set Repeated Email Notifications for Events from NetScaler MAS
How to Suppress Events by Using NetScaler MAS
How to View Event Reports for NetScaler SD-WAN WO instances
How to Set Multiple Event Rules Notifications in NetScaler MAS
How to Modify the Reported Severity of Events that Occur on NetScaler Instances
How to View the Events Summary in NetScaler MAS
How to Display Event Severities and Skews of SNMP Traps on the Infrastructure Dashboard of NetScaler MAS

How to Cascade External Authentication Servers
How to Add RADIUS Authentication Servers
How to Add LDAP Authentication Servers
How to Add TACACS Authentication Servers
How to Extract Authentication Server Group in NetScaler MAS
How to Enable Fallback Local Authentication

How to Upgrade NetScaler MAS
How to Generate a Tech Support File for NetScaler MAS
How to Back up and Restore your NetScaler MAS Server in a Single-Server Deployment
How to Back Up and Restore a NetScaler MAS Configuration in an HA Pair
How to Enable Shell Access for Non-Default Users in NetScaler MAS
How to Configure NTP Server on NetScaler MAS
How to Configure SSL Settings for NetScaler MAS
How to Configure Syslog Purging Interval for MAS
How to View Auditing Information of NetScaler MAS
How to Configure System Notification Settings of NetScaler MAS

How to Monitor CPU, Memory, and Disk Usage of NetScaler MAS

How to Configure a Cipher Group for NetScaler MAS

How to Create SNMP Traps, Managers, and Users on NetScaler MAS

How to Assign a Host Name to a NetScaler MAS Server

Managing System Settings
How to View Event Reports for NetScaler SD-WAN WO Instances

Mar 21, 2017

You can view the events of the Top 10 SD-WAN WAN Optimization (WO) instances as a graphical representation by navigating to Infrastructure > Events > Reports > NetScaler SD-WAN WO.

The events are displayed based on their severity for each instance, you can click each severity to know more information on the number of events, when it occurred and what category it belongs to.
How to View Network Reports for NetScaler SD-WAN WO Instances

Mar 21, 2017

You can view WAN optimization network related reports in NetScaler MAS, using this data you can troubleshoot network issues or analyze the behavior of your NetScaler SDWAN WAN Optimization (WO) devices. You can view the reports of network statistics of your WAN optimization devices for the past one hour, one day, one week or one month.

You can view the following reports:

<table>
<thead>
<tr>
<th>Reports</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceleration</td>
<td>Use this report to analyze the pattern of accelerated traffic (KBPS by service class) and the number of accelerated TCP connections passing through the WAN optimization appliance. This includes the number of TCP connections passing through the WAN optimization device that undergo acceleration, the number of open and half-closed connections that have been selected for acceleration, and the number of half-open connections that are candidates for acceleration.</td>
</tr>
<tr>
<td>Pass through Connection</td>
<td>Use this report to view the non-accelerated connections for the WAN optimization device.</td>
</tr>
<tr>
<td>Service Class</td>
<td>Use this report to view the sent and receive bandwidth savings based on the service class type defined for the WAN optimization device.</td>
</tr>
<tr>
<td>Application</td>
<td>Use this report to view the sent and received data volume in bits-per-second for the applications running on the WAN optimization device.</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>Use this report to view the CPU utilization of the WAN optimization device as a percentage.</td>
</tr>
<tr>
<td>Capacity Increase</td>
<td>Use this report to view the cumulative send compression ratio for the WAN optimization device.</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Data reduction</td>
<td>Use this report to view the transmit and receive bandwidth savings as a percentage. You can also analyze the transmit bandwidth and receive bandwidth saving values separately for the WAN optimization device.</td>
</tr>
<tr>
<td>Link Utilization</td>
<td>Use this report to view the transmit link utilization and receive link utilization for the WAN optimization as a percentage.</td>
</tr>
<tr>
<td>Plugin Usage</td>
<td>Use this report to view the number of plugins connected to the WAN optimization device.</td>
</tr>
<tr>
<td>Packet Loss</td>
<td>Use this report to view the link dropped sent packets and link dropped received packets for the links defined in the WAN optimization device.</td>
</tr>
<tr>
<td>Throughput</td>
<td>Use this report to view the link sent volume and link received volume in bits-per-second for the WAN optimization device.</td>
</tr>
<tr>
<td>QoS</td>
<td>Use this report to view the QoS Sent and QOS Receive volume in bits-per-sec for the WAN optimization device.</td>
</tr>
</tbody>
</table>
To view NetScaler SD-WAN WO network reports:

1. In NetScaler MAS, navigate to **Analytics** > **Network Reporting** > **NetScaler SD-WAN WO**.

2. From the **Report Name** drop-down list select a report that you want to view.

3. From the **Instances** drop-down list, select the NetScaler SD-WAN WO instance for which you want to view the report.

4. From the **Duration** drop-down list, select the time interval.

5. Click **Run**.
StyleBooks

Aug 10, 2017

StyleBooks simplify the task of managing complex NetScaler configurations for your applications. A StyleBook is a template that you can use to create and manage NetScaler configurations. You can create a StyleBook for configuring a specific feature of NetScaler, or you can design a StyleBook to create configurations for an enterprise application deployment such as Microsoft Exchange or Lync.

StyleBooks fit in well with the principles of Infrastructure-as-code that is practiced by DevOps teams, where configurations are declarative and version-controlled. The configurations are also repeated and are deployed as a whole. StyleBooks offer the following advantages:

- **Declarative**: StyleBooks are written in a declarative rather than imperative syntax. Stylebooks allow you to focus on describing the outcome or the "desired state" of the configuration rather than the step-by-step instructions on how to achieve it on a particular NetScaler instance. NetScaler MAS computes the diff between existing state on a NetScaler and the desired state you specified, and makes the necessary edits to the infrastructure. Because StyleBooks use a declarative syntax, written in YAML, components of a StyleBook can be specified in any order, and NetScaler MAS determines the correct order based on their computed dependencies.

- **Atomic**: When you use StyleBooks to deploy configurations, the full configuration is deployed or none of it is deployed and this ensures that the infrastructure is always left in a consistent state.

- **Versioned**: A StyleBook has a name, namespace, and a version number that uniquely distinguishes it from any other StyleBook in the system. Any modification to a StyleBook requires an update to its version number (or to its name or namespace) to maintain this unique character. The version update also allows you to maintain multiple versions of the same StyleBook.

- **Composable**: After a StyleBook is defined, the StyleBook can be used as a unit to build other StyleBooks. You can avoid repeating common patterns of configuration. It also allows you to establish standard building blocks in your organization. Because StyleBooks are versioned, changes to existing StyleBooks results in new StyleBooks, therefore ensuring that dependent StyleBooks are never unintentionally broken.

- **App-Centric**: StyleBooks can be used to define the NetScaler configuration of a full application. The configuration of the application can be abstracted by using parameters. Therefore, users who create configurations from a StyleBook can interact with a simple interface consisting of filling a few parameters to create what can be a complex NetScaler configuration. Configurations that are created from StyleBooks are not tied to the infrastructure. A single configuration can thus be deployed on one or multiple NetScalers, and can also be moved among instances.

- **Auto-Generated UI**: NetScaler MAS auto-generates UI forms used to fill in the parameters of the StyleBook when configuration is done using the NetScaler MAS GUI. StyleBook authors do not need to learn a new GUI language or separately create UI pages and forms.

- **API-driven**: All configuration operations are supported by using the NetScaler MAS GUI or through REST APIs. The APIs can be used in synchronous or asynchronous mode. In addition to the configuration tasks, the StyleBooks APIs also allow you to discover the schema (parameters description) of any StyleBook at runtime.

You can use one StyleBook to create multiple configurations. Each configuration is saved as a config pack. For example, consider that you have a StyleBook that defines a typical HTTP load balancing application configuration. You can create a configuration with values for the load balancing entities and execute it on a NetScaler instance. This configuration is saved as a config pack. You can use the same StyleBook to create another configuration with different values and execute it on the same or a different NetScaler instance. A new config pack is created for this configuration. A config pack is saved both on NetScaler MAS and on the NetScaler instance on which the configuration is executed.
You can either use StyleBooks shipped with NetScaler MAS to create configurations for your deployment, or design your own StyleBooks, import them to NetScaler MAS, and then use them to create configurations either by using NetScaler MAS GUI or by using APIs.

This document includes the following information:

- How to Use StyleBooks Shipped with NetScaler MAS
- How to Create Your Own StyleBooks
- How to Use User-Defined StyleBooks in NetScaler MAS
- How to Use API to Create Configurations from StyleBooks
- How to Enable Analytics and Configure Alarms on a Virtual Server Defined in a StyleBook
- How to Create a StyleBook to Upload SSL Certificate and Certificate Key Files to NetScaler MAS
- How to Use Microsoft Exchange StyleBook for Business Enterprises
- How to Use Microsoft Skype for Business StyleBook for Business Enterprises
- StyleBooks Grammar
How to Use StyleBooks Shipped with NetScaler MAS

Jan 24, 2017

A set of StyleBooks are provided by Citrix with NetScaler MAS. When you use such a StyleBook, you have to specify values for the parameters in the StyleBook and select the IP addresses of the NetScaler instances where you want to execute the configuration. After you submit the configuration, NetScaler MAS validates the parameter values you have specified, creates a graph of the configuration, connects to the NetScaler instances, and executes the configuration on the instances.

To create configuration from a StyleBook by using the NetScaler MAS GUI

1. Navigate to Applications > Configurations, and then click Create New. A list of StyleBooks is displayed.

2. Select a StyleBook that is suitable to your requirements and specify the required values for the parameters.
3. Under **Target Instances**, click and select the IP address of the NetScaler instance where you want to execute the configuration. If you want to execute this configuration on multiple instances, click '++' to add more instances.

If you want to test or validate your configuration before executing it on the NetScaler instance, select **Dry Run** and then click **Create**. If your configuration is valid, the objects that are created on the basis of the values you have provided are displayed.
4. Clear the **Dry Run** check box and click **Create** to create the config pack and execute the configuration on the NetScaler instance. The StyleBook configuration (config pack) that you have created appears in the list of configurations, as shown below.

![Objects](objects.png)

You can now examine, update, or remove this configuration (config pack) by using the NetScaler MAS GUI.
How to Create Your Own StyleBooks

Mar 09, 2017

You can write your own StyleBook for your deployment, import it to NetScaler MAS, and create configuration objects. You can also use API to create configurations from your StyleBooks.

This document includes the following information:

- Before You Begin
- Anatomy of a StyleBook
- StyleBook to Create a Load Balancing Virtual Server
- StyleBook to Create a Basic Load balancing Configuration
- Create a Composite StyleBook
- Customize Your StyleBook By Using GUI Attributes

Before you begin creating StyleBooks, make sure you have knowledge of the following:

- NITRO API
- YAML

StyleBook files use the YAML format. For information about the YAML format, see: http://learn.getgrav.org/advanced/yaml.

The following is a list of YAML guidelines you must be aware of while creating StyleBooks:

- YAML is case sensitive.
- YAML requires proper indentation
- Use <spacebar> key to create proper indentation. Do not use <tab> key. Using <tab> key will create compilation error while importing your StyleBook to MAS.
- Do not use strings within quotation marks. Include the string within quotation marks only if a string contains punctuation marks (dashes, colons, and so on.) If you want to interpret a number as a string, either include the number within quotation marks or use the str() built-in function of StyleBooks.
- Literals like YES/Yes/yes/Y/y/NO/no/No/n/N, ON/On/on/OFF/Off/off, and TRUE/true/truthy/FALSE/False/false/falsey are considered Booleans, and are equivalent to true and false respectively. To interpret them as strings, include them within quotation marks. For example: "YES", "No", "True", "False", and so on.

Note

Before importing your StyleBook file into NetScaler MAS, it is recommended that you validate if your file is compliant with the YAML format. To validate your file, you can use the online tool: http://www.yamllint.com/
Writing StyleBooks requires that you understand the grammar, syntax, and structure of StyleBooks. A typical StyleBook has the following sections:

- **Header**: This section lets you define the identity of a StyleBook and describe what it does. This is a mandatory section.
- **Import StyleBooks**: This section lets you declare which other StyleBook you want to refer to from your current StyleBook. Importing NetScaler NITRO configuration StyleBooks or other StyleBooks is required to write a StyleBook. This is a mandatory section.
- **Parameters**: This section lets you define the parameters you require in your StyleBook to create a configuration. It describes the input that your StyleBook takes. This is an optional section.
- **Components**: This section lets you define the entities (configuration objects) that are created by the StyleBook for a specific configuration. This section is considered as the core of a StyleBook. Components generally use the input provided in the parameters section to adapt the configuration generated by the StyleBook. This is an optional section.

A StyleBook may have a parameters section, or a components section, or both. A StyleBook with only the parameters section is useful to define a list of parameters that can be used by other StyleBooks. This promotes reusability of parameter groups across a set of StyleBooks. A StyleBook with only a components section may be used when you want to specify the values for attributes in the StyleBook instead of defining parameters to take user input.

- **Outputs**: While the parameters section defines the inputs of the StyleBook, this optional section defines its outputs. In this optional outputs section, you can specify the components that you want to expose to users creating a configuration from this StyleBook and to other StyleBooks that import this StyleBook. Users and importing StyleBooks can then reference the properties of the exposed components.
- **Operations**: A StyleBook may contain an optional section to enable Analytics in NetScaler MAS on any virtual server that is part of the StyleBook.

The following figure shows a simple outline of a StyleBook.
The following examples help you learn about the grammar and structure of a StyleBook and how to write StyleBooks with increasing levels of complexity.

- StyleBook to Create a Load Balancing Virtual Server
- StyleBook to Create a Basic Load Balancing Configuration
- Create a Composite StyleBook
- Customize Your StyleBook By Using GUI Attributes

In this example, you design a basic StyleBook that creates a load balancing virtual server of HTTP protocol type and listening on port 80. The virtual server name, IP address, and load balancing method parameters accept user-defined values, that is, they are the parameters of the StyleBook.

Header

The first six lines of a StyleBook comprise the header section. In this example, the header section is written as follows:

```plaintext
name: lb-vserver
description: This StyleBook defines a load balancing virtual server configuration.
display-name: Load Balancing Virtual Server (HTTP)
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
```

The header section includes the following details:

- **name**: A name for this StyleBook.
- **description**: A description defining what this StyleBook does. This description appears on the NetScaler MAS GUI.
- **display-name**: A descriptive name for the StyleBook that appears on the NetScaler MAS GUI.
- **namespace**: A namespace forms part of a unique identifier for a StyleBook to avoid name collisions.
- **schema-version**: Always takes the value “1.0” in this release.
- **version**: The version number of the StyleBook. You can change the version number when you update the StyleBook.

The combination of **name**, **namespace**, and **version** uniquely identifies a StyleBook in the system. You cannot have two StyleBooks with the same combination of name, namespace, and version in NetScaler MAS. However, you can have two StyleBooks with the same name and version but different namespaces, or with the same namespace and version but different names.

Note

Consider that you have updated your StyleBook and you have an updated version number. Now if you are referring to (that is, if you are importing) this StyleBook in other StyleBooks, ensure to update the version number in other StyleBooks too, so that they use the correct version of the imported StyleBook.
Import StyleBooks

The section after header is called “import-stylebooks.” In this section, you must declare the namespace and version number of any other StyleBook that you want to refer to in your current StyleBook. This enables you to import and reuse other StyleBooks instead of rebuilding the same configuration in your own StyleBook.

In this example, the import-stylebooks section is written as follows:

```yaml
import-stylebooks:

- namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
```

Every StyleBook must refer to the netscaler.nitro.config namespace if it uses any of the NITRO configuration objects directly. This namespace contains all the NetScaler NITRO types, such as lbvserver. Versions 10.5, 11.0, and 11.1 are supported, which means that you can use your StyleBook to create and run configurations on any NetScaler instance running release 10.5 or later.

The prefix used in the import-stylebooks section is a shorthand to refer to the combination of namespace and version. In this case, ns refers to netscaler.nitro.config of version 10.5. In the later sections of your StyleBook, instead of using the namespace and version to refer to the imported StyleBook, you can use the prefix string chosen, for example, ns, in the example above.

**Note**

To ensure that your StyleBooks can be used to configure any NetScaler instance of version 10.5 or above, Citrix recommends that for maximum compatibility you should import the Nitro 10.5 namespace in your StyleBooks that directly use Nitro built-in StyleBooks (namespace: netscaler.nitro.config, version: 10.5).

Parameters

The parameters section lets you declare all the parameters that you need in your StyleBook. You, as the StyleBook developer, have to decide what is the input that you want the users of your StyleBook to specify. In this example, you have built your StyleBook in a way that requires its users to provide the name of the virtual server, its IP address, and the load balancing method.

The parameters section would look as follows:

```yaml
parameters:

- name: name
  type: string
```
**label**: Application Name

**description**: Name of the application configuration.

**required**: true

- **name**: ip
  **type**: ipaddress
  **label**: Application Virtual IP (VIP)
  **description**: Application VIP that the clients access.
  **required**: true

- **name**: lb-alg
  **type**: string
  **label**: LoadBalancing Algorithm
  **description**: Choose the load balancing algorithm (method) used for load balancing client request between the application servers.
  **allowed-values**:
  - ROUNDROBIN
  - LEASTCONNECTION
  **default**: ROUNDROBIN

**Note**

If you do not provide the label of a parameter, then NetScaler MAS will use the name attribute when displaying this parameter. You must always define a label for your parameters so that you can control how they show up in the NetScaler MAS GUI.

When using the APIs however, the parameter is designated by its name.

In this section, you have declared three parameters indicated by their **name** attribute values - **name** for virtual server name, **ip** for IP address of the virtual server, and **lb-alg** for the load balancing method.

**type** refers to the type of value these parameters can take. For example, name and lb-alg can take a string value and the ip value has to be of type ip address. Parameters in a StyleBook can be of any of the following built-in types:

- **string**: An array of characters. If a length is not specified, the string value can take any number of characters. However, you can limit the length of a string type by using the attributes min-length and max-length.
- **number**: An integer number. You can specify the minimum and maximum number that this type can take by using the attributes min-value and max-value.
- **boolean**: Can be either true or false. Also, note that all the literals are considered by YAML as booleans (for example, Yes or No).
- **ipaddress**: A string that represents a valid IPv4 or IPv6 address.
- **tcp-port**: A number between 0 and 65535 that represents a TCP or UDP port.
- **password**: An opaque/secret string value. When NetScaler MAS GUI displays a value for this parameter, it is shown as asterisks (*****).
- **certfile**: A certificate file.
- **keyfile**: A certificate private key file.
- **file**: A parameter of this type requires the user to upload a file, for example, a certificate or key file.
- **object**: Consists of multiple elements and each of these elements is a parameter. This type can be used to group multiple related parameters under one parent parameter.

**required** states whether a parameter is mandatory or optional. If it is set to true, the parameter is mandatory and the user has to provide a value for this parameter when creating configurations using this StyleBook. By default, all parameters are optional. In this example, **name** and **ip** are mandatory parameters while **lb-alg** is an optional parameter, the default value of which is "ROUNDROBIN."

Use the **default** attribute to assign a default value to an optional parameter. While creating a configuration, if a user does not specify a value, the default value is used. For example, for the **lb-alg** parameter, the default value is ROUNDROBIN.

Use the **allowed-values** attribute to define specific values that a user can choose from when creating a configuration. In this example, you have specified two values for the **lb-alg** parameter - ROUNDROBIN and LEASTCONNECTION.

When you import your StyleBook into NetScaler MAS and use it, the GUI displays a form with these three parameters. The fields displayed for name and ip allow string and ipaddress type of value to be entered, and the lb-alg field is displayed as a drop-down list with ROUNDROBIN selected as the default value.

---

**Note**

In addition to built-in types, a parameter can have another StyleBook as its type. This is a way of reusing parameters defined in other StyleBooks.

---

**Components**

The last section in this StyleBook is called the components section and is considered as the most important section in the StyleBook. In this section, you define the configuration objects that have to be created by the StyleBook.

For this example, you have to write the components section as follows:

```yaml
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
```
This example contains only one component. The main attributes of a component are name, type, and properties. The type of a component determines what properties this component provides. Components have two kind of types:

- **Built-in type**: This type is provided by the system and you do not have to define it, for example, the NITRO entity types “lbvserver” or “servicegroup.” In this example, you are using a built-in component type.
- **Composite type**: This type is the StyleBook that you created and imported into NetScaler MAS, or the StyleBook that is shipped with NetScaler MAS. You can learn more about Composite StyleBooks in Create a Composite StyleBook.

In this example, you have defined a component called `lbvserver-comp`. This component is of type `ns::lbvserver` (a built-in Nitro type), where “ns” is the prefix that refers to the namespace netscaler.nitro.config and version 10.5 that you had specified in the import-stylebooks section, and “lbvserver” is a Nitro resource in this namespace.

The properties defined here are the attributes of the “lbvserver” resource. To learn more about all the available NetScaler Nitro resources and their attributes, see the NetScaler NITRO REST API documentation.

The properties in this section include the mandatory attributes of the “lbvserver” resource and allows you to specify values for these attributes. In this example, you are specifying static values for servicetype and port while the name, ipv46, and lbmethod properties get their values from the input parameters. In the rest of the StyleBook, you can refer to the parameter names defined in the parameters section by using `$parameters.<parameter-name>` expression, for example, `$parameters.ip`.

**Note**

By convention, the prefix “ns” is always used to designate a NetScaler Nitro namespace in the “import-stylebooks” section. Though it is not mandatory, Citrix recommends to use the same convention in your own StyleBooks for consistency.

**Build Your StyleBook**

Now that you have defined all the required sections of this StyleBook, bring them all together to build your first StyleBook. Copy and paste the StyleBook content to a text editor, and then save the file as `lb-vserver.yaml`. Run the contents of your StyleBook through the online tool [http://www.yamllint.com/](http://www.yamllint.com/) to validate the YAML syntax.

The full content of the file `lb-vserver.yaml` is reproduced below:

```yaml
name: lb-vserver
```
namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Virtual Server (SSL)

description: This stylebook defines a very simple load balancing SSL virtual server configuration

schema-version: "1.0"

import-stylebooks:

-

namespace: netscaler.nitro.config

version: "10.5"

prefix: ns

-

namespace: com.citrix.adc.stylebooks

version: "1.0"

prefix: stlb

parameters:

-

name: name

type: string

label: Application Name

description: Give a name to the application configuration.
description: Give a name to the application configuration.

required: true

- name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true

- name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the loadbalancing algorithm (method) used for loadbalancing client requests between the application servers.
  allowed-values:
  - ROUNDROBIN
  - LEASTCONNECTION
  default: ROUNDROBIN

components:

- name: lbvserver-comp
To start using your StyleBook to create configurations, you have to import it to NetScaler MAS and then use it. For more information, see How to Use User-Defined StyleBooks.

You can also import this StyleBook into other StyleBooks (using the import-stylebooks construct.) Or, you can modify this StyleBook to include more parameters and components as described in the next section.

In the previous section, you have built a basic StyleBook to create a load balancing virtual server. You can save this StyleBook with a different name and then update it to include additional parameters and components for a basic load balancing configuration. Save this StyleBook file as basic-lb-config.yaml.

In this section, you will design a new StyleBook that creates a load balancing configuration comprising of load balancing virtual server, a service group, and a list of services. It also binds the services to the service group and binds the service group to the virtual server.

Header

To build this StyleBook, you have to start by updating the header section. This section is similar to the one you created for load balancing virtual server StyleBook. In the header section, change the value of name to basic-lb-config. Also, update description and display-name to describe this StyleBook appropriately. You do not have to change the namespace and version values. Because you have changed the name, the combination of name, namespace, and version creates a unique identifier for this StyleBook in the system.

name: basic-lb-config

description: This StyleBook defines a simple load balancing configuration.
display-name: Load Balancing Configuration

namespace: com.example.stylebooks

schema-version: "1.0"

version: "0.1"

Import StyleBooks

The import-stylebooks section remains the same. It refers to the netscaler.nitro.config namespace to use the Nitro configuration objects.

import-stylebooks:

- namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"

Parameters

You have to update the parameters section to add two additional parameters to define the list of services or servers and the port on which the services listen to. The first three parameters, name, ip, and lb-alg remain the same.

parameters:

- name: name
  type: string
  label: Application Name
  description: Name of the application configuration
  required: true

- name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: Application VIP that the clients access
  required: true

-
name: lb-alg

type: string

label: LoadBalancing Algorithm

description: Choose the load balancing algorithm used for load balancing client requests between the application servers.

allowed-values:
- ROUNDROBIN
- LEASTCONNECTION

default: ROUNDROBIN

- name: svc-servers
  type: ipaddress[]
  label: Application Server IPs
  
description: The IP addresses of all the servers of this application
  required: true

- name: svc-port
  type: tcp-port
  label: Server Port
  
description: The TCP port open on the application servers to receive requests.
  default: 80

In this example, the parameter svc-servers is added to accept a list of IP addresses of the services that represent the backend servers of the application. This is a mandatory parameter as indicated by required: true. The second parameter, svc-port, denotes the port number on which the servers listen. The default port number is 80 for svc-port parameter, if it is not specified by the user.

Components

You have to also update the components section to define additional components such that they use the two new parameters and build the complete load balancing configuration.

For this example, you have to write the components section as follows:

components:
- **name**: lbvserver-comp
  
  **type**: ns:lbvserver
  
  **properties**:
  
  - **name**: $parameters.name + "-lb"
  - **servicetype**: HTTP
  - **ipv46**: $parameters.ip
  - **port**: 80
  - **lbmethod**: $parameters.lb-alg

  **components**:
  
  - **name**: svcg-comp
    
    **type**: ns:servicegroup
    
    **properties**:
    
    - **name**: $parameters.name + "-svcgrp"
    - **servicetype**: HTTP

  **components**:
  
  - **name**: lbvserver-svg-binding-comp
    
    **type**: ns:lbvserver_servicegroup_binding
    
    **properties**:
    
    - **name**: $parent.parent.properties.name
    - **servicegroupname**: $parent.properties.name

  - **name**: members-svcg-comp
    
    **type**: ns:servicegroup_servicegroupmember_binding
    
    **repeat**: $parameters.svc-servers
In this example, the original component `lbvserver-comp` (from the previous example) now has a child component called `svcg-comp`. And, the `svcg-comp` component has two child components within it. Nesting a component within another component allows the nested component to create configuration objects by referring to attributes in the parent component. The nested component can create one or more objects for each object created in the parent component.

The `svcg-comp` component is used to create a service group on the NetScaler instance by using the values provided for the attributes of the resource “servicegroup”. In this example, you are specifying static value for servicetype, while name gets its value from the input parameter. You refer to the parameter `name` defined in the parameters section by using `$parameters.name + "-svcgrp"` notation, where “-svcgrp” is appended (concatenated) to the user-defined name.

The component `svcg-comp` has two child components, `lbvserver-svg-binding-comp` and `members-svcg-comp`.

The first child component, `lbvserver-svg-binding-comp`, is used to bind a configuration object between the service group created by its parent component and the load balancing virtual server (lbvserver) created by the parent’s parent component. The `$parent` notation, also called the parent reference, is used to refer to entities in the parent components. For example, `servicegroupname: $parent.properties.name` refers to the service group created by the parent component `svcg-comp`, and `name: $parent.parent.properties.name` refers to the virtual server created by the parent’s parent component `lbvserver-comp`.

The `members-svcg` component is used to bind configuration objects between the list of services to the service group created by the parent component. The creation of multiple binding configuration objects is achieved by using the `repeat` construct of StyleBook to iterate over the list of servers specified in the parameter `svc-servers`. During the iteration, this StyleBook component creates a Nitro configuration object of type `servicegroup_servicegroupmember_binding` for each service (referred to as `srv` in the `repeat-item` construct) in the service group, and it sets the `ip` attribute in each Nitro configuration object to the IP address of the corresponding server.

Generally, you can use the `repeat` and `repeat-item` constructs in a component to make that component build multiple configuration objects of the same type. You can assign a variable name to the `repeat-item` construct, for example, `srv`, to designate the current value in the iteration. This variable name is referred to in the properties of the same component or in child components as `$<varname>`, for example `$svr`.

In the above example, you have used nesting of components inside each other to easily construct this configuration. In this particular case, nesting of components was not the only way of building the configuration. You could have achieved the same result without nesting, as shown below:

```
components:
  - name: members-svcg-comp
```

```xml
repeat-item: srv

properties:
  ip: $srv
  port: str($parameters.svc-port)
  servicegroupname: $parent.properties.name
```
type: ns::servicegroup_servicegroupmember_binding
repeat: $parameters.svc-servers
repeat-item: srv
properties:
  ip: $srv
  port: str($parameters.svc-port)
  servicegroupname: $components.svcg-comp.properties.name

name: lbvserver-svg-binding-comp
type: ns::lbvserver_servicegroup_binding
properties:
  name: $components.lbvserver-comp.properties.name
  servicegroupname: $components.svcg-comp.properties.name

name: lbvserver-comp
type: ns::lbvserver
properties:
  name: $parameters.name + "-lb"
  servicetype: HTTP
  ipv46: $parameters.ip
  port: 80
  lbmethod: $parameters.lb-alg

name: svcg-comp
type: ns::servicegroup
properties:
  name: $parameters.name + "-svcgrp"
  servicetype: HTTP
Here, all the components are at the same level (that is, they are not nested) but the result achieved (the NetScaler configuration generated) is the same as that of the nested components used earlier. Also, the order in which the components are declared in the StyleBook does not impact the order of creation of the configuration objects. In this example, the components svcg-comp and lbvserver-comp, even though declared last, will have to be built before building the second component lbvserver-svg-binding-comp because there are forward references to these components in the second component.

**Note**

By convention, the names of StyleBooks, parameters, substitutions, components and outputs are in lowercase. When they contain multiple words, they are separated by a “-” character. For example “lb-bindings”, “app-name”, “rewrite-config”, and so on. Another convention is to suffix component names with “-comp” string.

**Outputs**

The last section you can add to the new StyleBook is the outputs section where you specify what this StyleBook exposes to its users (or in other StyleBooks) after it is used to create a configuration. For example, you can specify in the outputs section to expose the lbvserver and the servicegroup configuration objects that would be created by this StyleBook.

```
outputs:

- 
  name: lbvserver-comp
  value: $components.lbvserver-comp
  description: The component that builds the Nitro lbvserver configuration object

- 
  name: servicegroup-comp
  value: $components.svcg-comp
  description: The component that builds the Nitro servicegroup configuration object
```

The outputs section of a StyleBook is optional. A StyleBook does not need to return outputs. However, by returning some internal components as outputs, it allows any StyleBooks that import this StyleBook more flexibility as you can see when creating a composite StyleBook.

**Note**

It is a good practice to expose an entire component of the StyleBook in the outputs section, rather than just a single property of a component (for example, expose the whole $components.lbvserver-comp rather than just the name $components.lbvserver-comp.properties.name). Also add a description to the output explaining what the specific output represents.
Build Your StyleBook

Now that you have defined all the required sections of this StyleBook, bring them all together to build your second StyleBook. You have already saved this StyleBook file as `basic-lb-config.yaml`. Run the contents of your StyleBook through the online tool [http://www.yamllint.com/](http://www.yamllint.com/) to validate the YAML syntax.

The full content of the file `basic-lb-config.yaml` is reproduced below:

```yaml
name: basic-lb-config

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Configuration

description: This StyleBook defines a simple load balancing configuration.

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    version: "10.5"

    prefix: ns

parameters:

  -

    name: name

    type: string

    label: Application Name
```
description: Give a name to the application configuration.

required: true

name: ip

type: ipaddress

label: Application Virtual IP (VIP)

description: The Application VIP that clients access

required: true

name: lb-alg

type: string

label: LoadBalancing Algorithm

description: Choose the loadbalancing algorithm (method) used for loadbalancing client requests between the application servers.

allowed-values:

- ROUNDROBIN

- LEASTCONNECTION

default: ROUNDROBIN

name: svc-servers

type: ipaddress[]
label: Application Server IPs

description: The IP addresses of all the servers of this application

required: true

-  

name: svc-port

type: tcp-port

label: Server Port

description: The TCP port open on the Application Servers to receive requests.

default: 80

components:

-  

name: lbvserver-comp

type: ns::lbvserver

properties:

name: $parameters.name + "-lb"

servicetype: HTTP

ipv46: $parameters.ip

port: 80

lbmethod: $parameters.lb-alg
components:

- name: svcg-comp

type: ns::servicegroup

properties:

  servicegroupname: $parameters.name + ^-svgrp_

  servicetype: HTTP

components:

- name: lbvserver-svg-binding-comp

type: ns::lbvserver_servicegroup_binding

properties:

  name: $parent.parent.properties.name

  servicegroupname: $parent.properties.servicegroupname

- name: members-svcg-comp

type: ns::servicegroup_servicegroupmember_binding

repeat: $parameters.svc-servers

repeat-item: srv

properties:
To start using your StyleBook to create configurations, you have to import it to NetScaler MAS and then use it. For more information, see How to Use User-Defined StyleBooks.

You can also import this StyleBook into other StyleBooks and use its properties as described in the next section.

An important and powerful feature of StyleBooks is that they can be used as building blocks for other StyleBooks. A StyleBook can be imported into another StyleBook and it can be referred to as a type that is used by components of the second StyleBook similar to a Nitro built-in StyleBook.

For example, you can use the basic-lb-config StyleBook that you built in the previous section, to build another StyleBook called composite-example. To use the “basic-lb-config” StyleBook, you have to import it in the new StyleBook in the import-stylebooks section.

The new StyleBook would look as follows:

```yaml
ip: $srv

port: $parameters.svc-port

servicegroupname: $parent.properties.servicegroupname

outputs:

-

  name: lbvserver-comp

  value: $components.lbvserver-comp

  description: The component that builds the Nitro lbvserver configuration object

-

  name: servicegroup-comp

  value: $components.lbvserver-comp.components.svcg-comp

  description: The component that builds the Nitro servicegroup configuration object
```
name: composite-example

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Virtual Server (HTTP/RoundRobin)

description: This StyleBook defines a RoundRobin load balancing configuration with a monitor.

schema-version: "1.0"

import-stylebooks:

-

  namespace: netscaler.nitro.config

  version: "10.5"

  prefix: ns

-

  namespace: com.example.stylebooks

  version: "0.1"

  prefix: stlb

parameters:

-

  name: name

  type: string
label: Application Name

description: Give a name to the application configuration.

required: true

- name: ip
type: ipaddress

label: Application Virtual IP (VIP)

description: The Application VIP that clients access

required: true

- name: svc-servers
type: ipaddress[]

label: Application Server IPs

description: The IP addresses of all the servers of this application

required: true

components:

- name: basic-lb-comp
type: stlb::basic-lb-config

description: This component's type is another StyleBook that builds the NetScaler lbvserver, servicegroups and services configuration.
properties:

name: $parameters.name

ip: $parameters.ip

svc-servers: $parameters.svc-servers

-

name: monit-comp

type: ns::lbmonitor

description: This component is a basic Nitro type (a Builtin StyleBook) that builds the NetScaler monitor configuration object.

properties:

monitorname: $parameters.name + "-mon"

type: HTTP

respcode: str("200")

httprequest: "GET /

lrtm: ENABLED

secure: "YES"

components:

-

name: monit-svcgrp-bind-comp

type: ns::servicegroup_lbmonitor_binding

properties:
In the import-stylebooks section, you import the basic-lb-config StyleBook by using its namespace and version, referred to with the prefix "stlb".

In the components section, two components are defined. The first component is of type stlb::basic-lb-config, where "basic-lb-config" is the name of the StyleBook you created in StyleBook to Create a Basic Load Balancing Configuration. The properties that are defined for this component correspond to the mandatory parameters declared in the basic-lb-config StyleBook. You can however use any parameter of the StyleBook (both required and optional). Instead of re-building an lbvserver, a service group, and service and service group bindings, you import the StyleBook that does all of this as a component and use it to create these configuration objects in the new StyleBook.

StyleBook adds a second component "monit-comp" that uses the attributes of the Nitro resource "lbmonitor" (a built-in StyleBook) to create a monitor configuration object. It also has a sub-component "monit-svcgrp-bind-comp" to create the binding configuration object that binds the monitor to the servicegroup created in the first component. Because the servicegroup component created in the "basic-lb-config" StyleBook is exposed as an output, this StyleBook can access it using the expression $components.basic-lb-comp.outputs.servicegroup-comp. This is an example of how the outputs section can be used by the importing StyleBooks to have access to components in the imported StyleBooks that they would not have been able to access otherwise.

Next, copy and paste the StyleBook content to a text editor, and then save the file as composite-example.yaml. Run the contents of your StyleBook through the online tool http://www.yamllint.com/ to validate the YAML syntax. Then, import it to NetScaler MAS and create one or several configurations by using this StyleBook.

You can add GUI attributes in the parameters section of your StyleBook to make the fields intuitive when displayed on the NetScaler MAS GUI.

**Example:** You can add a descriptive name for the parameter by using the label attribute, and add a tooltip for this parameter by using the description attribute.

```
name: ip
label: Virtual Server IP Address
description: IP address of the virtual server that represents the load balanced application.
type: ipaddress
required: true
```

**Example:** If you have a parameter of type object, you can define the layout by using the gui attribute. In this example, the
layout is a collapsible object where fields are displayed in two columns.

```yaml
name: svcg-advanced
label: Advanced Application Server Settings
type: object
required: false
gui:
  collapse_pane: true
  columns: 2
```

**Example:** Some StyleBooks are used as building blocks for other StyleBooks and you may not want to display these StyleBooks on the NetScaler MAS GUI, since they are not intended to be used directly by users. For this, you can use the private attribute to prevent a StyleBook from being listed on the NetScaler MAS GUI.

```yaml
name: basic-lb-config
description: This stylebook defines a simple load balancing configuration.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
private: true
schema-version: "1.0"
version: "0.1"
```
How to Use User-Defined StyleBooks in NetScaler MAS

Jul 01, 2016

After you have built your StyleBook, you have to import it to NetScaler MAS to use it. The NetScaler MAS system validates your StyleBook on import, and it appears on the GUI ready to be used for creating configurations.

To use your StyleBook in NetScaler MAS

1. Navigate to Applications > Configuration > StyleBooks, and then click Import StyleBook.

2. In the Import StyleBook text box, copy and paste your StyleBook content and click Create. In this example, import the "lb-vserver.yaml" StyleBook that you had created in StyleBook to Create a Load Balancing Virtual Server.

3. The imported StyleBook is listed on the StyleBooks page (if it is not a private StyleBook). You can view the name, namespace, and version of the StyleBook, and also the NetScaler versions it is compatible with. You can also view the description and display name that you had defined in the header section of your StyleBook.

4. To create configurations from this StyleBook, navigate to Applications > Configuration, and then click Create New.

5. Select the StyleBook you have created and specify the required values for the parameters. You can see that name and ip are displayed as mandatory fields and can accept user values. lb-alg has only two values that you can choose from and...
by default, ROUNDROBIN is selected.

6. Under **Target Instance**, click and select the IP address of the NetScaler instance where you want to run the configuration.

If you want to have a look at the configuration objects that would be created on your NetScaler before actually creating the configuration, select **Dry Run** and then click **Create**. If your configuration is valid, the configuration objects that would be created on the basis of the values you have provided are displayed. In this example, only one object of type lbvserver is created. This lbvserver is the component type that you had used while building your StyleBook.

7. Clear **Dry Run** and click **Create** to actually create the config pack and the configuration on the NetScaler instance. The StyleBook configuration that you have created appears as shown below.
How to Use API to Create Configurations from StyleBooks

Jan 30, 2017

After you have built your StyleBook, you have to import it to NetScaler MAS to use it either by using the NetScaler MAS GUI or by using NetScaler MAS APIs. NetScaler MAS validates your StyleBook when you import it, and if the validation is successful, your StyleBook appears on the NetScaler MAS GUI catalog of StyleBooks, ready to be used for creating configurations.

You can now use the StyleBook APIs to create configurations based on this StyleBook. You can use any tool such as the curl command line tool or the Postman chrome browser extension to send HTTP requests to NetScaler MAS.

Consider the “lb-vserver” StyleBook you have created in StyleBook to Create a Load Balancing Virtual Server. Use REST API to create a config pack from this StyleBook as follows:

```
POST
https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/lb-vserver/configpacks

Content-Type: application/json
Accept: application/json

{
  "configpack": {
    "parameters": {
      "name": "lb1",
      "ip": "10.102.117.31"
    }
  }
}
```
In this HTTP request, the id (for example, "deecee30-f478-4446-9741-a85041903410") is the instance ID of the NetScaler instance on which the load balancing virtual server lb1 with IP address 10.102.117.31 is created. The instance ID of the NetScaler instance is retrieved from NetScaler MAS.

To obtain the ID of an instance managed by NetScaler MAS, you can use NetScaler MAS APIs. For example, to retrieve the instance ID of a NetScaler instance whose IP address is 192.168.153.160, you can use the following API:

```plaintext

Accept: application/json
```

The response contains the ID in the payload:

```plaintext
200 OK
Content-Type: application/json

{
    "errorcode": 0,
    "message": "Done",
    "operation": "get",
    "resourceType": "ns",
    "username": "nsroot",
    "tenant_name": "Owner",
    "resourceName": "",
    "ns": [
        {
            "is_grace": "false",
            "hostname": "",
            "std_bw_config": "0",
            "gateway_deployment": "false",
            ...
            "id": "deecee30-f478-4446-9741-a85041903410",
            ...
        }
    ]
}
```
If the configuration (config pack) is successfully created, you receive the following HTTP response:

200 OK
Content-Type: application/json

```
{
  "configpack": {
    "config_id": "1460806080"
  }
}
```

You have created your first configuration (config pack) that is uniquely identified by using the id 1460806080. You can use this ID to query, update, or delete the configuration.

You can use the same StyleBook to create another configuration or config pack and execute it on the same or different NetScaler instances. In this example, create another configuration and provide a different name and IP address for the virtual server and also specify LEASTCONNECTION as the load balancing method. Deploy this configuration on two NetScaler instances.

The HTTP request is as follows:

```
POST
https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/lb-vserver/configpacks
Content-Type: application/json
Accept: application/json

{
  "configpack": {
    "parameters": {
      "name": "lb2",
      "ip": "10.102.117.32",
      "lb-alg": "LEASTCONNECTION"
    }
  }
}
```
In this HTTP request, the load balancing virtual server lb2 with IP address 10.102.117.32 is created on the two NetScaler instances represented by the ids "deecee30-f478-4446-9741-a85041903410" and "debecc60-d589-4557-8632-a74032802412".

On successful creation of the config pack, the following HTTP response is received:

```
200 OK
Content-Type: application/json
{
    "configpack":{
        "config_id": "1657696292"
    }
}
```

This new config pack has a different id 165769629. You can update or remove this configuration by using this id.

Consider the “basic-lb-config” StyleBook you have created in StyleBook to Create a Basic Load balancing Configuration. Use REST API to create a config pack from this StyleBook as follows:

```
POST
http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/basic-lb-config/configpacks
```
In this HTTP request, the load balancing configuration is executed on two NetScaler instances. You can log on to these NetScaler instances to verify whether a virtual server and a service group with two services bound are created.

Consider the composite StyleBook `composite-example` you created in Create a Composite StyleBook. Use REST API to create a config pack from this StyleBook as follows:

```
POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks

Content-Type: application/json
```
In this HTTP request, the configuration is created on two NetScaler instances represented by their ids. If you log on to the NetScaler instances, you can view the configuration objects created by the "basic-lb-config" StyleBook that was imported into the "composite-example" StyleBook. You can also see a new HTTP monitor called "myapp-mon" that was part of the "composite-example" StyleBook.

On successful creation of the config pack, the following HTTP response is received:

200 OK

```
Accept: application/json

{
  "configpack": {
    "parameters": {
      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52", "10.102.29.53"]
    },
    "target_devices": [
      {
        "id": "deecee30-f478-4446-9741-a85041903410"
      },
      {
        "id": "debecc60-d589-4557-8632-a74032802412"
      }
    ]
  }
}
```
Updating a Configuration

To update this configuration, for example, by adding a new backend server with IP address 10.102.29.54 to the load balancing virtual server myapp, use the API for updating a config pack as follows:

```
PUT http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks/4917276817

Content-Type: application/json
Accept: application/json

{
  "configpack": {
    "parameters": {
      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52", "10.102.29.53", "10.102.29.54"]
    },
    "target_devices": [
      {
        "id": "deecee30-f478-4446-9741-a85041903410"
      },
      {
        "id": "debecc60-d589-4557-8632-a74032802412"
      }
    ]
  }
}
```

On successful update of the config pack, the following HTTP response is received:
Deleting a Configuration

To delete this configuration (from all the NetScaler instances), you can use the API for deleting a config pack as follows:

```plaintext
DELETE http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks/4917276817
```

```
Accept: application/json
```

On successful deletion of the config pack, the following HTTP response is received:

```plaintext
200 OK
Content-Type: application/json

{
  "configpack": {
    "config_id": "4917276817"
  }
}
```

You can log on to the NetScaler instance and verify that all the configuration objects that are part of this config pack have been removed.

If you want to remove the configuration from specific NetScaler instances instead of from all, use the update configpack operation described above and change the "target_devices" attribute in the JSON payload to remove the specific NetScaler instance IDs.
How to Enable Analytics and Configure Alarms on a Virtual Server Defined in a StyleBook

Sep 30, 2016

You can use the operations construct to configure NetScaler MAS analytics to collect appflow records on all or some of the traffic transactions handled by any virtual server component that is part of a StyleBook. You can also use this construct to configure alarms to get insight into the traffic managed by the virtual server.

The following example shows an operations section of a StyleBook:

```
operations:
  analytics:
    -
      name: lbvserver-ops
      properties:
        target: $components.basic-lb-comp.outputs.lbvserver
        filter: HTTP.REQ.URL.CONTAINS("catalog")
  alarms:
    -
      name: lbvserver-alarm
      properties:
        target: $outputs.lbvserver
        email-profile: $parameters.emailprofile
        sms-profile: "NetScalerSMS"
      rules:
        -
          metric: "total_requests"
          operator: "greaterthan"
          value: 25
          period-unit: $parameters.period
```
metric: "total_bytes"
operator: "lessthan"
value: 60
period-unit: "day"

The attributes in the analytics section are used to instruct NetScaler MAS analytics feature to collect appflow records on a virtual server component identified by the target property. You can also optionally specify a filter property that accepts a NetScaler policy expression to filter requests for which appflow records are collected on the virtual server.

When a config pack is created from this StyleBook, the NetScaler MAS analytics feature is configured to collect appflow records on the virtual servers that were specified when these are created in the process of creating a config pack.

The attributes in the alarms section are used to set thresholds to generate alarms and send notifications on the virtual server identified by the target property. In the above example, the email-profile and sms-profile properties are used to specify where the notifications should be sent. The rules section defines the thresholds. For example, if the total requests handled by the virtual server are greater than 25 and for a period defined by the user, an alarm is set and notification is sent. The "period-unit" specifies how frequently an alarm is triggered. It can take the value of day, hour, or weekly.

You can use the following operators when comparing the metric value to the threshold value:

- "greaterthan" for ">"
- "lessthan" for "<"
- "greaterthanequal" for "\>="
- "lessthanequal" for "\<="

Note that StyleBooks use API names for the metrics and not the names displayed on the NetScaler MAS analytics GUI.

To learn how to view and analyze data collected on virtual servers that were created as part of a config pack, see the NetScaler MAS analytics documentation.
How to Create a StyleBook to Upload SSL Certificate and Certificate Key Files to NetScaler Instances

Jan 30, 2017

When creating a StyleBook configuration that uses the SSL protocol, you must upload the SSL certificate files and certificate key files as required by the StyleBook parameters. StyleBook allows you to directly upload the SSL files and key files from your local system by using the NetScaler MAS GUI. You can also use NetScaler MAS APIs to upload certificate files and key files that are already managed by NetScaler MAS.

StyleBook Configuration

The StyleBook provided as an example here creates a basic load balancing virtual server configuration on the selected NetScaler instance. The configuration uses the SSL protocol. To create a configuration using this StyleBook, you must provide the name and IP address of the virtual server, select the load balancing method parameters, and upload the certificate file and the certificate key file for the virtual server, or use a certificate file and certificate key file that are already present in the NetScaler MAS. These are specified in the "parameters" section, as shown below:

parameters:
- name: name
type: string
required: true
-
  name: ip
type: ipaddress
required: true
-
  name: lb-alg
type: string
allowed-values:
  - ROUNDROBIN
  - LEASTCONNECTION
default: ROUNDROBIN
name: certificate
label: "SSL Certificate File"
description: "The file name of the SSL certificate file"
type: certfile
-
name: key
label: "SSL Certificate Key File"
description: "The file name of the server certificate's private key file"
type: keyfile

Two components are then created in the components section of the StyleBook, as shown below. The "my-lbvserver-comp" component is of type ns::lbvserver, where:

- "ns" is the prefix that refers to the built-in namespace netscaler.nitro.config and version 10.5 that you had specified in the import-stylebooks section.
- "lbvserver" is a built-in StyleBook in this namespace. It corresponds to the NetScaler NITRO lbvserver resource of the same name.

The second component "lbvserver-certificate-comp" is of type stlb::vserver-certs-binds. The prefix "stlb" refers to the namespace "com.citrix.adc.stylebooks" and version 1.0 that is specified in the import-stylebooks section of the StyleBook. If the "com.citrix.adc.stylebooks" namespace can be thought of as a folder, "vserver-certs-binds" is another StyleBook (or a file) in that folder. StyleBooks that are in the namespace "com.citrix.adc.stylebooks" are shipped as part of NetScaler MAS.

The "vserver-certs-binds" StyleBook used by user-defined StyleBooks allows you to easily configure the certificates by uploading the certificate and key files to the target NetScaler instance, and by configuring the binding of the certificate and key files to the appropriate virtual servers. The properties for this component are - the name of the lb virtual server and the names of the SSL certificates that you provide while creating the config pack.

components:
-
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
    name: $parameters.name
    servicetype: SSL
    ipv46: $parameters.ip
    port: 80
lbmethod: $parameters.lb-alg

- name: lbvserver-certificate-comp
type: stlb:vserver-certs-binds
description: Binds lbvserver with server certificate
properties:
  vserver-name: $components.my-lbvserver-comp.properties.name
certificates:
- cert-name: $parameters.name + "-lb-cert"
cert-file: $parameters.certificate
ssl-inform: PEM
key-name: $parameters.name + "-key"
key-file: $parameters.key

When you use the API to create a configuration from such a StyleBook, use just the file names (not the full file path). These files are expected to be already available in the certificate and key file folders on NetScaler MAS. The uploaded SSL certificate file is stored on NetScaler MAS in the /var/mps/tenants/.../ns_ssl_certs directory, and the SSL certificate key file is stored in /var/mps/tenants/.../ns_ssl_keys directory in NetScaler MAS.

The following procedure creates a basic load balancing virtual server configuration on a selected NetScaler instance using the SSL protocol from the StyleBook specified above. You can use this procedure to upload the SSL certificate files and the certificate keys files in NetScaler MAS.

**To create a configuration for uploading files**

1. In NetScaler MAS, navigate to Applications > Configuration, and click Create New. The Choose StyleBook page displays all the StyleBooks that are available in your NetScaler MAS. Scroll down and select Load Balancing Virtual Server (SSL).

   The StyleBook parameters appear as a user-interface page that allows you to enter the values for all the parameters defined in this StyleBook.

2. Enter the name of the load balancer and the virtual IP address in the basic load balancer settings section.

3. In SSL Certificates Settings section, select the respective files from your local storage folder. Alternatively, you can select the files present on the NetScaler MAS itself.

4. Select the target NetScaler instance on which the configuration needs to be created, and click Create.
Note

In NetScaler MAS, the following StyleBooks, which are shipped as part of NetScaler MAS, enable you to create SSL support by uploading the SSL certificates and keys.

- HTTP/SSL LoadBalancing StyleBook (lb)
- HTTP/SSL LoadBalancing (with Monitors) StyleBook (lb-mon)
- HTTP/SSL Content Switched Application with Monitors (cs-lb-mon)
- Sample Application StyleBook using CS, LB and SSL features (sample-cs-app)

You can also create your own StyleBooks that make use of SSL certificates in the same way as described in the above StyleBook.

Sample Configuration

The full content of the file lb-vserver-ssl.yaml is shown below:

```yaml
name: lb-vserver-ssl
```
description: "This stylebook defines a load balancing virtual server configuration."

display-name: "Load Balancing Virtual Server (SSL)"

namespace: com.example.ssl.stylebooks

schema-version: "1.0"

version: "0.1"

import-stylebooks:

-

  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"

-

  namespace: com.citrix.adc.stylebooks
  prefix: stlb
  version: "1.0"

parameters:

-

  name: name
  type: string
  required: true
- name: ip
  type: ipaddress
  required: true

- name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN

- name: certificate
  label: "SSL Certificate File"
  description: "The file name of the SSL certificate file"
  type: certfile

- name: key
  label: "SSL Certificate Key File"
  description: "The file name of the server certificate's private key file"
type: keyfile

components:

-

  name: my-lbvserver-comp
type: ns::lbvserver

properties:

  name: $parameters.name

  servicetype: SSL

  ipv46: $parameters.ip

  port: 80

  lbmethod: $parameters.lb-alg

-

  name: lbvserver-certificate-comp
type: stlb::vserver-certs-binds
description: Binds lbvserver with server certificate

properties:

  vserver-name: $components.my-lbvserver-comp.properties.name

  certificates:

  -

    cert-name: $parameters.name + "-lb-cert"
Viewing the Objects Defined on the NetScaler Instance

After the StyleBook configuration (configpack) is created on NetScaler MAS, click View objects created to display all the NetScaler objects created on the target NetScaler instance.
How to Use Microsoft Exchange StyleBook in Business Enterprises

Mar 09, 2017

You can use the Microsoft Exchange 2016 StyleBook to deploy a NetScaler configuration that optimizes and secures a Microsoft Exchange 2016 enterprise application in your network. Microsoft Exchange 2016 is a key enterprise application for providing email, personal information management, and messaging services to your employees and other stakeholders.

The Microsoft Exchange 2016 StyleBook enables and configures the following NetScaler features for Microsoft Exchange 2016 servers:

- **Load balancing** - Basic load balancing that enables load balancing of multiple Exchange servers
- **Content switching** - Content switching that enables single-IP access and redirection of queries to the correct load balancing virtual servers
- **Rewrite** - Redirects users to secure pages
- **SSL offload** - Offloads SSL processing to the NetScaler, therefore reducing the load on the Exchange server

The following figure diagrammatically represents the deployment of Exchange servers in the network:

- For certificate-based authentication, all addressable hosts that are part of the network setup must have resolvable domain names and not just IP addresses.
To Configure Microsoft Exchange Application

1. In NetScaler MAS, navigate to Applications > Configuration, and click Create New. The Choose StyleBook page displays all the StyleBooks that are available in your NetScaler MAS for your usage. Scroll down and select the Microsoft Exchange 2016 StyleBook. The StyleBook appears as a user interface form on which you can enter the values for all the parameters defined in this StyleBook.

2. Enter the details for the following parameters:

- **Exchange Application Name** - Name of the Microsoft Exchange Application in your network
- **Exchange Content-Switching VIP** - Virtual IP address on NetScaler that receives client requests for the Microsoft Exchange application
- **Exchange Server IPs** - IP addresses of all the Exchange servers in the network. You can add multiple addresses by clicking the plus (+) icon. Usually, two Exchange servers are configured in the network.

3. In the Exchange Certificates section, upload the Exchange certificates to NetScaler MAS in the Exchange Certificates section. Enter the names of both the certificate and the key files and upload them by selecting them from the local storage. You can also provide a private key password to encrypt the key file.

   **Note:** Ensure that the certificate files are of ".pem" or ".der" format. NetScaler MAS rejects files in any other format.

4. In the Exchange AD Authentication config section, configure the AD Settings by entering the data.

   - **AD Authentication VIP** - The virtual IP address used to create and configure the AD (LDAP) virtual server on a NetScaler appliance.
   - **Active Directory Server IP** - The IP address of your Active Directory domain controller.
   - **Active Directory Base String** - The LDAP Base String in Active Directory. For example, CN=Users,DC=CTXNSSFB,DC=COM.
   - **AD Login Name** - the attribute name in AD (LDAP) that designates the login name for accessing the external LDAP server. For example, "sAMAccountName."
   - **AD group Attribute/Sub-Attribute Name** - the LDAP group attribute and subattribute names configured on the LDAP server. For example, "memberOf" for the group attribute in LDAP and "cn" for the subattribute.
   - **AD Authentication Domain** - The AD/LDAP domain name. For example, ctxnssfb.com.

5. In the Target Instances section, select the NetScaler instance on which to deploy this Exchange configuration. Click Create to create the configuration file and execute the configuration on the selected NetScaler instance.

   **Note:** Citrix recommends that you first select Dry Run to check the configuration objects that are created on the target instance before executing the actual configuration on the instance.

When the configuration has been created successfully, you can find that the StyleBook has created a content switching virtual server, five load balancing virtual servers, and one LDAP policy bound to one LDAP authentication virtual server. You can also find the corresponding service groups created and bound to the load balancing virtual servers.

   **Note:** After creation of the configuration pack from the StyleBook, you must manually add the LDAP Bind domain name.
and the password. Log on to the NetScaler instance GUI, and navigate to **Traffic Management > Content Switching > Virtual Servers**. Select the Exchange content switching virtual server created by the StyleBook and click **Edit**. In the Authentication section, click the edit icon, and edit the Exchange authentication virtual server. Select the LDAP policy, click **Edit**, and in **Connection Settings**, enter the LDAP administrator Bind DN values configured on the LDAP server, and provide the administrator password.

You can also do this from the NetScaler CLI as shown in the following example:

```plaintext
set authentication ldapAction exch-ad-auth-action -ldapBindDn "CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword "usepass3"
```

Add a DNS record in NetScaler for your authentication domain after the creation of the StyleBook configuration, for example, by using the following CLI:

```plaintext
add dns addRec auth1.ctxnssfb.com 10.105.157.59
```
How to Use Microsoft Skype for Business StyleBook in Business Enterprises

Mar 09, 2017

The Skype for Business 2015 application relies on several external components to function. The Skype for Business network consists of various systems, such as servers and their operating systems, databases, authentication and authorizing systems, networking systems and infrastructure, and telephone PBX systems. Skype for Business Server 2015 is available in two versions, Standard Edition and Enterprise Edition. The primary difference is in support for high-availability features that are only included in the Enterprise Edition. To implement high availability, multiple Front-End servers must be deployed to a pool and SQL servers must be mirrored.

An Enterprise Edition deployment enables the creation of multiple servers with different roles.

The primary components in Skype for Business 2015 application are:

- Front-End servers
- Edge servers
- Director servers
- Database (SQL) servers

The following figure diagrammatically represents the deployment of Skype servers in the network:

This document includes the following information:

- Configuring Front-End Servers in an Enterprise Using Skype for Business StyleBook
- Configuring Edge Servers in an Enterprise Using Skype for Business StyleBook
- Configuring Director Servers in an Enterprise Using Skype for Business StyleBook

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved. p.275
The Skype for Business Front-End server is the core server in your network. It provides the links and services for user authentication, registration, presence, address book, A/V conferencing, application sharing, instant messaging, and web conferencing. If you are deploying Skype for Business 2015 Enterprise edition, the topology typically consists of at least two Front-End servers load balanced in a Front-End pool with a database server that hosts the SQL Server instance holding the Skype for Business database.

The following table lists the IP addresses used in the sample configuration included in the instructions below:

<table>
<thead>
<tr>
<th>Skype for Business Servers</th>
<th>Virtual IP Address</th>
<th>Server IP Addresses</th>
<th>NetScaler Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front-End Servers</td>
<td>10.10.10.10</td>
<td>10.10.10.11</td>
<td>10.102.29.60</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.10.10.12</td>
<td></td>
</tr>
</tbody>
</table>

To Configure Front-End Servers

1. In NetScaler MAS, navigate to Applications > Configuration, and click Create New. The Choose StyleBook page displays all the StyleBooks available for your use in NetScaler MAS. Scroll down and select the Microsoft Skype for Business 2015 StyleBook (Front-End Server). The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.
2. Enter the IP address for the virtual Front-End server (VIP) that is to be created for the Skype for Business Front-End servers. Also enter the IP addresses of all the Skype for Business Front-End servers in the network.

The List of Ports section lists the default port numbers and protocols used by servers, load balancers, and clients in a Skype for Business Front-End server deployment. Each port listed here must be open on each Front-End server role. You can retain the default port numbers or edit them. However, make sure that these ports are reachable on the Front-End servers.

The following table lists the 14 default ports and protocols on the Front-End server:

<table>
<thead>
<tr>
<th>Label</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Port</td>
<td>80</td>
<td>HTTP</td>
<td>Used for communication from Front-End Servers to the web farm FQDNs when HTTPS is not used.</td>
</tr>
<tr>
<td>HTTPS Port</td>
<td>443</td>
<td>HTTPS</td>
<td>Used for communication from Front-End Servers to the web farm FQDNs.</td>
</tr>
<tr>
<td>AutoDiscover Internal Port</td>
<td>4443</td>
<td>HTTPS</td>
<td>HTTPS (from Reverse Proxy) and HTTPS Front-End inter-pool communications for AutoDiscover sign-in.</td>
</tr>
<tr>
<td>RPC Port</td>
<td>135</td>
<td>DCOM and remote procedure call</td>
<td>Used for DCOM based operations such as moving users, user replicator synchronization, and address book synchronization.</td>
</tr>
<tr>
<td></td>
<td>(RPC)</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>SIP Port</td>
<td>5061</td>
<td>TCP (TLS) Used by Front-End servers for all internal SIP communications.</td>
<td></td>
</tr>
<tr>
<td>SIP Focus Port</td>
<td>444</td>
<td>HTTPS, TCP Used for HTTPS communication between the Focus (the component that manages the Skype conference state) and the individual servers.</td>
<td></td>
</tr>
<tr>
<td>SIP Group Port</td>
<td>5071</td>
<td>TCP Used for incoming SIP requests for the response group application.</td>
<td></td>
</tr>
<tr>
<td>SIP AppSharing Port</td>
<td>5065</td>
<td>TCP Used for incoming SIP listening requests for application sharing.</td>
<td></td>
</tr>
<tr>
<td>SIP Attendant Port</td>
<td>5072</td>
<td>TCP Used for incoming SIP requests for the attendant (that is, for dial-in conferencing).</td>
<td></td>
</tr>
<tr>
<td>SIP Conf Announcement Port</td>
<td>5073</td>
<td>TCP Used for incoming SIP requests for the Skype for Business server conferencing announcement service (that is, for dial-in conferencing).</td>
<td></td>
</tr>
<tr>
<td>SIP CallPark Port</td>
<td>5075</td>
<td>TCP Used for incoming SIP requests for the CallPark application.</td>
<td></td>
</tr>
<tr>
<td>SIP Call Admission Port</td>
<td>448</td>
<td>TCP Used for call admission control by the Skype for Business server bandwidth policy service.</td>
<td></td>
</tr>
<tr>
<td>SIP Call Admission TURN Port</td>
<td>5080</td>
<td>TCP Used for call admission control by the bandwidth policy service for Audio/Video Edge TURN traffic.</td>
<td></td>
</tr>
<tr>
<td>SIP Audio Test Port</td>
<td>5076</td>
<td>TCP Used for incoming SIP requests for the audio test service.</td>
<td></td>
</tr>
</tbody>
</table>

3. Click **Target Instances** and select the NetScaler instance on which to deploy the Skype for Business configuration for Front-End servers.

4. Click **Create** to create the configuration on the selected NetScaler instance.

**Note:** Citrix recommends that you select **Dry Run** to check the configuration objects that will be created on the target instance before you execute the actual configuration on the instance.

When the configuration is successfully created, the StyleBook creates 14 load balancing virtual servers. That is, for each port, one load balancing virtual server is defined along with one service group, and the service group is bound to the load balancing virtual server. The configuration also adds the Front-End servers as service group members and binds them to the service group. The number of service group members created is equal to the number of Front-End servers created.
The following figure shows the objects created for one port:

<table>
<thead>
<tr>
<th>Objects Added on Instance: 10.102.29.60</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong>: lbvserver</td>
</tr>
<tr>
<td><strong>appflowlog</strong>: ENABLED</td>
</tr>
<tr>
<td><strong>downstateflush</strong>: ENABLED</td>
</tr>
<tr>
<td><strong>ipv46</strong>: 10.10.10.10</td>
</tr>
<tr>
<td><strong>lbmethod</strong>: LEASTCONNECTION</td>
</tr>
<tr>
<td><strong>name</strong>: sfb-fe-http-lb</td>
</tr>
<tr>
<td><strong>persistencetype</strong>: SOURCEIP</td>
</tr>
<tr>
<td><strong>port</strong>: 80</td>
</tr>
<tr>
<td><strong>servicetype</strong>: TCP</td>
</tr>
</tbody>
</table>

| **Type**: servicegroup                   |
| **servicegroupname**: sfb-fe-http-svgrp  |
| **servicetype**: TCP                     |

| **Type**: lbvserver_servicegroup_binding |
| **name**: sfb-fe-http-lb                 |
| **servicegroupname**: sfb-fe-http-svgrp  |

| **Type**: servicegroup_servicegroupmember_binding |
| **ip**: 10.10.10.11                           |
| **port**: 8080                                |
| **servicegroupname**: sfb-fe-http-svgrp       |

| **Type**: servicegroup_servicegroupmember_binding |
| **ip**: 10.10.10.12                           |
Deploying Edge servers for Skype for Business is necessary if external users who are not logged into your organization's internal network need to be able to interact with internal users. These external users could be authenticated and anonymous remote users, federated partners, or other mobile clients.

There are four types of roles in Skype For Business Edge server:

- **Access Edge**, which handles SIP Traffic and authenticates external connections, allows remote connection, and allows federation connection
- **Web Conferencing**, which handles Data Conferencing Packets, and allows external users to access Skype for Business
- **A/V Conferencing**, which handles A/V Conferencing Packets, and extends audio and video, app sharing and file transfer to external users
- **XMPP Proxy**, which handles XMPP packets, and allows XMPP based servers or clients to connect to Skype for Business.

The following table lists the IP addresses used in the sample configuration included in the instructions below:

<table>
<thead>
<tr>
<th>Skype for Business Servers</th>
<th>Virtual IP Address</th>
<th>Server IP Addresses</th>
<th>NetScaler Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Servers</td>
<td>External VIP - 192.20.20.20</td>
<td>192.20.20.21, 192.20.20.22</td>
<td>10.106.76.199</td>
</tr>
<tr>
<td></td>
<td>Internal VIP - 10.10.10.20</td>
<td>10.10.10.21, 10.10.10.22</td>
<td></td>
</tr>
</tbody>
</table>

**To Configure Edge Servers**

1. In NetScaler MAS, navigate to **Applications > Configuration**, and click **Create New**. The **Choose StyleBook** page displays all the StyleBooks that are available in your NetScaler MAS for your usage. Scroll down and select the **Microsoft Skype for Business 2015 StyleBook (Edge Server)** for Edge servers.
2. Enter the following virtual IP (VIP) addresses and IP addresses of all the Edge servers in the network.
   - External VIP address and IP addresses for the Edge servers that will be used for access Edge, web conferencing Edge and A/V Edge.
   - Internal VIP address and IP addresses for the Edge servers that will be connected with the internal network.
3. Create at least two external and two internal Edge servers in your network.

   **The List of Ports** section provides a list of default port numbers and protocols in a Skype for Business Edge server deployment.

   The following table lists the 7 default ports - four external ports and three internal ports, and protocols on the Edge server:
<table>
<thead>
<tr>
<th>Label</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS External Port</td>
<td>443</td>
<td>HTTPS</td>
<td>Used for external ports for SIP/ TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.</td>
</tr>
<tr>
<td>HTTPS Internal Port</td>
<td>443</td>
<td>HTTPS</td>
<td>Used for internal ports for SIP/ TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.</td>
</tr>
<tr>
<td>SIP External Remote Access Port</td>
<td>5061</td>
<td>TCP</td>
<td>Used for external ports for SIP/MTLS communication for remote user access or federation.</td>
</tr>
<tr>
<td>SIP Internal Remote Access Port</td>
<td>5061</td>
<td>TCP</td>
<td>Used for internal ports for SIP/MTLS communication for remote user access or federation.</td>
</tr>
<tr>
<td>SIP External STUN UDP Port</td>
<td>3478</td>
<td>UDP</td>
<td>Used for external ports for STUN/UDP inbound and outbound media communications.</td>
</tr>
<tr>
<td>SIP Internal STUN UDP Port</td>
<td>3478</td>
<td>UDP</td>
<td>Used for internal ports for STUN/UDP inbound and outbound media communications.</td>
</tr>
<tr>
<td>SIP Internal IM Port</td>
<td>5062</td>
<td></td>
<td>Used for internal ports for SIP/MTLS authentication of IM communications flowing outbound through the internal firewall.</td>
</tr>
</tbody>
</table>

4. Click **Target Instances** to select the NetScaler instance on which to deploy the Skype for Business configuration for Edge servers.

5. Click **Create** to create the configuration on the selected NetScaler instance.

**Note**: Citrix recommends that you select **Dry Run** to check the configuration objects that will be created on the target instance before you execute the actual configuration on the instance.

When the configuration is successfully created, the StyleBook creates seven load balancing virtual servers, that is, for each port one load balancing virtual server is defined along with one service group and the service group is bound to the load balancing virtual server. The configuration also adds the Edge servers (either internal or external) as service group members and binds them to the service group. Note that the names of the load balancing virtual servers and the other objects created depends on whether they are created on external or internal ports.

For example, the following load balancing virtual server is created on an external port:

**Type**: lbvserver

**ipv46**: 192.20.20.20
name: sfb-edge-externalsip-lb

While, the following load balancing virtual server is created on an internal port:

**Type:** lbvserver  
**ipv46:** 10.20.20.23

**name:** sfb-edge-internalsip-lb

The following image displays the objects created for one external port and one internal port:

<table>
<thead>
<tr>
<th>Objects Added on Instance: 10.106.76.199</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type:</strong> lbvserver</td>
</tr>
<tr>
<td><strong>ipv46:</strong> 192.20.20.20</td>
</tr>
<tr>
<td><strong>name:</strong> sfb-edge-externalsip-lb</td>
</tr>
<tr>
<td><strong>port:</strong> 443</td>
</tr>
<tr>
<td><strong>servicetype:</strong> TCP</td>
</tr>
</tbody>
</table>

| **Type:** servicegroup                     |
| **servicename:** sfb-edge-externalsip-svcgrp |
| **servicetype:** TCP                       |

| **Type:** lbvserver_servicegroup_binding   |
| **name:** sfb-edge-externalsip-lb          |
| **servicename:** sfb-edge-externalsip-svcgrp |

| **Type:** servicegroup_servicegroupmember_binding |
| **ip:** 192.20.20.21                           |
| **port:** 443                                 |
| **servicename:** sfb-edge-externalsip-svcgrp |
Type : servicegroup_servicegrouppmember_binding

<table>
<thead>
<tr>
<th>field</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>192.20.20.22</td>
</tr>
<tr>
<td>port</td>
<td>443</td>
</tr>
<tr>
<td>servicegroupname</td>
<td>sfb-edge-externalsip-svgrp</td>
</tr>
</tbody>
</table>

Type : lbvserver

<table>
<thead>
<tr>
<th>field</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>appflowlog</td>
<td>ENABLED</td>
</tr>
<tr>
<td>downstateflush</td>
<td>ENABLED</td>
</tr>
<tr>
<td>ipv4</td>
<td>10.10.10.20</td>
</tr>
<tr>
<td>lbmethod</td>
<td>LEASTCONNECTION</td>
</tr>
<tr>
<td>name</td>
<td>sfb-edge-internalsip-lb</td>
</tr>
<tr>
<td>persistencetype</td>
<td>SOURCEIP</td>
</tr>
<tr>
<td>port</td>
<td>443</td>
</tr>
<tr>
<td>servicetype</td>
<td>TCP</td>
</tr>
</tbody>
</table>

Type : servicegroup

<table>
<thead>
<tr>
<th>field</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>servicegroupname</td>
<td>sfb-edge-internalsip-svgrp</td>
</tr>
<tr>
<td>servicetype</td>
<td>TCP</td>
</tr>
</tbody>
</table>

Type : lbvserver_servicegroup_binding

<table>
<thead>
<tr>
<th>field</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>sfb-edge-internalsip-lb</td>
</tr>
<tr>
<td>servicegroupname</td>
<td>sfb-edge-internalsip-svgrp</td>
</tr>
</tbody>
</table>

Type : servicegroup_servicegrouppmember_binding

<table>
<thead>
<tr>
<th>field</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>10.10.10.21</td>
</tr>
<tr>
<td>port</td>
<td>443</td>
</tr>
<tr>
<td>servicegroupname</td>
<td>sfb-edge-internalsip-svgrp</td>
</tr>
</tbody>
</table>

Type : servicegroup_servicegrouppmember_binding

<table>
<thead>
<tr>
<th>field</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>10.10.10.22</td>
</tr>
<tr>
<td>port</td>
<td>443</td>
</tr>
</tbody>
</table>
The main function of the Director server in Skype for Business 2015 is to authenticate endpoints and "direct" the users to the pool that contains their account. In Skype for Business 2015, the Director is a completely dedicated and specific role on a standalone server. This facilitates security by making it easier to deploy or remove the configurations.

Directors are most useful where multiple pools exist, because they provide a single point of contact for authenticating endpoints. Also, for remote users, a Director serves as an extra hop between the Edge pool and Front-End pool, adding an extra layer of protection against attacks.

The following table lists the IP addresses used in the sample configuration included in the instructions below:

<table>
<thead>
<tr>
<th>Skype for Business Servers</th>
<th>Virtual IP Address</th>
<th>Server IP Addresses</th>
<th>NetScaler Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Director Server</td>
<td>10.10.10.30</td>
<td>10.10.10.31</td>
<td>10.102.58.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.10.10.32</td>
<td></td>
</tr>
</tbody>
</table>

To Configure Director Servers

1. In NetScaler MAS, navigate to Applications > Configuration, and click Create New. The Choose StyleBook page displays all the StyleBooks that are available in your NetScaler MAS for your usage. Scroll down and select the Microsoft Skype for Business 2015 StyleBook (Director) for Director servers.

2. Enter the virtual IP address (VIP) for the Director servers that is to be created for the Skype for Business application. Enter the IP addresses for all the Skype for Business Director servers in the network. Create at least two Director servers for high-availability.

The List of Ports section provides a list of default port numbers and protocols in a Skype for Business Director server deployment.

The following table lists the 4 default ports and protocols on the Director server:

<table>
<thead>
<tr>
<th>Label</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Port</td>
<td>80</td>
<td>TCP</td>
<td>Used for initial communication from Directors to the web farm FQDNs.</td>
</tr>
<tr>
<td>HTTPS Port</td>
<td>443</td>
<td>HTTPS</td>
<td>Used for communication from Directors to the web farm FQDNs.</td>
</tr>
<tr>
<td>AutoDiscover</td>
<td>4443</td>
<td>HTTPS</td>
<td>Used for HTTPS (from Reverse Proxy) and HTTPS Director inter-</td>
</tr>
</tbody>
</table>
3. Click **Target Instances** to select the NetScaler instance on which to deploy the Skype for Business configuration for Director servers.

4. Click **Create** to create the configuration on the selected NetScaler instance.

**Note**: Citrix recommends that you select **Dry Run** to check the configuration objects that will be created on the target instance before you execute the actual configuration on the instance.

When the configuration is successfully created, the StyleBook creates four load balancing virtual servers, that is, for each port one load balancing virtual server is defined along with one service group and the service group is bound to the load balancing virtual server. The configuration also adds the Director servers as service group members and binds them to the service group. The number of service group members created is equal to the number of Director servers created.

The following image displays the objects created for one port on a Director server:

**Objects**

**Objects Added on Instance : 10.102.58.78**

**Type : lbvserver**
- `applflowlog` : ENABLED
- `downstateflush` : ENABLED
- `ipv46` : 10.10.10.30
- `lbmethod` : LEASTCONNECTION
- `name` : sfb-dir-http-lb
- `persistencetype` : SOURCEIP
- `port` : 80
- `servicetype` : TCP

**Type : servicegroup**
- `servicegroupname` : sfb-dir-http-svgrp
- `servicetype` : TCP
### Type: lbvserver_servicegroup_binding

<table>
<thead>
<tr>
<th>name</th>
<th>sfb-dir-http-lb</th>
</tr>
</thead>
<tbody>
<tr>
<td>servicegroupname</td>
<td>sfb-dir-http-svgrp</td>
</tr>
</tbody>
</table>

### Type: servicegroup_servicegroupmember_binding

<table>
<thead>
<tr>
<th>ip</th>
<th>10.10.10.31</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>8080</td>
</tr>
<tr>
<td>servicegroupname</td>
<td>sfb-dir-http-svgrp</td>
</tr>
</tbody>
</table>

### Type: servicegroup_servicegroupmember_binding

<table>
<thead>
<tr>
<th>ip</th>
<th>10.10.10.32</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>8080</td>
</tr>
<tr>
<td>servicegroupname</td>
<td>sfb-dir-http-svgrp</td>
</tr>
</tbody>
</table>
You can design your own StyleBooks, import them to NetScaler MAS, and then use them to create configurations either by using NetScaler MAS GUI or by using APIs. To be able to create your own StyleBooks, you must first understand the grammar and syntax of the different constructs and attributes you can use.

This document describes the different constructs and references you can use while creating StyleBooks.

Click a section, construct, or reference name in the table below to view the details.

<table>
<thead>
<tr>
<th>Table Name</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header</td>
<td>Import StyleBooks</td>
</tr>
<tr>
<td>Parameters</td>
<td>Parameters-Default-Sources Construct</td>
</tr>
<tr>
<td>Substitutions</td>
<td>Components</td>
</tr>
<tr>
<td>Optional Properties</td>
<td>Nested Components</td>
</tr>
<tr>
<td>Condition Construct</td>
<td>Repeat Construct</td>
</tr>
<tr>
<td>Repeat-Condition Construct</td>
<td>Outputs</td>
</tr>
<tr>
<td>Parameter Reference</td>
<td>Parent Reference</td>
</tr>
<tr>
<td>Components Reference</td>
<td>Substitutions Reference</td>
</tr>
<tr>
<td>Variable Reference</td>
<td>Operations</td>
</tr>
<tr>
<td>Analytics</td>
<td>Alarms</td>
</tr>
<tr>
<td>Expressions</td>
<td>Built-in Functions</td>
</tr>
</tbody>
</table>

For information and examples about how to design your own StyleBooks, see How to Create Your Own StyleBooks.
Header

Oct 21, 2016

The first six lines of a StyleBook comprise the header section. This section lets you define the identity of a StyleBook and describe what it does. This is a mandatory section.

The following table describes the attributes of the header section:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>A name to identify the StyleBook. This attribute is mandatory.</td>
</tr>
<tr>
<td>description</td>
<td>A description defining what a StyleBook does. This description appears on the NetScaler MAS GUI. This is an optional attribute.</td>
</tr>
<tr>
<td>display-name</td>
<td>A descriptive name for the StyleBook. This name appears on the NetScaler MAS GUI. This is an optional attribute.</td>
</tr>
<tr>
<td>author</td>
<td>The author person or organization who creates the StyleBook. This is an optional attribute.</td>
</tr>
</tbody>
</table>
| namespace      | A namespace forms part of a unique identifier for a StyleBook to avoid name collisions. A namespace can be any string, but a good practice is to use it for naming the company, department, or unit that created or owns a set of StyleBooks. For example, you can use the following format: `<company>.<department>.<unit>.stylebooks`
|                | This is a mandatory attribute.                                                                                                               |
| version        | The version number of the StyleBook. You can change the version number when you update a StyleBook. StyleBooks of different versions can co-exist together. This is a mandatory attribute. |
| schema-version | The version of the StyleBooks schema. It takes the value "1.0" in the current release of NetScaler MAS. This is a mandatory attribute.            |
| private        | If this attribute is set to true, the StyleBook is not displayed on the NetScaler MAS GUI. This is a useful setting for StyleBooks that are building blocks for other StyleBooks and are not intended to be used by users directly. This is an optional attribute. Its default value is false. |

Example:

name: lb

description: "This stylebook defines a sample load balancing configuration."

display-name: "Load Balancing StyleBook (HTTP)"

author: Mike Smith (ACME Infra team)

namespace: com.example.stylebooks
The combination of name, namespace, and version uniquely identifies a StyleBook in the system. You cannot have two StyleBooks with the same combination of name, namespace, and version in NetScaler MAS. However, you can have two StyleBooks with the same name and version but different namespaces, or with the same namespace and version but different names.
Import StyleBooks

Oct 21, 2016
This is the second section of your StyleBook and lets you declare which other StyleBook you want to refer to from your current StyleBook. This enables you to import and reuse other StyleBooks instead of rebuilding the same configuration in your own StyleBook. This is a mandatory section.

You must declare the namespace and version number of the StyleBook(s) that you want to refer to in your current StyleBook. Every StyleBook must refer to the netscaler.nitro.config namespace if it uses any of the NITRO configuration objects directly. This namespace contains all the NetScaler NITRO types, such as lbvserver service or monitor. StyleBooks for NetScaler versions 10.5, 11.0, and 11.1 are supported, which means that you can use your StyleBook to create and run configurations on any NetScaler instance running release 10.5 or later.

The prefix attribute used in the import-stylebooks section is a shorthand to refer to the combination of namespace and version. For example, the “ns” prefix can be used to refer to the namespace netscaler.nitro.config with version 10.5. In the later sections of your StyleBook, instead of using the namespace and version each time you want to refer to a StyleBook with this namespace and version, you can simply use the prefix string chosen together with the name of the StyleBook to uniquely identify it.

Example:

```plaintext
import-stylebooks:

- namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns

- namespace: com.acme.stylebooks
  version: "0.1"
  prefix: stlb
```

In the above example, the first prefix defined is called ns and refers to the namespace netscaler.nitro.config and version 10.5. The second prefix that is defined is called stlb, and refers to the namespace comacme.stylebooks and version 0.1.

After you define a prefix, every time you want to refer to a type or a StyleBook that belongs to a certain namespace and version, you can use the notation `<namespace-shorthand>::<type-name>`. For example, ns::lbvserver refers to the type lbvserver that is defined in the namespace netscaler.nitro.config, version 10.5.

Similarly, if you want to refer to a StyleBook with version "0.1" in the comacme.stylebooks namespace, you can use the notation stlb::<stylebook-name>.
Note

By convention, the prefix "ns" is used to refer to the NITRO namespace of NetScaler.
Parameters

Oct 18, 2016

This section lets you define all the parameters that you require in your StyleBook to create a configuration. It describes the input that your StyleBook takes. Although this is an optional section, but most StyleBooks might need one. You can consider the parameters section to define the questions you want users to answer when they use the StyleBook to create a configuration on a NetScaler instance.

When you import your StyleBook into NetScaler MAS and use it to create a configuration, the GUI uses this section of the StyleBook to display a form that takes input for values of the parameters you have defined.

The following table describes the attributes that you need to specify for each parameter in this section:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the parameter you want to define. You can specify an alphanumeric name. The name must begin with an alphabet, and can include additional alphabets, numbers, hyphen (-), or underscore (_). Note that when writing a StyleBook, you can use this &quot;name&quot; attribute to refer to the parameter in other sections by using the notation $parameters.&lt;name&gt;$.</td>
<td>Yes</td>
</tr>
<tr>
<td>label</td>
<td>A string that is displayed in the NetScaler MAS GUI as the name of this parameter.</td>
<td>No</td>
</tr>
<tr>
<td>description</td>
<td>A help string that describes what the parameter is used for. The NetScaler MAS GUI displays this text when the user clicks the help icon for this parameter.</td>
<td>No</td>
</tr>
</tbody>
</table>

The type of value these parameters can take. Parameters can be of any of the following built-in types:

- **string**: An array of characters. If a length is not specified, the string value can take any number of characters. However, you can limit the length of a string type by using the attributes min-length and max-length.

- **number**: An integer number. You can specify the minimum and maximum number that this type can take by using the attributes min-value and max-value.

- **boolean**: Can be either true or false. Also, note that all the literals are considered by YAML as booleans (for example, Yes or No).

- **ipaddress**: A string that represents a valid IPv4 or IPv6 address.

- **tcp-port**: A number between 0 and 65535 that represents a TCP or UDP port.

- **password**: Represents an opaque/secret string value. When NetScaler MAS GUI displays a value for this parameter, it is shown as asterisks (****).
**type**

- **certfile**: Represents a certificate file. This allows you to upload the files directly from your local system when you are creating a StyleBook configuration using the NetScaler MAS GUI. The uploaded certificate file is stored in the directory `/var/mps/tenants/<tenant_path>/ns_ssl_certs` in NetScaler MAS. The certificate file will be added to the list of certificates managed by NetScaler MAS.

- **keyfile**: Represents a certificate key file. This allows you to upload the file directly from your local system when you are creating a StyleBook configuration using the NetScaler MAS GUI. The uploaded certificate file is stored in the directory `/var/mps/tenants/<tenant_path>/ns_ssl_keys` in NetScaler MAS. The certificate key file will be added to the list of certificate keys managed by NetScaler MAS.

- **file**: Represents a file.

- **object**: This type is used when you want to group several related parameters under a parent element. You have to specify the parent parameter the type as “object”. A parameter of type “object” can have a nested “parameters” section to describe the parameters it contains.

- **Another StyleBook**: When you use this type of parameter, then this parameter expects its value to be in the form of the parameters defined in the StyleBook denoting its type.

A parameter can also have a type that is a list of any of the types listed above, by adding “[]” to the end of the type. For example, if the **type** attribute is **string[]**, this parameter takes a list of strings as input. You can provide one, two, or several strings for this parameter when creating a configuration from this StyleBook.

| key | Specify true or false to indicate if this parameter is a key parameter for the StyleBook. A StyleBook can have only one parameter defined as the “key” parameter. When you create different configurations from the same StyleBook (on the same or different NetScaler instances), each configuration has a different/unique value for this parameter. Default value is false. |
| required | Specify true or false to indicate whether a parameter is mandatory or optional. If it is set to true, the parameter is mandatory and the user has to provide a value for this parameter when creating configurations. The NetScaler MAS GUI forces the user to provide a valid value for this parameter. Default value is false. |
| Use this attribute to define a list of valid values for a parameter, when the type is set to “string.” When creating a configuration from the NetScaler MAS GUI, the user is |
| **allowed-values** | prompted to select a parameter value from this list.  
  **Example:**  
  ```yaml  
  name: color  
  type: string  
  allowed-values:  
  - Blue  
  - Green  
  - Yellow  
  ``` |
|-------------------|---------------------------------------------------------------------------------------------------------------|
| **default**       | Use this attribute to assign a default value to an optional parameter. While creating a configuration, if a user does not specify a value, the default value is used.  
  When creating the configuration from the NetScaler MAS GUI, if a user does not provide a value for a parameter that does not have a default value, then no value is set for that parameter.  
  **Example 1:**  
  ```yaml  
  name: timeout  
  type: number  
  default: 20  
  ```  
  **Example 2** (where, the default value of the parameter is a list of values):  
  ```yaml  
  name: protocols  
  type: string[]  
  default:  
  - TCP  
  - UDP  
  - IP  
  ``` |
| **pattern**       | Use this attribute to define a pattern (regular expression) for the valid values of this parameter, when the type of the parameter is "string."  
  **Example:**  
  ```yaml  
  name: appname  
  type: string  
  pattern: 
  ```
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| **min-value** | Use this attribute to define the minimum value for parameters of type "number" or "tcp-port." | **Example:**
  - name: audio-port
  - type: tcp-port
  - min-value: 5000 |
| **max-value** | Use this attribute to define the maximum value for parameters of type "number" or "tcp-port." | **Example:**
  - name: audio-port
  - type: tcp-port
  - min-value: 5000
  - max-value: 15000 |
| **min-length** | Use this attribute to define the minimum length of values accepted for a parameter of type "string." | **Example:**
  - name: appname
  - type: string
  - min-length: 3 |
| **max-length** | Use this attribute to define the maximum length of values accepted for a parameter of type "string." | **Example:**
  - name: appname
  - type: string
  - max-length: 64 |
<p>| <strong>No</strong> | Use this attribute to define the minimum number of items in a parameter that is a list. | <strong>Example:</strong> |</p>
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| min-items  | name: server-ips  
  type: ipaddress[]  
  min-items: 2 | No                                                                       |
| max-items  | Use this attribute to define the maximum number of items in a parameter that is a list.  
  Example:  
  name: server-ips  
  type: ipaddress[]  
  min-items: 2  
  max-items: 250 | No                                                                       |
| gui        | Use this attribute to customize the layout of the parameter of type “object” in the NetScaler MAS GUI. | No                                                                       |
| columns    | This is a sub-attribute of the gui attribute. Use this to define the number of columns to display in the NetScaler MAS GUI. | No                                                                       |
| updatable  | This is a sub-attribute of the gui attribute. Use this to specify whether the parameter can be updated after the configuration is created. If the value is set to false, the parameter field is greyed out when you update the configuration. | No                                                                       |
| collapsePane | This is a sub-attribute of the gui attribute. Use this to specify whether the pane defining the layout of this object parameter is collapsible. If the value is set to true, the user can expand or collapse the child parameters under this parent parameter.  
  Example:  
  gui:  
    collapsePane: true  
    columns: 2  
    updatable: false | No                                                                       |

Example of a complete parameters section:

```json
parameters:
  - name: name
```

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved. p.295
<table>
<thead>
<tr>
<th>label</th>
<th>Description</th>
<th>Type</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the application</td>
<td>string</td>
<td>true</td>
</tr>
<tr>
<td>ip</td>
<td>IP Address</td>
<td>ipaddress</td>
<td>true</td>
</tr>
<tr>
<td>svc-servers</td>
<td>Servers</td>
<td>object[]</td>
<td>true</td>
</tr>
<tr>
<td>svc-ip</td>
<td>Server IP</td>
<td>ipaddress</td>
<td>true</td>
</tr>
<tr>
<td>svc-port</td>
<td>TCP port of the server</td>
<td>tcp-port</td>
<td>80</td>
</tr>
</tbody>
</table>
- name: lb-alg
  label: LoadBalancing Algorithm
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN

- name: enable-healthcheck
  label: Enable HealthCheck?
  type: boolean
  default: true
Parameters-Default-Sources Construct

Feb 03, 2017
You can use this construct to reuse parameter definitions from other StyleBooks.

Consider a scenario where a parameter or a group of parameters is used repeatedly in multiple StyleBooks. To avoid redefining these parameters, each time you want to create a new StyleBook, you can define them once, and then import their definitions into the StyleBooks that need these parameters by using the parameters-default-sources construct.

For example, if many of your StyleBooks need to configure a virtual IP, you might have to define the same parameters related to virtual IPs in each new StyleBook you create. Instead, you can create a separate StyleBook called, for example, "vip-params" where you define all the parameters related to it as shown in the following example:

```
- name: vip-params
  namespace: com.acme.commontypes
  version: "1.0"
  description: This StyleBook defines a typical virtual IP config.
  private: true
  schema-version: "1.0"
  parameters:
  -
    name: lb-appname
    label: Load Balanced Application Name
    description: Name of the Load Balanced application
    type: string
    required: true
  -
    name: lb-virtual-ip
    label: Load Balanced App Virtual IP address
    description: Virtual IP address representing the Load Balanced application
    type: ipaddress
    required: true
```
Then, you can create other StyleBooks that make use of these parameters. Following is an example of such a StyleBook.

```json
- name: acme-biz-app
  namespace: com.acme.stylebooks
  version: "1.0"
  description: This stylebook defines the NetScaler configuration for Biz App
  schema-version: "1.0"
  import-stylebooks:
    - namespace: com.acme.commontypes
      prefix: cmtypes
```
In the StyleBook, acme-biz-app, first, the namespace and version of the vip-params StyleBook is imported by using the "import-stylebooks" section. Then the parameters-default-sources construct is added, and the StyleBook name, that is, vip-params is specified. This has the same effect as defining the parameters of the vip-params StyleBook directly in this StyleBook.

You can include parameters from multiple StyleBooks because the parameters-default-sources is a list, and each item in the list is expected to be a StyleBook.

In addition to including parameters from other StyleBooks, you can also define your own parameters by using the...
parameters section. The complete list of parameters of the StyleBook is the combination of parameters included from other StyleBooks and parameters defined in this StyleBook. Therefore, the expression $parameters refers to this combination of parameters.

Note that if a parameter is defined both in an imported StyleBook as well as in the current StyleBook, the definition in the current StyleBook overrides the definition imported from another StyleBook. You can use this effectively by customizing a few of the imported parameters if required, while using the rest of the imported parameters as they are.

The parameters-default-sources construct can also be used in nested parameters as shown:

```yaml
parameters:
  -
    name: vip-details
    label: Virtual IP details
    description: Details of the Virtual IP
    type: object
    required: true
    parameters-default-sources:
      - cmtypes::vip-params
```

This is similar to having the parameters of the StyleBook vip-params added directly as child parameters of the vip-details parameter in this StyleBook.
Substitutions

Jan 20, 2017

The substitutions section is used to define shorthand names for complex expressions that can be used in the rest of the StyleBook to make reading the StyleBook easier. They are also useful when the same expression or value is repeated more than once in the StyleBook, for example, a constant value. Using a substitution name for this value allows you to update only the substitution value when this value needs to be changed rather than updating it at every location it appears in the StyleBook, which could be prone to error.

Substitutions are also used for defining mappings between values as described in examples later in this document.

Each substitution in the list is made up of a key and a value. The value can be a simple value, an expression, a function, or a map.

In the following example, two substitutions are defined. The first one is “http-port” that can be used as a shorthand for 8181. By using a substitution, you can refer to this in the rest of the StyleBook as $substitutions.http-port instead of 8181.

substitutions:

  http-port: 8181

This allows you to specify a mnemonic name to a port number as well as define this port number in one place in the StyleBook, irrespective of the number of times it is used. If you want to modify the port number to 8080, you can modify it in the substitution section, and the change will take effect wherever the mnemonic name http-port is used. The following example shows how a substitution is used in a component.

components:

- name: my-lbvserver-comp
type: ns::lbvserver
properties:
  name: $parameters.name + "-lb"
servicetype: HTTP
ipv46: $parameters.ip
  port: $substitutions.http-port
  lbmethod: $parameters.lb-alg

A substitution can also be a complex expression. The following example shows how two substitutions use expressions.

substitutions:
A substitution expression can also use existing substitution expressions as shown in the following example.

**substitutions:**

```plaintext
http-port: 8181
app-name: str("acme-") + $parameters.name + str($substitutions.http-port) + str("-app")
```

Another useful feature of substitutions is maps, where you can map keys to values. The following is an example of a map substitution.

**substitutions:**

```plaintext
secure-port[]:
  true: int("443")
  false: int("80")
secure-protocol[]:
  true: SSL
  false: HTTP
```

Note that the name of a map substitution always ends with `[]`.

The following example shows how to use the maps `secure-port` and `secure-protocol`.

**components:**

```plaintext
-
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
    name: $parameters.name + "-lb"
    servicetype: $substitutions.secure-protocol[$parameters.is-secure]
    ipv46: $parameters.ip
    port: $substitutions.secure-port[$parameters.is-secure]
    lbmethod: $parameters.lb-alg
```

This implies that if the user of the StyleBook specifies the Boolean value "true" to the parameter `is-secure`, or selects the
checkbox corresponding to this parameter in the NetScaler MAS GUI, the servicetype property of this component is assigned the value SSL and the port property is assigned the value 443. However, if the user specifies “false” for this parameter or clears the corresponding checkbox in the NetScaler MAS GUI, the servicetype property is assigned the value HTTP and the port is assigned the value 80.

You can also use functions to parameterize a substitution. Consider the following example:

```
substitutions:
  cspol-priority(priority): 10100 - 100 * $priority
```

The substitution cspol-priority is a function that takes an argument called priority and uses it to calculate a value. In the rest of the StyleBook, this substitution can be referred as shown in the following example:

```
components:
  -
    name: cspolicy-binding-comp
    type: ns::csvserver_cspolicy_binding
    condition: not $parameters.is-default
    properties:
      name: $parameters.csvserver-name
      policyname: $components.cspolicy-comp.properties.policyname
      priority: $substitutions.cspol-priority($parameters.pool.priority)
```

Substitution can also be made up of a key and a value. The value can be a simple value, an expression, a function, a map, a list, or a dictionary.

The following is an example of a substitution called 'slist' whose value is a list:

```
substitutions:
  slist:
    - a
    - b
    - c
```

The value of a substitution can also be a dictionary of key-value pairs as seen in the following example of a substitution called 'sdict' below:

```
substitutions:
  sdict:
    a: 1
```
You can create more complex attributes by combining the lists and dictionaries. For example, a substitution called "slistofdict" returns a list of key-value pairs.

**slistofdict:**

```
- a: $parameters.cs1.lb1.port
  b: $parameters.cs1.lb2.port
  
- a: $parameters.cs2.lb1.port
  b: $parameters.cs2.lb2.port
```

But, in the following example, a substitution "sdictoflist" returns a key-value pair, where the value itself is another list.

**sdictoflist:**

```
a:
  - 1
  - 2
  
b:
  - 3
  - 4
```

In components, these substitutions may be used in condition, properties, repeat, repeat-condition constructs.

The following example of a component shows how a substitution can be used to when specify the properties:

**properties:**

```
a: $substitutions.slist
b: $substitutions.sddict
c: $substitutions.slistofdict
d: $substitutions.sdictoflist
```

A use case for defining a substitution whose value is a list or a dictionary is when you are configuring a content switching virtual server and multiple load balancing virtual servers. Since all lb virtual servers tied to the same cs virtual server might have an identical configuration, you can use substitution list and dictionary to build this configuration to avoid repeating that
configuration for each lb virtual server.

The following example shows the substitution and the component in the cs-lb-mon StyleBooks to create a content switching virtual server configuration. While constructing the properties of cs-lb-mon StyleBooks, the complex substitution "lb-properties" specify the properties of the lb virtual servers associated with the cs virtual server. The "lb-properties" substitution is a function that takes the name, service type, virtual IP address, port, and servers as parameters and generates a key-value pair as the value. In "cs-pools" component, we assign the value of this substitution to lb-pool parameter for each pool.

substitutions:

<table>
<thead>
<tr>
<th>cs-port[]:</th>
</tr>
</thead>
<tbody>
<tr>
<td>true: int(&quot;80&quot;)</td>
</tr>
<tr>
<td>false: int(&quot;443&quot;)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>lb-properties(name, servicetype, vip, port, servers):</th>
</tr>
</thead>
<tbody>
<tr>
<td>lb-appname: $name</td>
</tr>
<tr>
<td>lb-service-type: $servicetype</td>
</tr>
<tr>
<td>lb-virtual-ip: $vip</td>
</tr>
<tr>
<td>lb-virtual-port: $port</td>
</tr>
<tr>
<td>svc-servers: $servers</td>
</tr>
<tr>
<td>svc-service-type: $servicetype</td>
</tr>
<tr>
<td>monitors:</td>
</tr>
<tr>
<td>-</td>
</tr>
<tr>
<td>monitorname: $name</td>
</tr>
<tr>
<td>type: PING</td>
</tr>
<tr>
<td>interval: $parameters.monitor-interval</td>
</tr>
<tr>
<td>interval_units: SEC</td>
</tr>
<tr>
<td>retries: 3</td>
</tr>
</tbody>
</table>

components:

- name: cs-pools |
  type: stlb:cs-lb-mon |
  description: |
Updates the cs-lb-mon configuration with the different pools provided.

Each pool with rule result in a dummy LB vserver, cs action, cs policy, and csvserver_cspolicy_binding configuration.

condition: $parameters.server-pools
repeat: $parameters.server-pools
repeat-item: pool
repeat-condition: $pool.rule
repeat-index: ndx

properties:
  appname: $parameters.appname + "-cs"
  cs-virtual-ip: $parameters.vip
  cs-virtual-port: $substitutions.cs-port($parameters.protocol == "HTTP")
  cs-service-type: $parameters.protocol

pools:

- 
  lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP", "0.0.0.0", 0, $pool.servers)
  rule: $pool.rule
  priority: $ndx + 1
The Components construct in a StyleBook is considered as the most important section in the StyleBook. In this section, you define the configuration objects that have to be created. Using this construct, you can build one or multiple configuration objects of the same type.

The components construct can use the input provided in the parameters section to adapt the configuration generated by the StyleBook. This is an optional section, although most StyleBooks have a components section.

The following table describes the main attributes of a component.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the component. You can specify an alphanumeric name. The name must begin with an alphabet, and can include additional alphabets, numbers, hyphen (-), or underscore (_).</td>
</tr>
<tr>
<td>description</td>
<td>A description of the role of this component in the StyleBook.</td>
</tr>
</tbody>
</table>
| type      | The type determines what properties this component provides. Components have two kind of types:  
  * **Built-in type**: This type is provided by the system and you do not have to define it, for example, the NITRO entity types "lbvserver" or "servicegroup."  
    
    When a component has a built-in type attribute, it creates a configuration object of that type on the NetScaler. For example, if a component refers to the built-in type "lbvserver," this component creates a load balancing virtual server on the NetScaler instance that is the target of the configuration.  
  * **Composite type**: This type refers to an existing StyleBook that you created and imported into NetScaler MAS.  
    
    When a component has a composite type attribute, it creates all the configuration objects, which are specified in the referenced StyleBook, on the NetScaler instance that is the target of the configuration. This enables you to combine multiple StyleBooks where each StyleBook creates a part of the final configuration.  
    
    For more information about composite StyleBooks, see Create a Composite StyleBook. |
| properties | The sub-attributes that can be used for a component type attribute.  

The properties that are valid for a component are dictated by its type. For a built-in type, these are the properties or attributes of the corresponding Nitro object. For a component whose type is another StyleBook, that is, a composite type, the properties correspond to the parameters defined in that StyleBook. |
components:

- name: my-lbvserver-comp
type: ns::lbvserver

properties:
  name: $parameters.name
  servicetype: HTTP
  ipv46: $parameters.ip
  port: 80
  lbmethod: $parameters.lb-alg

In this example, you have defined a component called my-lbvserver-comp. This component is of type ns::lbvserver (a built-in type), where "ns" is the prefix that refers to the namespace netscaler.nitro.config and version 10.5 that you had specified in the import-stylebooks section, and "lbvserver" is a NITRO resource in this namespace.

The properties in this section include four mandatory and one optional attribute (lbmethod) of the "lbvserver" resource and allows you to specify values for these attributes. In this example, you are specifying static values for servicetype and port while the name, ipv46, and lbmethod properties get their values from the input parameters. You refer to the parameter names defined in the parameters section by using $parameters.<name> notation, for example, $parameters.ip.

To learn more about all the available NetScaler NITRO resources and their attributes/properties, see the NetScaler NITRO REST API documentation.

Note
You have to use lower case for the attribute names of NITRO resource types (its component properties). Otherwise, the import of a StyleBook will fail.
Optional Properties

Oct 20, 2016

In some cases, a property of a component takes its value from an expression, which can be a simple expression such as a parameter reference, or a more complex one. Setting this property value is optional in the component. You can choose to set the property value only if the expression returns an actual value, else you can choose not to set this property.

For example, consider that one of the properties you want to set is the lbmethod (loadbalancing algorithm) of a component whose type is ns::lbvserver. The value of the property lbmethod is taken from a parameter value provided by the user, as shown below:

```
components

  name: lbvserver_comp
  type: ns:lbvserver
  properties:
    name: $parameters.lb-appname + "-lb"
    servicetype: $parameters.lb-service-type
    ipv46: $parameters.lb-virtual-ip
    port: 80
    lbmethod: $parameters.lb-advanced.algorithm
```

Now, consider that the parameter lb-advanced.algorithm is an optional parameter. And, if the user does not provide a value for this parameter because it is optional, the expression $parameters.lb-advanced.algorithm evaluates to blank value. Therefore, an invalid value is passed for the lbmethod property. In order to avoid such a situation, you can annotate the property as optional by suffixing its name with "?" as follows:

```
components

  name: lbvserver_comp
  type: ns:lbvserver
  properties:
    name: $parameters.lb-appname + "-lb"
    servicetype: $parameters.lb-service-type
    ipv46: $parameters.lb-virtual-ip
    port: 80
    lbmethod?: $parameters.lb-advanced.algorithm
```
lbmethod?: $parameters.lb-advanced.algorithm

The use of "?" omits the property if the expression on the right evaluates to nothing, which would be equivalent, in this case, to a component defined as follows:

components
-
  name: lbvserver_comp
  type: ns::lbvserver
  properties:
    name: $parameters.lb-appname + "-lb"
    servicetype: $parameters.lb-service-type
    ipv46: $parameters.lb-virtual-ip
    port: 80

Because lbmethod is optional, omitting it still makes this a valid component. Note that lbmethod might take its default value if one is defined in its type "ns::lbvserver."
Nested Components

Oct 20, 2016
Nesting a component within another component allows the nested component to create its configuration objects by referring to configuration objects or the context created by the parent component. The nested component can create one or more objects for each object created in the parent component. Nesting a component within another component does not indicate any relationship between the configuration objects created. Nesting is a way to facilitate the task of components to construct configuration objects within an existing context of the parent components.

Example:

components:

- 
  name: my-lbvserver-comp
  type: ns:lbvserver
  properties:
    name: $parameters.name + "-lb"
    servicetype: HTTP
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
  components:
    - 
      name: my-svcg-comp
      type: ns:servicegroup
      properties:
        name: $parameters.name + "-svcgrp"
        servicetype: HTTP
  components:
    - 
      name: lbvserver-svg-binding-comp
      type: ns:lbvserver_servicegroup_binding
properties:

  name: $parent.parent.properties.name

  servicegroupname: $parent.properties.name

-

  name: members-svcg-comp

  type: ns::servicegroup_servicegroupmember_binding

  repeat: $parameters.svc-servers

  repeat-item: srv

  properties:

    ip: $srv

    port: str($parameters.svc-port)

    servicegroupname: $parent.properties.name

In this example, multi-level nesting is used. The component my-lbvserver-comp has a child component called my-svcg-comp. And, the my-svcg-comp component has two child components within it. The my-svcg-comp component is used to create a service group configuration object on the NetScaler instance by providing values to the attributes of the built-in NITRO resource type “servicegroup.” The first child component of the my-svcg component, lbvserver-svcg-binding-comp, is used to bind the service group created by its parent component to the load balancing virtual server (lbvserver) created by the parent’s parent component. The $parent notation, also called the parent reference, is used to refer to entities in the parent components. The second child component, members-svcg-comp, is used to bind the list of services to the service group created by the parent component. The binding is achieved by using the repeat construct of StyleBook to iterate over the list of services specified for the parameter svc-servers. For information on repeat constructs, see Repeat Construct.

You can also create the same configuration objects without using nesting of components. For more information and examples, see StyleBook to Create a Basic Load Balancing Configuration.
Condition Construct

Oct 20, 2016

You can make a component conditional by using a condition construct. The value of a conditional construct is a boolean expression that evaluates to true or false. If the condition is true, the component is used to build its configuration objects. If the condition is false, the component is skipped, and no configuration objects are created through it. The boolean expression is often based on parameter values.

Example:

components:

- name: servicegroup-comp
type: ns:servicegroup
condition: $parameters.svc-server-ips
properties:
  name: $parameters.name + "-svcgrp"
servicetype: HTTP

In this example, if the user specifies a value for the optional parameter svc-server-ips, then the component, servicegroup-comp, is processed by the StyleBook engine. If the condition is false, that is, if the user does not provide a value to this parameter, a null value is assigned to this parameter and evaluates to false, then the StyleBook engine ignores the presence of this component, and no servicegroup is created.

Note that the boolean expression can be based on any valid expression supported in StyleBooks (for example, whether another component is present, or whether a parameter has a certain value).

The following example builds the configuration object of NITRO type ns:systemfile if the condition is evaluated to true.

Example:

components

- name: pem_key_files
type: ns:systemfile
condition: "$components.der-certificate-files-comp or $components.pem-certificate-files-comp"
properties:
  filecontent: Scertificate.keyfile.contents
  fileencoding: "BASE64"
filelocation: "\nsconfig/ssl"

filename: $certificate.keyfile.filename

In this example, the condition is a complex "or" expression, where you want this configuration object to be created by the StyleBook only if two other components in the StyleBook have been processed (not skipped), therefore, creating a dependency between components.
Repeat Construct

You can use the repeat and repeat-item constructs of a component to build multiple configuration objects of the same type.

In the following example, the members-svcg-comp component is used to bind the list of services to the service group created by the parent component. In order to create a configuration object that binds each server to the service group, use the repeat construct to iterate over the list of services specified for the parameter svc-servers. During the iteration, the component creates a NITRO object of type servicegroup_servicegroupmember_binding for each service (referred to as srv in the repeat-item construct) in the service group, and it sets the ip attribute in each NITRO object to the IP address of the corresponding service.

Example:

components:

- name: my-lbvserver-comp
type: ns:lbvserver
properties:
  name: $parameters.name + "-lb"
servicetype: HTTP
ipv46: $parameters.ip
port: 80
lbmethod: $parameters.lb-alg
components:

- name: my-svcg-comp
type: ns:servicegroup
properties:
  name: $parameters.name + "-svgrp"
servicetype: HTTP
components:
name: lbvserver-svg-binding-comp
type: ns::lbvserver_servicegroup_binding

properties:
  name: $parent.parent.properties.name
  servicegroupname: $parent.properties.name

- name: members-svcg-comp
type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv

properties:
  ip: $srv
  port: str($parameters.svc-port)
  servicegroupname: $parent.properties.name

Note that repeat-item construct is optional, and is used to give a friendly name to the current item in the iteration. If it is not specified, the current item can be accessed using the expression $repeat-item. The last component in the above example can also be written as follows:

- name: members-svcg-comp
type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers

properties:
  ip: $repeat-item
  port: str($parameters.svc-port)
  servicegroupname: $parent.properties.name

In addition to being able to refer to the current item while iterating over a list, it is also possible to refer to the current index of the item in the list using the expression $repeat-index. In the following example, $repeat-index is used to calculate a port number based on the current index:
name: services

type: ns::service

repeat: $parameters.app-services

properties:
  ip: $parameters.app-ip
  port: str($parameters.base-port + $repeat-index)
  servicegroupname: $parent.properties.name

Similar to the repeat-item construct, you can assign a different variable name to refer to the current index of the iteration. The previous example is equivalent to the following example:

- name: services
  type: ns::service
  repeat: $parameters.app-services
  repeat-index: idx

  properties:
    ip: $parameters.app-ip
    port: str($parameters.base-port + $idx)
    servicegroupname: $parent.properties.name
Repeat-Condition Construct

Nov 16, 2016

The repeat-condition construct is evaluated in each iteration of a repeat construct and the result determines whether to build the configuration object in that iteration or to move to the next iteration. The following example shows the use of the repeat-condition construct:

Example:

```
components

- name: der-key-files-comp
type: ns::systemfile
repeat: $parameters.certificates
repeat-item: certificate
repeat-condition: "$certificate.ssl-inform == \"DER\"

properties:
  filecontent: base64($certificate.keyfile.contents)
  fileencoding: BASE64
  filelocation: /nsconfig/ssl
  filename: $certificate.keyfile.file
```

In this example, the der-key-files-comp component iterates over all the certificates given by the user but it only builds configuration objects that correspond to certificates with DER encoding. In each iteration, the repeat-condition expression is evaluated to test whether the certificate encoding is of type DER. If it is not of type DER, no configuration object is built in the current iteration, and the iteration moves to the next certificate in the list.
Outputs

Oct 20, 2016

In the outputs section, you specify what a StyleBook exposes to its users after it has completed creating all the configuration objects successfully. The outputs section of a StyleBook is optional. A StyleBook does not need to return outputs. However, by returning some internal components as outputs, it allows any StyleBooks that import it more flexibility as you can see when creating a composite StyleBook.

The following table describes the attributes used in the outputs section.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the output corresponding to the configuration object you want to expose.</td>
<td>Yes</td>
</tr>
<tr>
<td>description</td>
<td>A text string describing the output.</td>
<td>No</td>
</tr>
<tr>
<td>value</td>
<td>This attribute specifies how to extract the value that is returned by a StyleBook.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Example:

`outputs:`

- `name: lbvserver`
  
  `description: LBVServer component`
  
  `value: $components.my-lbvserver-comp`

- `name: svc-grp`

  `description: ServiceGroup name`
  
  `value: $components.my-svcg.properties.name`

In this example, you expose the `lbvserver` component and the servicegroup `name` that would be created by the StyleBook. The value of the output called `lbvserver` is the component `my-lbvserver-comp`. Similarly, the value of the output called `svc-grp` is the name of the servicegroup created by the component `my-svcg`. 
Parameter Reference

Oct 20, 2016

In the components construct, you refer to the parameters defined in the parameters section by using $parameters.<parametername> notation. If <parametername> itself contains parameters (when type is object), then you must use the notation $parameters.<parametername>.parameters, and so on.

Example:

parameters:

  -
    name: name
    type: string
    required: true

  -
    name: vip
    label: Virtual IP and Port
    type: object
    required: true
    parameters:

      -
        name: ip
        label: Virtual IP
        description: The Virtual IP Address
        type: ipaddress
        required: true

      -
        name: port
        label: The Virtual Port
        description: The TCP port for the Virtual IP
        type: tcp-port
        default: 80
components:

- name: my-lbvserver-comp
  type: ns:lbvserver

  properties:
    name: $parameters.name
    servicetype: HTTP
    ipv46: $parameters.vip.parameters.ip
    port: $parameters.vip.parameters.port
If you are using nested components, you can refer to the parent component using the $parent notation. If the parent component builds multiple configuration objects using the repeat construct, and within each iteration, child components build other configuration objects, then the $parent notation always refers to the current iteration of the parent component. For example, $parent.properties.name refers to the name property of the configuration object built in the current iteration by the parent.

Example:

```components:
-
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
    name: $parameters.name + "-lb"
    servicetype: HTTP
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg

components:
-
  name: my-svcg-comp
  type: ns::servicegroup
  properties:
    name: $parameters.name + "-svcgrp"
    servicetype: HTTP

components:
-
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
```
properties:

  name: $parent.parent.properties.name

  servicegroupname: $parent.properties.name

- name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
    ip: $srv
    port: str($parameters.svc-port)
    servicegroupname: $parent.properties.name

You can also navigate upward through the hierarchy of components by accessing the properties of the parents of parents all the way to top-level components. For example, the property name of the component lbvserver-svg-binding-comp takes its value from the property name of the parent of its parent, the my-lbvserver-comp component, by using the $parent.parent notation.
Components Reference

In the components construct, you refer to top-level component in the StyleBook by using the $components.<componentname> notation. If there are nested components within a top-level component, then the notation used is $components.<componentname>.components.<component-name> to refer to them, and so on.

Example:

components:

- name: my-lbvserver-comp
type: ns:lbvserver

properties:
  name: Sparameters.name + "-lb"
servicetype: HTTP
ipv46: $parameters.ip
port: 80
lbmethod: $parameters.lb-alg

- name: my-svcg-comp
type: ns:servicegroup

properties:
  name: Sparameters.name + "-svcgrp"
servicetype: HTTP

- name: members-svcg-comp
type: ns:servicegroup_servicegroupmember_binding
repeat: $parameters.svc-servers
repeat-item: srv

properties:
  ip: $srv
**port**: `str($parameters.svc-port)`

**servicegroupname**: `$components.my-svcg-comp.properties.name`

**name**: lbvserver-svg-binding-comp

**type**: `ns:lbvserver_servicegroup_binding`

**properties**:

- **name**: `$components.my-lbvserver-comp.properties.name`
- **servicegroupname**: `$components.my-svcg-comp.properties.name`

In this example, the components **my-svcg-comp** and **my-lbvserver-comp** have to be built before building the last component **lbvserver-svg-binding-comp** because there are references to these components in this last component. These references are provided by using the components references denoted by `$components.<componentname>`. 
Substitutions Reference

Oct 20, 2016

In the components section or operations section, you refer to substitutions defined in the substitutions section by using the $substitutions.<substitution-name>$ notation. For example, $substitutions.http-port$.

If a substitution is a map, you can refer to an element in the map as $substitutions.<substitutions-name>[/map-key]$. For example, $substitutions.protocol-map[parameters.port]$. 
Variable Reference

Oct 20, 2016

When you use the repeat and repeat-item constructs in components to build multiple configuration objects, you can assign a variable name to the repeat-item construct. This variable can be then referenced in the properties of that component or in child components by using the notation $<varname>$. Note that when the repeat construct is used without the repeat-item construct in a component, a default variable called $repeat-item$ can be used to access the iteration items.

Example:

components:

```
- name: server-members-comp
  type: ns:server
  condition: $parameters.svc-server-domain-names
  repeat: $parameters.svc-server-domain-names
  repeat-item: server-name
  properties:
    name: $server-name + "-server"
    domain: $server-name

components:

- name: service-members-comp
  type: ns:service
  properties:
    name: $server-name + "-service"
    servername: $parent.properties.name
    servicetype: $parameters.svc-service-type
    port: $parameters.svc-server-port
```

In the above example, a variable name, server-name, is assigned to the repeat-item construct. This variable name is referred to in the properties of the same component as well as in the child components $<varname>$. 

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved. p.328
A StyleBook may also contain an optional operations section where the StyleBook developer can configure NetScaler MAS Analytics to collect appflow records on all or some of the traffic transactions handled by any virtual server that is created when creating a configuration by using the StyleBook. Through this section, the StyleBook developer can also configure alarms to be triggered by NetScaler MAS when certain traffic conditions are met on a virtual server.

Example:

```yaml
operations:

  analytics:

  -

    name: lbvserver-ops-comp

    properties:

      target: $components-basic-lb-comp.outputs.lbvserver-name

      filter: HTTP.REQ.URL.CONTAINS("catalog")
```

For information about the analytics construct, see Analytics.
The analytics sub-section of the operations section has a structure similar to the components section. Each element in the analytics section is used to configure the NetScaler MAS Analytics feature for one or more virtual servers created by the StyleBook.

An element in the analytics section has the following attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the analytics element.</td>
<td>Yes</td>
</tr>
<tr>
<td>description</td>
<td>A text string describing what this element is.</td>
<td>No</td>
</tr>
<tr>
<td>condition</td>
<td>A boolean expression. When this condition evaluates to false, the entire analytics element is skipped.</td>
<td>No</td>
</tr>
<tr>
<td>repeat</td>
<td>Iterates over a list.</td>
<td>No</td>
</tr>
<tr>
<td>repeat-condition</td>
<td>A boolean expression. If the expression evaluates to false, the current iteration is skipped.</td>
<td>No</td>
</tr>
<tr>
<td>repeat-item</td>
<td>Name of the item in the current iteration.</td>
<td>No</td>
</tr>
<tr>
<td>repeat-index</td>
<td>Name of the index value of the current iteration.</td>
<td>No</td>
</tr>
<tr>
<td>properties</td>
<td>The list of properties of analytics.</td>
<td>Yes</td>
</tr>
<tr>
<td>target</td>
<td>One of the properties in the list. The target expression is the name of a virtual server, configured on the NetScaler, for which analytics will be collected.</td>
<td>Yes</td>
</tr>
<tr>
<td>filter</td>
<td>One of the properties in the list. The value of this attribute is a NetScaler advanced policy expression that is used to filter the requests on the virtual server for which analytics will be collected. By default, the analytics data is collected on all the traffic passing through the virtual server.</td>
<td>No</td>
</tr>
</tbody>
</table>

Example:

```
operations:
  analytics:
    name: lbvserver-ops-comp
```
properties:

- **target**: $components-basic-lb-comp.outputs.lbvserver-name
- **filter**: HTTP.REQ.URL.CONTAINS("catalog")

Each attribute in the analytics section is used to instruct the NetScaler MAS Analytics feature to configure the NetScaler instances to collect appflow records on the virtual server identified by the target property.
The alarms sub-section of the operations section has a similar structure and the same attributes as in the analytics sub-section. The only difference is in the properties attribute. For a list of all the attributes (other than the properties attribute), see Analytics.

The following properties are available in an alarms sub-section:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>An expression that evaluates to the name of a virtual server, configured on the NetScaler, for which alarms are configured.</td>
<td>Yes</td>
</tr>
<tr>
<td>email-profile</td>
<td>Name of an email profile that is defined in the NetScaler MAS Analytics feature and contains a list of email addresses that you want to notify when the alarm is triggered.</td>
<td>No (either an email-profile or an sms-profile must be defined)</td>
</tr>
<tr>
<td>sms-profile</td>
<td>Name of an SMS profile that is defined in the NetScaler MAS Analytics feature and contains a list of phone numbers that you want to notify when the alarm is triggered.</td>
<td>No (either an email-profile or an sms-profile must be defined)</td>
</tr>
<tr>
<td>rules</td>
<td>A list of rules that define the conditions that would trigger an alarm for the virtual server defined by the target property.</td>
<td>Yes</td>
</tr>
<tr>
<td>metric</td>
<td>An attribute of rule. The name of a metric you want to track pertaining to the NetScaler virtual server.</td>
<td>Yes</td>
</tr>
<tr>
<td>operator</td>
<td>An attribute of rule. The operator to use to compare the metric to the value. Valid operators are &quot;greaterthan&quot; and &quot;lessthan.&quot;</td>
<td>Yes</td>
</tr>
<tr>
<td>value</td>
<td>An attribute of rule. The threshold value that the metric is compared to by using the operator. If the metric value exceeds this threshold, the associated alarms are triggered.</td>
<td>Yes</td>
</tr>
<tr>
<td>period-unit</td>
<td>An attribute of a rule. The frequency at which to alert users if the alarm rule is met. This can contain the value day, hour, or weekly. This means that if the rule is met, an alarm will be sent once a period-unit (for example, once a day).</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The following table provides a list of metrics that are tracked pertaining to the NetScaler virtual server.

<table>
<thead>
<tr>
<th>Counters</th>
<th>Description</th>
<th>Detailed Description</th>
<th>NetScaler MAS Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>For a VPN virtual server:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>total_requests</td>
<td>Total number of active sessions on this VPN virtual server started during a time interval specified by the user. Monotonically increasing counter, incremented on each new session launch.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>app_count</td>
<td>Total number of unique VPN applications on this VPN virtual server launched during a time interval specified by the user. Monotonically increasing counter on each new application launch.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>app_launch_duration</td>
<td>Average time taken to launch an application (in milliseconds). Average value calculated across the launch time durations of all VPN applications launched on this VPN virtual server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other virtual servers (CS, LB, Auth, GSLB)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>total_requests</td>
<td>Number of client requests on this virtual server since the last appliance reboot, or since the creation of the virtual server, whichever is more recent. Monotonically increasing counter, incremented on each new request to this virtual server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>total_bytes</td>
<td>Total bytes transferred from the virtual server to NetScaler MAS over the specified time interval. Monotonically increasing counter to account for the total number of bytes served by this virtual server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>application_response_time</td>
<td>Average response time of the virtual server. The average value of the response times of all requests received by this virtual server since the last reboot of the appliance (or since the creation of the virtual server), whichever is last.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- 

  **name**: lbvserver_alarm

  **properties**:

  - **target**: $outputs.lbvserver
  
  - **email-profile**: $parameters.emailprofile
  
  - **sms-profile**: "NetScalerSMS"

  **rules**:

  - 
    - **metric**: "total_requests"
    
    - **operator**: "greaterthan"
    
    - **value**: 25
    
    - **period-unit**: weekly

  - 
    - **metric**: "total_bytes"
    
    - **operator**: "lessthan"
    
    - **value**: 1024
    
    - **period-unit**: day
One of the most powerful features of StyleBook is the use of expressions. You can use StyleBooks expressions in various scenarios to compute dynamic values. The example below shows an expression to concatenate a parameter value with a literal string.

**Example:**

```javascript
$parameters.appname + "-mon"
```

This expression retrieves the parameter named `appname`, and concatenates it with the string 

You can also merge two lists together using the notation: `$parameters.list1 + $parameters.list2`

The following types of expressions are supported:

<table>
<thead>
<tr>
<th>Expression</th>
<th>Supported Operators</th>
<th>Examples</th>
</tr>
</thead>
</table>
| **Arithmetic Expressions** | • + : Addition  
• - : Substraction  
• * : Multiplication  
• / : Division | • Adding two numbers: `$parameters.a + $parameters.b`  
• Multiplying two numbers: `$parameters.a * 10` |
| **String Expressions** | • + : Concatenate two strings  
• in : Tests whether the first argument is a substring of the second argument | • Concatenate two strings: `str("app-") + $parameters.app-name`  
• Tests if one string is a substring of another: "abcd" in `$parameters.name` |
| **List Expressions** | • + : Merges two lists  
• in : Tests if an item is part of a list | • Concatenate two lists: `$parameters.external-servers + $parameters.internal-servers`  
• Tests if an item is part of a list: `80 in $parameters.ports` |
| **Relational Expressions** | • == : Tests if two operands are equal and returns true if they are equal, else returns false.  
• != : Tests if two operands are different and returns true if they are different, else returns false.  
• > : Returns true if the first operand is greater than the second operand, else returns false.  
• >= : Returns true if the first operand is greater than or equal to the second operand, else returns false.  
• < : Returns true if the first operand is lesser than the second operand, else returns false.  
• <= : Returns true if the first operand is lesser than | • Use of Equality operator: `$parameters.name == "abcd"`  
• Use of Inequality operator: `$parameters.name != "default"` |
| Logical (Boolean) Expressions | and: The logical 'and' operator. If both operands are true, the result is true, else it is false. | Example of an "and" expression: $parameters.num > 10 \text{ and }$ $parameters.num <= 20$ |
|                             | or: The logical 'or' operator. If one of the operands is true, the result is true, else it is false. | Example of an "or" expression: $parameters.x \text{ or }$ $parameters.y$ |
|                             | not: The unary operator. If the operand is true, the result is false, and vice-versa. | Example of "not": not $parameters.is-secure$ |
# Built-in Functions

Expressions in StyleBooks can make use of built-in functions.

For example, you can use the built-in "string" function, `str()` to transform a number as a string.

\[
\text{str(}\$\text{parameters.order})
\]

Or, you can use the built-in "integer" function, `int()` to do the reverse, that is, transform a string into an integer.

\[
\text{int(}\$\text{parameters.priority})
\]

The following is the list of built-in functions supported in StyleBook expressions with examples of how they can be used:

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Examples of Functions in StyleBook Expressions</th>
</tr>
</thead>
</table>
| `str()`  | The "string" function takes a number or a string as an argument, and returns a string. | name: "set-" + str(10)  
Returns:  
"set-10" |
| `int()`  | The "integer" function takes a string as an argument and returns a number. | integer: int("10")  
Returns:  
10 |
| `bool()` | The "boolean" function takes any value as an argument. If the value is false, empty, or non-existent, this function returns false. Otherwise, it returns true. | bool(true)  
Returns:  
true  
bool(false)  
Returns:  
false  
bool($\text{parameters.a}) returns false if the $\text{parameters.a} is false, empty, or not present. Otherwise, it returns true. |

You can now use the following expression to obtain the number of items in the list:

\[
\text{len(}$\text{substitutions.items}$\text{)}
\]
| Function | Description | Example
|-----------|-------------|---------|
| `len()` | Takes a string or a list as an argument, and returns the number of characters in a string or the number of items in a list. | For example, if you define a substitution as follows: items: ["123", "abc", "xyz"]

```python
len(items)
```

Returns:
3

| Function | Description | Example
|-----------|-------------|---------|
| `min()` | Takes a list of numbers as an argument, and returns the smallest number. | Examples of expressions:

- `min(80, 100, 1000)` returns 80
- `min(-20, 100, 400)` returns -20
- `min(-80, -20, -10)` returns -80
- `min(0, 100, -400)` returns -400

| Function | Description | Example
|-----------|-------------|---------|
| `max()` | Takes a list of numbers as an argument, and returns the largest number. | Examples of expressions:

- `max(80, 100, 1000)` returns 1000
- `max(-20, 100, 400)` returns 400
- `max(-80, -20, -10)` returns -10
- `max(0, 100, -400)` returns 100

| Function | Description | Example
|-----------|-------------|---------|
| `oct()` | Takes a number as an argument, and returns a string that represents the number in octal format. | Examples of expressions:

- `oct(10)` returns "0o12"
- `oct(0b101)` returns "0o5"
- `oct(0XA)` returns "0o12"

| Function | Description | Example
|-----------|-------------|---------|
| `hex()` | Takes a number as an argument, and returns a lowercase string that represents the number in hexadecimal format. | Examples of expressions:

- `hex(435)` returns "0x1b3"
- `hex(0)` returns "0x0"
- `hex(-34)` returns "-0x22"

| Function | Description | Example
|-----------|-------------|---------|
| `lower()` | Takes a string as an argument and returns the same string in lowercase. | `lower("ABC")`

Returns:
"abc"

| Function | Description | Example
|-----------|-------------|---------|
| `upper()` | Takes a string as an argument and returns the same string in uppercase. | `upper("aBc")`

Returns:
"ABC"
<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>sum()</strong></td>
<td>The &quot;summation&quot; function takes a list of numbers as arguments and returns the sum of the numbers.</td>
<td>You can now use the following expression to obtain the sum of numbers in the list: <code>sum($substitutions.list-of-numbers)</code> For example, if you define a substitution as follows: substitutions: list-of-numbers: - 11 - 22 - 55 <code>sum($substitutions.list-of-numbers)</code> Returns: 88 (the sum of the elements of the list)</td>
</tr>
<tr>
<td><strong>pow()</strong></td>
<td>The &quot;power&quot; function takes two numbers as arguments and returns a number that represents the first argument to the power of the second one.</td>
<td><code>pow(3,2)</code> Returns: 9</td>
</tr>
<tr>
<td><strong>base64()</strong></td>
<td>The &quot;base64&quot; function takes a string argument and returns the BASE64 encoding of that string.</td>
<td>Example of an expression encoding a string using BASE64 encoding, which returns the resulting string: <code>base64($certificate.key-file.contents)</code></td>
</tr>
</tbody>
</table>
Monitoring HAProxy Instances with NetScaler MAS

Mar 07, 2017

HAProxy (High Availability Proxy) is an open-source load-balancer that can load balance any TCP service. For more information about HAProxy, see [http://www.haproxy.org/](http://www.haproxy.org/).

The NetScaler Management and Analytics System (MAS) supports HAProxy version 1.4.24 or later. When you add a host on which you have provisioned the HAProxy instances to NetScaler MAS, NetScaler MAS discovers the HAProxy instances on the host and enables you to monitor them. It shows you the following details of the HAProxy configuration on the instances:

- Frontend – Defines how requests should be forwarded to the backend.
- Backend – Defines the set of servers that receives the forwarded requests.
- Servers – The servers among which HAProxy load balances the traffic.

For more information, see [http://www.haproxy.org/download/1.7/doc/configuration.txt](http://www.haproxy.org/download/1.7/doc/configuration.txt).

Make sure that you have deployed an HAProxy instance on a host in your deployment. For more information, see [http://www.haproxy.org/#docs](http://www.haproxy.org/#docs).

To add an HAProxy instance to NetScaler MAS:

1. In a web browser, type the IP address of the NetScaler Management and Analytics System (for example, http://192.168.100.1).
2. In the User Name and Password fields, enter the administrator credentials. The default administrator credentials are nsroot and nsroot.
3. Navigate to Infrastructure > Instances. Under Instances, select HAProxy and click Add.
4. In the Add HAProxy Host dialog box, do the following:
   a. In the IP Address field, enter the IP address of the host on which you have provisioned the HAProxy instances.
   b. In the HAProxy Profile drop-down list, create and select the HAProxy profile. To create an HAProxy profile, click the + icon and do the following in the Add HAProxy Profile dialog box:
i. In the **Profile Name** field, enter the profile name.

ii. In the **Username** field, enter the username of the host.

iii. In the **SSL private key** field, enter the private key of the host.

iv. In the **Passphrase** field, enter the passphrase of the private key.

v. Click **Create**.

c. Click **OK**.

NetScaler MAS discovers the HAProxy instances provisioned on the host, and you can view all the HAProxy instances on the **Instances** tab.
In NetScaler MAS, you can view the configuration of an HAProxy instance. Navigate to **Infrastructure > Instances > HAProxy** and, on the **Instances** tab, select the HAProxy instance and click **View Configuration**.
How to Use the Dashboard to Monitor HAProxy Instance from NetScaler MAS

Feb 02, 2017

The HAProxy dashboard in NetScaler MAS displays graphs that help you keep track of CPU and memory usage of an HAProxy instance. The dashboard also displays graphs that indicate the following:

- Percentage of the CPU used by the HAProxy instance.
- Percentage of memory used by the HAProxy instance.

To monitor HAProxy instance in NetScaler MAS, navigate to Infrastructure > Instances > HAProxy > Instances tab. Select the HAProxy instance and click Dashboard.
How to View the Details of the Frontend Configured on HAProxy Instances From NetScaler MAS

Feb 08, 2017

NetScaler MAS reports the following details of the frontend configured on an HAProxy instance:

- **Host IP Address.** IP address of the host
- **Configuration Path.** The HAProxy instance path on the host.
- **Name.** Name of the frontend that handles the incoming traffic.
- **Bind Host.** IP address to which the frontend is bound.
- **Bind Port.** Port to which the frontend is bound.

To view the frontend configured on the HAProxy instances:

In NetScaler MAS, navigate to **Applications > Dashboard > HAProxy > Frontends.**
How to View the Details of the Backend Configured on HAPerxy Instances From NetScaler MAS

Feb 08, 2017

NetScaler MAS reports the following details of a backend application configured on an HAPerxy instance:

- **Host IP Address.** IP address of the host.
- **Configuration Path.** HAPerxy instance path on the host.
- **Name.** Name of the backend to which the traffic is forwarded.
- **Algorithm.** Load balancing algorithm used to balance the traffic.

To view the backend configured on the HAPerxy instances:

In NetScaler MAS, navigate to Applications > Dashboard > HAPerxy > Backends.
How to View the Details of the Servers Configured on HAProxy Instances From NetScaler MAS

Feb 08, 2017

NetScaler MAS reports the following details of servers configured on an HAProxy instance:

- **Host IP Address**: Name of the host.
- **Configuration Path**: HAProxy instance path on the host.
- **Backend Name**: Name of the backend in the HAProxy configuration.
- **Name**: Name of the Server in the HAProxy configuration.
- **Server Address**: IP address of the server.
- **Server Port**: Port used by the server.

To view the servers configured on the HAProxy instances:

In NetScaler MAS, navigate to **Applications > Dashboard > HAProxy > Servers**.

![Servers Configuration](image-url)
How to Use the Application Dashboard to View the HAProxy Instances That Have the Highest Number of Frontends or Servers

Feb 08, 2017

On the Application Dashboard, NetScaler MAS displays the number of HAProxy instances that it discovers, and it lists the top five HAProxy instances that are configured with highest number of frontends or servers.

To view the Application Dashboard, in NetScaler MAS, navigate to Applications > Dashboard.

The number of HAProxy instances discovered by NetScaler MAS is displayed in the top row, as shown below:

To view the list of top five HAProxy instances that are configured with highest number of frontends or the highest number of servers, scroll down the dashboard:
NetScaler MAS as an API Proxy Server

Nov 08, 2016

In addition to being able to receive NITRO REST API requests for its own management and analytics functionality, NetScaler MAS can function as a REST API proxy server for its managed instances. Instead of sending API requests directly to the managed instances, REST API clients can send the API requests to NetScaler MAS. NetScaler MAS can differentiate between the API requests to which it must respond and the API requests that it must forward unchanged to a managed instance.

As an API proxy server, NetScaler MAS provides you with the following benefits:

- **Validation of API requests.** NetScaler MAS validates all API requests against configured security and role-based access control (RBAC) policies. NetScaler MAS is also tenant-aware and ensures that API activity does not cross tenant boundaries.

- **Centralized auditing.** NetScaler MAS maintains an audit log of all API activity related to its managed instances.

- **Session management.** NetScaler MAS frees API clients from the task of having to maintain sessions with managed instances.

When you want NetScaler MAS to forward a request to a managed instance, you configure the API client to include any one of the following HTTP headers in the API request:

- `_MPS_API_PROXY_MANAGED_INSTANCE_NAME`. Name of the managed instance.
- `_MPS_API_PROXY_MANAGED_INSTANCE_IP`. IP address of the managed instance.
- `_MPS_API_PROXY_MANAGED_INSTANCE_ID`. ID of the managed instance.

The presence of any of these HTTP headers helps NetScaler MAS identify an API request as one that it must forward to a managed instance. The value of the header helps NetScaler MAS identify the managed instance to which it must forward the request.

This flow is depicted in the following figure:
As shown in the above figure, when one of these HTTP headers appears in a request, NetScaler MAS processes the request as follows:

1. Without modifying the request, NetScaler MAS forwards the request to the instance API proxy engine.

2. The instance API proxy engine forwards the API request to a validator and logs the details of the API request in the audit log.

3. The validator ensures that the request does not violate configured security policies, RBAC policies, tenancy boundaries, and so on. It performs additional checks, such as a check to determine whether the managed instance is available.

If the API request is valid and can be forwarded to the managed instance, NetScaler MAS identifies a session that is maintained by the instance session manager and then sends the request to the managed instance.

The following examples show REST API requests that an API client sends to a NetScaler MAS server that has an IP address of 192.0.2.5. NetScaler MAS is required to forward the requests, unchanged, to a managed instance with IP address 192.0.2.10. All examples use the _MPS_API_PROXY_MANAGED_INSTANCE_IP header.

Before sending NetScaler MAS the API requests, the API client must log in to NetScaler MAS, obtain a session ID, and include the session ID in subsequent API requests. The logon API request is of the following form:
POST /nitro/v1/config/login HTTP/1.1

Host: 192.0.2.5

Cache-Control: no-cache

object=

{

"login":

{

    "username":"nsroot",

    "password":"nsroot"

    }

  }

NetScaler MAS responds to the logon request with a response that includes the session ID. The following sample response body shows a session ID:

{

  "errorcode": 0,

  "message": "Done",

  "operation": "add",

  "resourceType": "login",

  "username": "***********",

  "tenant_name": "Owner",

  "resourceName": "nsroot",

  "login": [
Example 1: Retrieve Load Balancing Virtual Server Statistics

The client must send NetScaler MAS an API request of the following form:

```json
{
    "tenant_name": "Owner",
    "permission": "superuser",
    "session_timeout": "36000",
    "challenge_token": "",
    "username": "",
    "login_type": "",
    "challenge": "",
    "client_ip": "",
    "client_port": "-1",
    "cert_verified": "false",
    "sessionid": "##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
    "token": "b2f3f935e93db6a"
}
```
Example 2: Create a Load Balancing Virtual Server

The client must send NetScaler MAS an API request of the following form:

```
GET /nitro/v1/stat/lbvserver HTTP/1.1
Host: 192.0.2.5
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
SESSID: ##D2BF9C5F40E5B2E84A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
Content-type: application/json
Cache-Control: no-cache
```

Example 3: Modify a Load Balancing Virtual Server

```
POST /nitro/v1/config/lbvserver/sample_lbserver HTTP/1.1
Host: 192.0.2.5
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
SESSID: ##D2BF9C5F40E5B2E84A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
Content-type: application/vnd.com.citrix.netscaler.lbvserver+json
Accept-type: application/vnd.com.citrix.netscaler.lbvserver+json
Cache-Control: no-cache

{"lbvserver":{"name":"sample_lbserver","servicetype":"HTTP","ipv46":"10.102.1.11","port":"80"}}
```
The client must send NetScaler MAS an API request of the following form:

```
PUT /nitro/v1/config/lbvserver HTTP/1.1
Host: 192.0.2.5
SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
Content-type: application/vnd.com.citrix.netscaler.lbvserver+json
Accept-type: application/vnd.com.citrix.netscaler.lbvserver+json
Cache-Control: no-cache

{"lbvserver":{"name":"sample_lbvserver","appflowlog":"DISABLED"}}
```

Example 4: Delete a Load Balancing Virtual Server

The client must send NetScaler MAS an API request of the following form:

```
DELETE /nitro/v1/config/lbvserver/sample_lbvserver HTTP/1.1
Host: 192.0.2.5
SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
Cache-Control: no-cache
```
Multi-Tenancy: Provide Exclusive Management Environment to Your Tenants

Jun 29, 2016

NetScaler MAS provides multi-tenancy functionality where you can configure the system for multiple tenants. Each tenant can add their network instances, manage, and monitor these instances and applications, and create their own users and groups. No tenant has visibility into the instances and applications of the other tenants. Only the system admin has visibility into all instances, applications, and reports of all tenants. However, the system admin cannot create users for the tenants. All system-level tasks can be performed only by the system admin.

Consider a scenario where an organization such as example.com has an infrastructure group and multiple business units within it. They want to centrally manage all instances in their network. However, they want to provide exclusive environment to each business unit.

The following image shows how the example.com organization infrastructure group is structured. They want each of the four business units to have exclusive management environments. This image also shows the number of instances each business unit wants to manage.

Chris, the ADC group head, is the system admin of NetScaler MAS. Chris creates two tenants for the two business units, Example-online and Example-Retail, and assigns two users as administrators of these tenants. Each tenant administrator can now add more users, add instances they want to manage, and create sub-tenants within their tenant environment.

The following image shows the tenants and users that are created in NetScaler MAS for this example.
In this example, Chris, the system admin creates two tenants: example-online and example-retail. While creating the tenants, Chris also creates a default admin user for each tenant.

**To add tenants**

1. Navigate to **System > Tenants**, and click **Add**.

2. On the **Create Tenant** page, specify the tenant name and the tenant user name whom you want to assign as the administrator for this tenant. Also, provide the password.

3. Click **Create**.
On the **Tenants** page, you can view the list of tenants that are created.

You can also view the list of admin users for each tenant on the **System > User Administration > Users** page.
When you create the tenants, two default system groups are created, admin group and read-only group for each tenant as shown in the image below. For example, example-online_admin_group and example-online_readonly_group are created for tenant example-online.

After the tenants are created, a tenant user can log on to NetScaler MAS using the tenant user credentials. To do so, a tenant has to provide both the domain name and the user name, for example, example-online\John.
Adding Instances as a Tenant User

After a tenant logs on, NetScaler MAS prompts the tenant to add instances. Click + New to add the instances you want to manage. Alternatively, you can click Do it Later and add the instances at a later time from the Infrastructure tab. For details, see Adding an Instance to NetScaler MAS.

In this example, John adds two NetScaler SDX instances.

Specify the instance type, the IP addresses (separated by comma), and the profile name that NetScaler MAS can use to access the instances, and then click OK.
John, the tenant admin, now wants to create a user for David so that David can monitor all the instances and applications of this tenant. However, Chris does not want David to perform any configuration task on the instances or change any system settings for the tenant. So, Chris creates a user david with readonly permissions.

To create a user

1. Navigate to System > User Administration > Users and click Add.
2. On the Create System User page, specify the user name and password for the user you want to create.
3. Under Groups, select the group you want to assign to this user. In this example, the example-online_readonly_group is assigned to user david.
A tenant administrator can create sub-tenants if he wants to partition his tenant further. However, he can create only one level of sub-tenants. In this example, John creates two sub-tenants, example-digital and example-ecommerce. While creating these two sub-tenants, Chris assigns Jane and Mike as the admin user respectively.

To create a tenant within a tenant, follow the steps described in Adding Tenants.

You can view the tenants created on the Tenants page.

You can also view the permissions assigned to the users. Navigate to System > User Administration > Users, select a
user, and click **Edit**.

On the **Configure System User** page, under Groups, you can view the groups assigned to that user. In this example, you can see that example-digital_admin_group is assigned to Jane.

As a tenant admin if you have already added instances to NetScaler MAS, you can assign the instances to users in your tenant or sub-tenants for management and monitoring. For example, John can assign one VPX instance to Jane for management purposes.

1. Navigate to **System > User Administration > Group**.
2. Select the group to which the user is assigned and click **Edit**.
3. On the **Modify System Group** page, on the **Users and Instances** tab, clear the **All Instances** check box.

4. Under **Instances**, select the instance you want the user to manage as shown in the figure below.
Manage Admin Partitions of NetScaler Instances

Jun 30, 2016

You might have configured admin partitions on your NetScaler instances so that different groups in your organization are assigned different partitions on the same NetScaler instance. A network administrator might be assigned to manage multiple partitions on multiple NetScaler instances.

NetScaler MAS provides a seamless way of managing all partitions owned by an administrator from a single console and without disrupting other partition configurations.

To enable multiple users to manage different admin partitions, you have to create groups and assign users and the respective partitions to those groups. Each user is able to view and manage only the partitions in the group to which the user belongs. Each admin partition is considered as an instance in NetScaler MAS. When you discover a NetScaler instance, the admin partitions configured on that NetScaler instance get added automatically to the system, as shown in the image below.

Consider that you have two NetScaler VPX instances with two partitions configured on each instance. For example, NetScaler instance 10.102.216.49 has Partition_1, Partition_2, and Partition_3, and NetScaler instance 10.102.29.120 has p1 and p2 as shown in the image below.

To view the partitions, navigate to Infrastructure > Instances > NetScaler VPX, and then click Partitions.
You want to assign user-p1 the following partitions: 10.102.29.120-p1 and 10.102.216.49-Partition_1. And, you want user-p2 to manage partitions 10.102.29.80-p2, 10.102.216.49-Partition_2, and 10.102.216.49-Partition_3.

First, you have to create two groups with admin permissions and include the required admin partition instances in each group. For example, create system group partition1-admin and add NetScaler admin partitions 10.102.29.120-p1 and 10.102.216.49-Partition_1 to this group. Also create system group partition2-admin and add NetScaler admin partitions 10.102.29.120-p2, 10.102.216.49-Partition_2, and 10.102.216.49-Partition_3 and to this group.

To create groups

1. Navigate to System > User Administration > Groups, and then click Add.
2. In the Create System User page, on the Users and Instances tab, specify the group name and permissions. Optionally, configure the session timeout.
3. To allow access to specific instances, clear the All Instances check box, and then add the instances from the Available list to the Configured list.
4. Click Next, and then click Finish.
Then, you have to create the two users, user-p1 and user-p2, and you have to assign the users to the groups that you created for them.

To create users

1. Navigate to System > User Administration > Users, and then click Add.
2. On the Create System User page, specify the user name and password, and then assign the user to a group by adding the group name from the Available list to the Configured list.
3. Click Create.
Now log out and log on with user-p1 credentials. You can view and manage only the admin partitions assigned to you to manage and monitor.
Monitor Globally Distributed Data Centers

Nov 21, 2016

As a network administrator, you might have to monitor and manage network instances deployed across geographical locations. However, it is not easy to gauge the requirements of the network when managing network instances in geographically distributed datacenters.

Geomaps in NetScaler MAS provides you with a graphical representation of your datacenters and breaks down your network monitoring experience by geography. With geomaps, you can visualize your network instance distribution by location and monitor network issues.

For example, if you have network instances deployed in three datacenters in Santa Clara (USA), Bangalore (India), and Kingston (Australia), the geomap on the Infrastructure > Dashboard page provides a visual representation of these datacenters on the world map as shown in the image below. The blue markers represent the cities where the network instances are deployed.

When you hover your mouse pointer over a marker (for example, Santa Clara), you can view the high-level details of the number of instances deployed at that location. In the following image, there are twenty instances deployed at Santa Clara. You can also view the number of critical and major events raised on the instances at that location.
Click the marker on Santa Clara to view the list of critical and major events raised on the instances located here as shown in the image below.

Click the **Instances** tab to view the IP address of each network instance, the type of instance, such as NetScaler VPX or NetScaler SDX, and the number of events raised on an instance.
Before configuring a data center that you can view on geomaps, you must create IP blocks, so that NetScaler MAS can recognize which data center an instance belongs to when it is added to the NetScaler MAS server.

A NetScaler MAS data center is a logical grouping of NetScaler instances in a specific geographical location. You can have several NetScaler instances within a data center that can be monitored and managed by the NetScaler MAS server. You can use the NetScaler MAS server to manage data such as syslog, appflow, and SNMP etc from the managed instances.

Before configuring a data center, you must create IP blocks, so that NetScaler MAS can recognize which data center an instance belongs to when it is added to the NetScaler MAS server. For example, if the instance's IP address falls within the range of an IP block associated with Data Center 1, the instance being added to NetScaler MAS is known to be located in Data Center 1.

To create an IP block

1. Navigate to Infrastructure > Data Centers > IP Blocks, and then click Add.
2. In Configure IP Blocks, specify the name of the IP block and the starting and ending IP addresses in the IP block. Then, specify the country, region, and city. You might have to specify the latitude and longitude of the city if it is not already saved in the geo database.
3. Click Create to finish.

To configure a data center

1. Navigate to Infrastructure > Data Centers, and then click Add.
2. In Configure Data Center, specify the name of the data center.
3. From the list of available IP blocks, select one or more blocks to associate with the data center.
4. Click Create.

For more information on adding NetScaler instances to NetScaler MAS, see Adding an Instance to NetScaler MAS.
Configuration Jobs: Use Record-and-Play to Create Configuration templates

Dec 27, 2016

If you are accustomed to using the NetScaler GUI to configure a NetScaler instance, at times, you might find it difficult to recall the exact CLI commands to create a configuration task and run it on multiple NetScaler instances.

NetScaler MAS enables you to record the configuration tasks performed using the GUI of a NetScaler instance and convert it into CLI commands. You can then create a configuration task from these CLI commands and run this task on multiple instances.

1. Navigate to Infrastructure > Configuration Jobs, and then click Create Job.

2. Specify the job name and the type of instance.

3. From the Configuration Source list, select Record and Play, and then select the source instance from which you want to record the configuration. Click Record.

4. The NetScaler GUI opens. Configure the features and settings that you want the configuration task to contain. Then, close the NetScaler GUI window and click Stop in the Configuration Editor. The commands appear as a link in the left pane. Drag and drop the commands to the right pane, and then click Next.
5. Click **Add Instances** and select the instances on which you want to run the configuration job. Click **OK**, and then click **Next**.

6. If you have specified variables in the commands, on the **Specify Variable Values** tab, click **Download Input Key File**. In the downloaded file, specify values for the variables, and then upload the file to NetScaler MAS.

7. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

8. On the **Execute** tab, specify how and when you want to run the commands, and click **Finish**.
9. On the Jobs page, you can then view the progress of your configuration task execution on all the instances.
Configuration Jobs: Replicate Configuration from One Instance to Multiple Instances

Dec 27, 2016
You might have configured both load balancing and front-end optimization (FEO) on a NetScaler instance for your deployment. However, now you want to replicate only the FEO configuration to other NetScaler instances.

You can use the Configuration Jobs feature of NetScaler MAS to extract the FEO configuration from a NetScaler instance and replicate it on multiple instances.

To retrieve and replicate configuration from one instance to other NetScaler Instances

1. Navigate to Infrastructure > Configuration Jobs, and then click Create Job.

2. Specify the job name and the type of instance.

3. Select Instance as the Configuration Source, select the source instance whose configuration you want to replicate, select the time period when you had run this configuration, and then click Extract.

The number of commands executed on that instance in the time duration you selected is displayed on the screen as highlighted in the image below.
4. Drag and drop the commands to the **Commands** field in the right pane.

    Retain only the commands related to FEO and manually delete the commands related to load balancing, or commands related to any other configuration, and then click **Next**.
6. Click **Add Instances** and add the instances on which you want to apply the FEO configuration. Click **OK**, and then, click **Next**.

If you have specified variables in the commands, on the Specify Variable Values tab, click **Download Input Key File**. In the downloaded file, specify values for the variables, and then upload the file to NetScaler MAS.

On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

On the **Execute** tab, click **Finish** to execute the job on the selected NetScaler instances.
Get Configuration Advice on Network Configuration

Jun 30, 2016

You set up your NetScaler instances with optimal configurations so that you can achieve optimal performance on your applications. However, it may happen that some configurations might not be standard configurations and this might affect the performance of your applications.

To help you optimize your application performance, NetScaler MAS analyzes the NetScaler instance configuration and provides you with recommendations. You can apply the recommended configurations from NetScaler MAS.

To analyze the NetScaler instance

1. Navigate to **Infrastructure > Configuration Audit > Configuration Advice**.
2. Do one of the following:
   - Click **Upload Configuration File** and upload the configuration file of your network instance.
   - Click **Select Device** and select the NetScaler instance that you want to analyze.

NetScaler MAS analyzes the configuration on your instance and provides a list of configuration recommendations as shown in the image below. Click the check box next to a configuration advice to view the corrective commands.
If you want to update your configuration, specify the values for the variables in the corrective commands and click **Apply Now** as shown in the image below.

When the command is successfully run on the network instance, the check box next to the advice disappears.

If you want to view the details of the commands run on your network instance, navigate to **Infrastructure > Instances > <Instance_Type>**, select the IP address of the instance, and then click **Events** from the **Actions** drop-down list.
On the **Events** page, you can view the details of the configuration change.
Optimize Resource Usage by Monitoring Your Network Performance

Jun 30, 2016

You may have a distributed deployment with many applications deployed at multiple locations. To ensure optimal performance of your applications, you have also deployed multiple NetScaler instances to load balance, content switch, or compress the traffic. The application performance can be impacted by network performance. To continue to maintain performance of your applications, you have to regularly monitor your network performance and make sure all resources are used optimally.

For example, you may want to monitor the client and server connections so that you can gather data about the number of active and idle connections. You can then disconnect idle client connections and free up your resources.

To view performance reports on client and server connections

Navigate to Analytics > Network Reporting. In Report Name, select the report Client – Server connections. Specify the instance and the load balancing virtual server on which you want to monitor the connection statistics.

Following is an example of a report generated of client versus server connections for a period of one hour on a specific instance and a specific virtual server.

![Example of a report generated of client versus server connections](image-url)
Again, you may want to determine at what rate the NetScaler instance is processing traffic. Based on the throughput distribution you can decide whether you need to upgrade your resources or not.

**To view performance reports on throughput distribution**

Navigate to Analytics > Network Reporting, and select the report Throughput Distribution. Specify the instance and the load balancing virtual server on which you want to monitor the statistics.

Following is an example of a report generated of throughput distribution for a period of one day on a specific instance and a specific virtual server.
Audit Configuration Changes Across Instances

Dec 27, 2016

You want to make sure that certain configurations are running on specific instances for optimal performance of your network. You also want to monitor configuration changes across managed NetScaler instances, troubleshoot configuration errors, and recover unsaved configurations after a sudden system shutdown.

You can create audit templates with specific configurations you want running on certain instances. The NetScaler MAS compares these instances with the audit template and reports if there is a mismatch in configuration. This enables you to troubleshoot and rectify the errors.

To create audit templates

1. Navigate to Infrastructure > Configuration Audit > Audit Templates, and click Add.
2. On the Create Template page, specify the template name and its description.
3. In the Configuration Editor, type in your commands. Click Next.
4. Select the instances on which you want this configuration to be available. Click Finish.

The audit template appears in the Audit Templates list and is run every 12 hours against the configurations in the specified instances.
You can also use the Configuration Audit dashboard to view high-level details about configuration changes such as the top ten instances by configuration change or the number of saved and unsaved configurations.

You can also force an audit on an instance. To do so, click the **NetScaler Config Saved Status** chart or **NetScaler Config Drift** chart. On the **Audit Reports** page, select the instance and, in the **Action** list, select **Poll Now**.
To set configuration audit notifications

1. Navigate to **Infrastructure > Configuration Audit**.
2. On the **Configuration Audit** page, click **Settings**.
3. On the **Notification Settings** page, click the **Edit** icon, to enable the notification settings.
4. Select the **Enabled** check box and then, choose an email distribution list from the drop-down list. You can also create an email distribution list by clicking the **+** icon and specifying email server details.
Analytics: Web Insight

Jul 05, 2016
Web Insight enables visibility into enterprise web applications and allows IT administrators to monitor all web applications being served by the NetScaler ADC by providing integrated and real-time monitoring of applications. Web Insight provides critical information such as user and server response time, enabling IT organizations to monitor and improve application performance.

This document includes the following:

- Latency in Applications
- Inaccessibility Issues
- Thresholds
- Browsers and Operating Systems
- End User Experience
- Geomaps

Latency in Applications

As an administrator, you can now identify the source of latency issues faced by users while accessing web applications. You can determine whether the issue is occurring on the server side of the network, the client side of the network, or on the application server itself.

Using NetScaler MAS, you can locate the issue by navigating to Dashboard > Applications and selecting an application. The response time for an application is typically broken down into 3 sub-parts to show whether the problem is a client network latency issue, server network latency issue, or an overloaded or malfunctioning server.

You can also see which specific server has highest server processing time for that application.

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved. p.388
Inaccessibility Issues

As an administrator, you can now see which application servers are currently generating erroneous response codes, such as unauthorized, bad request, or page not found, so that you can take appropriate corrective measures.

Navigate to Dashboard > Response Status, and click on a specific error code (such as Unauthorized) to identify which application servers sent that response code.

Thresholds

Administrators can use Web Insight to configure thresholds and notify users about threshold breaches. In a typical deployment, you can automate the process of tracking various application metrics, to facilitate planning and be notified whenever the applications metric value exceeds the set threshold. You can set thresholds for any metric, such as hits, bandwidth, or response time.

For example, you can configure a threshold for response time. When the response time of a particular application exceeds the threshold value, you will receive a notification on your dashboard. Also, under Threshold Breaches, your dashboard displays a list of threshold breaches that have occurred for a specific duration (such as Today).

To configure a new threshold, navigate to System > Analytics Settings > Thresholds, and click Add.
Browsers and Operating Systems

You can use Web Insight to help you segregate L7 latency issues and understand mobile device usage uptake. This can help you, as an administrator, to understand different operating system uptakes across your user base.

You can go to the Browser pane to see why there is slowness in user access and if it is due to incompatibility across certain browsers. You can also see which operating systems are being used across certain clients, and the browsers being accessed. You can compare the rendered time across the different browsers and further drill-down to particular a browser to identify which application pages are associated with the highest rendering time for that browser.

For example, you can select Google Chrome and see the corresponding rendering times for the different URL pages for a particular application.

End-User Experience

End-user experience can be analyzed by looking at metrics such as load time and render time. Higher load times and render times create a negative end-user experience.
To view the render time and load time for the URLs in an application, navigate to Dashboard > URLs. You can see the list of URLs and their corresponding load times and rendering times in a table or as a graph. You can then tune the corresponding web pages to reduce wait time and improve the overall end-user experience.

Geomaps

Your clients using Web Insight might be spread out across distributed geographies, making it difficult for you, as the administrator, to identify their geographical locations.

Using NetScaler MAS Geomaps feature, you can understand the origination and distribution of traffic from different geographic regions, the regions with the highest number of hits, and the number of hits coming from each country in a region. You can also drill-down to a particular region to see the number of hits from that region, the bandwidth used, and the response times.
You can monitor the NetScaler Integrated Caching (IC) using NetScaler MAS. Cache Insight enables you to see and monitor the various actions performed by the NetScaler cache. For example, you can view the cache analytics on the devices, applications, content type, URLs, etc on your Netscaler Cache.

You can find the following cache metrics details in NetScaler MAS:

- **Integrated Cache Utilization.** Data, in bytes, sent from the NetScaler cache to serve requests.
- **Integrated Cache Hits.** Number of client requests served from the NetScaler cache.
- **Integrated Cache Refreshes.** Number of revalidations of cache data during a specified time frame.
- **Integrated Cache Misses (Storable).** Number of client requests that could not be served from the cache.
  
  **Note:** The response received from the origin server for this requests will be stored in the integrated cache.

- **Integrated Cache Misses (Non-Storable).** Number of client requests that could not be served from the cache.
  
  These requests might be affected by a policy, response size, minimum hits, or so on, specifying not to store the data in the cache.

- **Uncached Resources.** Reasons not storing an object in the cache (for example, policy, size of object, cache bypass).

**Cache Insight Inter-operability**

**Note**

Integrated Cache Metrics are not supported on NetScaler MAS with NetScaler appliances running on version 10.5 and below.

<table>
<thead>
<tr>
<th>NetScaler Version</th>
<th>NetScaler MAS version</th>
<th>Supportable Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>11.1</td>
<td>Cache Metrics, Web Insight Reports</td>
</tr>
<tr>
<td>Below 11.0 66.x (Eg 65.x)</td>
<td>11.1</td>
<td>Cache Metrics, Web Insight Reports</td>
</tr>
<tr>
<td>11.0 66.x</td>
<td>11.1</td>
<td>Web Insight Reports</td>
</tr>
</tbody>
</table>

**Configuring Cache Insight**

**Important Notes:**

- You need to install an Integrated Cache (IC) license on the NetScaler appliance before you enable this feature.
- You need to set a memory limit for the NetScaler cache after enabling the integrated caching.
Cache Metrics are displayed as a part of Web Insight reports. You need to enable AppFlow for Web Insight to enable Cache Insight.

When you enable integrated caching, the NetScaler appliance begins caching server responses. If you have not configured any policies or content groups, the built-in policies store cached objects in the default content groups. You can configure new policies to allow or restrict objects and object types to cache in NetScaler Integrated Cache.

Install Integrated Cache License

To Install Integrated Cache License by using the command line interface

1. Obtain a license code from Citrix, go to the command line interface, and log in.
2. At the command line interface, copy the license file to the /nsconfig/license folder.
3. Reboot the NetScaler appliance by using the following command:

```command
reboot
```

For information about licenses, see information about obtaining NetScaler licenses at http://support.citrix.com/article/ctx121062.

Enable Integrated Caching

To enable integrated caching by using the command line interface

At the command prompt, type the following command to enable integrated caching:

```command
enable ns feature IC
```

To enable integrated caching by using the configuration utility

Navigate to Configuration > System > Settings, click Configure Basic Features, and select Integrated Caching.

Enable AppFlow Feature

Note

You can enable the Appflow feature either from NetScaler MAS or from the NetScaler instance.
To enable the AppFlow feature from NetScaler MAS

1. In a web browser, type the IP address of the NetScaler Management and Analytics System (for example, http://192.168.100.1).

2. In User Name and Password, enter the administrator credentials.

3. Navigate to Infrastructure > Instances, and select the NetScaler instance you want to enable analytics.

4. From the Action drop-down, select Enable/Disable Insight.

5. Select the virtual servers, and click Enable AppFlow.

6. In the Enable AppFlow field, type true, and select Web Insight.

7. Click Ok.

Note
You cannot enable data collection on a virtual server if the operational state of the virtual server is other than UP.

To enable the AppFlow feature from the NetScaler command line

At the command prompt, type:

```
command

enable ns feature AppFlow
```

To enable the AppFlow feature by using the configuration utility

Navigate to Configuration > System > Settings, click Configure Advanced Features and select AppFlow.

Set Memory Limit

To set memory limit by using the command line interface

At the command prompt, type one of the following commands to enable or disable integrated caching:

```
command

set cache parameter [-memLimit <MBytes>]
```

To set memory limit by using the configuration utility
Navigate to **Configuration > Optimization > Integrated Caching**, click **Change Cache Settings**, and in the **Cache Global Settings** set the **Memory Usage Limit (MB)** field.

For an overview of enabling the integrated caching on a NetScaler appliance, see [Setting Up the Integrated Cache](https://docs.citrix.com).

**Enable Cache Insight Parameter**

**Note**

Enabling cache insight parameter is supported only on CLI.

**To enable cache insight parameter**

At the command prompt, type one of the following commands to enable or disable integrated caching:

```
cmd
appflow param –cacheInsight ENABLED
```

**Configuring a Policy in the Integrated Cache**

You can configure new policies in a NetScaler appliance to handle data that the built-in policies cannot process. You configure separate policies for caching, preventing caching from occurring, and for invalidating cached data.

**To configure a policy for caching by using the command line interface**

At the NetScaler command prompt, type:

```
cmd
```
add cache policy <policyName> -rule <expression> -action CACHE|MAY_CACHE|NOCACHE|MAY_NOCACHE [ -storeInGroup <contentGroupName>] [-undefAction NOCACHE|RESET]

Examples:

> add cache policy image_cache -rule "http.req.url.contains("jpg") || http.req.url.contains("jpeg")" -action CACHE -storeInGroup myImages_group -undefAction NOCACHE


> add cache policy my_form_policy -rule "http.req.header("Host")contains("my.company.com") && http.req.method.eq("GET") && http.req.url.query.contains("v=7")" -action CACHE -storeInGroup my_form_event

> add cache policy viewproducts_policy –rule "http.req.url.contains("viewproducts.aspx")" –action CACHE -storeInGroup Product_Details

To configure a policy for caching by using the configuration utility

1. In a web browser, type the IP address of the NetScaler appliance (for example, http://192.168.100.1).
2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. Navigate to **Optimization** > **Integrated Caching** > **Policies**. and create the new policy.

For an overview of Configuring a Policy in the Integrated Cache, see [Configuring a Policy in the Integrated Cache](https://docs.citrix.com).

**Viewing the Integrated Cache Metrics**

NetScaler MAS cache metrics provide a detailed view of the performance of the NetScaler Integrated Caching. With the help of these metrics, you can analyze and optimize your NetScaler integrated cache and track performance issues.

**To monitor Cache Metrics in NetScaler MAS**

1. On the **Dashboard** tab, navigate to **Web Insight** and click the node for which to display the metrics.
2. In the right pane, select a timeframe from the drop-down list. You can further customize the time frame by using the timeframe slider. Click **Go**.
3. Select the type of metrics you want to see from the drop-down list at the right of the dialog box. The metrics displays bar graphs, which you can click for details.
Use Cases

Reduction of origin server load

You can reduce the load on your origin server by using integrated caching. The integrated cache provides in-memory storage on the Citrix NetScaler appliance and serves web content to users without requiring a round trip to an origin server. The cache metrics show the number of bytes that the origin servers did not have to process.

The total bytes served by the cache can be calculated by the formula \((\text{Bandwidth} - \text{Integrated Cache Utilization})\). You can configure policies to enhance the IC performance.

Improving server time

As a NetScaler administrator, monitoring the cached objects through NetScaler MAS, if you notice that a large number of requests are served by the backend serves, you can configure a policy to cache frequently requested objects. If a policy is already configured not to cache those objects, you will be notified in the Uncached Details section.

For example, if 25 users request the same object, and the object is cacheable, the first user request is classified as Integrated Cache Miss (Storable), and the object returned in the response is stored in the cache memory. The subsequent requests for the same object are served by the integrated cache. This reduces the origin server's load by 24 times. It also reduces the response time, because it eliminates 24 round trips to and from the origin server.
Analysis of all types of requests

In various situations, origin-server header values might not allow some otherwise cacheable objects to be cached in the NetScaler Integrated Cache (IC). With strict header checking, any requests for these types of objects become cache misses. Too many cache misses for cacheable data might decrease server performance to the point that the purpose and utility of integrated caching is lost.

Monitoring how many cacheable requests were cache hits, and observing the content type of cache hits (for example, text file or .js file) can produce a granular analysis that facilitates a solution.

Another possibility is that caching large objects (for example, images larger than 1 MB, or 3.5 MB videos) might consume a large portion of the IC memory, causing numerous requests for smaller cacheable objects to become cache misses. Configuring a policy to not store such objects can reduce the load on the origin servers.

What can a NetScaler Administrator determine by viewing the Integrated Cache Metrics?

As a NetScaler administrator, you can monitor the NetScaler cache through NetScaler MAS. You can view the details such as efficiency of the cache (Integrated Cache Hits), cache misses (Integrated Cache Misses (Storable)), non-storable cache misses (Integrated Cache Misses (non-Storable)), and so on.

With Cache insight, you can view the cache misses that have occurred and can determine whether or not the objects were cacheable. You can also view the policy names that resulted in the failures.

For example, if 70% of the requests resulted in cache misses (Integrated Cache Misses (Storable) and Integrated Cache Misses (Non-Storable)), and 50% of those requests were for objects that can be cached, you can view the Uncached details to identify the policy or configuration causing the cache misses, and take remedial action.
Analytics: HDX Insight

HDX Insight provides end-to-end visibility for ICA traffic passing through NetScaler ADC.

HDX Insight enables administrators to view real-time client and network latency metrics, historical reports, End-to-end performance data, and troubleshoot performance issues.

Availability of both real-time and historical visibility data enables NetScaler MAS to support a wide variety of use cases.

The following Thin Clients support HDX Insight:

- WYSE Windows based Thin Clients
- WYSE Linux based Thin Clients
- WYSE ThinOS based Thin Clients
- 10Zig Ubuntu based Thin Clients

This document includes the following details:

- Identifying the root cause of slow performance issues
- Geo Maps for HDX Insight

Identifying the root cause of slow performance issues

**Scenario 1**

User is experiencing delays while accessing XenApp and XenDesktop.

The delays might be due to latency on the server network, ICA traffic delays caused by the server network, or latency on the client network.

To identify the root cause of the issue, analyze the following metrics:

- WAN Latency
- DC Latency
- Host Delay

**To view the client metrics**

1. On the **Analytics** tab, navigate to **HDX Insight > Users**.
2. Scroll down and select the user name.
3. On the **Current Application Sessions** table, hover the mouse over the **RTT** value and note the host delay, DC latency, and WAN latency values.

On the **Current Application Sessions** table, click the hop diagram symbol to display information about the connection between the client and the server, including latency values.
Summary

In this example, the **DC Latency** is 1 millisecond, the **WAN latency** is 592 milliseconds and **Host Delays** is 0 seconds.

This indicates that the user is experiencing delay due to latency caused by the client network.

**Scenario 2**

User is experiencing delay while launching an application on XenDesktop or XenApp

The delay might be due to latency on the server network, ICA-traffic delays caused by the server network, latency on the client network, or time taken to launch an application.

To identify the root cause of the issue, analyze the following metrics:

- WAN latency
- DC Latency
- Application Launch Duration

**To view the user metrics**

1. On the **Analytics** tab, navigate to **HDX Insight > Users**.
2. Scroll down and click on the user name.
3. In the graphical representation, note the WAN Latency, DC Latency and RTT values for the particular session.
4. In the Current Application Sessions table, click the first session ID.
5. Scroll down, and in the Applications pane, from the dropdown list, select **Launch Duration** to view the time taken for the
Summary

In this example, the **DC Latency** is 1 millisecond, the **WAN latency** is 13 milliseconds, and the **Launch Duration** value of 2.37 seconds. This indicates that the cause for the delay in launching the application is high application launch time.

**Note:** HDX Insight also displays additional user metrics, such as WAN jitter and Server Side Retransmits if you are using NetScaler MAS running software 11.1 build 51.21 or later. To view these metrics, navigate to **Analytics > HDX Insight > Users**, and select a user name. The user metrics appear in the table next to the graph.
Geo Maps for HDX Insight

The NetScaler MAS geo maps functionality displays the usage of applications across different geographical locations on a map. Administrators can use this information to understand the trends in application usage across various geographical locations.

You can configure NetScaler MAS to display the geo maps for a particular geographical location or LAN by specifying the private IP range (start and end IP address) for the location.

To configure a geo map for data centers

On the **Infrastructure** tab, navigate to **Dashboard** and click **Data Centers** to configure geo maps for a particular location.

**Use Case**

Consider a scenario in which organization ABC has 2 branch offices, one in Santa Clara and the other in India.
The Santa Clara users use the NetScaler Gateway appliance at SClara.x.com to access VPN traffic. The Indian users use the NetScaler Gateway appliance at India.x.com to access VPN traffic.

During a particular time-interval, say 10 AM to 5 PM, the users in Santa Clara connect to SClara.x.com to access VPN traffic. Most of the users access the same NetScaler Gateway, causing a delay in connecting to the VPN, so some users connect to India.x.com instead of SClara.x.com.

A NetScaler administrator analyzing the traffic can use the geo map functionality to show the traffic in Santa Clara office. The map shows that the response time in the Santa Clara office is very high, because the Santa Clara office has only one NetScaler Gateway appliance through which users can access VPN traffic. The administrator might therefore decide to install another NetScaler Gateway, so that users have two local NetScaler Gateway appliances through which to access the VPN.

Limitations

If NetScaler instances have Enterprise license, thresholds set on NetScaler MAS for HDX Insight will not be triggered since analytical data is collected for only 1 hour.
Enabling HDX Insight Data Collection

Oct 01, 2016

HDX Insight enables IT to deliver an exceptional user experience by providing unprecedented end-to-end visibility into the ICA traffic that passes through the NetScaler instances or CloudBridge appliances, and is a part of NetScaler MAS Analytics. HDX Insight delivers compelling and powerful business intelligence and failure analysis capabilities for the network, virtual desktops, applications and application fabric. HDX Insight can both instantly triage on user issues, collects data about virtual desktop connections, and generates AppFlow records and presents them as visual reports.

The configuration to enable data collection in the NetScaler differs with the position of the appliance in the deployment topology. This topic includes the following details:

- Enabling Data Collection for Monitoring NetScaler ADCs Deployed in Transparent Mode
- Enabling Data Collection for NetScaler Gateway Appliances Deployed in Single-Hop Mode
- Enabling Data Collection for NetScaler Gateway Appliances Deployed in Double-Hop Mode
- Enabling Data Collection for Monitoring NetScaler ADCs Deployed in LAN User Mode
Enabling Data Collection for Monitoring NetScaler ADCs Deployed in Transparent Mode

Oct 01, 2016

When a NetScaler ADC is deployed in transparent mode the clients can access the servers directly, with no intervening virtual server. If a NetScaler appliance is deployed in transparent mode in a XenApp/XenDesktop environment, the ICA traffic is not transmitted over a VPN.

After you add the NetScaler ADC to the NetScaler MAS inventory, you must enable AppFlow for data collection. Enabling data collection depends on the device and the mode. In that case, you have to add NetScaler MAS as an AppFlow collector on each NetScaler appliance, and you must configure an AppFlow policy to collect all or specific ICA traffic that flows through the appliance.

Note

- You cannot enable data collection on a NetScaler ADC deployed in transparent mode by using the NetScaler MAS configuration utility.
- For detailed information about the commands and their usage, see Command Reference.
- For information on policy expressions, see Policies and Expressions.

The following figure shows the network deployment of a NetScaler MAS when a NetScaler ADC is deployed in a transparent mode:

To configure data collection on a NetScaler appliance by using the command line interface

At the command prompt, do the following:

1. Log on to an appliance.
2. Specify the ICA ports at which the NetScaler appliance listens for traffic.
   ```plaintext
going set ns param --icaPorts <port>...
```
   **Example:**
   ```plaintext
going set ns param -icaPorts 2598 1494
```
   **Note:**
   - You can specify up to 10 ports with this command.
   - The default port number is 2598. You can modify the port number as required.

3. Add NetScaler Insight Center as an appflow collector on the NetScaler appliance.
   ```plaintext
going add appflow collector <name> -IPAddress <ip_addr>
```
   **Example:**
   ```plaintext
going add appflow collector MyInsight -IPAddress 192.168.1.101
```
   **Note:** To view the appflow collectors configured on the NetScaler appliance, use the `show appflow collector` command.

4. Create an appflow action and associate the collector with the action.
   ```plaintext
going add appflow action <name> -collectors <string> ...
```
   **Example:**
   ```plaintext
going add appflow action act -collectors MyInsight
```

5. Create an appflow policy to specify the rule for generating the traffic.
   ```plaintext
going add appflow policy <policyname> <rule> <action>
```
   **Example:**
   ```plaintext
going add appflow policy pol true act
```

6. Bind the appflow policy to a global bind point.
   ```plaintext
going bind appflow global <policyname> <priority> -type <type>
```
   **Example:**
   ```plaintext
going bind appflow global pol 1 -type ICA_REQ_DEFAULT
```
   **Note:** The value of `type` should be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT in order to apply to ICA traffic.

7. Set the value of the flowRecordInterval parameter for Appflow to 60 seconds.
   ```plaintext
going set appflow param -flowRecordInterval 60
```
   **Example:**
   ```plaintext
going set appflow param -flowRecordInterval 60
```

8. Save the configuration. `save ns config`
Enabling Data Collection for NetScaler Gateway Appliances Deployed in Single-Hop Mode

Oct 01, 2016

When NetScaler Gateway is deployed in single-hop mode, the NetScaler Gateway is at the edge of the network and proxies ICA connections to the desktop delivery infrastructure. This is the simplest and most common deployment. This mode provides security if an external user tries to access the internal network in an organization.

In single-hop mode, users access the NetScaler appliances through a virtual private network (VPN).

To start collecting the reports, you must add the NetScaler Gateway appliance to the NetScaler MAS inventory and enable AppFlow on NetScaler MAS.

Figure 2. NetScaler MAS deployed in single-hop mode

To enable the AppFlow feature from NetScaler MAS

1. In a web browser, type the IP address of the NetScaler Management and Analytics System (for example, http://192.168.100.1).
2. In User Name and Password, enter the administrator credentials.
3. Navigate to Infrastructure > Instances, and select the NetScaler instance you want to enable analytics.
4. From the Action drop-down, select Enable/Disable Insight.
5. Select the VPN virtual servers, and click Enable AppFlow.
6. In the **Enable AppFlow** field, type **true**, and select **ICA**.

7. Click **OK**.

Note: The following commands are executed in the background when you enable AppFlow in single-hop mode. These commands are explicitly specified here for troubleshooting purposes.

- add appflow collector <name> -IPAddress <ip_addr>
- add appflow action <name> -collectors <string>
- set appflow param -flowRecordInterval <secs>
- disable ns feature AppFlow
- enable ns feature AppFlow
- add appflow policy <name> <rule> <expression>
- set appflow policy <name> -rule <expression>
- bind vpn vserver <vsname> -policy <string> -type <type> -priority <positive_integer>
- set vpn vserver <name> -appflowLog ENABLED
- save ns config
Enabling Data Collection for NetScaler Gateway Appliances Deployed in Double-Hop Mode

Oct 01, 2016

The NetScaler Gateway double-hop mode provides additional protection to an organization’s internal network because an attacker would need to penetrate multiple security zones or Demilitarized zones (DMZ) to reach the servers in the secure network. If you want to analyze the number of hops (NetScaler Gateway appliances) through which the ICA connections pass, and also the details about the latency on each TCP connection and how it fairs against the total ICA latency perceived by the client, you must install NetScaler MAS so that the NetScaler Gateway appliances report these vital statistics.

Figure 3. NetScaler MAS deployed in double-hop mode

The NetScaler Gateway in the first DMZ handles user connections and performs the security functions of an SSL VPN. This NetScaler Gateway encrypts user connections, determines how the users are authenticated, and controls access to the servers in the internal network.

The NetScaler Gateway in the second DMZ serves as a NetScaler Gateway proxy device. This NetScaler Gateway enables the ICA traffic to traverse the second DMZ to complete user connections to the server farm.

The NetScaler MAS can be deployed either in the subnet belonging to the NetScaler Gateway appliance in the first DMZ or the subnet belonging to the NetScaler Gateway appliance second DMZ. In the above image, the NetScaler MAS and NetScaler Gateway in the first DMZ are deployed in the same subnet.

In a double-hop mode, NetScaler MAS collects TCP records from one appliance and ICA records from the other appliance. After you add the NetScaler Gateway appliances to the NetScaler MAS inventory and enable data collection, each of the appliances export the reports by keeping track of the hop count and connection chain ID.

NetScaler MAS uses the hop count and connection chain ID to co-relate the data from both the NetScaler Gateway appliances and generates the reports.

To monitor NetScaler Gateway appliances deployed in this mode, you must first add the NetScaler Gateway to NetScaler MAS inventory, enable AppFlow on NetScaler MAS and then view the reports on the NetScaler MAS dashboard.

Enabling Data Collection on NetScaler MAS

If you enable NetScaler MAS to start collecting the ICA details from both the appliances, the details collected are redundant. That is both the appliances report the same metrics. To overcome this situation, you must enable AppFlow for ICA on one of the first NetScaler Gateway appliance, and then enable AppFlow for TCP on the second appliance. By doing so, one of the appliances export ICA AppFlow records and the other appliance exports TCP AppFlow records. This also saves the processing time on parsing the ICA traffic.

To enable the AppFlow feature from NetScaler MAS

1. In a web browser, type the IP address of the NetScaler Management and Analytics System (for example, http://192.168.100.1).
2. In User Name and Password, enter the administrator credentials.
3. Navigate to Infrastructure > Instances, and select the NetScaler instance you want to enable analytics.
4. From the Action drop-down, select Enable/Disable Insight.
5. Select the VPN virtual servers, and click Enable AppFlow.
6. In the Enable AppFlow field, type true, and select ICA/TCP for ICA traffic and TCP traffic respectively.
   
   Note: If AppFlow logging is not enabled for the respective services or service groups on the NetScaler appliance, the NetScaler MAS dashboard does not display the records, even if the Insight column shows Enabled.
7. Click OK.
Configuring NetScaler Gateway Appliances to Export Data

After you install the NetScaler Gateway appliances, you must configure the following settings on the NetScaler gateway appliances to export the reports to NetScaler MAS:

- Configure virtual servers of the NetScaler Gateway appliances in the first and second DMZ to communicate with each other.
- Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ.
- Enable double hop on the NetScaler Gateway in the second DMZ.
- Disable authentication on the NetScaler Gateway virtual server in the second DMZ.
- Enable one of the NetScaler Gateway appliances to export ICA records.
- Enable the other NetScaler Gateway appliance to export TCP records.
- Enable connection chaining on both the NetScaler Gateway appliances.

Configuring NetScaler Gateway Using the Command Line Interface

1. Configure the NetScaler Gateway virtual server in the first DMZ to communicate with the NetScaler Gateway virtual server in the second DMZ.

   ```
   add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (ON|OFF)] [-imgGifToPng] ...
   ```

   ```
   add vpn nextHopServer nh1 10.102.2.33 8443 -secure ON
   ```

2. Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ. Run the following command on the NetScaler Gateway in the first DMZ:

   ```
   bind vpn vserver <name> -nextHopServer <name>
   ```

   ```
   bind vpn vserver vs1 -nextHopServer nh1
   ```

3. Enable double hop and AppFlow on the NetScaler Gateway in the second DMZ.

   ```
   set vpn vserver <name> [-doubleHop ( ENABLED |DISABLED )] [-appflowLog ( ENABLED |DISABLED )]
   ```

   ```
   set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
   ```

4. Disable authentication on the NetScaler Gateway virtual server in the second DMZ.

   ```
   set vpn vserver <name> [-authentication (ON|OFF)]
   ```

   ```
   set vpn vserver vs -authentication OFF
   ```

5. Enable one of the NetScaler Gateway appliances to export TCP records.

   ```
   bind vpn vserver <name> [-policy <string>] [-priority <positive_integer>] [-type <type>]
   ```

   ```
   bind vpn vserver vpn1 -policy appflowpol1 -priority 101 -type OTHERTCP_REQUEST
   ```

6. Enable the other NetScaler Gateway appliance to export ICA records.

   ```
   bind vpn vserver <name> [-policy <string>] [-priority <positive_integer>] [-type <type>]
   ```

   ```
   bind vpn vserver vpn2 -policy appflowpolp1 -priority 101 -type ICA_REQUEST
   ```

7. Enable connection chaining on both the NetScaler Gateway appliances:

   ```
   set appflow param -connectionChaining (ENABLED |DISABLED)
   ```

   ```
   set appflow param -connectionChaining ENABLED
   ```

Configuring NetScaler Gateway using Configuration Utility

1. On the Configuration tab expand NetScaler Gateway and click Virtual Servers.
2. In the right pane, double-click the virtual server, and in the Advanced group, expand Published Applications.
3. Click Next Hop Server and bind a next hop server to the second NetScaler Gateway appliance.
4. Enable double hop on the NetScaler Gateway in the second DMZ.
5. On the Configuration tab expand NetScaler Gateway and click Virtual Servers.
6. In the right pane, double-click the virtual server, and in the Basic Settings group, click the edit icon.
3. Expand More, select Double Hop and click OK.
4. Enable the other NetScaler Gateway appliance to export TCP records.
   1. On the Configuration tab expand NetScaler Gateway and click Virtual Servers.
   2. In the right pane, double-click the virtual server, and in the Advanced group, expand Policies.
   3. Click the + icon and in the from the Choose Policy drop-down list, select AppFlow and from the Choose Type drop-down list, select Other TCP Request.
   4. Click Continue.
   5. Add a policy binding, and click Close.

5. Enable connection chaining on both the NetScaler Gateway appliances.
   1. On the Configuration tab, navigate to System > Appflow.
   2. In the right pane, in the Settings group, click on Change Appflow Settings.
   3. Select Connection Chaining and Click OK.

   - Double hop on the NetScaler Gateway in the first DMZ.
     1. On the Configuration tab expand NetScaler Gateway and click Virtual Servers.
     2. In the right pane, double-click the virtual server, and in the Advanced group, expand Published Applications.
     3. Click Next Hop Server and bind a next hop server to the second NetScaler Gateway appliance.

   - Disable authentication on the virtual server on the NetScaler Gateway in the second DMZ.
     1. On the Configuration tab expand NetScaler Gateway and click Virtual Servers.
     2. In the right pane, double-click the virtual server, and in the Basic Settings group, click the edit icon.
     3. Expand More, select Double Hop and click OK.

   - Add authentication on the virtual server on the NetScaler Gateway in the second DMZ.
     1. On the Configuration tab expand NetScaler Gateway and click Virtual Servers.
     2. In the right pane, double-click the virtual server, and in the Basic Settings group, click the edit icon.
     3. Expand More, and uncheck Enable Authentication.

   - Add one of the NetScaler Gateway appliance to export TCP records.
     1. On the Configuration tab expand NetScaler Gateway and click Virtual Servers.
     2. In the right pane, double-click the virtual server, and in the Advanced group, expand Policies.
     3. Click the + icon and in the from the Choose Policy drop-down list, select AppFlow and from the Choose Type drop-down list, select Other TCP Request.
     4. Click Continue.
     5. Add a policy binding, and click Close.

   - Enable connection chaining on both the NetScaler Gateway appliances.
     1. On the Configuration tab, navigate to System > Appflow.
     2. In the right pane, in the Settings group, click on Change Appflow Settings.
     3. Select Connection Chaining and Click OK.
Enabling Data Collection for Monitoring NetScaler ADCs Deployed in LAN User Mode

Oct 01, 2016

External users who access XenApp or XenDesktop applications must authenticate themselves on the NetScaler Gateway. Internal users, however, might not require to be redirected to the NetScaler Gateway. Also, in a transparent mode deployment, the administrator must manually apply the routing policies, so that the requests are redirected to the NetScaler appliance.

To overcome these challenges, and for LAN users to directly connect to XenApp and XenDesktop applications, you can deploy the NetScaler appliance in a LAN user mode by configuring a cache redirection virtual server, which acts as a SOCKS proxy on the NetScaler Gateway appliance.

![Figure 4. NetScaler MAS deployed in LAN User Mode](image)

**Note:** NetScaler MAS and NetScaler Gateway appliance reside in the same subnet.

To monitor NetScaler appliances deployed in this mode, first add the NetScaler appliance to the NetScaler Insight inventory, enable AppFlow and then view the reports on the dashboard.

After you add the NetScaler appliance to the NetScaler MAS inventory, you must enable AppFlow for data collection.

**Note**
- You cannot enable data collection on a NetScaler ADC deployed in LAN User mode by using the NetScaler MAS configuration utility.
- For detailed information about the commands and their usage, see Command Reference.
- For information on policy expressions, see Policies and Expressions.
To configure data collection on a NetScaler appliance by using the command line interface

At the command prompt, do the following:

1. Log on to an appliance.

2. Add a forward proxy cache redirection virtual server with the proxy IP and port, and specify the service type as HDX.

   ```
   add cr vserver <name> <servicetype> <ipaddress> <port> [-cacheType <cachetype>] [-cltTimeout <secs>]
   ```

   Example

   ```
   add cr vserver cr1 HDX 10.12.2.2 443 –cacheType FORWARD –cltTimeout 180
   ```

   Note: If you are accessing the LAN network by using a NetScaler Gateway appliance, add an action to be applied by a policy that matches the VPN traffic.

   ```
   add vpn trafficAction <name> <qual> [-HDX ( ON | OFF )]
   ```

   Example

   ```
   add vpn trafficAction act1 tcp -HDX ON
   ```

   ```
   add vpn trafficPolicy <name> <rule> <action>
   ```

   Example

   ```
   add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
   ```

3. Add NetScaler MAS as an appflow collector on the NetScaler appliance.

   ```
   add appflow collector <name> -IPAddress <ip_addr>
   ```

   Example:

   ```
   add appflow collector MyInsight -IPAddress 192.168.1.101
   ```

4. Create an appflow action and associate the collector with the action.

   ```
   add appflow action <name> -collectors <string> ...
   ```

   Example:

   ```
   add appflow action act -collectors MyInsight
   ```

5. Create an appflow policy to specify the rule for generating the traffic.

   ```
   add appflow policy <policyname> <rule> <action>
   ```

   Example:

   ```
   add appflow policy pol true act
   ```

6. Bind the appflow policy to a global bind point.

   ```
   bind appflow global <policyname> <priority> -type <type>
   ```

   Example:
bind appflow global pol 1 -type ICA_REQ_DEFAULT

**Note:** The value of type should be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT in order to apply to ICA traffic.

7. Set the value of the flowRecordInterval parameter for Appflow to 60 seconds.
   
   `set appflow param -flowRecordInterval 60`

   Example:
   
   `set appflow param -flowRecordInterval 60`

8. Save the configuration.
   
   `save ns config`
Analytics: Gateway Insight

Nov 09, 2017

In a NetScaler Gateway deployment, visibility into a user's access details is essential for troubleshooting access failure issues. As the network administrator, you want to know when a user is not able to log on to NetScaler Gateway, and you want to know the user activity and the reasons for logon failure, but that information is typically not available unless the user sends a request for resolution.

Gateway Insight provides visibility into the failures encountered by all users, regardless of the access mode, at the time of logging on to NetScaler Gateway. You can view a list of all available users, number of active users, number of active sessions, and bytes and licenses used by all users at any given time. You can view the end-point analysis (EPA), authentication, single sign-on (SSO), and application launch failures for a user. You can also view the details of active and terminated sessions for a user.

Gateway Insight also provides visibility into the reasons for application launch failure for virtual applications. This enhances your ability to troubleshoot any kind of logon or application launch failure issues. You can view the number of applications launched, number of total and active sessions, the number of total bytes and bandwidth consumed by the applications. You can view details of the users, sessions, bandwidth, and launch errors for an application.

You can view the number of gateways, number of active sessions, total bytes and bandwidth used by all gateways associated with a NetScaler Gateway appliance at any given time. You can view the EPA, authentication, single sign-on, and application launch failures for a gateway. You can also view the details of all users associated with a gateway and their logon activity.

All log messages are stored in the NetScaler MAS database, so you can view error details for any time period. You can also view a summary of the logon failures and determine at what stage of the logon process a failure has occurred.

Points to Note

- Gateway Insight is supported on the following deployments:
  1. High Availability
  2. Unified Gateway
- The NetScaler MAS release and build must be same or later than that of the NetScaler Gateway appliance.
- One hour of Gateway Insight reports can be viewed for NetScaler instances with Enterprise license. A Platinum license is needed to view Gateway Insight reports beyond one hour.

Limitations

- Successful user logons, latency, and application-level details for virtual ICA applications and desktops are visible only on the HDX Insight Users dashboard.
- In a double-hop mode, visibility into failures on the NetScaler Gateway appliance in the second DMZ is not available.
- Remote Desktop Protocol (RDP) desktop access issues are not reported.
- The Gateway Insight records for the SAML authentication are not reported.

Enabling Gateway Insight

To enable Gateway Insight for your NetScaler Gateway appliance, you must first add the NetScaler Gateway appliance to NetScaler MAS. You must then enable AppFlow for the virtual server representing the VPN application. For information about adding device to NetScaler MAS, see Adding Devices.
Note
To view end-point analysis (EPA) failures in NetScaler MAS, you must enable AppFlow AAA Username logging on the NetScaler Gateway appliance.

To enable AppFlow for a virtual server in NetScaler MAS

1. Log on to NetScaler MAS.
2. On the **Infrastructure** tab, navigate to **Instances**, and select the instance for which you want to enable AppFlow.
3. From the **Action** drop-down, select **Enable/Disable Insight**.
4. In the **Configure Insight** page, under **Application List**, in the **View** list, select **VPN**.
5. Select the virtual server for which you want to enable AppFlow, and in the **Action** list, click **Enable AppFlow**.
6. On the **Enable AppFlow** screen, in the **Select Expression** list, click true.
7. Next to **Export Option**, select the **HTTP** check box.
8. Click OK.

To enable AppFlow AAA Username logging on a NetScaler Gateway appliance by using the CLI

At the command prompt, type:

```
set appflow param -AAAUserName ENABLED
```

To enable AppFlow AAA Username logging on a NetScaler Gateway appliance by using the GUI

1. Navigate to **Configuration > System > AppFlow > Settings**, and then click **Change AppFlow Settings**.
2. In the **Configure AppFlow Settings** screen, select **AAA Username**, and then click OK.

Viewing Gateway Insight Reports
In NetScaler MAS, you can view reports for all users, applications, and gateways associated with the NetScaler Gateway appliances, and you can view details for a particular user, application, or gateway. In the Overview section, you can view the EPA, SSO, Authentication, and Application Launch failures. You can also view a summary of the different session modes used by users to log on, the types of clients, and the number of users logged on every hour.

To view EPA, SSO, Authentication, Authorization and Application Launch Failures

1. In NetScaler MAS, navigate to Analytics > Gateway Insight.

2. Select the time period for which you want to view the user details. You can use the time slider to further customize the selected period. Click Go.

3. Click the EPA (End Point Analysis), Authentication, Authorization, SSO (Single Sign On), or Application Launch tabs to display the failure details.

To view a summary of session modes, clients, and the number of users

In NetScaler MAS, navigate to Analytics > Gateway Insight, scroll down to view the reports.
Users

You can view reports for all users associated with the NetScaler Gateway appliances. You can view the EPA, authentication, SSO, and application launch failures for a user. You can also view the details of active and terminated sessions for a user.

To view user details

1. In NetScaler MAS, navigate to **Analytics > Gateway Insight > Users**.

2. Select the time period for which you want to view the user details. You can use the time slider to further customize the selected period. Click **Go**.

3. You can now view the number of active users, number of active sessions, bytes and licenses used by all users during the time period.

Scroll down to view a list of available users and active users.
On the Users or Active Users tab, you can click on a user in the Username column to display the EPA, authentication, SSO, and application launch failures and other details for that user.

**Applications**

You can view the number of applications launched, number of total and active sessions, the number of total bytes and bandwidth consumed by the applications. You can view details of the users, sessions, bandwidth, and launch errors for an application.

**To view application details**

1. In NetScaler MAS, navigate to Analytics > Gateway Insight > Applications.
2. Select the time period for which you want to view the application details. You can use the time slider to further customize the selected time period. Click Go.

   You can now view the number of applications launched, number of total and active sessions, the number of total bytes and bandwidth consumed by the applications.

   Scroll down to view the numbers of sessions, bandwidth, and total bytes consumed by ICA and other applications.
On the Other Applications tab, you can click an application in the Name column to display details of that application.

**Gateways**

You can view the number of gateways, number of active sessions, total bytes and bandwidth used by all gateways associated with a NetScaler Gateway appliance at any given time. You can view the EPA, authentication, single sign-on, and application launch failures for a gateway. You can also view the details of all users associated with a gateway and their logon activity.

**To view gateway details**

1. In NetScaler MAS, navigate to Analytics > Gateway Insight > Gateways.
2. Select the time period for which you want to view the gateway details. You can use the time slider to further customize the selected time period. Click Go.

You can now view the number of gateways, number of active sessions, total bytes and bandwidth used by all gateways associated with a NetScaler Gateway appliance at any given time.

Scroll down to view the gateway details such as Gateway Domain Name, Virtual Server Name, NetScaler IP address, session modes, and Total Bytes.
You can click on a gateway in the **Gateway Domain Name** column to display the EPA, authentication, single sign-on, and application launch failures and other details for a gateway.

**Exporting reports**

you can save the Gateway Insight reports with all the details shown in the GUI in PDF, JPEG, PNG, or CSV format on your local computer. You can also schedule the export of the reports to specified email addresses at various intervals.

**Note:**
- Users with read only access cannot export reports.
- Geo map reports are exported only if the NetScaler MAS has internet connectivity.

**To export a report**

1. On the **Dashboard** tab, in the right pane, click the **export** button.

2. Under **Export Now**, select the required format, and then click **Export**.

**To schedule export**

1. On the **Dashboard** tab, in the right pane, click the **export** button.

2. Under **Schedule Export**, specify the details and click **Schedule**.

**To edit the export schedule**

1. On the **Configuration** tab, navigate to **Configuration > NetScaler Insight Center > Export Schedules**.

2. Select a report from the available list, and then click **Edit**.

3. After editing, click **Save**.

**Note:** Configure the email server settings before scheduling the report by navigating to **System > Notifications > Email** and by clicking **Add**.

**To add an email server or an email distribution list**

1. On the **Configuration** tab, navigate to **System > Notifications > Email**.
2. In the right pane, select **Email Server**, to add an email server or select **Email Distribution list** to create an email distribution list.

3. Specify the details and click **Create**.

**To export the entire Gateway Insight dashboard**

1. On the **Dashboard** tab, in the right pane, click the **export** button.

2. Under **Export Now**, select **PDF** format, and then click **Export**.

**Gateway Insight Use Cases**

The following use cases show how you can use Gateway Insight to gain visibility into users’ access details, applications, and gateways on NetScaler Gateway appliances.

**A user is not able to log in to the NetScaler Gateway appliance or to the internal web servers.**

You are a NetScaler Gateway administrator monitoring NetScaler Gateway appliances through NetScaler MAS, and you want to see why a user is unable to log in, or at what stage of the login process the failure has occurred.

NetScaler MAS enables you to view the user login error details in the following stages of the login process:

- Authentication
- End-point analysis (EPA)
- Single sign-on

In NetScaler MAS, you can search for a particular user and then view all the details for that user.

**To search for a user**

In NetScaler MAS, navigate to **Analytics > Gateway Insight** and, in the **Search for Users** text box, specify the user you want to search.

**Authentication Failures**

You can view authentication errors such as incorrect credentials or no response from the authentication server. If you have set up two-stage authentication, you can see whether the primary, secondary, or both stages of the authentication have failed.

**To view the authentication failure details**

1. In NetScaler MAS, navigate to **Analytics > Gateway Insight**.

2. In the **Overview** section, select the time period for which you want to view the authentication errors. You can use the time slider to further customize the selected time period. Click **Go**.
3. Click the **Authentication** tab. You can view the number of authentication errors at any given time in the **Failures** graph.

![Graph showing authentication logs](image)

Scroll down to view details of each authentication error such as **Username**, **Client IP Address**, **Error Time**, **Authentication type**, **Authentication Server IP Address**, and more from the table on the same tab. The **Error Description** column in the table displays the reason for the logon failure, and the **State** column displays at what stage of a two-stage authentication the failure occurred.

<table>
<thead>
<tr>
<th>Username</th>
<th>NetScaler IP Address</th>
<th>Client IP Address</th>
<th>Gateway IP Address</th>
<th>VPN</th>
<th>Error Time</th>
<th>Error Description</th>
<th>Error Count</th>
<th>State</th>
<th>Authentication Type</th>
<th>Authentication Server IP Address</th>
<th>Gateway Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>user101</td>
<td>10.102.61.201</td>
<td>10.104.2.35</td>
<td>10.102.61.216</td>
<td>attest</td>
<td>2/22/2016, 2:54:18 PM</td>
<td>Invalid credentials passed</td>
<td>1</td>
<td>PRIMARY</td>
<td>LDAP</td>
<td>10.102.61.134</td>
<td>attestor</td>
</tr>
<tr>
<td>user102</td>
<td>10.102.61.201</td>
<td>10.102.61.200</td>
<td>10.102.61.216</td>
<td>attest</td>
<td>2/22/2016, 2:26:18 PM</td>
<td>Invalid credentials passed</td>
<td>1</td>
<td>PRIMARY</td>
<td>LDAP</td>
<td>10.102.61.134</td>
<td>attestor</td>
</tr>
<tr>
<td>user103</td>
<td>10.102.61.201</td>
<td>10.102.61.200</td>
<td>10.102.61.216</td>
<td>attest</td>
<td>2/22/2016, 2:31:19 PM</td>
<td>Invalid credentials passed</td>
<td>1</td>
<td>PRIMARY</td>
<td>LDAP</td>
<td>10.102.61.134</td>
<td>attestor</td>
</tr>
</tbody>
</table>

You can click on a user in the **Username** column to display the authentication errors and other details for that user.

You can customize the table to add or delete columns by using the drop-down arrow as indicated in the following screen shot.
EPA Failures

You can view EPA failures at pre- or post-authentication stage.

To view EPA failure details

1. In NetScaler MAS, navigate to Analytics > Gateway Insight.

2. In the Overview section, select the time period for which you want to view the EPA errors. You can use the time slider to further customize the selected time period. Click Go.

Overview

3. Click the EPA (End Point Analysis) tab. You can view the number of EPA errors at any given time in the Failures graph.

Scroll down to view details of each EPA error such as Username, NetScaler IP Address, Gateway IP Address, VPN, Error Time, Policy Name, Gateway Domain Name and more from the table on the same tab. The Error Description column in the table displays the reason for the EPA failure, and the Policy Name column displays the policy that
resulted in the failure.

You can click on a user in the **Username** column to display the EPA errors and other details for that user.

You can customize the table to add or delete columns by using the drop-down arrow as indicated in the following screen shot.

### SSO Failures

You can view all the SSO failures at any stage for a user accessing any applications through the NetScaler Gateway appliance.

**To view the SSO failure details**

1. In NetScaler MAS, navigate to **Analytics > Gateway Insight**.
2. In the Overview section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click **Go**.

---

**Note**

NetScaler Gateway doesn't report the EPA failures when the "clientSecurity" expression is configured as a VPN session policy rule.
Overview

3. Click the **SSO (Single Sign On)** tab. You can view the number of SSO errors at any given time in the Failures graph.

![Failures Graph](image)

Scroll down to view details of each SSO error such as **Username**, **NetScaler IP Address**, **Error Time**, **Error Description**, **Resource Name** and more from the table on the same tab.

![SSO Error Table](image)

You can click on a user in the **Username** column to display the SSO errors and other details for that user.

You can customize the table to add or delete columns by using the drop-down arrow as indicated in the following screen shot.

![Customizable Table](image)

After successfully logging on to NetScaler Gateway, a user is not able to launch any...
virtual application.

For an application-launch failure, you can gain visibility into the reasons, such as inaccessible Secure Ticket Authority (STA) or XenApp server, or invalid STA ticket. You can view the time the error occurred, details of the error, and the resource for which STA validation failed.

To view the application launch failure details

1. In NetScaler MAS, navigate to Analytics > Gateway Insight.
2. In the Overview section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click Go.

Overview

3. Click the Application Launch tab. You can view the number of application launch failures at any given time in the Failures graph.

Scroll down to view details of each application launch error, such as NetScaler IP Address, Error Time, Error Description, Resource Name, Gateway Domain Name, and more, from the table on the same tab. The Error Description column in the table displays the IP address of the STA server and the Resource Name column displays the details of the resource for which the STA validation has failed.

You can click on a user in the Username column to display the application launch errors and other details for that user.

You can customize the table to add or delete columns by using the drop-down arrow as indicated in the following
After successfully launching a new application, a user wants to view the total bytes and bandwidth consumed by that application.

After you have successfully launched a new application, in NetScaler MAS, you can view the total bytes and bandwidth consumed by that application.

**To view total bytes and bandwidth consumed by an application**

In NetScaler MAS, navigate to Analytics > Gateway Insight > Applications, scroll down and, on the Other Applications tab, click the application for which you want to view the details.

You can view the number of sessions and the total number of bytes consumed by that application.

You can also view the bandwidth consumed by that application.
A user has logged on to NetScaler Gateway successfully, but is unable to access certain network resources in the internal network.

With Gateway Insight, you can determine whether the user has access to the network resources or not. You can also view the name of the policy that resulted in the failure.

To view user access for resources

1. In NetScaler MAS, navigate to Analytics > Gateway Insight > Applications.
2. On the screen that appears, scroll down, and on the Other Applications tab, select the application to which the user was unable to log on to.

On the screen that appears, scroll down, and in the Users table, all the users that have access to that application are displayed.

Different users might be using different NetScaler Gateway deployments or might log on to NetScaler Gateway through different access modes. The administrator should be able to view details about the deployment types and access modes.
With Gateway Insight, you can view a summary of the different session modes used by users to log on, the types of clients, and the number of users logged on every hour. You can also determine whether a user’s deployment is a unified gateway or classic NetScaler Gateway deployment. For unified gateway deployments, you can view the content switching virtual server name and IP address and the VPN virtual server name.

**To view the summary of session modes, type of clients, and number of users logged on**

1. In NetScaler MAS, navigate to **Analytics > Gateway Insight**.
2. In the **Overview** section, scroll down to view the **Session Mode, Operating Systems, Browsers,** and **User Logon Activity** charts display the different session modes used by users to log on, the types of clients, and the number of users logged on every hour.
Analytics: Security Insight

May 21, 2017

Web and web service applications that are exposed to the Internet have become increasingly vulnerable to attacks. To protect applications from attack, you need visibility into the nature and extent of past, present, and impending threats, real-time actionable data on attacks, and recommendations on countermeasures. Security Insight provides a single-pane solution to help you assess your application security status and take corrective actions to secure your applications.

This document includes the following information:

- How Security Insight Works
- Configuring Security Insight
- Configuring Geo Locations for Security Insight Reports
- Security Insight Use Cases
  - Obtain an Overview of the Threat Environment
  - Determine the Threat Exposure of an Application
  - Determine Existing and Missing Security Configuration for an Application
  - Identify Applications That Require Immediate Attention
  - Determine the Number of Attacks in a Given Period of Time
  - Obtain Detailed Information about Security Breaches
  - Determine the Safety Index before Deploying the Configuration

How Security Insight Works

Security Insight is an intuitive dashboard-based security analytics solution that gives you full visibility into the threat environment associated with your applications. Security Insight is included in NetScaler MAS, and it periodically generates reports based on your Application Firewall and NetScaler system security configurations. The reports include the following information for each application:

- **Threat index.** A single-digit rating system that indicates the criticality of attacks on the application, regardless of whether or not the application is protected by a NetScaler appliance. The more critical the attacks on an application, the higher the threat index for that application. Values range from 1 through 7.
  
  The threat index is based on attack information. The attack-related information, such as violation type, attack category, location, and client details, gives you insight into the attacks on the application. Violation information is sent to NetScaler MAS only when a violation or attack occurs. A large number of breaches and vulnerabilities lead to a high threat index value.

- **Safety index.** A single-digit rating system that indicates how securely you have configured the NetScaler instances to protect applications from external threats and vulnerabilities. The lower the security risks for an application, the higher the safety index. Values range from 1 through 7.
  
  The safety index takes into consideration both the application firewall configuration and the NetScaler system security configuration. For a high safety index value, both configurations must be strong. For example, if rigorous application firewall checks are in place but NetScaler system security measures, such as a strong password for the nsroot user, have not been adopted, applications are assigned a low safety index value.

- **Actionable Information.** Information that you need for lowering the threat index and increasing the safety index, which significantly improves application security. For example, you can review information about violations, existing and
missing security configurations for application firewall and other security features, the rate at which the applications are being attacked, and so on.

Security Insight Inter-operability

Note

Security Insight is supported on NetScaler instances running software version 11.0 Build 65.31 and later.

<table>
<thead>
<tr>
<th>NetScaler Version</th>
<th>NetScaler MAS version</th>
<th>Supportable Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1 Build 47.14</td>
<td>11.1 Build 47.14</td>
<td>Security Insight</td>
</tr>
<tr>
<td>11.0 Build 65.31 and later</td>
<td>11.1. Build 47.14</td>
<td>Security Insight</td>
</tr>
</tbody>
</table>

Configuring Security Insight

Note

Security Insight is supported on NetScaler instances with NetScaler Platinum license or NetScaler Enterprise license with AppFirewall license only.

To configure security insight on a NetScaler instance, first configure an application firewall profile and an application firewall policy, and then bind the application firewall policy globally.

Then, enable the AppFlow feature, configure an AppFlow collector, action, and policy, and bind the policy globally. When you configure the collector, you must specify the IP address of the NetScaler MAS server on which you want to monitor the reports.

To configure security insight on a NetScaler instance

1. Run the following commands to configure an application firewall profile and policy, and bind the application firewall policy globally or to the load balancing virtual server.

   add appfw profile <name> [-defaults { basic | advanced }]

   set appfw profile <name> [-startURLAction <startURLAction> ...]

   add appfw policy <name> <rule> <profileName>

   bind appfw global <policyName> <priority>

or,

   bind lb vserver <lb vserver> -policyName <policy> -priority <priority>
add appfw profile pr_appfw -defaults advanced

set appfw profile pr_appfw -startURLaction log stats learn

add appfw policy pr_appfw_pol "HTTP.REQ.HEADER("Host").EXISTS" pr_appfw

bind appfw global pr_appfw_pol 1

or,

bind lb vserver outlook –policyName pr_appfw_pol –priority “20”

2. Run the following commands to enable the AppFlow feature, configure an AppFlow collector, action, and policy, and bind the policy globally or to the load balancing virtual server:

```plaintext
add appflow collector <name> -IPAddress <ipaddress>

set appflow param [-SecurityInsightRecordInterval <secs>] [-SecurityInsightTraffic ( ENABLED | DISABLED )]

add appflow action <name> -collectors <string>

add appflow policy <name> <rule> <action>

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [-type <type>]

or,

bind lb vserver <vserver> -policyName <policy> -priority <priority>
```
To enable AppFlow from NetScaler MAS

1. In a web browser, type the IP address of the NetScaler Management and Analytics System (for example, http://192.168.100.1).

2. In User Name and Password, enter the administrator credentials.

3. Navigate to Infrastructure > Instances, and select the NetScaler instance you want to enable AppFlow.

4. From the Action drop-down, select Enable/Disable Insight.

5. Select the virtual servers, and click Enable AppFlow.

6. In the Enable AppFlow field, type true, and select Security Insight.

7. Click Ok.
Configuring Geo Locations for Security Insight Reports

If you configure geo locations in NetScaler MAS, Security Insight reports include the exact geographic locations from which client requests originate. To enable geo locations, specify a private IP block or range of IP addresses for every geographic location in your organization. Add that information in the Geo Database file, along with the city/state/country name and the latitude and longitude coordinates of each location. Contact your Citrix representative to obtain the Geo Database file, and then upload the file to the NetScaler instance.

To configure geo locations

1. Copy the Geo Database file, Citrix_Netscaler_InBuilt_GeoIP_DB.csv, to any location on the NetScaler appliance.
2. Open the Geo Database file with a text editor, such as vi editor, and add an entry for every location in your organization. The entry must be in the following format:
   
   <start IP>,<end IP>,<country>,<state>,<city>,longitude,latitude
   
   For example,
   
   4.17.142.224,4.17.142.239,,US,New York,,Harrison,,73.7304,41.0568

3. Run the following commands to enable geo-location logging and logging in the CEF format:

   ```
   add locationFile <Complete path with DB file>
   set appfw settings -geoLocationLogging ON
   set appfw settings -CEFLogging ON
   ```

IP Reputation

You can use NetScaler Insight Center to monitor and manage your incoming traffic’s IP Reputation. You can configure policies to add more IPs as malicious, and create a customized block list.

To know learn about configuring and using IP Reputation, see IP Reputation.

Monitoring IP Reputation
The IP Reputation feature provides attack-related information about malicious IP addresses. For example, it reports IP Reputation Score, IP Reputation category, IP Reputation attack time, Device IP, and details about the Client IP address.

IP Reputation score indicates risk associated with an IP address. The score has the following are the ranges:

<table>
<thead>
<tr>
<th>IP Reputation score</th>
<th>Level of Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-20</td>
<td>High Risk</td>
</tr>
<tr>
<td>21 – 40</td>
<td>Suspicious</td>
</tr>
<tr>
<td>41 – 60</td>
<td>Moderate Risk</td>
</tr>
<tr>
<td>61 – 80</td>
<td>Low Risk</td>
</tr>
<tr>
<td>81 – 100</td>
<td>Trustworthy</td>
</tr>
</tbody>
</table>

To monitor IP Reputation

1. Navigate to Analytics > Security Insight, and select the application you want to monitor.

2. In the Threat Index tab, select IP Reputation.

3. Select a severity to display more details of the attacks that were at that level. You can click on the bar graph or in the table under the graph.

4. Select the time period for which you want to view the details. You can use the time slider to further customize the selected period. Then, click Go.
5. To customize the display, click the settings button.

Thresholds

You can set and view thresholds on safety index and threat index of applications in Security Insight.

**To set a threshold**

1. Navigate to **System > Analytics Settings > Thresholds**, and select **Add**.
2. Select the traffic type as **Security** in the Traffic Type field, and enter required information in the other appropriate fields such as Name, Duration, and entity.
3. In the **Rule** section, use the Metric, Comparator, and Value fields to set a threshold.
   
   For example, "Threat Index" ">" "5"
4. Click **Create**.

**To view the threshold breaches**

1. Navigate to **Analytics > Security Insight > Devices**, and select the NetScaler instance.
2. In the **Application** section, you can view the number of threshold breaches occurred for each virtual server in the
Threshold Breach column.

Security Insight Use Cases

The following use cases describe how you can use security insight to assess the threat exposure of applications and improve security measures.

Obtain an Overview of the Threat Environment

In this use case, you have a set of applications that are exposed to attacks, and you have configured NetScaler MAS to monitor the threat environment. You need to frequently review the threat index, safety index, and the type and severity of any attacks that the applications might have experienced, so that you can focus first on the applications that need the most attention. The security insight dashboard provides a summary of the threats experienced by your applications over a time period of your choosing, and for a selected NetScaler device. It displays the list of applications, their threat and safety indexes, and the total number of attacks for the chosen time period.

For example, you might be monitoring Microsoft Outlook, Microsoft Lync, SharePoint, and a SAP application, and you might want to review a summary of the threat environment for these applications.

To obtain a summary of the threat environment, log on to NetScaler MAS, and then navigate to Analytics > Security Insight.

Key information is displayed for each application. The default time period is 1 hour.

To view information for a different time period, from the drop-down at the top-left, select a time period.
To view a summary for a different NetScaler instance, under **Devices**, click the IP address of the NetScaler instance. To sort the application list by a given column, click the column header.

**Determine the Threat Exposure of an Application**

After reviewing a summary of the threat environment on the Security Insight dashboard to identify the applications that have a high threat index and a low safety index, you want to determine their threat exposure before deciding how to secure them. That is, you want to determine the type and severity of the attacks that have degraded their index values. You can determine the threat exposure of an application by reviewing the application summary.

In this example, Microsoft Outlook has a threat index value of 6, and you want to know what factors are contributing to this high threat index.

To determine the threat exposure of Microsoft Outlook, on the **Security Insight** dashboard, click **Outlook**. The application summary includes a map that identifies the geographic location of the server.
Click **Threat Index > Security Check Violations** and review the violation information that appears.

Click **Signature Violations** and review the violation information that appears.
Determine Existing and Missing Security Configuration for an Application

After reviewing the threat exposure of an application, you want to determine what application security configurations are in place and what configurations are missing for that application. You can obtain this information by drilling down into the application's safety index summary.

The safety index summary gives you information about the effectiveness of the following security configurations:

- **Application Firewall Configuration.** Shows how many signature and security entities are not configured.
- **NetScaler System Security.** Shows how many system security settings are not configured.

In the previous use case, you reviewed the threat exposure of Microsoft Outlook, which has a threat index value of 6. Now, you want to know what security configurations are in place for Outlook and what configurations can be added to improve its threat index.

On the **Security Insight** dashboard, click **Outlook**, and then click the **Safety Index** tab. Review the information provided in the **Safety Index Summary** area.
On the **Application Firewall Configuration** node, click **Outlook_Profile** and review the security check and signature violation information in the pie charts.

Review the configuration status of each protection type in the application firewall summary table. To sort the table on a column, click the column header.

Click the **NetScaler System Security** node and review the system security settings and Citrix recommendations to improve the application safety index.

### Identify Applications That Require Immediate Attention

The applications that need immediate attention are those having a high threat index and a low safety index.

In this example, both Microsoft Outlook and Microsoft Lync have a high threat index value of 6, but Lync has the lower of the two safety indexes. Therefore, you might have to focus your attention on Lync before improving the threat environment for Outlook.
Determine the Number of Attacks in a Given Period of Time

You might want to determine how many attacks occurred on a given application at a given point in time, or you might want to study the attack rate for a specific time period.

For example, you might want to view the number of attacks on Microsoft Lync in the past week. On the Security Insight dashboard, click Lync > Total Violations. By default, the graph is plotted for the last one hour.

To plot the graph of violations for the past week, from the time period list, select 1 Week. In this example, you see a surge in attacks from February 1.
Obtain Detailed Information about Security Breaches

You might want to view a list of the attacks on an application and gain insights into the type and severity of attacks, actions taken by the NetScaler instance, resources requested, and the source of the attacks.

For example, you might want to determine how many attacks on Microsoft Lync were blocked, what resources were requested, and the IP addresses of the sources.

On the Security Insight dashboard, click **Lync > Total Violations**. In the table, click the filter icon in the **Action Taken** column header, and then select **Blocked**.

For information about the resources that were requested, review the **URL** column. For information about the sources of the attacks, review the **Client IP** column.

Determine the Safety Index before Deploying the Configuration

Security breaches occur after you deploy the security configuration on a NetScaler instance, but you might want to assess the effectiveness of the security configuration before you deploy it.

For example, you might want to assess the safety index of the configuration for the SAP application on the NetScaler instance with IP address 10.102.60.27.
On the Security Insight dashboard, under Devices, click the IP address of the NetScaler instance that you configured. You can see that both the threat index and the total number of attacks are 0. Threat index is a direct reflection of the number and type of attacks on the application. Zero attacks indicate that the application is not under any threat.

Click Sap > Safety Index > SAP_Profile and assess the safety index information that appears.

In the application firewall summary, you can view the configuration status of different protection settings. If a setting is set to log or if a setting is not configured, the application is assigned a lower safety index.
### Application Firewall Summary

<table>
<thead>
<tr>
<th>Protections</th>
<th>Configuration Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hawaii validation</td>
<td>Not Configured</td>
</tr>
<tr>
<td>HTTPS/FTP/Fault</td>
<td>Not Configured</td>
</tr>
<tr>
<td>URL Attachment</td>
<td>Not Configured</td>
</tr>
<tr>
<td>XML XSS</td>
<td>Not Configured</td>
</tr>
<tr>
<td>XML WS</td>
<td>Not Configured</td>
</tr>
</tbody>
</table>
Analytics: SSL Insight

SSl Insight provides visibility into secure web transactions (HTTPS) and allows IT administrators to monitor all the secure web applications being served by the NetScaler ADC by providing integrated and real-time and historic monitoring of secure web transactions. With this visibility the administrator can assess following:

- **Determine Configuration Change Impact on Customer Usage**: The administrator can understand the impact on clients for making a configuration change like turning off SSLv3 or removing a cipher like RC4-MD5. This can be done by assessing the historic transaction data on this protocol and cipher.
- **Quantify Client Performance**: Administrator can understand the impact on Application Response Time based on the SSL ciphers/protocol used or the certificates negotiated.
- **Application Security**: Assess if any of the application have transactions running on low security protocols, ciphers or weak key strength.

When SSL Analytics is enabled on a NetScaler instance, SSL statistics are recorded and logged for every SSL transaction. The statistics show the details of the SSL flow. Also, every successful connection is logged and displayed by NetScaler MAS Analytics.

**Note**

Information about SSL connections that are not successful is not logged or displayed by NetScaler MAS Analytics.

SSL Insight provides the following critical information, which is displayed by NetScaler MAS Analytics:

- SSL Protocol version negotiated
- Cipher negotiated, and the cipher strength
- Signature Hash algorithm of the certificate used
- Certificate Type & Size

**Note**

For successful SSL connections, SSL appflow logging happens at the end of every transaction.

This document includes the following information:

- Prerequisites
- Configuring SSL Insight
- Enabling the ApplFlow Feature
- Enabling ULFD Mode
- Enabling SSL Insight Parameters
- Viewing the SSL Insight Metrics
- SSL Insight Use Cases
  - Obtain an Overview of the SSL Transactions of Applications, Clients, or Servers
Prerequisites

- The NetScaler instance on which you intend to configure SSL Insight must be running a NetScaler software release no earlier than 11.1 build 51.21.
- The NetScaler MAS version should be no earlier than the NetScaler software version.

Configuring SSL Insight

SSL Insight Metrics are included in Web Insight reports if you enable the following elements:

- Enable AppFlow for Web Insight on each NetScaler instance.
- Enable ULFD mode on each NetScaler instance.
- Enable required AppFlow parameters on each NetScaler instance.

Enabling the AppFlow Feature

**Note**

You can enable the Appflow feature either from NetScaler MAS or from each NetScaler instance.

**To enable the AppFlow feature from NetScaler MAS**

1. In a web browser, type the IP address of the NetScaler MAS virtual appliance (for example, http://192.168.100.1).
2. In **User Name** and **Password**, enter the administrator credentials.
3. Navigate to **Infrastructure > Instances**, and select the NetScaler instance on which you want to enable analytics.
4. From the **Action** drop-down list, select **Enable/Disable Insight**.
5. Select the virtual servers, and click **Enable AppFlow**.
6. In the Enable AppFlow field, type **true**, and select **Web Insight**.
7. Repeat steps 3 through 6 on each NetScaler instance.
8. Click **OK**.
Note
You cannot enable data collection on a virtual server if the operational state of the virtual server is other than UP.

To enable the AppFlow feature from the NetScaler command line

On a NetScaler instance, at the command prompt, type:

`enable ns feature AppFlow`

To enable the AppFlow feature by using the NetScaler GUI

In a NetScaler instance's GUI, navigate to Configuration > System > Settings, click Configure Advanced Features, and select AppFlow.

Enabling ULFD Mode

After you enable ULFD mode on the NetScaler instances on which the virtual servers are configured, the ULFD server streams the analytics data from the NetScaler instances to NetScaler MAS.

To enable ULFD mode by using the NetScaler command line

1. On the NetScaler instance, at the command prompt, type:

   `enable mode ulfd`

2. Add the NetScaler MAS IP address as the ULFD server on the NetScaler instance by entering the following command:
add ulfd server <your_MAS_IP Address>

Enabling SSL Insight Parameters

On each NetScaler instance, you have to enable some HTTP parameters to display SSL Insight records in NetScaler MAS.

To enable SSL Insight parameters from the NetScaler command line

At the command prompt, type:

```
set appflow param -httpDomain ENABLED -httpHost ENABLED -httpMethod ENABLED -httpUrl ENABLED -
httpUserAgent ENABLED -httpContentType ENABLED
```

To enable SSL Insight parameters from the NetScaler configuration utility

2. Select the following check boxes: HTTP Domain, HTTP Host, HTTP Method, HTTP URL, HTTP User-Agent, HTTP Content-Type.
3. Click OK.

Viewing the SSL Insight Metrics

SSL Insight metrics in NetScaler MAS provide a detailed view of the performance of the SSL transactions served by the NetScaler instances. You can view the SSL Insight metrics at the client, server, or application level. With the help of these metrics, you can analyze and optimize your NetScaler HTTPS settings and SSL-certificate settings, and track performance issues.

To monitor SSL Insight Metrics in NetScaler MAS

1. On the Analytics tab, navigate to Web Insight and click the Client, Server, or Application node to display the metrics
about clients, the server, or the applications, respectively.

2. In the top-left pane, from the drop-down list, select the time frame whose metrics you want to display. You can customize the time frame by using the time-frame slider. Click **Go**.

3. The SSL Insight metrics appear as pie charts, which you can click for more details.

**Note**

The pie charts display the metrics of all the applications, clients or servers.

4. To display details for a specific application, client, or server, click the corresponding value on the bar graph.
SSL Insight Use Case

The following use case describes how you can use SSL Insight to assess the usage of various SSL Parameters in applications, clients and servers, and improve security measures.

Obtain an Overview of the SSL Transactions of Applications, Clients, or Servers

In this use case, you have a set of applications that are using SSL transactions (HTTPS) for communication, and you have configured NetScaler MAS to monitor the SSL components. You might need to frequently review the applications so that you can focus first on the applications that need the most attention. The SSL insight dashboard provides a summary of various SSL parameters used by your applications over a time period of your choosing, and for a selected NetScaler device. They are:

- SSL Certificates
- SSL Protocols
- SSL Cipher Negotiated
- SSL Key Strength
In the following example, you can see list of clients (identified by their IP addresses) and the SSL hits per client. Also, at the right, you can view the SSL Parameters for all the clients.
To display SSL details for a client, select the client on the bar graph or in the table below the graph. In the following example, the selected client’s transactions use an SHA1 SSL certificate and four major protocols: TSLv1.2, TSLv1.1, TSLv1, and SSLv3. You can also see that ciphers of various strengths were negotiated. The color code indicates the strength of the SSL protocol, which gives you information about weak ciphers and strong ciphers.
Analytics: TCP Insight

Dec 29, 2016

The TCP Insight feature of NetScaler Management and Analytics System (NetScaler MAS) provides an easy and scalable solution for monitoring the metrics of the optimization techniques and congestion control strategies (or algorithms) used in NetScaler appliances to avoid network congestion in data transmission. This feature uses "TCP Speed Report" capability, which measures TCP file download or upload performance with and without TCP optimization.

You can view the key Transport Layer metrics, such as data volume, throughput, and speed, and use that information to measure the traffic volume served by the NetScaler instances and validate the benefits of TCP Optimization. Breakdowns by stream direction (from client to NetScaler and NetScaler to origin server), TCP port, and virtual LAN are provided for the above metrics.

Prerequisites

Before you begin configuring the TCP Insight feature, make sure that the following prerequisites are met:

- The NetScaler instances are running on software version 11.1 build 51.21 or later.
- You have installed NetScaler MAS running on software version 11.1 build 51.21 or later.
- All the virtual servers configured for an application are licensed for management and monitoring on NetScaler MAS.
  For information about NetScaler MAS licensing, see Licensing.

Hardware requirements for NetScaler MAS:

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>4</td>
</tr>
<tr>
<td>Storage Space</td>
<td>120 GB</td>
</tr>
</tbody>
</table>

**Note:** Citrix recommends that you use 8 CPUs for better performance.

Enabling TCP Insight

Before you can view the TCP Insight metrics, you must enable the feature on NetScaler MAS.

**To Enable TCP Insight**

1. In a web browser, type the IP address of the NetScaler MAS virtual appliance (for example, http://192.168.100.1).

2. In **User Name** and **Password**, enter the administrator credentials.

3. Navigate to **System > Analytics Settings > Configure Features**, and select Enable TCP Insight.
4. In the confirmation window, click OK.

**Viewing the TCP Insight Metrics in NetScaler MAS**

After enabling TCP Insight in NetScaler MAS, you can view key Transport Layer information such as traffic mode (internet or mobile data), data volume, throughput, interfaces, ports, average upload speed, average download speed.

**To display TCP Insight metrics in NetScaler MAS**

1. In a web browser, type the IP address of the NetScaler MAS virtual appliance (for example, http://192.168.100.1).

2. In **User Name** and **Password**, enter the administrator credentials.

3. Navigate to **Analytics > TCP Insight**.

You can hover your mouse pointer on the bar graphs to view the data volume of the corresponding transport techniques. Also, you can view the data volume, and other metrics, in the table below the graph.

**NOTE:** You can customize the metrics displayed in the graph by using the settings icon on the table. You can also select the time period to which the metrics pertain, and use the time slider to adjust the time period.

You can also view metrics for such things as interfaces, ports, and bit rates by selecting from the TCP Insight drop-down menu.

**Use Cases**
The following use cases illustrate some of the ways to use TCP Insight on NetScaler appliances:

- Assess Benefits of TCP Optimization
- Tune TCP Parameters
- Measure Impact of TCP Optimization on Traffic Volume

**Assess Benefits of TCP Optimization**

How much does NetScaler TCP optimization actually benefit a mobile (radio) or enterprise network (internet). You can view the speed of data transfers that take place over TCP, and compare unoptimized and optimized performance. These measurements are displayed separately for the download and upload directions (always on the radio/client side), and for different destination ports, HTTP (80) and HTTPS (443).

By examining the TCP Insight metrics, you can quantify the speed improvement gained by optimizing TCP flows.

To see a summary of these parameters, log on to NetScaler MAS and click the **TCP Insight** tab. Then, click **Sides** and select **Internet** or **Radio** from the bar graph or the table below the graph.

![TCP Insight dashboard](https://docs.citrix.com)

**Tune TCP Parameters**

Using different TCP Profiles might yield different outputs for the same traffic. In such situations, you might want to view and compare the speed measurements of periods in which NetScaler is running different TCP optimization profiles. You can
use the results to tune TCP parameters for faster transmission, and develop a TCP profile that maximizes the user-perceived experience in a specific customer network.

To view the reports, log on to NetScaler MAS. Then, on the TCP Insight tab, click Bitrates, and select the desired bitrate from the bar graph or the table below the graph.

Measure Impact of TCP Optimization on Traffic Volume

Measurements of IP-layer Data Volume/Throughput handled by a NetScaler instance can be compared between different time periods, to evaluate the effect of TCP optimization on subscriber data consumption. The measurements can be applied separately for each side of the network (radio-side vs. internet-side), for different traffic segments (delineated by different interfaces or VLANs), for each direction (downlink vs. uplink) and for different destination ports (HTTP and HTTPS). The comparison can be used to confirm that TCP optimization encourages subscribers to consume more data.

For a summary of the measurements, log on to NetScaler MAS, and on the TCP Insight tab click Sides, and then select Internet or Radio from the bar graph or the table below the graph.

You can also select a different timeframe from the time drop-down list. You can customize the time frame by using the timeframe slider.
Analytics: WAN Insight

Feb 07, 2017

The NetScaler SD-WAN WAN optimization (WO) appliances optimize the delivery of a large number of applications through the WAN, by improving the efficiency of data flow across the network between the datacenter and the branch sites. WAN Insight analytics enable administrators to easily monitor the accelerated and unaccelerated WAN traffic that flows between the datacenter and branch WAN optimization appliances. WAN Insight provides visibility into clients, applications and branches on the network, to help troubleshoot network issues effectively. Live and historical reports enable you to proactively address issues, if any.

Enabling analytics on the datacenter WAN optimization appliance enables the NetScaler Management and Analytics System (MAS) to collect data and provide reports and statistics for the datacenter and the branch WAN optimization appliances.

To enable analytics on the WAN optimization appliance:

1. In a web browser, type the IP address of the NetScaler Management and Analytics System (for example, http://192.168.100.1).
2. In the **User Name** and **Password** fields, enter the administrator credentials.

3. Navigate to **Infrastructure > Instances > NetScaler SD-WAN WO**, and select the datacenter WAN optimization appliance.

4. From the **Action** drop-down, select **Enable Insight**.

5. Select the following parameters as required:

   * **Geo data collection for HDX Insight**: Shares client IP address with the Google Geo API.

   * **AppFlow**: Starts collecting data from WAN optimization instances.
     - **TCP and WANOpt**: Provides TCP and WANOpt Insight reports.
     - **HDX**: Provides HDX Insight reports.
     - **TCP only for HDX**: Provides TCP only for HDX Insight reports.
6. Click OK.

To view WAN Insight reports:

1. In a web browser, type the IP address of the NetScaler Management and Analytics System (for example, http://192.168.100.1).
2. In the User Name and Password fields, enter the administrator credentials.
3. Navigate to Analytics > WAN Insight.

Note
The WAN Insight option is visible only after you add an SD-WAN WO instance to NetScaler MAS.

You can view the following reports:

* **Applications** - Displays the usage and performance statistics of all the applications for the selected duration.
* **Branches** - Displays the usage and performance statistics of all the WAN optimization branch appliances.
* **Clients** - Displays the usage and performance statistics of all the clients accessing the WAN optimization appliances, in each branch.
The following metrics are displayed:

<table>
<thead>
<tr>
<th><strong>Metric</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Accelerated Connections</td>
<td>Number of active WAN connections that are accelerated.</td>
</tr>
<tr>
<td>Active Unaccelerated Connections</td>
<td>Number of active WAN connections that are not accelerated.</td>
</tr>
<tr>
<td>WAN Latency</td>
<td>Delay, in milliseconds, that the user experiences while interacting with an application.</td>
</tr>
<tr>
<td>Compression Ratio</td>
<td>Ratio of data compression between the branch office and datacenter appliances for the selected duration.</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>Number of packets that the WAN optimization appliance has sent over the network for the selected duration.</td>
</tr>
<tr>
<td>Packets Received</td>
<td>Number of packets that the WAN optimization appliance has received from the network for the selected duration.</td>
</tr>
<tr>
<td>Bytes Sent over WAN</td>
<td>Number of bytes that the NetScaler WAN optimization appliance has sent over the WAN for the selected duration.</td>
</tr>
<tr>
<td>Bytes Received over WAN</td>
<td>Number of bytes that the WAN optimization appliance received from the WAN for the selected duration.</td>
</tr>
<tr>
<td>LAN RTO</td>
<td>Number of times the WAN optimization appliance has timed out retransmission to the LAN for the selected duration.</td>
</tr>
<tr>
<td>WAN RTO</td>
<td>Number of times the WAN optimization appliance has timed out retransmission to the WAN for the selected duration.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Retransmit Packets (LAN)</td>
<td>Number of packets the WAN optimization appliance has retransmitted to the LAN network for the selected duration.</td>
</tr>
<tr>
<td>Retransmit Packets (WAN)</td>
<td>Number of packets the WAN optimization appliance has retransmitted to the WAN network for the selected duration.</td>
</tr>
</tbody>
</table>
Integrating NetScaler MAS with Director

Oct 03, 2016
Director integrates with NetScaler MAS for network analysis and performance management.

- Network analysis obtains HDX Insight reports from NetScaler MAS and provides an application and desktop view of the network. With this feature, Director provides an advanced analytics view of ICA traffic in your deployment.
- Performance management provides historical retention and trend reporting. With historical retention of data versus the real-time assessment, you can create Trend reports, including capacity and health trending.

After you integrate NetScaler MAS with Director, HDX Insight reports provide you with the following information in Director:

- The Network tab in the Trends page shows latency and bandwidth effects for applications, desktops, and users across your deployment.
- The User Details page shows latency and bandwidth information specific to a particular user session.

Prerequisites

Hardware Requirements for HDX Insight to NetScaler MAS Migration

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>8</td>
</tr>
<tr>
<td>Storage Space</td>
<td>500 GB</td>
</tr>
<tr>
<td>Virtual Network Interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>1Gbps or 100 Mbps</td>
</tr>
</tbody>
</table>

Software Requirements

Before migrating to the NetScaler MAS virtual appliance, verify that the following requirements have been met:

- Director version 7.11 is installed
- NetScaler HDX Insight version 10.1 or later is installed
- HDX Insight and NetScaler MAS supports XenDesktop VDA version 7.0 and later
- StoreFront is supported on XenDesktop version 7.0 and later
- Ensure that MAC Citrix Receiver for Mac version 11.8 and later, and Windows Citrix Receiver for Windows 14.0 and later are available to display accurate ICA RTT metrics
- NetScaler MAS version 11.0 and later is installed. For more information on how to install NetScaler MAS, see [http://docs.citrix.com/en-us/netscaler-mas/11-1/single-server-deployment.html](http://docs.citrix.com/en-us/netscaler-mas/11-1/single-server-deployment.html)

Limitations

- The availability of this feature depends on your organization's license and your administrator permissions.
- ICA session Round Trip Time (RTT) shows data correctly for Citrix Receiver for Windows 3.4 or later and for Citrix
Receiver for Mac 11.8 or later. For earlier versions of these Receivers, the data does not display correctly.

- In the Trends view, HDX connection logon data is not collected for VDAs earlier than version 7. For earlier VDAs, the chart data is displayed as 0.
- For deployments that already have an external hard disk with storage space less than 500 GB, you cannot add another hard disk.

For more information on Director and for steps to integrate NetScaler MAS with Director, see http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director.html.

For more information on HDX Insight, see http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html.
Integrating NetScaler MAS with OpenStack Platform

Apr 24, 2017

The Cloud Orchestration feature of NetScaler Management and Analytics System (MAS) enables integration of Citrix NetScaler products with OpenStack platform. By using this feature with OpenStack platform, the OpenStack users are able to avail the load balancing feature (LBaaS) of the NetScaler. After this, the OpenStack users can deploy their load balancer configurations from OpenStack in NetScaler instance.

The following sections provide a brief description of the features in NetScaler MAS and OpenStack integration workflow.

NetScaler Driver for OpenStack Neutron LBaaS

OpenStack Neutron LBaaS plugin includes a NetScaler driver that enables OpenStack to communicate with the NetScaler MAS. OpenStack uses this driver to forward any load balancing configuration done through LBaaS APIs, to the NetScaler MAS, which creates the load balancer configuration on the desired NetScaler instances. OpenStack also uses the driver to call NetScaler MAS at regular intervals to retrieve the status of different entities (such as VIPs and Pools) of all load balancing configurations from the NetScaler ADCs. NetScaler driver software for OpenStack platform is bundled along with the NetScaler MAS. To download and install the drivers, you have to first install NetScaler MAS and launch the application.

Registering NetScaler MAS and OpenStack with each other

You have to first register OpenStack information on the NetScaler MAS. Specify the OpenStack controller IP address and cloud administrative user credentials, and also the OpenStack NetScaler driver user credentials. You can later specify the same login credentials in the NetScaler_driver section of the Neutron configuration file (neutron.conf) so that NetScaler driver in OpenStack can connect to NetScaler MAS during LB configurations.

After OpenStack and NetScaler MAS are registered with each other, both can talk to each other. Also, OpenStack users can use their existing credentials in OpenStack to log on to the NetScaler MAS user interface to check how their LB configurations are performing in NetScalers.

Tenants in OpenStack

In OpenStack a tenant is also called a project. A tenant is a group of users; a tenant or a project can also be defined as a set of resources (compute, network, storage, and so on) assigned to an isolated group of users.

Placement policies

Placement policies provide the flexibility to decide on the NetScaler instance that is used in each load balancer configuration created by users. Alternatively, the NetScaler MAS also provides an option to assign a NetScaler instance based on OpenStack tenants.

Service packages

Service packages are bundles that tie together policies/SLAs, devices or auto-provision configuration specifications, and tenants/placement-policies. A service package is usually defined in terms of the isolation policies that are provided to the tenant.

The following are some points related to service packages:

- A tenant cannot be part of more than one service package.
Multiple tenants can be associated with the same service package.

In a service package that is set for auto-provisioning, virtual NetScaler instances can be created from only one platform type (on SDX platform or on OpenStack Compute platform).

Features Supported on LBaaS V1 and LBaaS V2

While LBaaS V1 driver in OpenStack supports operations from OpenStack Horizon user interface, LBaaS V2 driver supports only command line operations.

The following list shows the features supported on both LBaaS V1 and LBaaS V2 on OpenStack:

- LBaaS V1
  - Load Balancing
- LBaaS V2
  - Load Balancing
  - SSL Offload with certificates managed by Barbican, the Key Manager in OpenStack
  - Certificate Bundles (includes intermediary Certification Authorities)
  - SNI support

This document provides information about:

- Use Case Scenario
- NetScaler MAS Integration with OpenStack Workflow
- Prerequisites
- Pre-configuration Tasks in NetScaler MAS and OpenStack
- Configuration Steps for LBaaS V1 using Horizon
- Configuration Steps for LBaaS V2 using Command Line
- Manual Provisioning of NetScaler VPX Instance on OpenStack
- Integrating NetScaler MAS with OpenStack Heat Services
- Monitoring OpenStack Applications in NetScaler MAS

Use Case Scenario

The following use-case scenario explains the workflow of integrating NetScaler MAS with the OpenStack platform:

An enterprise, Example-Cloud-Provider, has used OpenStack components to set up a cloud to provide infrastructure to its tenants. Steve is the administrator of this cloud provider, while Tom is a tenant of the Example-Cloud-Provider's cloud infrastructure. Tom's organization, Example-SportsOnline.com, requires two servers S1 and S2, and Tom also requires a dedicated NetScaler device to load balance the traffic between servers S1 and S2 on OpenStack platform.

To meet this requirement, Steve has to install and configure both OpenStack and NetScaler MAS, and prepare them to work with each other. Steve has to create a tenant account named Example-SportsOnline in OpenStack, and then allocate resources to the tenant account. Steve also has to create different log-on credentials (users) for Example-SportsOnline for managing its resources and configuration. Tom can now create the two servers S1 and S2 on OpenStack to manage the traffic in his organization.

Steve has to register OpenStack details with NetScaler MAS, and configure the NetScaler LBaaS driver in OpenStack networking component, Neutron. After the registration is complete, NetScaler MAS displays the details of all tenants from the OpenStack. Steve can select Example-SportsOnline from the list who wants the NetScaler LBaaS features and configure Tom to get a dedicated NetScaler allotted for his load balancer configurations in NetScaler MAS.

For this, Steve can either provision a NetScaler VPX instance on the computing layer (Nova) of OpenStack using NetScaler MAS user interface or enable MAS to auto-provision a NetScaler VPX instance on demand, when Tom does his LB configuration in OpenStack. In either case, NetScaler MAS manages the VPX instance.

For achieving this, Steve creates a service package in NetScaler MAS, and defines the conditions in the service package that were agreed in the SLA with Tom. For example, Steve selects the 'dedicated' isolation policy to provide a dedicated instance for providing load balancer configurations to Tom. That is, Steve selects a non-shared instance for Tom in the service package. He then assigns many NetScaler VPX instances to the service package, and associates Example-SportsOnline, along with other tenants, who require a dedicated NetScaler with the service package. As a result, when Tom performs his first load balancer configuration, NetScaler MAS allocates one of the NetScaler VPX instances in the service package to Example-SportsOnline and also deploys his configuration in that NetScaler.

Tom can now create load balancing configurations, by creating pools, virtual IPs (VIP), and health monitors using OpenStack LBaaS/UI. Pools and the VIPs in OpenStack get deployed as service groups and virtual servers on the NetScaler instance. Tom can also create health monitors to monitor the servers, and send
application traffic to only those servers which are UP at any point of time and reachable from NetScaler.

The load balancing configuration created in OpenStack is now implemented on the NetScaler instance. Once fully configured, the NetScaler VPX instance then takes over the load balancing functionality and starts accepting application traffic and load balances the traffic between the servers S1 and S2 created by Tom.

NetScaler MAS Integration with OpenStack Workflow

The following flowchart depicts the workflow that you need to follow when you are configuring LBaaS V1 and LBaaS V2.

NetScaler MAS Integration with OpenStack Workflow

The following flowchart depicts the workflow that you need to follow when you are configuring LBaaS V1 and LBaaS V2.

---

**Pre-Configuration Tasks in OpenStack**

1. Install NetScaler Driver Software
2. Register NetScaler MAS on OpenStack

**Pre-Configuration Tasks in NetScaler MAS**

3. Register OpenStack with NetScaler MAS
4. Add OpenStack Tenants in NetScaler MAS
5. Add NetScaler Devices
6. Create Placement Policies (Optional)
7. Create Service Packages

---

**Configuration Tasks in LBaaS V1/LBaaS V2**

- 8. Create VIPs, members, pools, listeners and monitors on OpenStack
  - Using Horizon for LBaaS V1
  - Using Command Line for LBaaS V2
Prerequisites

Sep 17, 2016

Before you integrate the NetScaler virtual instance with OpenStack platform, ensure that the following requirements are met:

**NetScaler MAS and OpenStack Software Requirements:**

- NetScaler MAS 11.1 is installed on a supported hypervisor workstation that meets the minimum hardware requirements system
- OpenStack components are installed and running
- OpenStack versions - Liberty, Mitaka, and Newton are supported by NetScaler MAS 11.1

**NetScaler MAS Hardware Requirements:**

The following table lists the virtual computing resources that you should have on your OpenStack server to install NetScaler virtual instances.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>8</td>
</tr>
<tr>
<td>Storage Space</td>
<td>500 GB</td>
</tr>
<tr>
<td>Virtual Network Interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>1 Gbps or 100 Mbps</td>
</tr>
</tbody>
</table>

**Note**

The memory and hard disk requirements specified above are for deploying NetScaler MAS on the OpenStack platform, considering that there are no other virtual machines running on the host. The hardware requirements for OpenStack depends on the number of virtual machines running on it.
Pre-configuration Tasks in NetScaler MAS and OpenStack

Perform the following tasks before you configure NetScaler MAS and OpenStack:

- Installing NetScaler MAS
- Installing NetScaler Driver Software and Registering NetScaler MAS on OpenStack
- Registering OpenStack on NetScaler MAS
- Creating a Tenant on OpenStack
- Adding OpenStack Tenants
- Provisioning NetScaler VPX
  - Pre-provisioning NetScaler Devices
  - Auto-provisioning NetScaler Devices
  - Creating a Service Package on NetScaler MAS
  - Creating a Flexible Placement Policy on NetScaler MAS (Optional)
  - Auto-Provisioning NetScaler VPX Devices Deployed on NetScaler SDX Platform

Installing NetScaler Management and Analytics System

Install NetScaler MAS on a supported hypervisor. For more information on how to download and install NetScaler MAS, see NetScaler MAS Single Server Deployment.

Installing the NetScaler Driver Software and Registering NetScaler MAS on OpenStack

Download the NetScaler bundle for OpenStack from the NetScaler MAS Downloads page.

To install NetScaler driver on OpenStack platform using NetScaler MAS GUI

1. In NetScaler MAS, click Downloads. The Downloads page in NetScaler MAS, provides you links to download NetScaler bundle for OpenStack software required for Liberty, Mitaka, and Newton OpenStack versions.
2. Download the latest NetScaler bundle tar file to a temporary directory (for example, /tmp) in OpenStack Controller. This bundle includes the following drivers and plugins:
   - LBaaS V1 and LBaaS V2 drivers for OpenStack Liberty and Mitaka releases
   - LBaaS V2 driver for OpenStack Newton release
   - Heat plug-in for all OpenStack releases.
3. Run the following command to extract the files from the NetScaler driver tar file:

   ```
tar -xvzf <name_of_tar_file>
   ```

4. If you have an OpenStack <Release Name> setup, at the prompt, type the following command:

   ```
   cd <Release Name>
   ```

   **Example**:
   ```
   cd Liberty
   ```

5. Run the following command to install the driver and specify the NetScaler MAS IP address, the NetScaler driver password that you configured when you registered OpenStack with NetScaler MAS, and the protocol:

   ```
   ./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory-path>
   ```

   **Example for single node OpenStack setup**:
   ```
   ./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/opt/stack/neutron-lbaas
   ```

   **Example for multinode OpenStack setup**:
   ```
   ./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/usr/lib/python2.7/site-packages
   ```

**Note**

Providing the path of the neutron-lbaas directory of the system is optional. Providing the path might assist the script to find the drivers.
Note

After NetScaler MAS is registered successfully on OpenStack, you can log on to NetScaler MAS using your OpenStack user credentials also.

After NetScaler MAS is registered successfully on OpenStack, restart the OpenStack Neutron services.

Registering OpenStack with NetScaler MAS

To register OpenStack with NetScaler MAS using NetScaler MAS GUI

1. In NetScaler MAS, navigate to Orchestration > Cloud Orchestration > OpenStack.
2. Click Configure OpenStack Settings.
3. In Configure OpenStack Settings page, you can set the parameters to configure OpenStack in NetScaler MAS. You have two options here - Default and Customized.
4. Select Default, if the OpenStack services are running on default ports. For example, the default portal for Neutron services is 9696, the default portal for Keystone services is 5000.
   1. OpenStack Controller IP Address - IP address of the OpenStack controller (both the KeyStone service and the Neutron service should be reachable on this IP address). For example, enter the IP address 10.102.205.23.
   2. OpenStack Admin Username - administrative user name of the OpenStack controller. For example, enter admin1.
   3. Password - password of the administrative user of the OpenStack controller.
   4. OpenStack Admin Tenant - name of the administrative tenant on OpenStack. For example, enter admin.
Select deployment type as **Customized** if the OpenStack services are running on ports different from the default ports. If these services are running on different ports, specify them here.

- Specify the port numbers for the various OpenStack services.
- Specify the OpenStack Admin user name, password and OpenStack Admin Tenant user name as in Default settings.
5. In **OpenStack Neutron LBaaS - Credentials Used by NetScaler Driver** section, set the NetScaler Driver Password for the OpenStack NetScaler driver user account. NetScaler MAS authenticates the calls from the OpenStack NetScaler driver by using these credentials. You must specify the same password when you execute the NetScaler driver installation script in the OpenStack controller.
6. Click **OK**.

Creating a Tenant on OpenStack

Create a project or a tenant on OpenStack, add users to the project or tenant, and assign roles to all of the users. KeyStone, the Identity service in OpenStack provides authentication services for each OpenStack service. The authentication service uses a combination of domains, projects (tenants), users, and roles.

For more information on how to create a project, and to perform other tasks in OpenStack, see the OpenStack documentation at [http://docs.openstack.org/](http://docs.openstack.org/).

Adding OpenStack Tenants

1. In NetScaler MAS, navigate to **Orchestration > Cloud Orchestration > OpenStack > OpenStack Tenants**, and then click **Add**.
2. In **Add OpenStack Tenants** page, click **+Add**, and then select the OpenStack tenant.
3. Click **OK**.

Provisioning NetScaler Devices

Based on whether you are using pre-provisioned instance or auto-provisioning the instance when you are integrating the OpenStack, follow one of these two tasks:

**Pre-provisioning NetScaler Devices**

Install the NetScaler device on any of the hypervisor platforms like XenServer, KVM, or ESX, and add the instance to NetScaler MAS. NetScaler MAS then manages this device that load balances the traffic in the servers.

**To add an existing NetScaler VPX instance in NetScaler MAS**

1. In NetScaler MAS, navigate to **Infrastructure > Instances > NetScaler VPX**, and then click **Add**.
2. On the **Add NetScaler VPX** page, specify the IP address of the NetScaler VPX instance and select an instance profile from the **Profile Name** list. The instance profile contains the credentials used to logon to the NetScaler VPX. You can also create a new instance profile by clicking the + icon. Click **OK**.
Autoprosioning NetScaler Devices

Download the required NetScaler instance image from the Citrix download page, and upload it on Glance, the OpenStack Imaging service. Having an image available on Glance allows you to configure a NetScaler instance on-demand when assigning the instance to the tenant.

To auto-provision the NetScaler VPX devices on OpenStack

1. In NetScaler MAS, navigate to Orchestration > Cloud Orchestration > OpenStack.
2. Click Deployment Settings.
3. Set the following parameters:
   1. Management Network - select the management network on OpenStack, to which the auto-provisioned NetScaler VPX is connected.
   2. Profile Name - select the profile from the drop-down list. The NetScaler MAS uses the password contained in this profile to configure new auto-provisioned NetScaler VPX instances.
   3. Licenses - provide the NetScaler MAS license activation codes (LAC) used to license new auto-provisioned NetScaler instances. NetScaler MAS provisions NetScaler instances on OpenStack compute in management network, then triggers license installation on them using the specified license code. The NetScaler instance then downloads the license files from Citrix website using the LAC specified here.
   4. NetScaler VPX Image in Glance - select the NetScaler VPX image available in the OpenStack Glance that is used to create a NetScaler VPX instance.
   5. Proxy Settings - provide details of NetScaler proxy server for installing licenses. This may be required when NetScaler does not have direct access to the Internet through the management network.
4. Click OK.
Creating a Service Package in NetScaler MAS

To create service packages for a tenant in NetScaler MAS

1. In NetScaler MAS, navigate to Orchestration > Cloud Orchestration > OpenStack > Service Packages, and then click Add.
2. On the Service Package page specify the following parameters:
   1. Name - name for the service package. For example, enter SVC-PKG-GOLD.
   2. NetScaler Instance Allocation - the type of instance allocation defined in the service package based which NetScaler instance resources are allocated to a tenant. Select Dedicated. For more information on policies, see Service Package Isolation Policies.
   3. NetScaler Instance Provisioning - select Existing Instance to allocate an existing NetScaler instance to a tenant. If you want to create NetScaler instances during the configuration itself, select Create Instance OnDemand.
   4. NetScaler Instance Type - select NetScaler VPX.
      
      Note: Select NetScaler VPX to allocate pre-provisioned NetScaler instances hosted on SDX platform.
   3. Click Continue to associate a tenant with a service package.
      
      Note: Enable Provision pair of NetScaler instances for high availability, if you are deploying the NetScaler instances in high availability mode.
   5. In Assign Instances section, click Add, and then select the NetScaler instance that you want to assign to the tenant, and click Continue.
   6. In Assign OpenStack Tenants/Placement Policies section, under OpenStack Tenants, click Add, and select the
7. Click **Continue**, and then click **Done**.

**Note**: If the policy is not found, the fallback mechanism is revived, and the NetScaler MAS assigns NetScaler instances based on tenants. If the tenant is not part of any service package, the NetScaler MAS displays an error message that says: "Tenant <admin> is not part of any Service Package and there is no default Service Package."

Creating Placement Policies (Optional)

Isolation Policies are not tenant-based only. You can create flexible placement policies, where the policies are not only based on tenant name or id, but on other custom attributes also.

**To create placement policies for a tenant in NetScaler MAS**

1. In NetScaler MAS, navigate to **Orchestration > Cloud Orchestration > OpenStack > Placement Policy**, and then click **Add**.
2. On the **Add Placement Policy** page, set the following parameters:
   1. **Name** - type a name for the placement policy
   2. **Sample Expressions** - select a sample expression from the list. These examples are helpful to construct the placement policy.
   3. **Expression** - a Boolean expression is populated in this field based on the sample expression that you have selected in the earlier field. Edit the field names as required.
3. Click **OK**.

Auto-Provisioning NetScaler VPX Devices Deployed on NetScaler SDX Platform

Add the NetScaler SDX platform in NetScaler MAS, so that NetScaler MAS provisions the instances on this platform on-demand.

**To auto-provision NetScaler Instances Deployed on NetScaler SDX Platform**

1. In NetScaler MAS GUI, navigate to **Networks > Instances > NetScaler SDX**, and click **Add** to add a NetScaler SDX platform.
2. Navigate to **Orchestration > Cloud Orchestration > OpenStack > Deployment Settings**.
3. In **Management Network** section, select the management network on OpenStack to which the auto-provisioned NetScaler SDX is connected.
   1. In **Profile Name**, select the profile from the drop-down list. The NetScaler MAS uses the password contained in this profile to configure new auto-provisioned NetScaler VPX instances.
   2. Click **OK**.

4. To provision the NetScaler SDX platform in OpenStack, navigate to **Orchestration > Cloud Orchestration > OpenStack > Service Package**.
   1. Click **Add** to create a new service package.
   2. Enter the name of the service package.
   3. In **NetScaler Instance Allocation** field, select **Dedicated**.
   4. In **NetScaler Instance Provisioning** field, select **Create Instance OnDemand**, and in **Auto Provision Platform** field, select **NetScaler SDX**.
   5. By default, only NetScaler VPX instances are provisioned on NetScaler SDX platform.
   6. Click **Continue**.
   7. In **Auto Provision Settings** section, set the **Resources** properties.
      1. **Throughput** field. Enter 1000 Mbps.
      2. **NetScaler Version** field. From the drop-down field, select the right version of the NetScaler VPX image present on the NetScaler SDX platform.
   8. In **NetScaler SDX Platforms** section, click **Add** to add the SDX platform to the service package.
   9. Click **Continue**.
   10. In **Configure OpenStack Tenants** section, click **Add** to add the tenants. You can also add new tenants by clicking **New**.
   11. Click **Done**.

5. LBaaS V2 API implementations are performed through Neutron LBaaS commands. Connect to any Neutron client and execute the configuration tasks. For more information on how to execute configuration commands, see **Configuring LBaaS V2 using Command Line**.
Tom can now log on to the OpenStack Horizon portal and create an LBaaS pool and select a subnet where all the members of this pool are located in. Tom has to add a virtual IP (VIP) address and assign this VIP to the pool that he has created. Tom can also perform this on command line or through APIs. External clients for Tom's servers can connect to this VIP address, which is hosted on the assigned NetScaler, and NetScaler distributes all requests to the pool members on the configured ports.

LBaaS pool members are the load balanced servers that are added to the selected pool. Tom can assign a weight and a port to each of these members.

Health monitors are used to watch the health and good functioning of all members of the pool. Tom can create a health monitoring template in OpenStack by specifying delay, timeout, and retry limits, and also specify method, URL path, and expected HTTP codes upon success. After creating a monitor, Tom has to associate the monitor with the pool that was previously created.

For more information on how to create a pools, and other LBaaS configuration tasks in OpenStack, see OpenStack Documentation.

Important
LBaaS V1 is not supported in Liberty release of OpenStack. For more information, see OpenStack Release Notes.
Configuring LBaaS V2 using Command Line

Sep 17, 2016

LBaaS V2 supports SSL offload with certificates managed by Barbican, certificate bundles (includes intermediary Certification Authorities), SNI support along with the regular load balancing features. LBaaS V2 supports only command line interface to execute configuration tasks. LBaaS V2 API implementations are performed through Neutron LBaaS commands.

**Note**

Upload certificate and key to Barbican service when you require SSL offloading feature. Perform steps 1, 2, and 3 if SSL offloading is supported, else continue from step 4 to create a load balancer, a listener, a pool and a member.

1. Upload certificate to Barbican service using the following command:

   ```shell
   barbican secret store --payload-content-type <content_type> --name <certificate_name> --payload <certificate_location>
   
   Example: barbican secret store --payload-content-type='text/plain' --name='hp_server_certificate' --payload="hp_server/tmp/server_certificate"
   ```

2. Upload key to Barbican service using the following command:

   ```shell
   barbican secret store --payload-content-type <content_type> --name <key_name> --payload <key_location>
   
   Example: barbican secret store --payload-content-type='text/plain' --name='shp_server_key' --payload="hp_server/tmp/server_key"
   ```
Note

When you execute these two Barbican commands to load the certificate and the key, the Secret href fields provide a location or url. This is where the certificate and the key are stored on the system where OpenStack is installed. Copy these links and provide these links as parameters when you create the container on Barbican service in step 3.

3. Create a container in Barbican service to store the certificate and the key using the following command:

   In the command, replace `<certificate_url>` with the url that you obtained from the Secret href field when you uploaded the certificate. Similarly, replace `<key_url>` with the url that you obtained from the Secret href field when you uploaded the key.

   ```
   barbican secret container create --name <container_name> --type <container_type> --secret <certificate_url> --secret <key_url>
   Example: barbican secret container create --name="hp_container" --type='certificate' --secret="certificate=http://localhost:9311/v1/secrets/e36a4a82-87e4-4873-9efe-55108875ef58" --secret="private_key=http://localhost:9311/v1/secrets/1b9e1a93-2aeb-4101-8002-e52acab987b0"
   ```

   Copy the container href value. You have to provide the link to the container when creating the listener in step 6.

4. Set the environment variables in OpenStack. The variables enable the OpenStack client commands to communicate with the OpenStack services.

   ```
   export OS_PASSWORD=hp
   export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/
   export OS_USERNAME=hp_user
   export OS_TENANT_NAME=hp
   export OS_IDENTITY_API_VERSION=2.0
   export BARBICAN_ENDPOINT="http://10.106.43.15:9311/"
   ```
Note

Set these variables for every SSH session before running other commands. For more information about OpenStack environment variables, see [OpenStack environment variables](#).

5. Create a load balancer using the following command:

```
neutron lbaas-loadbalancer-create --name <loadbalancer-name> <subnet-name> --provider <netscaler>
```

**Example:**
```
neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --provider netscaler
```

The status changes from PENDING_CREATE to ACTIVE after the load balancer is successfully created.

6. Create a listener using the following command:

```
neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol_type> --protocol-port <port_number> --default-tls-container-id <container_url>
```

**Example:**
```
neutron lbaas-listener-create --name hp-lb-test-list --loadbalancer hp-lb-test --protocol TERMINATED_HTTPS --protocol-port 443 --default-tls-container-id http://10.106.43.15/v1/containers/d688676f-c256-4a0d-b84d-a310419cd0a
```

**Note**

If you are creating a listener without SSL offload support, execute the following command without providing locations to the container:

```
neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol_type> --
7. Create a pool using the following command:

```
neutron lbaas-pool-create --lb-algorithm <algorithm_type> --listener <listener-name> --protocol <protocol_type> --name <pool-name>
```

**Example:**
```
neutron lbaas-pool-create --lb-algorithm LEAST_CONNECTIONS --listener demolistener --protocol http --name demopool
```

8. Create a member using the following command:

```
neutron lbaas-member-create --subnet <subnet-name> --address <ip-address of the web server> --protocol-port <port_number> <pool-name>
```

**Example:**
```
neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --protocol-port 80 hp-lb-test-pool
```

Monitoring OpenStack Applications in NetScaler MAS

Your tenants can log on to NetScaler MAS using their OpenStack credentials to monitor VIPs and pools created from
OpenStack from any browser. The URL should be in the following format:

```
http://<mas_ip>/<admin_ui>/mas/ent/html/cc_tenant_main.html
```

Where, `<mas-ip-address>`, is the NetScaler MAS IP address that is registered with the OpenStack.

**Note**

- OpenStack VIPs correspond to virtual servers in NetScaler MAS.
- OpenStack Pools correspond to service groups in NetScaler MAS.
- OpenStack Pool members correspond to service group members in NetScaler MAS.
Manual Provisioning of NetScaler VPX Instance on OpenStack

Apr 24, 2017

In a few enterprise networks, NetScaler VPX instances cannot connect to Citrix license server to automatically download the licenses, for security reasons. In such a scenario, you need to manually deploy NetScaler VPX instances on OpenStack platform. Using the License Activation Code (LAC) received by you from Citrix, download the appropriate netScaler VPX license and save it on your local system.

To Manually Provision NetScaler VPX Instance on OpenStack

1. Install the NetScaler Driver Software and Register NetScaler MAS on OpenStack
   1. In NetScaler MAS, navigate to Orchestration > Cloud Orchestration > OpenStack.
   2. Click Configure OpenStack Settings. In Configure OpenStack Settings page, you can set the parameters to configure OpenStack in NetScaler MAS. You have two options here - Default and Customized.
   3. Select Default, if the OpenStack services are running on default ports.

2. Navigate to Orchestration > Cloud Orchestration > OpenStack, and click Deployment Settings.
   1. Management Network - select the management network on OpenStack, to which the auto-provisioned NetScaler VPX is connected.
   2. Profile Name - select the profile from the drop-down list. The NetScaler MAS uses the password contained in this profile to configure new auto-provisioned NetScaler VPX instances.
   3. NetScaler VPX Image in Glance - select the NetScaler VPX image available in the OpenStack Glance that is used to create a NetScaler VPX instance. The drop-down list will display only those images that are present on OpenStack Glance.

3. In NetScaler MAS, navigate to Orchestration > Cloud Orchestration > OpenStack > Service Packages, and then click Add.

4. On the Service Package page specify the following parameters:
   1. Name - name for the service package. For example, enter SVC-PKG-GOLD.
   2. NetScaler Instance Allocation - select Dedicated or Partitioned as the type of instance allocation defined in the service package.
   3. NetScaler Instance Provisioning - select Create Instance OnDemand to create NetScaler instances during the configuration itself.
   4. Auto Provision Platform - select OpenStack Compute. By default, NetScaler VPX will be selected as the instance type.
   5. Assign OpenStack Tenants/Placement Policies - section, under OpenStack Tenants, click Add, and select the tenant.
   6. Click Continue, and then click Done.

5. Navigate to System > System Administration > Change System Settings and select http from the drop-down list.

6. Navigate to Networks > Instances > NetScaler VPX.

7. In NetScaler VPX page, click Admin drop-down list and select Provision Device.
1. On the **Device Provisioning** page, enter the name of the device, and select the service package that you created in the previous step.

2. Click **OK**.

8. Navigate to **Orchestration > Cloud Orchestration > OpenStack > Requests** tab. Select the request and click **Tasks** to view the tasks. When the status of the task changes to **Finished**, it means that the NetScaler VPX is provisioned in NetScaler MAS.

9. Navigate to **Networks > Instances > NetScaler VPX** to check that the NetScaler VPX instance appears in NetScaler VPX page.

10. Click the NetScaler VPX instance. When the NetScaler VPX instance opens in your browser window, log on to the instance. Navigate to **Configuration > System > Licenses**, and manually add the new license. For more information on how to add new license, see [NetScaler Licensing Overview](#).

11. Restart the NetScaler VPX instance.
12. After a few minutes, you can log on to OpenStack and in System > Instances, you can see that the NetScaler VPX instance is deployed on OpenStack.

13. LBaaS V2 API implementations are performed through Neutron LBaaS commands. Connect to any Neutron client and execute the configuration tasks. For more information on how to execute configuration commands, see Configuring LBaaS V2 using Command Line.
Integrating NetScaler MAS with OpenStack Heat Services

Dec 27, 2016

The OpenStack Neutron LBaaS enables core load balancing services, such as load balancing, SSL offloading, and content switching, for applications. LBaaS is managed through a RESTful API, and the API allows tenants to make REST calls to create, update, and delete LBaaS objects. Because LBaaS provides load balancing services, it does not allow use of the more advanced NetScaler features during the orchestration process. The NetScaler Heat plug-in overcomes this limitation.

Heat Orchestration Service

The OpenStack Heat orchestration service allows deployment of complex cloud applications on the basis of templates. The Heat orchestration template (HOT) describes the infrastructure for a cloud application in text files that are readable and writable by humans, and can be managed by version control tools. YAML, a structured language, is used to write these templates. The HOT template allows you to create most of the OpenStack resource types and specifies the relationships among the resources defined within it. The NetScaler Heat plug-in allows you to configure advanced application delivery controller (ADC) functionalities on any NetScaler instance.

NetScaler StyleBooks

NetScaler MAS StyleBooks can be used to create and configure NetScaler ADC functionalities. Just like Heat templates, the StyleBooks are also written in YAML. A separate StyleBooks can be created for each functionality, and a single StyleBooks can be used to deploy configurations on multiple NetScaler instances.

The StyleBooks shipped with NetScaler MAS enables you to create configurations for your deployment. During NetScaler integration with OpenStack, NetScaler MAS publishes these StyleBooks as a resource in the Heat service. The Heat template allows you to configure the advanced features of NetScalers using these StyleBooks resources.

Workflow to Configure NetScaler Instances using Heat

The following flowchart illustrates the workflow for deploying the Heat stack:
Perform the following tasks as a cloud administrator:

**To configure Heat services in OpenStack**

1. **Download NetScaler bundles for OpenStack**
   
   Install the NetScaler bundles in OpenStack. In NetScaler MAS, navigate to **Downloads** and download the NetScaler driver bundles, untar the bundles, and copy the contents of the Heat folder in the bundle to the Heat engine resources directory in OpenStack. The directory path is as follows:

   `/opt/stack/heat/heat/engine/resources/netscaler_resources`

2. **Create a section “netscaler_plugin” in the heat.conf file, and update the following parameters in that section:**

   ```
   [netscaler_plugin]
   NMAS_BASE_URI=<openstack_uri:port>>
   NMAS_USERNAME=<openstack_driver_username>
   NMAS_PASSWORD=<openstack_driver_password>
   ```

3. **Restart the Heat service in OpenStack.**

   When you restart the NetScaler Heat services in OpenStack, all the defined NetScaler MAS StyleBooks are imported into Heat as resources. Also, the NetScaler network resource and the certificate resource are imported into OpenStack as NetScaler Heat resources.

4. **Register NetScaler MAS with OpenStack.**

   1. In NetScaler MAS, navigate to **Orchestration > Cloud Orchestration > OpenStack**, and click **Configure**
OpenStack Settings.

2. In **Configure OpenStack Settings** page, you can set the parameters to configure OpenStack. You have two options here: Default and Customized.

3. Select **Default** if the OpenStack services are running on default ports. Enter the following parameters:
   
   a. OpenStack Controller IP Address
   b. Admin Username
   c. Password
   d. OpenStack Admin Tenant
   e. NetScaler Driver and Heat password

   **Note**: This is the same password (NMAS_PASSWORD) that you entered in the heat.conf file.

5. Create service packages and define the SLAs with your tenant.

   A tenant is created in NetScaler MAS for each user during OpenStack registration, and the tenant information is used by both the LBaaS driver and the Heat plug-in. The Heat plug-in uses this information to contact NetScaler MAS to import StyleBooks as Heat resources in OpenStack.

   **Note**: For more information about creating service packages and other pre-configuration tasks in NetScaler MAS and OpenStack, see [Integrating NetScaler MAS with OpenStack Platform](https://docs.citrix.com).

6. Observe that all the relevant Stylebooks in NetScaler MAS are imported into OpenStack Heat as resources. Also, observe that the NetScaler network resource and NetScaler certificate resource are imported into OpenStack Heat as resources.

   **Note**: Currently, you can use only the StyleBooks that are shipped with NetScaler MAS.

Your tenant can now create the Heat template in OpenStack, enter the values of the required Heat parameters, and deploy the Heat stack. When the Heat stack is deployed, the configuration is pushed to NetScaler MAS, and the required NetScaler instances are configured.

**To prepare Heat template and launch Heat stack**

1. In OpenStack, the tenant can create a Heat orchestration template (HOT) by using the Heat resources.
2. In OpenStack Horizon, the tenant admin can navigate to **Project > Orchestration > Stacks** to create the Heat template and launch the Heat Stack. There are two ways to create HOT:
   - **File**: Select the updated template from the local directory
   - **Direct input**: Copy and paste the YAML contents from the template in the window

   **Note**: After successfully deploying the stack, the tenant can update the stack by using the Change Stack Template. But the subnet information and the virtual IP address (VIP) that was provided initially during creation of stack cannot be
After the tenant deploys the stack, navigate to **Orchestration > Cloud Orchestration > OpenStack > Requests** in NetScaler MAS to observe the lists of tasks. Also, navigate to **Applications > Configuration** in NetScaler MAS to observe that the NetScaler instances are successfully configured in the form of StyleBooks configpacks.

### An Example of a NetScaler MAS StyleBooks

The following image shows an example of how a NetScaler MAS StyleBooks is constructed and briefly explains the components. For more information about NetScaler MAS StyleBooks and how to use the shipped StyleBooks, see [StyleBooks](#).

![NetScaler MAS StyleBooks Example](image)

### An Example of a Heat Template

The following image shows the structure of a Heat template defined in YAML, and points to the StyleBooks resources and NetScaler network resources that are imported as Heat resources.
For more information about Heat services and how to create templates, see OpenStack Heat documentation.
Configuring Layer 7 Content Switching

Dec 29, 2016
NetScaler MAS orchestrates with OpenStack to configure the Layer 7 (L7) switching or content-based switching functionalities on NetScaler instances. Content switching differs from simple load balancing in that specific types of requests can be directed to specific servers. When the L7 configurations are created in OpenStack with a NetScaler instance as the provider, NetScaler MAS allots a NetScaler instance, and deploys content switching and responder configurations corresponding to the L7 configurations. The NetScaler instances can then distribute and load balance user requests on the basis of application-layer characteristics of the requests.

The OpenStack layer 7 (L7) load balancing feature combines load balancing and content switching to provide optimized delivery of specific types of content. This improves the performance of the load balancer by executing only those policies that are applicable to the content. Layer 7 load balancing also facilitates increased efficiency of the application infrastructure. The ability to separate out content according to type, URI, or data allows better allocation of physical resources in the application infrastructure. For example, an end user browsing to "http://example-sports.com/about-us" should be served by a pool of servers hosting content about the company and the services, while a user browsing to "http://example-sports.com/shopping-cart-football" should be served by a different pool of servers that allows the users to make online purchases.

In L7 switching, a load balancer is implemented as a content switching virtual server that accepts HTTP requests from users and distributes those requests to the application servers. L7 switching or content switching allows you to have a single-point entry to access a variety of the back-end services (for example, not just web applications, web service portals, web mails, but also mobile management, content in different languages, and so on). That is, you can provide one public IP address for all services you are offering your users.

Unlike lower-level load balancing, Layer 7 switching does not require that all servers in the pool have the same content. A load balancer configuration using L7 switching expects the application or back-end servers from different pools to have different content. L7 switches can direct requests on the basis of URI, host, HTTP headers, or anything else in the application message. The application servers should essentially serve specific types of content. For example, one server could serve only images, another could execute server-side scripting languages, such as PHP and ASP, and another could serve static content such as HTML, CSS, and JavaScript.

L7 Rules

The following attributes are defined in a rule for evaluating the traffic and they are compared against the values defined in the rule:

- hostname: The hostname in the HTTP request is compared against the value parameter in the rule. For example, "www.example-sports.com"
- path: The path portion of the HTTP URI is compared against the value parameter in the rule. For example, "www.example-sports.com/shopping-cart/football_pump.html"
- file_type: The last portion of the URI is compared against the value parameter in the rule. For example, txt, html, jpg, png, xls, and others.
- header: The header defined in the key parameter is compared against the value parameter in the rule.
- cookie: The cookie named by the key parameter is compared against the value parameter in the rule. The cookie request-header field value contains a name and value pair of information stored for that URL; the general syntax is as follows - Cookie: name=value. For example, a rule that is looking for a cookie named 'stores' with the value starting with
Comparison Types

When evaluating the traffic, the L7 policy compares the following expressions against the attributes defined in the rule.

- regex: Perl type regular expression matching
- starts_with: String start with
- ends_with: String ends with
- contains: String contains
- equal_to: String equals

Note: The hostname, path, header, and cookie attributes support all comparison types, but the file_type attribute supports only regex and equal_to.

L7 Policies

An L7 policy processes the incoming HTTP traffic and returns a "true" value when all the rules defined in the policy are matched.

In any L7 policy, all the rules are logically joined with an AND operator. A request must match all the rules so that the policy returns a "true" value. The action taken by the load balancer is based on the value returned by the policy. You can create a second policy with the same action to achieve a logical OR operation between the rules.

For example, you can create one policy where the incoming HTTP request can contain the words "EXAMPLE-SPORTS," "SPORTS-FOOTBALL," or "EXAMPLE-FOOTBALL" so that the load balancer takes the appropriate action of forwarding these requests to the server-pool of the Example-sports ecommerce company to serve the requested content. You can create another policy that takes the same action but matches "example-sports," "example-sports-football," or "example-football." When a user sends an HTTP request with any of these six keywords, the load balancer forwards the request to the Example-Sports server.

Depending on the rules defined in the policy, an L7 policy can take any of the following actions:

- Redirect to pool - Forward the request to the application server pool identified by the rules associated with the L7 policy. That is, you can create an application rule to direct requests to a specific load balancer pool according to domain name. For example, you can create a rule that directs some requests to example-football.com to pool_1, and other requests to example-sports-online_purchase.com to pool_2.
- Redirect to URL - Send the client a redirect HTTP response in which the location response header contains the new location. The browser will update the address bar with the new location and issue a new request. The use cases are many. For example, if a website address has changed, you can redirect requests to the new address instead of dropping. Or, during website maintenance, you can redirect the users to a read-only site.
- Reject - Rejects the request and takes no further action. For example, you can return a 401 Unauthorized response to deny access to the users for restricted web pages.

A content switching configuration consists of a content switching virtual server, a load balancing setup consisting of load balancing virtual servers and services, and content switching policies. After you create your content switching virtual server and policies, you bind each policy to the content switching virtual server. When binding the policy to the content switching virtual server, you specify the target load balancing virtual server. When a request reaches the content switching virtual server, the virtual server applies the associated content switching policies to that request. The priority of the policy defines
the order in which the policies bound to the content switching virtual server are evaluated.

Any pool that has the listener ID can be assigned as a default pool of virtual servers to which traffic is diverted. The pool is loosely bound with a listener, and becomes associated with a listener only through implementation of an L7 policy. A pool can also be created directly under a load balancer without necessarily being tied to a listener. In such a case, the pool is created in a "pending_create" state. Because the L7 policies are tightly bound with the listeners, an L7 policy containing the pool ID must be created and implemented for the pool to become "active" and start receiving traffic requests.

A pool can be served by multiple L7 policies, but remains in the "active" state if at least one policy is attached to it. When the last policy is removed, the pool goes back into the "pending_create" state until another policy is created and associated with it. If the pool itself is removed, all HTTP requests that it would otherwise have received are redirected to the default pool.

**Mapping Between OpenStack L7 Policies and NetScaler Entities**

<table>
<thead>
<tr>
<th>OpenStack</th>
<th>NetScaler Entity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L7 policy with action REDIRECT_TO_POOL</td>
<td>Content switching policy &gt; Content switching action</td>
<td>NetScaler MAS creates a content switching policy that is bound to the content switching virtual server and associated with a content switching action that specifies the target pool of application servers for content retrieval and presentation to the user.</td>
</tr>
<tr>
<td>L7 policy with action REDIRECT_TO_URL</td>
<td>Responder policy &gt; Responder action</td>
<td>NetScaler MAS creates a responder policy that is bound to the content switching virtual server and associated with a responder action that specifies the target URL to be presented to the users.</td>
</tr>
<tr>
<td>L7 policy with action REJECT</td>
<td>Responder policy &gt; Drop the request</td>
<td>NetScaler MAS creates a responder policy that is bound to the content switching virtual server and associated with a responder action that drops the request.</td>
</tr>
</tbody>
</table>

If the action of an L7 policy that evaluates to "true" redirects traffic to a pool that is in "create_pending" state, NetScaler MAS implements the specified pool along with a load balancing virtual server. NetScaler MAS creates a content switching policy out of the L7 policy and uses the corresponding content switching action to redirect the requests to the load balancing virtual server associated with that pool. If a second L7 policy redirects to the same pool, NetScaler MAS creates a content switching policy and a content switching action to redirect the traffic to the existing load balancing virtual server associated with the pool.

**Policy Positioning**

Evaluation of L7 policies in OpenStack is determined by their priorities. In OpenStack, by default, the policies are assigned priorities in the order in which they are created. The policy created first is numbered "1," and subsequently created policies
are numbered consecutively. But you can change the priorities of the policies and assign them different priorities. The policies are always evaluated in the order of their priorities. The first policy that matches a specific request is always executed first.

When creating policies, note the following points:

- If you assign a new policy the same priority as an existing policy, the new policy takes that priority. The existing policy's priority is lowered. If necessary, the priorities of other policies are also lowered to retain the order in which the policies are evaluated.
- If you create a new policy without specifying a position, the new policy will just be appended to the list.
- If you create a new policy and assign it a position that is greater than the number of policies already in the list, the new policy will be appended to the list, that is, the new policy always takes the next available priority. For example, if there are three policies A, B, and C with priorities 1, 2, and 3, and if you create a policy and assign a priority of 8, the new policy's priority becomes 4.
- If you add a policy to the list or delete a policy from the list, the policy position values are re-ordered from 1 without skipping numbers. For example, if policy A, B, C, and D have position values of 1, 2, 3, and 4, and if you delete policy B from the list, policy C now takes the second position, and policy D takes the third position.

In NetScaler MAS, there is always a default policy associated with a csvserver with a priority of 1. This default policy specifies the number of TCP connections that an lbvserver should process at any given point of time. Therefore, when the corresponding responder policies and content switching policies are created in NetScaler, they are always assigned a priority 1 greater than the priority of the corresponding L7 policy. For example, when an L7 policy with a priority of 1 is evaluated and a content switching policy is created with a priority of 2. Similarly, when an L7 policy with a priority of 2 is evaluated and a responder policy is created with a priority of 3.

In OpenStack, the "reject" and/or "redirect_to_url" policies are first evaluated, and then the "redirect_to_pool" policy is evaluated. In a NetScaler instance, the responder policies are always evaluated first to either drop the request or present the user with a redirected web address, and the content switching policies are evaluated last. This order of evaluation usually does not cause any conflict if the content switching and responder policies are mutually exclusive. That is, two L7 policies should not have identical expressions. The derived expressions should be added in the responder and content switching policies to avoid such conflicts. For example, write an expression to reject all requests to "sports-football.com" and another expression to allow requests to "example-sports-football.com." Create the L7 policies so that all the responder policies to reject the request are arranged at the top of the evaluation list, followed by the responder policies for web direct, followed by the content switching policies.

In NetScaler MAS, there is always a default policy associated with a csvserver with a priority of 1. This default policy specifies the number of TCP connections that an lbvserver should process at any given point of time. Therefore, when the corresponding responder policies and content switching policies are created in NetScaler, they are always assigned a priority 1 greater than the priority of the corresponding L7 policy. For example, when an L7 policy with a priority of 1 is evaluated and a content switching policy is created with a priority of 2. Similarly, when an L7 policy with a priority of 2 is evaluated and a responder policy is created with a priority of 3.

In OpenStack, the "reject" and/or "redirect_to_url" policies are first evaluated, and then the "redirect_to_pool" policy is evaluated. In NetScaler, the responder policies are always evaluated first to either drop the request or present the user with a redirected web address, and the content switching policies are evaluated last. This order of evaluation usually does not cause any conflict if the content switching and responder policies are mutually exclusive. That is, no two L7 policies should have similar expressions. Similar derived expressions should be added in the responder and content switching policies to avoid such conflicts. For example, write an expression to reject all requests to "sports-football.com" and another expression
to allow requests to "example-sports-football.com." Create the L7 polices so that all the responder policies to reject the request are arranged at the top of the evaluation list, followed by the responder policies for web direct, followed by the content switching policies.

Configuration Tasks

The L7 policy and action implementations are performed through Neutron LBaaS commands.

Set the environment variables in OpenStack and create the load balancer (for example, LB1). After the load balancer is successfully created, create the listener and pools (for example, L1, P1, and P2), and add members and monitors to the pools. For example, P1 is the default pool for L1, while P2 is the pool tied to LB1 and managing the application servers.


The following commands create the policies and define the specific actions:

Create L7 Policy to Drop Requests

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <listener name> --action <action-name>
```

**Example:**

```
neutron lbaas-l7policy-create --name policy11 --action REJECT --listener L1
```

The above command creates and binds policy11, a responder policy, to the content switching server to reject requests. Because no rule was created for this policy, the policy evaluates to "false" and the request is rejected.

Create L7 Policy to Redirect Requests to Particular URL

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <listener name> --action <action-name> --redirect-url <redirect-url>
```

**Example:**

```
neutron lbaas-l7policy-create --name policy12 --action REDIRECT_TO_URL --listener admin-list1 --redirect-url http://example-sports/about-us.html
```

The above command creates a responder action to redirect requests to a URL, creates a responder policy with action, and binds this policy to the content switching virtual server.
The above two rules can be connected with an AND operator to derive the expression for the responder policy.

Create L7 Policy to Redirect Requests to a Pool

```
neutron lbaas-l7rule-create --type HOST_NAME --compare-type CONTAINS --value <value-string> <L7 policy name>
```

```
neutron lbaas-l7rule-create --type PATH --compare-type CONTAINS --value <value-string> <L7 policy name>
```

Example:

```
neutron lbaas-l7policy-create --name policy13 --action REDIRECT_TO_POOL --listener admin-list1 --redirect-pool admin-pool2
```

If this is the first L7 policy, the above command implements P2 along with LB1, creates the content switching redirect action and redirects the requests to LB1. If P2 already exists, the command creates the content switching redirect action and redirects the requests to LB1.
For tenants connecting from private networks, the NetScaler MAS supports isolation policy so that each tenant has its own dedicated partition, a dedicated VLAN, and dedicated servers. For tenants connecting from public networks, a dedicated VLAN will require too many IP addresses to be used. A shared VLAN circumvents this problem by creating one virtual IP address on each partition thus creating a single IP subnet.

When an tenant configures a VIP or a listener, an admin partition is created in the NetScaler device for that tenant. All load balancer configuration is pushed to that admin partition that is created. If the tenant is using a shared network or an external network to create a load balancer, then the VLAN of that network is added and the sharing feature is enabled. When a different tenant uses the same shared network to create its load balancer, the VLAN is not added to the NetScaler again, but the VLAN will be bound to the second partition as well. Thus, any tenant who uses the same shared network gets a partition which is bound to the same VLAN.

The NetScaler MAS supports virtual destination MAC address. When tenants share a VLAN, the NetScaler MAS assigns different MAC addresses to the partition on the NetScaler device. This allows a VLAN to be shared across partitions or across all tenants and all traffic domains.

Configuring Shared VLAN from NetScaler Instance

1. In a NetScaler instance, navigate to Configuration > System > Network > VLANS, select a VLAN profile, and click Edit
to set the partition sharing parameter.

2. On the **Configure VLAN** page, select the **Partitions Sharing** check box.

3. Click **OK**.

---

**Configuring Shared VLAN from OpenStack Orchestration**

1. In OpenStack, navigate to **Admin > System > Networks**, and then click **Create Network**.

2. In **Create Network**, set the following parameters:
   1. Name - enter the name of the network
   2. Project - select a project from the drop-down list
   3. Provider Network Type - select **VLAN** from the drop-down list. This defines that the virtual network is established as VLAN.
   4. Physical Network - the default physical network is selected here. You can edit this.
   5. Admin State - by default, the administrative state of the network is UP
   6. Select **Shared** and **External Network** to define that the VLAN is shared and is using an external network.

3. Click **Create Network**.
Create a new network for any project as you need. Provider specified network can be created. You can specify a physical network type (like Flat, VLAN, GRE, and VXLAN) and its segmentation ID or physical network name for a new virtual network.

In addition, you can create an external network or a shared network by checking the corresponding checkbox.
Trial Licensing Workflow Enhancement

Jun 29, 2016

During auto-provisioning of the NetScaler VPX instance using OpenStack orchestration, the NetScaler Management and Analytics System (MAS) uses OpenStack Compute to launch a NetScaler VPX instance. The newly provisioned NetScaler VPX instance contacts the Citrix licensing portal during the set up, and uses the License Activation Code (LAC) to automatically download and install the license files.

Trial Licenses

Technical support staff use trial licenses when they install NetScaler MAS and NetScaler VPX devices in field. A trial or evaluation license for NetScaler VPX is valid for 90 days. If there is a need to evaluate more than one NetScaler or extend the testing after 90 days, a new evaluation license needs to be requested. Instead of automatic installation of trial license files, NetScaler MAS provides you an alternate solution. You can manually download the license files and install them on NetScaler VPX to complete the installation of the instance.

If the NetScaler VPX is unable to connect to the internet, configure the NetScaler MAS to act as a proxy server for the Citrix Licensing Portal and install the license files.

NetScaler VPX instances that have a trial license can communicate with NetScaler MAS on HTTP only. To configure HTTP communication in NetScaler MAS, navigate to System > System Administration, and click Change System Settings. Select http from the drop-down list to set the communication method, and click OK.

Modify System Settings

- Communication with instance(s): http
- Secure Access Only
- Enable Session Timeout
- Allow Basic Authentication
- Enable nsrecover Login
- Enable Certificate Download
- Enable Shell access for non-nsroot User

OK Close
Service Package Isolation Policies

Jun 29, 2016

Dedicated Isolation Policy

Every tenant associated with the NetScaler MAS service package of a dedicated policy is assigned a NetScaler instance from among the instances that are part of this service package. This assigned NetScaler instance is not shared with other tenants.

Partition Isolation Policy

Every tenant associated with the service package of partition policy is assigned a dedicated logical admin partition of a NetScaler instance that is part of the service package.
Shared Isolation Policy

Tenants associated with the service package share the NetScaler instances that are part of the service package. All configurations of a tenant are assigned to one NetScaler instance. In this mode, configurations from multiple tenants can be hosted on the same NetScaler instance. You can select **NetScaler VPX** or **NetScaler MPX** as device type. You can choose to allot only one NetScaler instance or many instances to the service package. That is, multiple tenants can share one or multiple virtual instances of the NetScaler device.

**Note:** Add NetScaler SDX instances in the service packages as NetScaler VPX instances only, as a NetScaler SDX has a NetScaler VPX provisioned on it.
You can also create flexible placement policies, where the policies are not only based on tenant name or ID, but on other custom attributes. For more information on flexible placement policies, see **Flexible Policy-Based Device Allotment**.
Flexible Policy-Based Device Allotment

Jul 01, 2016

NetScaler Management and Analytics Systems (MAS) assigns NetScaler virtual instances to tenants, based on the SLAs agreed with the tenants. The assignment of virtual instances to tenants creates a one-to-one relation between the instance and the tenant, where a tenant can be assigned to only one service package in the data center.

In some situations, tenants might require more than one instance, or the assignment of instances might not be based on tenants as a criterion, but on other factors such as network ID, or application. In such cases, NetScaler MAS allows you to precisely define placement policies based on user-defined expressions in order to assign a load balancer configuration to one of the managed instances.

Placement policies provide the flexibility to decide on the NetScaler instance that is used in each load balancer configuration created by users. Flexible placement policies in NetScaler MAS provide an added option to the existing method of assigning NetScaler instances based on tenants.

Note

You can assign instances to tenants manually or use placement policies to assign instances based on the expressions created. You cannot use both these methods simultaneously on a single service package.

Placement policies are based on Boolean expressions defined over properties of the main LBaaS configuration objects, such as pools and load balancers. The placement policy user interface in NetScaler MAS provides pre-defined expressions that you can choose from, to define a customized policy. You can create multiple placement policies for different expressions. So, each tenant can have multiple devices that are defined by the tenant's requirement.

You have to first select an expression to match a root object that has to be configured later. The root object can be a pool object in case of LBaaS V1, and a load balancer object in case of LBaaS V2. So, the NetScaler MAS policy based placements are supported for both LBaaS V1 and V2 APIs. These placement policies are then associated with service packages. Once the root object is placed in an instance, the successive objects in the model are added in the instance.

For example, the pool configuration object can have the following properties:

- tenant_id
- name
- description
- protocol
- lb_method
- subnet_id
- subname_name
- admin_state_up
- status
- network_id
- network_type
- segmentation_id
- subnet_cidr
The following are examples that show some of the expressions that uses pool properties to define an expression for the policy:

1. Pool Name based policy expression
   
   ```python
   config["pools"]["name"] == "high-end-pool"
   ```

2. Pool Subnet Name based policy expression
   
   ```python
   config["pools"]["subnet_name"] == "us-west-payment-subnet1"
   ```

3. Load Balancer Subnet Name based policy expression
   
   ```python
   config["loadbalancers"]["subnet_name"] == "mas-subnet"
   ```

Adding Placement Policy

1. From the NetScaler MAS home page, navigate to **Orchestration > Cloud Orchestration > Placement Policy**, and then click **Add**.

2. On the **Add Placement Policy** page, set the following parameters:
   1. Name - type a name for the placement policy
   2. Frequently Used Expressions - select an expression from the drop-down list.
   3. Expression - a logical (Boolean) expression is populated in this field based on the expression you have selected in the earlier field. Edit the field names as required.

   **Note:** When creating multiple policies, make sure that the policies are exclusive to one another.

3. Click **OK**.

4. Navigate to **Orchestration > Cloud Orchestration > OpenStack > Service Packages**, and then click **Add**.
5. On the **Service Package** page, set the following parameters:
   a. Name - type a name for the service package
   b. Isolation Policy - select **Shared** policy
      In shared isolation policy, the load balancer configuration of a tenant coexists with the load balancer configuration of other tenants in the device allocated to the tenant.
   c. Device Type - select a preprovisioned **NetScaler VPX** or **NetScaler MPX**
      Select **Allot one device** if you want all the load balancer configurations of a tenant to be tied to one device. Select **Allot many devices** if you want each load balancer configurations of a tenant to be distributed on several devices based on placement policies.
      **Note**: NetScaler SDX has to be added in the service packages as NetScaler VPX instances only, as a NetScaler SDX has a NetScaler VPX provisioned on it.
   d. Placement Method - select **Least Configured**
      When Least Configured is selected, the NetScaler instance that has the least number of pool members configured at that point in time is chosen as the device for the tenant.

6. Click **Continue**.
7. In Assign Devices section, add the available NetScaler devices to the configured devices list.

8. Click Continue.

9. In Assign Placement Policies/OpenStack Tenants section, add the placement policy that you created earlier.

Note: If the policy is not found, the fallback mechanism is revived, and the NetScaler MAS assigns NetScaler instances based on tenants. If the tenant is not part of any service package, the NetScaler MAS displays an error message that says: "Tenant <admin> is not part of any Service Package and there is no default Service Package."

10. Click Continue, and then click Done.
Integrating NetScaler Appliances with VMware NSX

Jul 01, 2016

In Software Defined Networking (SDN), a software application controller manages a network and its activities instead of hardware that supports the network. That is, SDN allows the network administrators to virtualize a physical network connectivity into a logical network connectivity and manage network services using a software based centralized management tool. SDN allows network engineers and administrators to respond to rapidly changing business requirements.

While the better known advantages of SDN are traffic programmability, greater agility, the ability to create policy driven network supervision, and implementing network automation, some of the specific advantages of SDN are listed below:

- Centralized network provisioning
- Increased network security at granular level
- Reduced operating costs
- Increased levels of cloud abstraction
- Guaranteed content delivery
- Reduced network downtime

NetScaler Management and Analytics System (MAS) supports SDN in enterprises network by integrating with SDN controllers of different vendors.

NetScaler MAS integrates with VMware network virtualization platform to automate the deployment, configuration, and management of NetScaler services. This integration abstracts away the traditional complexities associated with physical network topology, enabling vSphere/vCenter admins to programmatically deploy NetScaler services faster.

VMware NSX exposes logical firewalls, switches, routers, ports, and other networking elements to allow virtual networking among diverse hypervisors, cloud management systems, and associated network hardware. It also supports external networking, and security services.

The Cloud Orchestration feature of NetScaler MAS enables the integration of Citrix NetScaler products with VMware NSX, and provides the following capabilities:

- Ability to allocate a pre-provisioned VPX on-demand to a certain Edge gateway as part of service insertion.
- Ability to configure advanced features of NetScaler such as SSL and CS along with basic load balancing through application templates on the instances that are running inside NSX environment.
- Ability to de-allocate a VPX from a certain Edge gateway as part of service deletion and re-allocate the same VPX for another Edge gateway.
- Ability to rapidly deploy NetScaler ADC functions from the vCenter console as part of the deployment workflow of all the infrastructure required for an application.

Benefits:

- Automated, on-demand allocation of new ADC services as part of an application deployment workflow
- Simplified configuration of application specific, advanced ADC functionality through application templates
- Multi-tenant separation-of-duties and a self-service consumption model while providing cloud administrators a single point of control
- Easier integration with NetScaler MAS API's, which help to support unanticipated future uses.

Prerequisites

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved. p.513
• Install VMware ESXi version 4.1 or later with hardware that meets the minimum requirements.
• Install VMware Client on a management workstation that meets the minimum system requirements.
• Install VMware OVF Tool (required for VMware ESXi version 4.1) on a management workstation that meets the minimum system requirements.
• Install NetScaler Management and Analytics System on any of the supported hypervisors.

For tasks to install NetScaler MAS build 11.1, on any of the supported hypervisors, see Installing NetScaler MAS Single Server Deployment.

VMware ESXi Hardware Requirements

The following table lists the virtual computing resources that you require on your VMware ESXi server to install a NetScaler MAS virtual appliance.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td>Virtual CPU</td>
<td>8</td>
</tr>
<tr>
<td>Storage space</td>
<td>500 GB</td>
</tr>
<tr>
<td>Virtual Network Interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Throughput</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

**Note:** The memory and hard disk requirements specified above are for deploying NetScaler MAS on VMware ESXi server, considering that there are no other virtual machines running on the host. The hardware requirements for VMware ESXi server depends on the number of virtual machines running on it.

Integrating NetScaler MAS with VMware NSX

This section provides you with a list of tasks that you have to perform on both VMware NSX Manager and on NetScaler MAS.

**Note:** Make sure that VMware NSX for vSphere 6.2 and above is installed and configured, and the edge gateways, DLR, and virtual machines that have to be load balanced are already created.

Configuring VMware NSX

• Create a pool of NetScaler VPX instances of different capacities, which are added to the different service packages.

For example:

• Create five NetScaler VPX instances of VPX1000 (1 Gbps). These instances are added to the Gold service package.
Create five NetScaler VPX instances of VPX10 (10 Mbps). These instances are added to the Bronze service package.

In vSphere client, navigate to Networking, and create a port group of type VLAN trunking with range, for example, 101-105 (you can even provide the full range, but create port group of type VLAN for only the required VLANs).

![New Distributed Port Group](image)

Create a new interface for each NetScaler VPX instance, and attach it to the VLAN range trunk port group that was created above.
In vSphere client, navigate to **Networking**, and create a port group of type VLAN. For example, if the initial trunked port group was created with range 101-105, create five VLAN port groups one per VLAN, that is a port group with VLAN 101, another with VLAN102, and so on, until VLAN 105.
### Adding NetScaler VPX Instance in NetScaler MAS

Add NetScaler VPX instances in NetScaler MAS and specify the VLAN range of the trunked group for each device.

1. In NetScaler MAS, navigate to **Infrastructure > Instances > NetScaler VPX**, and click **Add**.

2. On the **Add NetScaler VPX** page, specify either the host names of the instances, the IP address of each instance, or a range of IP addresses, and then select an instance profile from the **Profile Name** list. You can also create a new instance profile by clicking the + icon.

3. Click **OK**.

4. Select the newly added NetScaler VPX instance from the list on the **NetScaler VPX** page, and click the down arrow button in **Action** field. Select **Configure Interfaces for Orchestration**.

---

**New Distributed Port Group**

- **Port binding:** Static binding
- **Port allocation:** Elastic
  - Elastic port groups automatically increase or decrease the number of ports as needed.
- **Number of ports:** 8
- **Network resource pool:** (default)

**VLAN**

- **VLAN type:** VLAN
- **VLAN ID:** 100

**Advanced**

- Customized default policies configuration
5. On the **Interfaces** page, select the management interface, and click **Disable** to disable VLAN from binding to the management interface.

6. On the **Interfaces** page, select the required interface, and click **Configure VLAN Range**.

7. Enter the VLAN range configured in NSX Manager, click **OK**, and then click **Close**.
Registering VMware NSX Manager with NetScaler MAS

Register VMware NSX manager with NetScaler MAS to create a communication channel between them.

1. In NetScaler MAS, navigate to Orchestration > Cloud Orchestration > Cloud Platform, select NSX Manager from the drop-down list, and click Get Started.

2. On Configure NSX Manager Settings page, set the following parameters:
   
a. NSX Manager IP Address - IP address of NSX Manager.
   
b. NSX Manager Username - Administrative user name of NSX Manager.
   
c. Password - Password of the administrative user of NSX Manager.

3. In NetScaler MAS account used by NSX Manager section, set the NetScaler Driver Username and Password for the NSX Manager. NetScaler MAS authenticates load balancer configuration requests from the NSX Manager by using these logon credentials.

4. Click OK.
5. Navigate to **Orchestration > System > Deployment Settings**. Provide the VLAN range which was configured in trunked port group.

6. Log on to the NSX Manager on vSphere Web Client, and navigate to **Service Definitions > Service Managers**.

You can view Citrix NetScaler MAS as one of the service managers. This indicates that the registration is successful and a communication channel is established between the NSX manager and NetScaler MAS.
Creating a Service Package in NetScaler MAS

1. From NetScaler MAS home page navigate to **Orchestration > Cloud Orchestration > Service Packages**, and click **Add** to add a new service package.

2. On **Service Package** page, in **Basic Settings** section, set the following parameters:
   a. Name – type the name of a service package
   b. Isolation Policy – by default, the isolation policy is set to Dedicated
   c. Device Type – by default, the device type is set to NetScaler VPX

   **Note**: These values are set by default in this version, and you cannot modify them.
   d. Click **Continue**.
3. In **Assign Devices** section, select the pre-provisioned VPX for this package, and click **Continue**.
4. In Publish Service Package section, click Continue to publish the service package to VMware NSX, and then click Done.
This procedure configures a service package in the NSX Manager. A service can have multiple devices added to it and multiple edges can use the same service package to offload the NetScaler VPX instance to NetScaler MAS.

5. Log on to the NSX Manager on vSphere Web Client, and navigate to **Service Definitions > Services**.

You can see that the NetScaler MAS service package is registered.
Performing Load Balancer Service Insertion for Edge

Perform load balancer service insertion on the previously created NSX Edge gateway (offload the load balancing function from NSX LB to NetScaler).

1. In NSX Manager, navigate to **Home > NSX Edges**, and select the edge gateway that you have configured.

2. Click **Manage**, and on the **Load Balancer** tab, select **Global Configuration**, and click **Edit**.

3. Select **Enable Load Balancer**, **Logging**, **Enable Service Insertion** to enable them.
   
   a) In **Service Definition**, select the service package that was created in NetScaler MAS and published to NSX Manager.
4. Select the existing runtime NICs and click the Edit icon to edit runtime NICs that have to be connected when NetScaler VPX is allocated.

5. Edit the name of the NIC, specify Connectivity Type as **Data**, and click **Change**.

6. Select the appropriate web logical switch.

7. In **Primary IP Allocation Mode**, select IP Pool from the drop-down list, and click the down-arrow button on IP Pool field.
8. In the **Select IP Pool** window, select the appropriate IP pool, and click **OK**.

The IP address is acquired and is set as the source net IP address in the NetScaler VPX appliance. A L2 gateway is created in the NSX Manager to map the VXLAN to VLAN.

**Note:** All data interfaces are connected as run-time NICs, and they should be part of interfaces for DLR.

9. Refresh the view to see the creation of the run time.
10. After the VM has started, the value of Status changes to **In Service** and that of Install State changes to **Enabled**.

**Note**: In NetScaler MAS, navigate to **Orchestration > Requests** to see progress details of completion of LB service insertion.

**Viewing L2 Gateway on NSX Manager**

1. Log on to the NSX Manager on vSphere Web Client, navigate to **NSX Edges**, and select the DLR created.
2. In the DLR page, navigate to Manage > Bridging. You can see the L2 gateway displayed in the list.

Note: An L2 gateway gets created for each data interface.

Viewing Allotted NetScaler

1. Log on to the NetScaler VPX instance using the IP address displayed in NetScaler MAS. Then, navigate to Configuration > System > Networking. In the right pane, you can see that the two IP address are added. Click the IP address hyperlink to see the details.

The subnet IP address is same as the IP address of the web interface added in the NSX.

2. Navigate to Configuration > System > Licenses to view the licenses that are applied to this instance.
Configuring NetScaler VPX Instance Using Stylebook

1. In NetScaler MAS, navigate to **Orchestration** > **Cloud Orchestration** > **Edge Gateways**.

   Make a note of the NetScaler instance IP that is allotted to the respective Edge Gateway on which Load Balancing configuration through Stylebooks has to be applied.

2. Create a new Stylebook. Navigate to **Applications** > **Configuration**, import the stylebook, and select the stylebook from the list.

   To create a new stylebook, see **Create Your Own Stylebook**.

3. Specify values for all the required parameters.
4. Specify the NetScaler VPX instance on which you want to run these configuration settings.

5. Select the IP instance noted earlier, and click **Select**.

6. Click **Create** to apply the configuration on the selected device.
Viewing Load Balancer Configuration

1. Log on to the NetScaler VPX instance, navigate to **Configuration > Traffic Management > Load Balancing** to view the load balancing virtual server that is created.

You can also view the service groups that are created.

2. Select the service group, and click **Manage Members**. The **Configure Service Group Member** page displays the members associated with the service group.
Deleting Load Balancer Service

1. In NetScaler MAS, navigate to Applications > Configuration, and click X icon to delete the application configuration.

2. Log on to the NSX Manager on vSphere Web Client and navigate to the edge gateway to which the NetScaler VPX instance is connected.

3. Navigate to the Manage > Load Balancer > Global Configuration, right-click on the runtime entry, and click Unprovision.

Note: Edge Gateways in NetScaler MAS corresponds to runtime entries in NSX manager.
The NetScaler VPX instance is rendered out of service.

4. Navigate to Orchestration > Cloud Orchestration > Edge Gateways. Verify that the respective mapping of Edge Gateway to the deleted instance is not present.
NetScaler Automation Using NetScaler MAS in Cisco ACI’s Hybrid Mode

Sep 22, 2016
Cisco ACI introduced support for Hybrid Mode in version 1.3 (2f). In Hybrid Mode, you can perform network automation through the Application Policy Infrastructure Controller (APIC), while delegating the L4-L7 configuration to NetScaler MAS, which acts as a Device Manager in the APIC.

The NetScaler Hybrid Mode solution is supported by a hybrid mode device package and NetScaler MAS. You need to upload the hybrid mode device package in the APIC. This package provides all network L2-L3 configurable entities from NetScaler. Application parity is mapped by StyleBook from NetScaler MAS to the APIC. In other words, StyleBook acts as reference between L2-L3 and L4-L7 configurations for a given application. You must provide a StyleBook name while configuring the network entities from the APIC for NetScaler.

The following illustration provides an overview of NetScaler in a hybrid mode solution:

In Hybrid Mode, the NetScaler configuration is performed in the following two phases:

1. Network stitching is done from the Cisco APIC
2. Configuration is done from the NetScaler MAS

For any given application, a network administrator has to provide network specific details, such as IP addresses, port, VLAN (automated) and so on, as part of the service graph creation and deployment in the Cisco APIC. These configuration details are then pushed to NetScaler MAS through the device package, and NetScaler MAS internally processes them and configures the NetScaler ADC. An application administrator creates the application’s ADC related configuration by using StyleBook in NetScaler MAS, and these configurations are then pushed from NetScaler MAS to the NetScaler ADC. The Cisco APIC and NetScaler MAS communicate with the ADC through the management network.

The following diagram shows a NetScaler workflow in the hybrid solution:
Prerequisites

Sep 22, 2016

Make sure that:

- You have conceptual knowledge of Cisco ACI components and Citrix NetScaler ADCs.
- For more information about the Citrix NetScaler ADCs, see the Citrix NetScaler product documentation at: http://docs.citrix.com/.
- All the required components of Cisco ACI, including a Cisco APIC in the datacenter, are 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.
- You have installed NetScaler 11.1 or later.
- You have configured NetScaler ADCs in Cisco ACI so that they can be managed by using the Cisco APIC.
- You have deployed NetScaler Management and Analytics System (MAS) in your environment. For more information, see http://docs.citrix.com/en-us/netscaler-mas/11-1.html.
- Management connectivity from APIC to NetScaler MAS and NetScaler ADC are established.
- Make a note of:
  - The connection interfaces and IP addresses that are used for management and data-path connectivity.
  - Leaf-switch details: NetScaler IP addresses, ports, interfaces, and so on.

Note

In this release, the hybrid mode solution supports NetScaler in a single-context, that is, admin partitions are not supported.
Configuring a NetScaler ADC in Hybrid Mode by using a Cisco APIC and NetScaler MAS

Sep 22, 2016

Perform the following tasks to configure a NetScaler ADC in Hybrid Mode by using Cisco APIC and NetScaler MAS:

2. Use NetScaler MAS to create a StyleBook for the application. For instructions, see Creating a StyleBook for the Application Using NetScaler MAS.
3. Import the NetScaler hybrid mode device package into Cisco APIC. For instructions, see Importing the NetScaler Hybrid Mode Device Package into Cisco APIC.
4. Add NetScaler MAS as a device manager in the Cisco APIC. For instructions, see Adding NetScaler MAS as a Device Manager in Cisco APIC.
5. Use Cisco APIC to add a NetScaler device in Cisco ACI. For instructions, see Adding the NetScaler as a Device in Cisco ACI.
6. Create and deploy a service graph template. For instructions, see Creating and Deploying a Service Graph.
7. Configure L4-L7 parameters by using StyleBook in NetScaler MAS. For instructions, see Configure L4-L7 parameter using StyleBook from NetScaler MAS.
8. Attach or detach endpoint events from the Cisco APIC. For more information, see Attaching or Detach endpoint events from APIC.
Creating a StyleBook for the Application by Using NetScaler MAS

Sep 22, 2016
A StyleBook is a configuration template that you can use to create and manage NetScaler configurations for any application. You can create a StyleBook for configuring a specific NetScaler feature, such as load balancing, SSL offload, or content switching. You can design a StyleBook to create configurations for an enterprise application deployment such as Microsoft Exchange or Lync. For more information, see StyleBooks.

You can create your own StyleBook for your application or modify and use the APIC-HTTP-LB StyleBook shipped with NetScaler MAS.

To create your own StyleBook for your application in NetScaler MAS, see How to Create Your Own StyleBooks.

While creating the StyleBook, make sure that you follow the the APIC’s service graph model in the StyleBook. In other words, the APIC’s service graph for any application follows consumer and provider model connected through an ADC function. Consumer and provider are represented as an End-Point Group (EPG) and have a 1:1 relationship. The same model must be followed in StyleBook as well, where the provider EPG must be represented as a servicegroup and each end point as a member of the service group. The ADC function node must be represented by a virtual server (for example, a load balancing virtual server), and there must be a 1:1 relationship between virtual server and servicegroup.

This essentially captures the essence of the service graph and allows you to handle the attach or detach event from the APIC, where an attach event binds the end point to the corresponding servicegroup and a detach event unbinds it. You must make sure that the service graph and StyleBook are in parity for seamless automation from network L2-L3 to ADC-feature L4-L7 configurations.
Importing the NetScaler Hybrid Mode Device Package into the Cisco APIC

Sep 22, 2016

The Hybrid Mode device package is a lightweight package compared to a fully managed mode. Only L2-L3 network parameters are available through the Device Model. The Device Model has only one generic ADC function defined in it, and four function profiles based on the NetScaler deployment in the fabric (for example, one-arm and two-arm and the same with RHI). The Hybrid Mode Device package name is Citrix-NetSCalerMAS-1.0. Download the Hybrid Mode device package from the Citrix Download Site and import the device package to the APIC.

Note

The hybrid mode device package can co-exist with a fully managed mode device package.

To import the hybrid mode device package to the APIC by using the APIC GUI:

1. On the menu bar, click the L4-L7 Services tab and select the Packages panel.
2. In the Navigation pane, right-click on L4-L7 Device Types and select Import Device Package.
3. In the Import Device Package dialog box, click Browse to select the downloaded NetScaler hybrid mode device package.
4. Click Submit.
   After successfully importing the device package to the APIC, in the Navigation pane, you can view the details of the device package by clicking Citrix-NetSCalerMAS-1.0.
Important

After you import the device package, make sure that there are no faults in the APIC. You can view the faults by clicking the **faults** tab in the Device Types window.
Adding NetScaler MAS as a Device Manager in the Cisco APIC

Sep 22, 2016

NetScaler MAS acts as a centralized device manager for NetScaler deployed on Cisco ACI. You need to add NetScaler MAS as a device manager in the Cisco APIC.

To add NetScaler MAS as a device manager in the APIC using the APIC GUI:

1. On the menu bar, go to Tenants > All Tenants.

2. In the Work pane, double-click the tenant's name.

3. In the Navigation pane, select tenant_name > L4-L7 Services.

4. Right-click on Device Managers and click Create Device Manager.

5. In the Create Device Manager dialog box, do the following:

   a. In the Device Manager Name field, enter a name for the NetScaler MAS deployment that you want register as a device manager.
b. In the **Management EPG** drop-down list, select the management EPG.

c. In the **Device Manager Type** drop-down list, select **Citrix-DevMgr-1.0**.

d. In the **Management** field, click + and add the IP address and port details of the NetScaler MAS deployment.

e. In the **Username** field, enter the user name to access NetScaler MAS.

f. In the **Password** and **Confirm Password** fields, enter the password to access NetScaler MAS.

g. Click **SUBMIT**.

Once the NetScaler MAS is successfully registered as a device manager in the APIC, the device manager is added and is displayed in the **Navigation** pane. To view the registered device manager, in the Navigation pane, go to **tenant_name > L4-L7 Services > Device Manager**.
Note

Make sure that there are no connectivity issues between the Cisco APIC and NetScaler MAS and that you provide the same credentials that you use to access the NetScaler MAS. Also make sure that the account has admin privileges.

Important

After you import the device package, make sure that there are no faults in the APIC. You can view the faults by clicking the **Faults** tab in the Device Types window.

You can also register NetScaler MAS as a device manager by using APIs. Following is a sample XML payload that shows how you can use APIs to add NetScaler MAS as a device manager.

XML Sample
<polUni>
  <fvTenant name="coke">
    <vnsDevMgr name="MAS1">
      <vnsRsDevMgrToMDevMgr tDn="uni/infra/mDevMgr-Citrix-DevMgr-1.0"/>
      <vnsCMgmts name="devMgmt" host="10.102.102.81" port="80"/>
      <vnsCCred name="username" value="nsroot"/>
      <vnsCCredSecret name="password" value="*****"/>
    </vnsDevMgr>
  </fvTenant>
</polUni>
Adding NetScaler as a Device in Cisco ACI by Using the APIC

Sep 22, 2016
You need to add a NetScaler ADC as an L4-L7 device to the APIC for the network automation. The APIC performs network stitching between Leaf and the NetScaler device, based on the deployed service graph. You need to configure the basic settings of the device configuration, such as configuration management IP addresses, device manager, and credentials.

To register the NetScaler as a device in the APIC by using the APIC GUI:

1. On the menu bar, go to Tenants > All Tenants.
2. In the Work pane, double-click the tenant’s name.
3. In the Navigation pane, select tenant_name > L4-L7 Services > L4-L7 Devices.
4. In the Work pane, select Actions > Create L4-L7 Devices.
5. In the Create L4-L7 Devices dialog box, in the General section, do the following:
   a. Select the Managed check box.
   b. In the Name field, enter a name for the device.
   c. In the Service Type drop-down list, select ADC.
   d. In the Device Type field, select Physical.
   
   Note: Make sure that for VMware ESX, you select Virtual and associate the respective Virtual Machine Manager (VMM) domain.

   e. In the Physical Domain drop-down list, select the physical domain.
   
   f. In the Mode field, select Single Node or HA Cluster, depending on your requirement.
   
   g. In the Device Package drop-down list, select Citrix-NetScalerMAS-1.0.
   
   h. In the Model drop-down list, select the device model. For example, NetScaler-MPX, or NetScaler-VPX.

6. In the Connectivity section, select Out-Of-Band or In-Band in the APIC to Device Management Connectivity field, depending on how NetScaler is configured in the fabric.
7. In the Credentials section, specify the user name and password for access to the device.
8. In the Device 1 and Device 2 section, respectively, complete the management related configuration.
9. In the Cluster section, complete the management related configuration for the cluster. Make sure that in the Device Manager drop-down list, you select the device manager you created in Adding NetScaler MAS as a Device Manager in Cisco APIC.
10. Click **NEXT**.

The Device Configuration page appears. The hybrid mode device package does not provide device and cluster specific configuration details such as high-availability, enable/disable features and modes, configuration for NTP, SNMP, SNMP Alarms, and so on. These configurations must be done by using NetScaler MAS.

11. Click **FINISH**.

When you have successfully registered the device in the APIC, the device is added and is displayed in the Navigation pane. To view the registered device, in the Navigation pane, go to **tenant_name > L4-L7 Services > L4-L7 Devices > device_name**.

**Important**

After you register the device, make sure that there are no faults in the APIC. You can view the faults by clicking the **Faults** tab in the **Work** pane.
You can also register a NetScaler device by using APIs. The following is a sample XML payload for adding L4-L7 Device:

```xml
<polUni>
  <fvTenant name="coke">
    <vnsLDevVip name="ADCCluster1" funcType="GoTo" svcType="ADC">
      <vnsRsMDevAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0" />
      <vnsRsALDevToPhysDomP tDn="uni/phys-phys"/>
      <vnsCMgmt name="devMgmt" host="10.102.102.67" port="80" />
      <vnsCCred name="username" value="nsroot"/>
      <vnsCCredSecret name="password" value="******"/>
      <vnsRsALDevToDeviceMgr tnVnsDevMgrName="MAS1"/>
      <vnsCDev name="ADC1" devCtxLbl="C1"/>
    </vnsLDevVip>
  </fvTenant>
</polUni>
```
<vnsCIf name="1_1">
  <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/33]"/>
</vnsCIf>

<vnsCIf name="1_2">
  <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/35]"/>
</vnsCIf>

<vnsCMgmt name="devMgmt" host="10.102.102.65" port="80"/>
<vnsCCred name="username" value="nsroot"/>
<vnsCCredSecret name="password" value="*****"/>
</vnsCDev>

<vnsCDev name="ADC2" devCtxLbl="C1">
  <vnsCIf name="1_1">
    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/34]"/>
  </vnsCIf>
  <vnsCIf name="1_2">
    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/36]"/>
  </vnsCIf>
  <vnsCMgmt name="devMgmt" host="10.102.102.66" port="80"/>
  <vnsCCred name="username" value="nsroot"/>
  <vnsCCredSecret name="password" value="*****"/>
</vnsCDev>
<vnsCCredSecret name="password" value="****"/>

</vnsCDev>

<vnsLIf name="outside">

<vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/mIfLbl-outside"/>

<vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/cIf-1_1"/>

<vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/cIf-1_1"/>

</vnsLIf>

<vnsLIf name="inside">

<vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/mIfLbl-inside"/>

<vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/cIf-1_2"/>

<vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/cIf-1_2"/>

</vnsLIf>

</vnsLDevVip>

</fvTenant>

</polUni>
Creating and Deploying a Service Graph

Sep 22, 2016

You have to use Cisco APIC service graph templates in APIC to create and deploy the NetScaler ADCs. Make sure that you use the ADC function profile while creating and deploying a service graph.

After the graph is configured in the APIC, the APIC automates the device configuration on the basis of the function definitions, device connectivity to the fabric, and the entities configured as part of the graph deployment. The APIC also automates the network configuration, such as VLAN allocation and its binding, as part of the service graph creation, and the configuration is removed once you delete the graph from the APIC.

A service graph is represented as two or more tiers of an application, with the appropriate service function inserted between them. A service graph is inserted between the source and destination EPGs by a contract.

To create a service graph by using the APIC GUI:

1. On the menu bar, go to Tenants > All Tenants.
2. In the Work pane, double-click the tenant’s name.
3. In the Navigation pane, select tenant_name > L4-L7 Services > L4-L7 Service Graph Templates.
4. In the Work pane, select Actions > Create a L4-L7 Service Graph Template.
5. In the Create a L4-L7 Service Graph Template dialog box, in the Device Clusters section, select a device cluster and do the following:
   a. In the Graph Name field, enter the name of the service graph template.
   b. In the Graph Type field, select Create A New One.
   c. From the Device Cluster section, drag the device and drop it between the consumer end-point group and provider end-point group to create a service node.
d. In the `<L4-L7 device_name information>` section, do the following:

i. In the ADC field, select **One-Arm** or **Two-Arm**, depending on how the NetScaler ADC is deployed in the fabric.

ii. In the Profile drop-down list, select the function profile provided in the device package.

e. Click SUBMIT.

6. In the Navigation pane, click the service graph template. The screen presents a graphic topology of the service graph template.

**Note**

The Cisco APIC supports the notion of connectors, and these connectors are visible in the ADCCluster node. The connectors define the network traffic direction and the device script that dynamically binds the allocated VLAN to a virtual IP (VIP) or subnet IP (SNIP) address, depending on whether the connection is external or internal. VLANs are also bound to specific interfaces used for inbound and outbound traffic.
Applying the Service Graph Template to Endpoint Groups

After you have created the service graph template, you need to apply the created service graph template by using the APIC GUI.

To apply the service graph template:

1. On the menu bar, go to Tenants > All Tenants.

2. In the Work pane, double click the tenant’s name.

3. In the Navigation pane, choose tenant_name > L4-L7 Services > L4-L7 Service Graph Templates.

4. Right-click on the template_name and click Apply L4-L7 Service Graph Template.
5. In the **Apply L4-L7 Service Graph Template To EPGs** dialog box, in the **EPG Information** section, complete the following fields:

   a. In the **Consumer EPG/External Network** drop-down list, select the consumer endpoint group.

   b. In the **Provider EPG/External Network** drop-down list, select the provided endpoint group.

   c. In the **Contract Information** section, complete the appropriate fields. The contract information is specific to the Cisco APIC and is configured as part of the security policies associated with the EPGs.
d. Click **Next**.

e. In the **Graph Template** drop-down list, select the service graph template that you created.

f. In the **Connector** section, do the following:

   i. In the **Type** field, select General.

   ii. In the **BD** drop-down list, select the bridge domain. Connector details are part of the bridge domain that is part of the Cisco APIC infrastructure model.

   iii. In the **Cluster Interface** drop-down list, select the appropriate cluster interface for the selected bridge domain. The Cisco APIC uses the selected bridge domains for data path traffic between the NetScaler device and the fabric as required by the selected service graph template.
g. Click **Next**.

On the **Parameters** screen, on the **Required Parameters** tab, enter the L2-L3 specific details, such as the IP address that is mandated by the profile. The other key parameter is the StyleBook name. It can be the built-in StyleBook **APIC-HTTP-LB** provided in NetScaler MAS, or you can provide the name of the StyleBook that you created in **Creating a StyleBook for the Application Using NetScaler MAS**.

**Note**

The StyleBook name links the Service Graph details with the L4-L7 configuration created with NetScaler MAS for a given application.
The Cisco APIC GUI allows you to filter the parameters on the basis of features (for example, load balancing). You can view and set all the mandatory parameters on the **Required Parameters** tab, and you can view and set all the other parameters related to the feature on the **All Parameters** tab.

![Cisco APIC GUI](image)

**Note**

By default, a built-in one-arm profile requires you to provide SNIP details such as IP address and netmask. You can view other networking parameters by clicking **All Parameters** and expanding the **Configure Network** tree in the Cisco APIC GUI. This lists all the network parameters supported by NetScaler. You can instantiate any entity and provide values for the listed attributes from the Cisco APIC GUI.

6. Click **Finish**.

**Important**

After you apply the service graph template, make sure that there are no faults in the deployed graph. You can view the faults by clicking the **Faults** tab in the **Work** pane.
As part of the Service Graph deployment, the Hybrid Mode Device package pushes the configuration details from the Cisco APIC to the NetScaler MAS. The NetScaler MAS internally processes these configurations to the respective NetScaler ADC and returns the response to the APIC. A successful graph deployment will have no fault, and the NetScaler ADC is successfully networked with the fabric for the corresponding graph.

The APIC supports different ways to configure and deploy graphs by using APIs, and graph deployment includes various dependencies on some APIC-specific constructs, such as Tenant, contract, VLAN and namespace.

The following sample approach illustrates one of the ways to make use of the APIC's APIs to create and deploy L4-L7 graphs, with the assumption that APIC specific artifacts are already configured in the APIC.

**Important**

Make sure that you use these XML payloads as a reference and make appropriate changes to the XML before you use them in your environment.

Following is an example of creating and deploying the service graph by using APIs:

1. Create AppProfile
2. Create service graph details
3. Attach the service graph to a contract

Following is a sample XML payload for creating an AppProfile. The AppProfile contains EPGs, and the provider EPG contains the NetScaler specific entities, attributes, and their values. In the following sample XML payload, NetScaler-specific network entities such as the NSIP are created with a set of attributes and StyleBook name.
<polUni>

<vTenant name="coke">

<!-- Application Profile -->

<vAp dn="uni/tn-coke/ap-sap" name="sap">

<!-- EPG 1 -->

<vAEPg dn="uni/tn-coke/ap-sap/epg-web" name="web">

<vRsBd tnFvBDName="BD_web" />

<!-- --------- CONFIG PAYLOAD ---------------- -->

<vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Network" name="Network">

<vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="snip1">

<vnsParamInst key="ipaddress" name="ip1" value="110.110.110.2"/>

<vnsParamInst key="netmask" name="netmask1" value="255.255.255.0"/>

<vnsParamInst key="type" name="tye" value="SNIP"/>

<vnsParamInst key="dynamicrouting" name="dynamicrouting" value="DISABLED"/>

<vnsParamInst key="hostroute" name="hostroute" value="DISABLED"/>

</vnsFolderInst>

<vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="snip2">

<vnsParamInst key="ipaddress" name="ip2" value="220.220.220.2"/>

<vnsParamInst key="netmask" name="netmask2" value="255.255.255.0"/>

<vnsParamInst key="type" name="tye" value="SNIP"/>

</vnsFolderInst>

</vnsFolderInst>

</vnsFolderInst>

</vTenant>

</polUni>
Following is a sample XML payload for creating service graph details:

```xml
<polUni>
  <fvTenant name="coke">
    <vnsAbsGraph name = "Graph1">
      sample XML payload for creating service graph details
    </vnsAbsGraph>
  </fvTenant>
</polUni>
```
<vnsAbsTermNodeProv name="Input1">
    <vnsAbsTermConn name="C1"></vnsAbsTermConn>
</vnsAbsTermNodeProv>

<vnsAbsNode name="ADC" funcType="GoTo">
    <vnsAbsTermConn name="outside" attNotify="true">
        <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/mFunc-ADCFunction/mConn-external" />
    </vnsAbsTermConn>
    <vnsAbsTermConn name="inside" attNotify="true">
        <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/mFunc-ADCFunction/mConn-internal" />
    </vnsAbsTermConn>
</vnsAbsNode>

<vnsRsNodeToMFunc tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/mFunc-ADCFunction"/>

<vnsRsDefaultScopeToTerm tDn="uni/tn-coke/AbsGraph-Graph1/AbsTermNodeProv-Input1/outtmnl"/>

<vnsRsNodeToAbsFuncProf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/absFuncProfContr/absFuncProfGrp-ADCOneArmServiceProfileGroup/absFuncProf-ADCOneArmFunctionProfile"/>

<vnsRsNodeToLDev tDn="uni/tn-coke/lDevVip-ADCCluster1"/>

</vnsAbsNode>

<vnsAbsTermNodeCon name="Output1">
    <vnsAbsTermConn name="C6"></vnsAbsTermConn>
</vnsAbsTermNodeCon>

<vnsAbsConnection name="CON1"/>
Following is a sample XML payload for attaching the service graph to a contract:

```xml
<vnsAbsConnection name = "CON2">
  <vnsRsAbsConnectionConnectionDn="uni/tn-coke/AbsGraph-Graph1/AbsNode-ADC/AbsFConn-inside" />
  <vnsRsAbsConnectionConnectionDn="uni/tn-coke/AbsGraph-Graph1/AbsTermNodeProv-Input1/AbsTConn" />
</vnsAbsConnection>
</vnsAbsGraph>
</fvTenant>
</polUni>
```
<polUni>

<fvTenant name="coke">

<vzBrCP name="Ctrct1">

<vzSubj name="http">

<vzRsSubjGraphAtt tnVnsAbsGraphName="Graph1"/>

</vzSubj>

</vzBrCP>

</fvTenant>

</polUni>
Configuring L4-L7 Parameters from NetScaler MAS by using StyleBook

Sep 22, 2016

In NetScaler MAS, you can view the deployed service graph details on the **Orchestration** tab, under **Cisco ACI**. The tabular view shows the service graph details such as graph name, tenant name, context, StyleBook name, and network configuration status.

![Network Configuration from APIC](image)

**Note**

If the graph is deleted from the Cisco APIC, the corresponding configuration is removed from the device, including the L4-L7 configuration.

Additionally, the tabular view allows you to sort on any column displayed in the table and filter the data by using the Search option. You can also customize the column details by selecting or unselecting the column names from the drop-down column list.
Also, you can click the **Search** button and use the search options to filter the data. You can select any column from the drop-down box and enter a corresponding value to filter the data displayed in the table.

**Note**

The Search functionality is case-sensitive, and you must provide the exact search criteria.
To deploy L4-L7 configuration by using StyleBook in NetScaler MAS:

1. Click the StyleBook name that appears as a URL in the tabular view.

2. In the Configuration window, double-click **StyleBook**.

3. In the Deploy Configuration window, do the following:
   
   a. In the **Application Name** field, enter the name for the ADC feature configuration that corresponds to the application's service graph in the APIC.
b. In the Service (ports) Settings section, click +.

c. In the **Settings for EPG & endpoints (ports) defined in the service graph** window, enter values for the parameter populated from the StyleBook and click **Create**.

d. Click **Create**.
The L4-L7 configuration specified in the StyleBook is deployed, in NetScaler MAS. You can view the StyleBook configuration from the Application tab, by navigating to Application > Configuration.
Attaching or Detaching Endpoint Events from the APIC

Sep 23, 2016

The hybrid-mode solution implicitly handles attach or detach endpoint events from the Cisco APIC. When the Cisco APIC triggers an attach endpoint event, the servicegroup_servicegroupmember_binding is automatically triggered by the StyleBook in NetScaler MAS, and the endpoint is unbound during the detach endpoint event.

Additionally, if you have not deployed the L4-L7 configuration in NetScaler MAS before the attach or detach endpoint event gets triggered in Cisco the APIC, the solution will retain the attach IP addresses in the database. These IP addresses are bound to the corresponding service group after the service group is created through StyleBook.
When you deploy a NetScaler device package in Cisco ACI, the Cisco APIC reports any failures. You can view the fault reports at any level of the APIC (for example, device, tenant, EPGs, or service graph). The screen shot below shows a fault report at the device level. For more information on faults, see http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/Faults/guide/b_APIC_Faults_Errors/b_IFC_Faults_Errors_chapter_01.html.

Select any APIC entity and click the **Faults** tab to display the faults reported by the APIC for that entity.
Logs Generated by Hybrid Mode Device Package

Sep 23, 2016

The NetScaler Hybrid Mode device package generates configuration-related logs and monitoring-related logs. The generated logs are located at /data/devicescript/Citrix.NetScalerMAS.1.0/logs.

Following is a sample snippet of a Cisco APIC's debug.log:

```
2016-06-28 03:06:53.879767 DEBUG Thread-20 18723 [10.102.102.62, 24063] Device manager details ip = 10.102.102.81, port = 80

2016-06-28 03:06:53.879856 DEBUG Thread-20 18724 [10.102.102.62, 24063] ++++++++++++++ serviceAudit request ++++++++++++++

2016-06-28 03:06:53.879929 DEBUG Thread-20 18725 [10.102.102.62, 24063] ++++++++++ getStyleBookObjects +++++++++++++


2016-06-28 03:06:53.880093 DEBUG Thread-20 18728 [10.102.102.62, 24063] NMAS collection retCol= {'Stylebook': 'APIC-HTTP-LB', 'tuple': ((0, '', 5230), (4, 'Stylebook', 'stylebook_1'))}


2016-06-28 03:06:54.135240 DEBUG Thread-20 18730 [10.102.102.62, 24063] ++++ Response from styleBookresCode ... u'1.1', u'uses_stylebooks': [{u'version': u'1.1', u'namespace': u'com.citrix.adc.stylebooks', u'name': u'APIC-ROOT'}]}


2016-06-28 03:06:54.359221 DEBUG Thread-20 18732 [10.102.102.62, 24063] ++++ Response from Device Mgr serviceAudit = [{"APIC":[]}

2016-06-28 03:06:54.359266 DEBUG Thread-20 18733 [10.102.102.62, 24063] ++++++++++++++ serviceAudit response = [{"APIC":[]}]

2016-06-28 03:06:54.359306 DEBUG Thread-20 18734 [10.102.102.62, 24063] ++++++++++++++ serviceAudit response headers content-type= application/json; charset=utf-8


2016-06-28 03:06:54.359713 DEBUG Thread-20 18738 [10.102.102.62, 24063] ++++++++++++++ pollingStatus = True, pollingTime = 0
```
Logs Generated by NetScaler MAS

Sep 23, 2016

NetScaler MAS provides extensive logging that can help troubleshoot issues. The generated logs (admin.log) are located at:/var/controlcenter/log/

You can log on to NetScaler MAS and use the shell to navigate to the NetScaler MAS directory structure. Following is a sample snippet of a NetScaler MAS log for an APIC’s graph deployment.

```
2016-06-29 10:58:33,816 DEBUG APIC Config = (0, "", 5230): {'dn': u'uni/vDev-[uni/tn-coke_SDX2/DevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2/DevVip-ADCHybridMode_1]'}, {'dn': u'uni/vDev-[uni/tn-coke_SDX2/DevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2/DevVip-ADCHybridMode_1]'},

2016-06-29 10:58:33,816 DEBUG get Graph Return details = {'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/DevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2/DevVip-ADCHybridMode_1]'}, {'graphInstanceId': 5790}, {'ctxName': 'cokectx1'}, {'graphInstanceName': 'HybridModeGraph_1'}, {'state': 1}, {'value': 'APIC-HTTP-LB'}, {'concept': 1}, {'transaction': 0}, {'ackedstate': 0},

2016-06-29 10:58:33,827 DEBUG SUCCESS created track 2.0

2016-06-29 10:58:33,833 DEBUG SUCCESS updated track with new task 2

2016-06-29 10:58:33,851 DEBUG SUCCESS updated track with new task 1

2016-06-29 10:58:33,867 DEBUG fn_wrapper:long_operation_thread_id:<eventlet.greenthread.GreenThread object at 0x80aa5c7d0>

2016-06-29 10:58:33,867 DEBUG +++++++ Service Audit Call for Device Details = 10.102.102.62 +++++++++++++++++

2016-06-29 10:58:33,867 DEBUG Inside APIC Cred Col If = 2

2016-06-29 10:58:33,867 DEBUG Host name from device = ADCHybridMode_1

"InProgress","message":null,"replication_status":","target":"10.102.102.81","operation":"POST","entity_type":"apic","entity_id":null}"

2016-06-29 10:58:44,141 DEBUG Save config Response = { "errorcode": 0, "message": "Done", "severity": "NONE" }

2016-06-29 10:58:44,141 DEBUG +++++++++ getContextAwareFlag = True

2016-06-29 10:58:44,141 DEBUG ++++ get context tenant name from Config ++++

2016-06-29 10:58:44,141 DEBUG ++++ getContextTenantName = {'state': 1, 'ctxName': 'cokectx1', 'tenant': 'coke_SDX2', 'vdev': 5230}

2016-06-29 10:58:44,142 DEBUG Service health details = [] collection length = 0
```
2016-06-29 10:58:44,142 DEBUG Count details Total = 0 Up = 0 Down = 0

2016-06-29 10:58:44,142 DEBUG Health Score details Up = 0

2016-06-29 10:58:44,142 DEBUG Service HEALTH final collection = {((0, "", 5230), (1, "", 5790), (3, 'ADCFunction', 'N1')): {'faults': [], 'state': 0, 'health': []}

2016-06-29 10:58:44,142 DEBUG ++++/getServiceHealth Fault List = []

2016-06-29 10:58:44,142 DEBUG Service HEALTH final response = {'devs': 'ADCHybridMode_1_Device_1', 'faults': [], 'state': 0, 'health': []

2016-06-29 10:58:44,236 DEBUG RESPONSE from NSLOGOUT = { "errorcode": 0, "message": "Done", "severity": "NONE" }, sessionId = 920778120

2016-06-29 10:58:44,237 DEBUG +++ Faults respCol = {'10.102.102.62': {'10.102.102.62': {u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity': u'NONE', u'operation_name': 'bind_op'}}

2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg = Done, statusCode = add_op

2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg = Done, statusCode = add_op

2016-06-29 10:58:44,237 DEBUG Fault details oprName = bind_op, erMsg = Done, statusCode = bind_op

2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg = Done, statusCode = add_op

2016-06-29 10:58:44,238 DEBUG Fault details oprName = bind_op, erMsg = Done, statusCode = bind_op

2016-06-29 10:58:44,238 DEBUG +++++++ get IP and Connector collection from Config with type 22 for attach & detach event ++++++

2016-06-29 10:58:44,238 DEBUG ----- connector with IP List = [0: [], 1: [], 3: []]


2016-06-29 10:58:44,264 DEBUG SUCCESS created task 2

2016-06-29 10:58:44,269 DEBUG SUCCESS updated track with new task 2

2016-06-29 10:58:44,308 DEBUG +++/ get IP and Connector collection from Config with type 22 for attach & detach event ++++

2016-06-29 10:58:44,308 DEBUG ------- connector with IP List = [0: [], 1: [], 3: []]

2016-06-29 10:58:44,308 DEBUG ------- attachIpList = [] detachIpList = []
2016-06-29 10:58:44,308 DEBUG ----- In _attachDettachIps attachIpList = [] detachIpList = []

2016-06-29 10:58:44,312 DEBUG ----- In _attachDettachIps row = {'deviceIP': u'10.102.102.62', 'responseToAPIC': None, 'graphInstanceId': 5790, 'createDate': None, 'serviceGroupIP': None}
The following table describes how to configure the system settings on your NetScaler MAS.

<table>
<thead>
<tr>
<th>If you want to …</th>
<th>Do this …</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the setup wizard settings</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>Set Up NetScaler MAS</strong>, select <strong>Setup Wizard Settings</strong>. You can select the <strong>NetScaler MAS Network</strong> option to modify network settings, such as IP address of NetScaler MAS, and its password. You can click <strong>System Settings</strong> to modify the host name, mode of communication with instance(s), or local time zone.</td>
</tr>
<tr>
<td>Configure the network settings</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>Set Up NetScaler MAS</strong>, select <strong>Network Configuration</strong>. You can choose IPV4, IPV6, or both, and enter network parameters.</td>
</tr>
<tr>
<td>View SSL certificate</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>Set Up NetScaler MAS</strong>, select <strong>View SSL Certificate</strong>. The GUI displays the SSL certificates and keys installed on the NetScaler MAS.</td>
</tr>
<tr>
<td>Change Time Zone</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>System Settings</strong>, select <strong>Change Time Zone</strong>. From the Time Zone drop-down list, select the time zone for your NetScaler MAS appliance's clock.</td>
</tr>
<tr>
<td>Change Hostname</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>System Settings</strong>, select <strong>Change Hostname</strong>. Enter a hostname that will be used to identify your NetScaler MAS, so that when you generate the universal license for NetScaler MAS Gateway, the hostname is displayed in the license.</td>
</tr>
</tbody>
</table>
| Change the system settings | Navigate to **System > System Administration**. Under **System Settings**, select **Change System Settings**. Then, select or clear check boxes to enable or disable the following features:  
  - Secure Access Only  
  - Enable Session Timeout  
  - Allow Basic Authentication  
  - Enable nsrecover Login  
  - Enable Certificate Download  
  Enable Shell access for non-nsroot User |
<p>| Configure the SSL settings | Navigate to <strong>System &gt; System Administration</strong>. Under <strong>System Settings</strong>, select <strong>Configure SSL Settings</strong> to display the current protocol settings and the applied cipher suites. If you want to modify any of the settings, under <strong>Edit Settings</strong>, select <strong>Protocol Settings</strong> or <strong>Cipher Suites</strong>. |
| Configure Enable the user experience improvement settings feature | Navigate to <strong>System &gt; System Administration</strong>. Under <strong>System Settings</strong>, select <strong>Configure User Experience Improvement Settings</strong>. Then select the <strong>Enable CUXIP</strong> check box. If you select this check box, usage statistics are collected for the sole purpose of improving the graphical user interface. The collected data is used only by Citrix engineers and is not shared with anyone. |
| Upgrade NetScaler MAS | Navigate to <strong>System &gt; System Administration</strong>. Under the <strong>System Administration</strong> subheading, select <strong>Upgrade NetScaler MAS</strong>, and then select the new image file. You can select a file that is already on the NetScaler MAS virtual appliance, or you can upload a file from your local computer. |</p>
<table>
<thead>
<tr>
<th>If you want to ...</th>
<th>Do this ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the system prune settings (for pruning old data)</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>Policy Administration</strong>, select <strong>System Prune Settings</strong>. In the <strong>Data to keep (days)</strong> field, enter the number of days for which to retain data in the system.</td>
</tr>
<tr>
<td>Configure the system backup settings</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>Policy Administration</strong>, select <strong>System Backup Settings</strong>, and then enter the number of system backups to retain on the MAS appliance. You can also elect to encrypt the backup files, and you can specify an external location to which to transfer them. Transferred backup files can be retained on or deleted from the system.</td>
</tr>
<tr>
<td>Configure the instance backup settings</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>Policy Administration</strong>, select <strong>Instance Backup Settings</strong>, and enter the time interval (in hours) at which to create a backup file backing up all the instances managed by the NetScaler MAS. You can specify the number of backup files to retain, and whether to encrypt them so that they cannot be accessed without a password.</td>
</tr>
<tr>
<td>View the system statistics</td>
<td>Navigate to <strong>System &gt; Statistics</strong>. A line graph displays information such as CPU usage, memory usage, and disk usage.</td>
</tr>
<tr>
<td>View and manage sessions</td>
<td>Navigate to <strong>System &gt; Sessions</strong>. You can then see all the active sessions, with details. To terminate a session, select its check box and click <strong>Cancel Session</strong>.</td>
</tr>
<tr>
<td>Add or modify a tenant</td>
<td>Navigate to <strong>System &gt; Tenants</strong>, and add a new tenant or edit the settings for an existing tenant. You can provide additional information, such as an organizational unit name, department, and URL for the tenant.</td>
</tr>
<tr>
<td>Change the user lockout policy</td>
<td>Navigate to <strong>System &gt; User Administration</strong>. Under <strong>User Configuration</strong>, select <strong>User Lockout Configuration</strong>, and then select the <strong>Enable User Lockout</strong> check box. You can specify the number of invalid attempts a user can make before their account is disabled, and for how long the user-lockout policy is effective.</td>
</tr>
<tr>
<td>Change the password complexity</td>
<td>Navigate to <strong>System &gt; User Administration</strong>. Under <strong>User Configuration</strong>, select <strong>Password Policy</strong>, and then select the <strong>Enable Password Complexity</strong> check box. In the <strong>Minimum Password Length</strong> field, enter the minimum number of characters required for a password on the NetScaler MAS.</td>
</tr>
<tr>
<td>Add or modify a user</td>
<td>Navigate to <strong>System &gt; User Administration &gt; Users</strong>. Under <strong>Users</strong>, add a new user or edit the settings for an existing user. When adding a user, you can enable options such as external authentication, session timeout, and assigning the user to specific groups.</td>
</tr>
<tr>
<td>Add or modify a user group</td>
<td>Navigate to <strong>System &gt; User Administration &gt; Groups</strong>. Under <strong>Groups</strong>, add a new group or edit the settings for an existing group. When adding a group, you can enable options such as assigning permissions for the group, configuring a session timeout, assigning users to the group, and allowing access to particular or all applications on the NetScaler MAS.</td>
</tr>
<tr>
<td>Change the authentication configuration</td>
<td>Navigate to <strong>System &gt; Authentication &gt; Authentication</strong>. Under <strong>Authentication</strong>, select <strong>Authentication Configuration</strong>, and select the type of authentication server.</td>
</tr>
<tr>
<td>Server If you want to ...</td>
<td>Do this ...</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Add or modify an LDAP server</td>
<td>Navigate to <strong>System &gt; Authentication &gt; LDAP</strong>. Under LDAP, add a new LDAP server or edit the settings for an existing LDAP server by entering or modifying the network parameters.</td>
</tr>
<tr>
<td>Add or modify a TACACS servers</td>
<td>Navigate to <strong>System &gt; Authentication &gt; TACACS</strong>. Under TACACS, add a new TACACS server or edit the settings for an existing TACACS server by entering or modifying the network parameters.</td>
</tr>
<tr>
<td>Add or modify a syslog server</td>
<td>Navigate to <strong>System &gt; Auditing &gt; Syslog Servers</strong>. Under Syslog Servers, add a new syslog server or edit the settings for an existing syslog server by entering or modifying the network parameters. You can provide additional information by selecting the kind of log levels you want to monitor.</td>
</tr>
<tr>
<td>Read syslog messages</td>
<td>Navigate to <strong>System &gt; Auditing</strong>. Under Audit Messages, select <strong>Syslog Messages</strong>. Summaries of all system log files are displayed in the Syslog Viewer. You can select the syslog file you want to view from the File drop-down option. Additionally, syslog files can be further filtered by module, event type, and severity.</td>
</tr>
<tr>
<td>Configure the syslog purge settings</td>
<td>Navigate to <strong>System &gt; Auditing</strong>. Under Settings, select <strong>Syslog Purge Settings</strong>, and then enter the number of days to retain syslog data before it is deleted from the NetScaler MAS.</td>
</tr>
<tr>
<td>View system events</td>
<td>Navigate to <strong>System &gt; Events</strong>. You can then see all the current events, with details.</td>
</tr>
<tr>
<td>Add or modify an NTP server</td>
<td>Navigate to <strong>System &gt; NTP Servers</strong> to add a new NTP server or edit the settings for an existing NTP server.</td>
</tr>
<tr>
<td>Configure NTP parameters</td>
<td>Navigate to <strong>System &gt; NTP Servers</strong>. Click <strong>NTP Parameters</strong> and enter the server's configuration details in given fields provided.</td>
</tr>
<tr>
<td>Enable NTP synchronization</td>
<td>Navigate to <strong>System &gt; NTP Servers</strong>. To synchronize the time displayed on the NTP server with your local clock, select the Enable NTP Synchronization check box.</td>
</tr>
<tr>
<td>Add or modify cipher groups</td>
<td>Navigate to <strong>System &gt; Cipher Groups</strong> to add a new cipher group or edit the settings of an existing cipher group. You must enter a description of your cipher group and assign it to a cipher suite.</td>
</tr>
<tr>
<td>Configure notification settings</td>
<td>Navigate to <strong>System &gt; Notifications</strong>. Under Settings, select <strong>Change Notification Settings</strong>. Choose the actions for which you want to send the notifications, and select Email, SMS, or both.</td>
</tr>
<tr>
<td>Configure event digest settings</td>
<td>Navigate to <strong>System &gt; Notifications</strong>. Under Settings, select <strong>Configure Event Digest Settings</strong>. After clearing the Disable Event Digest check box, you can set a recurrence period and choose an email distribution list for sending event digest notifications.</td>
</tr>
<tr>
<td>Add or modify email servers</td>
<td>Navigate to <strong>System &gt; Notifications &gt; Email</strong>. Under Email, select the <strong>Email Servers</strong> tab to add a new email server or edit the settings for an existing email server. You can enable additional checks to ensure that authentication is required for access to the email server, or to specify that your email server supports SSL authentication.</td>
</tr>
<tr>
<td>Add or modify email distribution lists</td>
<td>Navigate to <strong>System &gt; Notifications &gt; Email</strong>. Under Email, select the <strong>Email Distribution List</strong> tab to add a new email distribution list or edit the settings for an existing email distribution list.</td>
</tr>
<tr>
<td>If you want to...</td>
<td>Do this...</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Add or modify SMS servers</td>
<td>Navigate to System &gt; Notifications &gt; SMS. Under SMS, select the SMS Server tab to add a new SMS server or edit the settings for an existing SMS server.</td>
</tr>
<tr>
<td>Add or modify SMS distribution lists</td>
<td>Navigate to System &gt; Notifications &gt; SMS. Under SMS, select the SMS Distribution List tab to add a new SMS distribution list or edit the settings for an existing SMS distribution list.</td>
</tr>
<tr>
<td>Configure SNMP Engine ID</td>
<td>Navigate to System &gt; SNMP. Under Settings, select Configure Engine ID and specify the Engine ID.</td>
</tr>
<tr>
<td>Configure SNMP MIB</td>
<td>Navigate to System &gt; SNMP. Under Settings, select Configure SNMP MIB, and enter the SNMP MIB details.</td>
</tr>
<tr>
<td>Configure SNMP Traps</td>
<td>Navigate to System &gt; SNMP &gt; Trap Destinations. Under SNMP Traps, add a new SNMP trap destination or edit the settings for an existing SNMP trap destination.</td>
</tr>
<tr>
<td>Add or modify an SNMP manager</td>
<td>Navigate to System &gt; SNMP &gt; Managers. Under SNMP Manager, add a new SNMP manager or edit the settings for an existing SNMP manager.</td>
</tr>
<tr>
<td>Add or modify an SNMP user</td>
<td>Navigate to System &gt; SNMP &gt; Users. Under SNMP User, add a new SNMP user or edit the settings for an existing SNMP user.</td>
</tr>
<tr>
<td>Add or modify SNMP views</td>
<td>Navigate to System &gt; SNMP &gt; Views. Under SNMP View, add a new SNMP view or edit the settings for an existing SNMP view.</td>
</tr>
<tr>
<td>Modify SNMP alarms</td>
<td>Navigate to System &gt; SNMP &gt; Alarms and select the alarm whose settings you want to modify.</td>
</tr>
<tr>
<td>View the task log</td>
<td>Navigate to System &gt; Diagnostics &gt; Task Logs. You can then see all the task logs, with details. You can view additional information by selecting a task log and viewing its Device Log, and then viewing the Command Log for the selected device log.</td>
</tr>
<tr>
<td>Generate the technical support file</td>
<td>Navigate to System &gt; Diagnostics &gt; Technical Support. Under Technical Support, click Generate Technical Support File to generate an archive (TAR file) of the NetScaler MAS data and statistics, which you can send to Citrix Support for help with debugging an issue.</td>
</tr>
<tr>
<td>Configure Dashboard reporting time zone settings</td>
<td>Navigate to System &gt; Analytics Settings. Under Analytics Settings, select Configure Dashboard Reporting Time Zone Settings to set your local time or GMT time zone as the default for the reports displayed on your dashboard.</td>
</tr>
<tr>
<td>Configure ICA session timeout</td>
<td>Navigate to System &gt; Analytics Settings. Under Analytics Settings, select Configure ICA Session Timeout and enter the amount of time for which an ICA session can remain in idle state before being terminated.</td>
</tr>
<tr>
<td>Configure analytics features</td>
<td>Navigate to System &gt; Analytics Settings. Under Analytics Settings, select Configure Features to enable mutihop settings and/or adaptive threshold settings. If you select the Enable Multihop check box, NetScaler MAS collects and correlates the AppFlow records from all appliances deployed with more than one NetScaler appliance between a client and a server. If you select the Enable Adaptive Threshold check box, a syslog message is sent to the syslog server whenever the number of hits on a URL is greater than its threshold value.</td>
</tr>
<tr>
<td></td>
<td>Navigate to System &gt; Analytics Settings. Under Analytics Settings, select Configure Features to enable database index settings and/or database cleanup settings.</td>
</tr>
<tr>
<td>Settings</td>
<td>Do this</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Configure database settings</strong></td>
<td>By selecting the <strong>Enable Database Indexing</strong> check box, you can facilitate efficient querying of the NetScaler MAS database. If you select the <strong>Enable Database Cleanup</strong> check box, an attempt to clean up the database is repeated if a heavy load on the NetScaler MAS prevents cleanup at its regularly scheduled time.</td>
</tr>
</tbody>
</table>
| **Configure data record settings**           | **Analytics Settings**, select **Configure Data Record Settings**. You can enable features for the settings listed here:  
  - Data Record Log Settings  
  - Data Duration Persistency Settings  
  - Web Insight Report Settings  
  - Web Insight SLA Data Collection Settings  
  - Web Insight URL Data Collection Settings  
  - URL Parameter Settings                                                                                                                   |
<p>| <strong>Configure SLA Management for specific NetScaler IP addresses</strong> | Navigate to <strong>System &gt; Analytics Settings &gt; SLA Management</strong>. From the list displayed, select the NetScaler IP address of an appliance on which you want to manage SLA over server response time, hits/second, and bandwidth usage. |
| <strong>Configure the duration for which to retain database records for each Insight summarization level</strong> | Navigate to <strong>System &gt; Analytics Settings &gt; Database Summarization</strong>. Specify the duration for which you want to retain Insight data on NetScaler MAS. You can choose to store this data either hourly, daily, and once every minute. |
| <strong>Add or modify adaptive thresholds</strong>        | Navigate to <strong>System &gt; Analytics Settings &gt; Adaptive Thresholds</strong>. Under <strong>Adaptive Thresholds</strong>, add a new adaptive threshold or edit the settings for an existing adaptive threshold. The adaptive threshold functionality sets the threshold value for the maximum number of hits on each URL. If the maximum number of hits on a URL is greater than the threshold value set for the URL, a syslog message is sent to an external syslog server. The threshold value interval can be either days or weeks. |
| <strong>Add or modify threshold and alerts</strong>       | Navigate to <strong>System &gt; Analytics Settings &gt; Thresholds</strong>. Under <strong>Thresholds</strong>, add a new threshold or edit the settings for an existing threshold. You can provide additional action items while creating or modifying a threshold, such as enabling it, sending notifications by email or SMS, or configuring a rule for the threshold. |
| <strong>Upload SSL certificate files and SSL keys</strong> | Navigate to <strong>System &gt; Advanced Settings &gt; SSL Certificate Files</strong>. Under <strong>SSL Certificate Files</strong>, select the <strong>SSL Certificates</strong> tab to upload a new SSL certificate. Similarly, under <strong>SSL Certificate Files</strong>, select the <strong>SSL Keys</strong> tab to upload a new SSL key. |
| <strong>Add geo database files</strong>                   | Navigate to <strong>System &gt; Advanced Settings &gt; Geo Database Files</strong> to upload a new geo database file.                                                                                                                                                                     |
| <strong>View or edit report export schedule/s</strong>    | Navigate to <strong>System &gt; Advanced Settings &gt; Export Schedules</strong>. You can then see all the export schedules, with details. You can edit any export schedule from the list displayed here.                                                                                      |
| <strong>Schedule a report export</strong>                 | Navigate to <strong>System &gt; Advanced Settings &gt; Export Schedules</strong>. To add a new schedule, click the **button on the extreme right, and select the <strong>Schedule Export</strong> tab. Specify the details and click <strong>Schedule</strong>.                                                                     |</p>
<table>
<thead>
<tr>
<th>Use the backup and restore features</th>
<th>You can later use these backed up files to restore the NetScaler MAS to the state that you backed up.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do this</td>
<td>Citrix recommends using this feature before performing an upgrade, and in general as a precautionary measure.</td>
</tr>
<tr>
<td>Install an SSL certificate</td>
<td>Navigate to <strong>System &gt; System Administration</strong>. Under <strong>Set Up NetScaler MAS</strong>, select <strong>Install SSL Certificate</strong>. You can select a certificate file and SSL key file that are already on the NetScaler MAS virtual appliance, or you can upload the files from your local computer. You must enter the NetScaler MAS password in the <strong>Password</strong> field to successfully install the SSL certificate.</td>
</tr>
</tbody>
</table>
NetScaler Pooled Capacity

Sep 28, 2017
NetScaler pooled capacity is a licensing framework that comprises a common bandwidth and instance pool that is hosted on and served by NetScaler MAS. From this common pool, each NetScaler instance in your data center, regardless of platform or form factor, checks out one instance license and only as much bandwidth as it needs. The license file and, consequently, the bandwidth are not bound to the instance. When the instance no longer requires these resources, it checks them back in to the common pool, making the resources available to other instances that need them.

This licensing framework maximizes bandwidth utilization by ensuring that instances are not allocated bandwidth in excess of their requirement. The ability of NetScaler instances to check licenses and bandwidth in and out of a common pool also enables you to automate instance provisioning.

You can increase or decrease the bandwidth allocated to an instance at run time without impacting traffic. You can also transfer NetScaler licenses in the pool from one instance to another.

This document includes the following information:

- How NetScaler Pooled Capacity Works
- Configuring NetScaler Pooled Capacity
- NetScaler Pooled Capacity on NetScaler Instances in High Availability mode
- NetScaler Pooled Capacity on NetScaler Instances in Cluster Mode
- Health Monitoring
- Expected Behaviors when Issues Arise

How NetScaler Pooled Capacity Works

NetScaler pooled capacity has the following components:

- NetScaler instances, which can be categorized into:
  - Zero-capacity hardware
  - Standalone VPX instances or CPX instances
- Bandwidth pool
- Instance pool
- NetScaler License server

Zero-Capacity Hardware
When managed through NetScaler pooled capacity, MPX and SDX instances are referred to as “zero-capacity hardware” because these instances cannot function until they check resources out of the bandwidth and instance pools. Accordingly, these platforms are also referred to as MPX-Z, and SDX-Z appliances.

Zero-capacity hardware require a platform license to be able to check out bandwidth and an instance license from the common pool. However, you cannot use NetScaler pooled capacity to manage and install platform licenses. You must install a platform license manually, by using the hardware serial number or the license access code. After a platform license is installed, it is locked to the hardware and cannot be shared across NetScaler hardware instances on demand. However, you can manually move the platform license to another NetScaler hardware instance.

Currently, the following zero-capacity hardware, running the NetScaler software release 11.1 Build 54.14 and later, support NetScaler pooled capacity:

- MPX-14000Z
- MPX-14000Z-40G
- MPX-25000Z-40G
- SDX-14000Z
- SDX-14000Z-40G
- SDX-25000Z-40G

**Standalone NetScaler VPX Instances**

NetScaler VPX instances running NetScaler software release 11.1 Build 54.14 on the following hypervisors supports pooled-capacity

- VMware ESX 6.0
- Citrix XenServer
- KVM

Unlike zero-capacity hardware, VPX does not require platform license. To process traffic, it must check out bandwidth and an instance license from the pool.

**Standalone NetScaler CPX Instances**

NetScaler CPX instances deployed on a Docker host supports pooled-capacity. Unlike zero-capacity hardware, CPX does not require platform license. To process traffic, it must check out an instance license from the pool.

**Bandwidth Pool**

The bandwidth pool is the total bandwidth that can be shared by NetScaler instances, both physical and virtual. The bandwidth pool comprises separate pools for each software edition (Standard, Enterprise, and Platinum). A given NetScaler instance cannot have bandwidth from different pools checked out concurrently. The bandwidth pool from which it can check out bandwidth depends on its software edition for which it is licensed.

**Instance Pool**

The instance pool defines the number of VPX instances or CPX instances that can be managed through NetScaler pooled capacity or the number of VPX instances in an SDX-Z instance.
When checked out from the pool, a license unlocks the MPX-Z, SDX-Z, VPX, and CPX instance's resources, including CPUs/PEs, SSL cores, packets per second, and bandwidth.

**Note**

The Management Service of an SDX-Z does not consume an instance.

**NetScaler License Server**

NetScaler license server is a component in NetScaler Management and Analytics System (NetScaler MAS). NetScaler pooled capacity uses NetScaler license server to manage pooled capacity licenses: bandwidth pool licenses and instance pool licenses. You can use NetScaler MAS to manage pooled capacity licenses without a MAS license.

When checking out licenses from bandwidth and instance pool, NetScaler form factor and hardware model number on a zero-capacity hardware determines:

- The minimum bandwidth and the number of instance that a NetScaler instance must check-out before being functional.
- The maximum bandwidth and the number of instances that a NetScaler can check-out.
- The minimum bandwidth unit for each bandwidth check-out. Minimum bandwidth unit is the smallest unit of bandwidth that a NetScaler has to check-out from a pool. Any check-out must be an integer multiple of the minimum bandwidth unit. For example, if minimum bandwidth unit of a NetScaler is 1Gbps, 100Gbps can be checked out, but not 200Mbps or 150.5Gbps. Minimum bandwidth unit is different from the minimum bandwidth requirement. A NetScaler instance can only operate after it is licensed with at least the minimum bandwidth. Once the minimum bandwidth is met, the instance can check-out additional bandwidth with minimum bandwidth unit.

The following table summarizes the Maximum bandwidth/instances, minimum bandwidth/instances and minimum bandwidth unit for all supported NetScaler instances.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum Bandwidth (Gbps)</strong></td>
<td>8</td>
<td>100</td>
<td>100</td>
<td>200</td>
<td>100</td>
<td>100</td>
<td>200</td>
<td>1</td>
</tr>
<tr>
<td><strong>Minimum Bandwidth (Gbps)</strong></td>
<td>10 Mbps</td>
<td>20</td>
<td>20</td>
<td>100</td>
<td>20</td>
<td>20</td>
<td>100</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Minimum Instances</strong></td>
<td>1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>5</td>
<td>5</td>
<td>20</td>
<td>1</td>
</tr>
<tr>
<td><strong>Maximum Instances</strong></td>
<td>1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>25</td>
<td>25</td>
<td>115</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Minimum Bandwidth Unit</strong></td>
<td>10 Mbps</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
<td>N/A</td>
</tr>
</tbody>
</table>
The following table summarizes the license requirement for different form factors.

<table>
<thead>
<tr>
<th></th>
<th>MPX</th>
<th>SDX</th>
<th>VPX</th>
<th>CPX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero Capacity Hardware Purchase</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bandwidth &amp; Edition Subscription</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Instance Subscription</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>
You can allocate licenses in the license pool to NetScaler instances on demand. You can upload the pooled capacity license files (Bandwidth Pool or Instance Pool) to the license server. You can allocate the licenses from NetScaler MAS, or you can check-out the licenses from NetScaler instance (MPX-Z /SDX-Z/VPX/CPX) according to the minimum and maximum capacity of the instance.

This document includes the following information:

- Configuring the License Server
  - NetScaler Management and Analytics System
  - Citrix Licensing Server
- Configuring NetScaler Pooled Capacity on MPX-Z
- Configuring NetScaler Pooled Capacity on a NetScaler VPX Instance
- Allocating Pool Licenses to a NetScaler MPX-Z or NetScaler VPX Instance
- Configuring NetScaler Pooled Capacity on SDX-Z
  - Pool Capacity on NetScaler SDX
- Allocating Pool Licenses to a NetScaler SDX-Z Instance
- Configuring NetScaler Pooled Capacity on a NetScaler CPX Instance

## Configuring the License Server

You need to configure the license server to pool and allocate the licenses to the pooled-capacity enabled instances, or check-out licenses from the NetScaler pooled capacity enabled instance.

### Note

You need to configure the license server to pool and allocate the licenses to the pooled-capacity enabled instances, or check-out licenses from the NetScaler pooled capacity enabled instance.

## NetScaler Management and Analytics System

You can configure the NetScaler Management and Analytics System as a license server for the NetScaler Pooled capacity. There are two ways for a NetScaler Instance to get bandwidth and or instance license:
A NetScaler instance can initiate the check-out request to NetScaler MAS to obtain its bandwidth and/or instance licenses.

The licenses can be allocated to a NetScaler instance through NetScaler MAS.

Note
Pooled Capacity is displayed on NetScaler MAS only if pooled licenses are added to the NetScaler MAS.

Following are the operating modes of the NetScaler instances that are using the NetScaler Pooled Capacity:

- **Optimum** – Instance is running with proper license capacity.
- **Capacity mismatch** – Instance is running with a capacity less than user configured.
- **Grace** – Instance is running on grace license.
- **Grace & Mismatch** – Instance is running on grace but with a capacity less than user configured.
- **Not available** – Instance is not registered with NetScaler MAS for management or Nitro communication from NetScaler MAS to Instance is not working.
- **Not allocated** – License is not allocated in instance.

To install license files on the NetScaler Management and Analytics System:

1. In a web browser, type the IP address of the NetScaler Management and Analytics System (for example, http://192.168.100.1).
2. In User Name and Password, enter the administrator credentials.
3. On the Configuration tab, navigate to Infrastructure > Licenses > Settings, and click Add New License.
4. In the License Files section, select one of the following options:

   - Upload license files from a local computer - If a license file is already present on your local computer, you can upload it to the NetScaler MAS. To add license files, click Browse and select the license file (.lic) that you want add. Then click Done.

   Note
   If the uploaded license files does not add the licenses in the NetScaler Pooled capacity, you can select the license files and click Apply Licenses to add the licenses to the pool.
Use License Access Code - Citrix emails the License Access Code (LAC) for the licenses that you purchase. To add license files, enter the LAC in the text box and then click Get Licenses.

Note
At any time, you can add more licenses to the NetScaler Management and Analytics System (MAS) from the License Settings.

To allocate NetScaler Pooled Capacity licenses from the NetScaler Management and Analytics System:

Prerequisite: Before you can manage your instance's pool licenses through the NetScaler Management and Analytics System (MAS), you must register the NetScaler instance with the NetScaler MAS. In the NetScaler GUI, navigate to System > Licenses > Manage Licenses and select the Register with NetScaler MAS for manageability check box when adding the NetScaler MAS IP.

Note
If you have not registered the NetScaler instance with NetScaler MAS, you can check-out licenses from NetScaler MAS, but cannot allocate from NetScaler MAS to the NetScaler pooled capacity enabled Instance.
Note

In the Username and Password fields on the above screen, enter the NetScaler Management and Analytics System credentials.

After the instance is registered with the license server, allocate the licenses as follows:

1. In a web browser, type the IP address of the **NetScaler Management and Analytics System** (for example, http://192.168.100.1).
2. In User Name and Password, enter the administrator credentials.
3. On the Configuration tab, navigate to **Infrastructure > Licenses > Pooled Capacity**.
4. Click on the license pool that you want to manage.
5. Select a NetScaler instance from the list of available instances by clicking on the > button.

6. If you want to change or release a license allocation, click **Change allocation** or **Release allocation**.
7. If you click **Change allocation**, a pop-up window with the available licenses in the license server appears.

8. You can choose the bandwidth or instance allocation to the NetScaler instance by setting the **Allocate** drop-down options. After making your selections, click **Allocate**.

9. You can also change the allocated license edition from the drop-down options in the Change License Allocation window.

### Citrix Licensing Server

The Citrix License Server (Windows or VPX) can be used to serve NetScaler Pooled Capacity licenses. You can check-out licenses from the Citrix Licensing Server to the pooled capacity enabled instances (MPX-Z/SDX-Z/VPX/CPX), but cannot allocate licenses from the Citrix Licensing Server to the pooled capacity enabled instances.

**Note**

You can always change your NetScaler pooled capacity enabled Instances to use a different license server (NetScaler Management and Analytics System or Citrix Licensing Server) by entering a new license server's IP address in the **System > Licenses** section of the NetScaler Instance's GUI. It is recommended to check-in the licenses to the old licensing server and check-out again from new licensing server.

### Configuring NetScaler Pooled Capacity on MPX-Z

MPX-Z is the NetScaler pooled-capacity enabled NetScaler MPX appliance. MPX-Z supports bandwidth pooling for Platinum, Enterprise, or Standard edition licenses.

MPX-Z requires its platform licenses before it can connect to the license server. You can install the MPX-Z platform license by either uploading the license file from a local computer or using the instance's hardware serial number, or the License Access Code from **System > Licenses** section of the NetScaler Instance's GUI. If you remove the MPX-Z platform license, the pooled-capacity feature is disabled and all the checked-out licenses are checked in to the license server.
You can dynamically modify the Bandwidth of a MPX-Z instance without a restart. A restart is required only if you want to change the license edition.

Note
When you restart the instance, it automatically checks out the pooled licenses required for its configured capacity.

Configuring NetScaler Pooled Capacity on a NetScaler VPX Instance

A pooled-capacity enabled NetScaler VPX instance can check-out licenses from a bandwidth pool (Platinum/Enterprise/Standard editions). You can use the NetScaler GUI to check-out licenses from the license server.

You can dynamically modify the Bandwidth of a VPX instance without a restart. A restart is required only if you want to change the license edition.

Note
When you restart the instance, it will automatically check-out the pooled licenses required for its configured capacity.

Allocating Pool Licenses to a NetScaler MPX-Z or NetScaler VPX Instance

To allocate your licenses:

1. In a web browser, type the IP address of the NetScaler instance (for example, http://192.168.100.1).
2. In the User Name and Password fields, enter the administrator credentials.
3. On the Configuration tab, navigate to System > Licenses > Manage Licenses, click Add New License and select Use Pooled Licensing.
4. Enter the details of the license server in the **Server Name/IP Address** field.

5. If you want to manage your instance's pool licenses through the NetScaler Management and Analytics System (MAS), select the **Register with NetScaler MAS for manageability** check box and enter the NetScaler Management and Analytics System credentials.

6. Select the license edition and the required bandwidth, click **Get Licenses**.

7. You can change or release the license allocation by selecting **Change allocation** or **Release allocation**.
8. If you click **Change allocation**, a pop-up window shows the licenses available on the license server.

**Note**

A restart is not required if you change the bandwidth allocation, but a warm restart is required if you change the license edition.

9. You can allocate bandwidth or instances to the NetScaler instance from the **Allocate** drop-down list. Then click **Get Licenses**.

10. You can choose the license edition and the bandwidth required from the drop-down lists in the pop-up window.

**Note**

Bandwidth allocation should be a multiple of the minimum bandwidth unit.

---

**Configuring NetScaler Pooled Capacity on SDX-Z**

An SDX-Z instance is a pooled-capacity enabled instance of NetScaler SDX. SDX-Z supports bandwidth pooling for Platinum, Enterprise, and Standard editions, and instance pooling. After you apply the SDX-Z platform license, the Management Service provides options for checking licenses out from and back into the licensing server, and for allocating bandwidth capacity to the NetScaler instances running on the SDX-Z platform.
Note

NetScaler VPX instances running on SDX-Z cannot directly check licenses out from or in to the license server. This can be done by the Management Service in SDX.

You can install the SDX-Z platform license by either uploading the license file from the local computer or using the instance’s hardware serial number, or the License Access Code.

If you remove the SDX-Z platform license, the pooled-capacity feature is disabled and all the licenses are checked back into the licensing server.

Note

If you reboot the instance, it checks-out the pooled licenses required for its configured capacity.

Pool Capacity on NetScaler SDX

**Instance Pool:**

An SDX appliance can provision same number of instances that are available in the instance pool of the SDX appliance.

**Bandwidth Pool:**

During NetScaler instance provisioning, bandwidth is allocated to the instance. You can select the edition and required bandwidth to provision a Virtual NetScaler instance. The Management Service allows the provisioning to continue only if the instance has sufficient bandwidth for the requested edition. You are notified if the bandwidth is insufficient.

Note

Bandwidth modification does not require an instance restart.

Allocating Pool Licenses to a NetScaler SDX-Z Instance

To allocate your licenses:

1. In a web browser, type the IP address of your NetScaler SDX-Z instance (for example, http://192.168.100.1).
2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. On the Configuration tab, navigate to **System > Licenses**, and go to **Pooled Capacity**.
4. Enter the details of the license server in the **Server Name/IP Address** field.

5. If you want to manage your instance's pool licenses through the NetScaler Management and Analytics System (MAS), select the **Register with NetScaler MAS** check box and enter the NetScaler Management and Analytics System credentials.

6. You can change or release the license allocation by selecting **Change allocation** or **Release allocation**.

**Note**

The checked out licenses are stored in a separate pool by the Management Service.

7. To change the license allocation for a specific VPX instance in the SDX-Z instance, select the instance from the **Instances** section, and click **Change allocation**. A new window displays the available licenses.
8. You can change the bandwidth edition of the instance from the Feature License drop-down list, and the required bandwidth in the Throughput (mbps) field. Then click Done.

**Note**

Bandwidth allocation should be an integer multiple of the minimum bandwidth unit of the corresponding form factor.

## Configuring NetScaler Pooled Capacity on a NetScaler CPX Instance

While provisioning the NetScaler CPX instance, you can configure the NetScaler CPX instance to use NetScaler Pooled Capacity. In the `docker run` command, you need to provide the NetScaler Licensing Server (NetScaler MAS) details. The NetScaler CPX instance checks-out licenses from the Instance pool.

**Note**

By default, NetScaler CPX instance checks-out an instance license from the instance pool and the throughput is automatically set to 1000 Mbps. You cannot modify the 1000 Mbps bandwidth allocated to the instance.

You can download NetScaler CPX from the Docker App Store. On the Docker host, to download NetScaler CPX, run the following command:
To configure NetScaler Pooled Capacity while provisioning the NetScaler CPX Instance:

While provisioning a NetScaler CPX instance, define the NetScaler Licensing Server (NetScaler MAS) as an environmental variable in the `docker run` command as shown below:

```
docker run -dt -P -e LS_IP=\<LS_IP_ADDRESS\> -e LS_PORT=\<LS_PORT\> --name \<container_name\> --ulimit core=-1 -e EULA=yes -v ...
```

Where:

- `<LS_IPADDRESS>` is the IP address of the NetScaler Licensing Server (NetScaler MAS).
- `<LS_PORT>` is the port of the NetScaler Licensing Server. By default, the port is 27000.
NetScaler Pooled Capacity on NetScaler Instances in High Availability mode

Aug 17, 2018
You can configure NetScaler Pooled Capacity on the NetScaler instances configured in high availability mode, on a new NetScaler HA pair or an existing HA pair. When a fail over happens, the secondary instance in a HA Pair checks-out the same capacity that was present in the primary instance.

To migrate an existing HA setup to NetScaler pooled capacity

1. Remove the existing platform licenses and warm restart both instances to make them unlicensed.

2. For an MPX instance, add NetScaler Pooled Capacity Platform license on both the instances.

3. On the Configuration tab, navigate to System > Licenses > Manage Licenses, click Add New License and select Use Pooled Licensing.

4. Enter the details of the license server in the Server Name/IP Address field.

5. If you want to manage your instance's pool licenses through the NetScaler Management and Analytics System (MAS), select the Register with NetScaler MAS for manageability check box and enter the NetScaler Management and Analytics System credentials.

6. Warm reboot both the instances.
Note

If you try to use NetScaler Pooled Capacity with the existing platform licenses on a VPX instance, the following error message appears in the NetScaler GUI:

To allocate NetScaler Pooled capacity licenses on NetScaler HA pair

1. In a web browser, type the IP address of the primary NetScaler instance in the HA pair (for example, http://192.168.100.1).
2. In the User Name and Password fields, enter the administrator credentials.
3. Select the license edition and the required bandwidth, click Get Licenses.
4. You can change or release the license allocation by using the Change allocation or Release allocation option.

The same amount of capacity needs to be assigned to both primary and secondary NetScaler instances in a HA pair.
5. If you click **Change allocation**, a pop-up window shows the licenses available on the license server.

**Note**

A reboot is not required if you change the bandwidth allocation, but a warm reboot is required if you change the license edition.

---

6. You can allocate bandwidth or instances to the NetScaler instance from the **Allocate** drop-down list. Then click **Get Licenses**.

7. You can choose the license edition and the bandwidth required from the drop-down lists in the pop-up window.

**Note**

Bandwidth allocation must be an integral multiple of the minimum bandwidth unit of the corresponding form factor.
NetScaler Pooled Capacity on NetScaler Instances in Cluster Mode

Aug 17, 2018

You can configure NetScaler pooled capacity on the NetScaler instances configured as a cluster. Following are the prerequisites for configuring pooled capacity on NetScaler instances in cluster mode:

- Instances should be individually running in a pooled-capacity license mode to form the cluster.
- All the instances should be running with same bandwidth.
- All the instances should check out the pooled capacity from the same NetScaler MAS.
- New instances cannot be added to an existing NetScaler cluster unless their capacity and NetScaler MAS configurations are same as those of the existing instances in the cluster.

Any capacity check-out from the NetScaler cluster will assign same capacity to all the cluster nodes and the checkout Bandwidth = Bandwidth provided * number of nodes.

For example, if you check-out 50 Mbps of bandwidth from the NetScaler cluster, and the cluster includes 12 instances, each instance automatically receives 50 Mbps; and 600 mbps is checked out from the pool.

Note

If one or more instances in the cluster become unresponsive, the cluster continues to work with the capacity of the remaining instances.

To allocate NetScaler Pooled capacity on NetScaler instances in cluster mode

1. In a web browser, type the IP address of the Cluster IP (CLIP) address (for example, http://192.168.100.1).
2. In the User Name and Password fields, enter the administrator credentials.
3. On the Configuration tab, navigate to System > Licenses > Manage Licenses, click Add New License, and select Use Pooled Licensing.
4. Enter the name or address of the license server in the **Server Name/IP Address** field.

5. If you want to manage your instance's pool licenses through the NetScaler Management and Analytics System (MAS), select the **Register with NetScaler MAS for manageability** check box and enter the NetScaler Management and Analytics System credentials.

6. Select the license edition and the required bandwidth, and click **Get Licenses**.

7. You can change or release the license allocation by selecting **Change allocation** or **Release allocation**.
8. If you click **Change allocation**, a pop-up window shows the licenses available on the license server.

**Note**

Bandwidth allocation must be an integral multiple of the minimum bandwidth unit of the corresponding form factor.

9. You can allocate bandwidth or instances to the NetScaler instance from the **Allocate** drop-down list. Then click **Get Licenses**.

10. You can choose the license edition and the bandwidth required from the drop-down lists in the pop-up window.

**Note**

A restart is not required if you change the bandwidth allocation, but a warm restart is required if you change the license edition.
Health Monitoring

Aug 17, 2018

The license server continuously monitors the health of the NetScaler pooled-capacity enabled instance. The instances communicate through periodical messages to the license server. If few consecutive messages are not received, the license server reports that connectivity has been lost.

You can create custom notifications to supplement the default alarms.

Grace Period

When a NetScaler pooled-capacity enabled instance is in a healthy state and the license server stops responding, the instance continues to operate with the current capacity for 30 days. If the connectivity to the license server is not restored after 30 days, the instance loses its capacity and stops processing traffic.

Notifications and Alarms

Notifications can be enabled from NetScaler Management and Analytics System (MAS) for any action performed on the instance. Apart from the custom notification settings, some alarms are configured by default. For example: To configure an alarm for replenishing a pool that has depleted a certain percentage of its capacity, navigate to Infrastructure > Licenses > Settings > Notification Settings and click the edit button.
Expected Behaviors when Issues Arise

Aug 17, 2018
Following are the expected behaviors of the license servers and NetScaler instances when they experience the issues described:

License Server stops responding

*Warning message (syslog): The license Server is not responding. NetScaler will continue to operate with the current capacity for 30 days. After 30 days, if the connectivity to the license server is not restored, the NetScaler will loses its current capacity and stops processing traffic.*

If the license server stops responding, the NetScaler instance enters the Grace Period until connectivity is restored.

NetScaler pooled-capacity enabled instance stops responding

If the NetScaler pooled-capacity enabled instance stops responding and the license server is in a healthy state, the license server checks in all the NetScaler instance’s licenses after 10 minutes. When the instance reboots, it sends a request to check-out all the licenses from the licensing server.

Both license server and NetScaler pooled-capacity enabled instance stop responding

If both the license server and the NetScaler pooled-capacity enabled instance restarts and reestablishes the connection, the license server checks-in all its licenses after 10 minutes, and the NetScaler pooled capacity enabled instances automatically check-out the licenses after the reboot is completed.

The NetScaler pooled-capacity enabled instance shuts down gracefully

During a graceful shutdown, you can choose to check the licenses in or keep the licenses that were allocated before the graceful shutdown. If you choose to check the licenses in, the NetScaler pooled-capacity enabled instance is unlicensed after the it restarts. If you choose to keep the licenses, they are checked in to the licensing server when the instance shuts down. After the instance restarts, it reestablishes the connection with the licensing server and checks out the licenses as specified in the saved configuration.

If system reboots and the check-out fails due no capacity available in the pool, the NetScaler will check the inventory of
NetScaler MAS pool licenses and will check-out any available capacity. An SNMP alarm is raised to notify this condition to the user if NetScaler is not running with full capacity as per configuration. If no capacity is available in the bandwidth pool, the pool capacity enabled instance will become unlicensed.

Network loses connectivity

Error message (syslog): License Server is not responding.

If the license server and NetScaler pooled-capacity enabled instances are in healthy states but network connectivity is lost, the instances continue to operate with their current capacity for 30 days. After 30 days, if the connectivity to the license server is not restored, the instances lose their capacity and stop processing traffic, and the license server checks-in all its licenses. After the license server reestablishes connectivity with the NetScaler instances, the instances check the licenses out again.
NetScaler VPX Check-In/Check-Out Licensing

Jun 20, 2017
You can allocate VPX licenses to NetScaler VPX instances on demand from NetScaler MAS. The Licenses are stored and managed by NetScaler MAS, which has a licensing framework that provides scalable and automated license provisioning. A NetScaler VPX instance can check out the license from the NetScaler MAS when a NetScaler VPX instance is provisioned, or check back in its license to NetScaler MAS when an instance is removed or destroyed.

This document includes the following information:

- Prerequisites
- Installing Licenses in NetScaler MAS
- Allocating VPX Licenses to a NetScaler VPX Instance by using the NetScaler GUI
- Allocating VPX Licenses to a NetScaler VPX Instance by using the NetScaler CLI
- Allocating VPX Licenses to a NetScaler VPX Instance by using the API

Make sure that the following prerequisites are met:

- You are using a NetScaler VPX image running software version 11.1 Build 54.14 or later.
- You have installed NetScaler MAS running version 11.1 build 54.14 or later.

Note:
To manage existing VPX licenses by NetScaler MAS, you need to rehost the licenses to NetScaler MAS.

Note:
Before installing licenses, restart the NetScaler MAS virtual appliance if you have changed the software edition or bandwidth.

To install license files on the NetScaler Management and Analytics System:

1. In a web browser, type the IP address of the NetScaler MAS (for example, http://192.168.100.1).
2. In User Name and Password, enter the administrator credentials.
3. On the Configuration tab, navigate to Networks > Licenses, and click Add License File.
4. In the License Files section, select one of the following options:
   - Upload license files from a local computer - If a license file is already present on your local computer, you can upload it to the NetScaler MAS.
     To add license files, click Browse and select the license file (.lic) that you want add. Then click Finish.
   - Use License Access Code - Citrix emails the License Access Code (LAC) for the licenses that you purchase.
     To add license files, enter the LAC in the text box and then click Get Licenses.

   Note: Make sure you are connected to internet before using LAC code for installing the licenses.
At any time, you can add more licenses to the NetScaler MAS from the License Settings.

You can view the available and allocated licenses in the NetScaler MAS GUI.

**To display the licenses**

1. In a web browser, type the IP address of the NetScaler Management and Analytics System (for example, http://192.168.100.1).

2. In **User Name** and **Password**, enter the administrator credentials.

3. On the Configuration tab, navigate to **Networks > Licenses > VPX Licenses**.

   **VPX Licenses**

<table>
<thead>
<tr>
<th>VPX 25</th>
<th>VPX 200</th>
<th>VPX 1000</th>
<th>VPX 8000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total 1</td>
<td>Total 1</td>
<td>Total 1</td>
<td>Total 2</td>
</tr>
<tr>
<td>Used 0</td>
<td>Used 0</td>
<td>Used 0</td>
<td>Used 1</td>
</tr>
</tbody>
</table>

   The following instances are consuming VPX 8000 Enterprise Edition license.

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Allocation Status</th>
<th>Running</th>
</tr>
</thead>
<tbody>
<tr>
<td>--</td>
<td>10.102.29.99</td>
<td>Optimum</td>
<td></td>
</tr>
</tbody>
</table>

4. You can view the allocated licenses in the table under the available licenses section.

1. In a web browser, type the IP address of the NetScaler instance (for example, http://192.168.100.1).

2. In the **User Name** and **Password** fields, enter the administrator credentials.

3. On the Configuration tab, navigate to **System > Licenses > Manage Licenses**, click **Add New License** and select **Use Remote Licensing**.

4. Enter the details of the license server in the **Server Name/IP Address field**.
5. If you want to manage your instance's VPX licenses through the NetScaler MAS, select the **Register with NetScaler MAS** check box and enter the NetScaler MAS credentials.

6. Select the license edition with the required bandwidth, click **Get Licenses**.

7. Click **Reboot**, your NetScaler VPX instance will reboot.

8. You can change or release the license allocation by navigating to **System > Licenses > Manage Licenses**, and selecting **Change allocation** or **Release allocation**.
9. If you click Change allocation, a pop-up window shows the licenses available on the license server. Select the required license, click Get Licenses.

1. In a SSH client, enter the IP address of the NetScaler instance, and log on by using administrator credentials.

2. To add a licensing server, enter the following command

   ```
   add ns licenseserver (<licenseServerIP> | <serverName>) [-port <port number>]
   ```

   Example:
   ```
   > add ns licenseserver 10.102.29.97 -port 27008
   ```

3. To show the available licenses on the licensing server, enter the following command

   ```
   sh licenseserverpool
   ```

   Example:
   ```
   > sh licenseserverpool
   ```
4. To assign a license to the NetScaler VPX appliance, enter the following command

```
set capacity -platform V[S/E/P][Bandwidth]
```

In a web browser or an API client, log on to the NetScaler VPX instance by using the administrator credentials.

**To add a licensing server**

1. Set the request type to **Post**.
2. Set the path to `/nitro/v1/config/nslicensingserver`.
3. Set the payload as follows:

```plaintext
content-type: application/x-www-form-urlencoded

object = {"params": {"warning": "yes"}, "nslicensing server": {"servername": "<NetScaler MAS IP>", "port": "27000"}}
```

NetScaler MAS responds to the request. The following sample response shows success.

```
RESPONSE
HTTP/1.1 201 Created
Date: Fri, 06 Jan 2017 19:03:21 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 57
Content-Type: application/json; charset=utf-8

{ "errorcode": 0, "message": "Done", "severity": "NONE" }
```

**To view the available licenses on the licensing server**

1. Set the request type to **Get**.
2. Set the path to `/nitro/v1/config/nslicenseserverpool`.
NetScaler MAS responds to the request. The following sample response shows success, and the list of available licenses on the license server.

```HttpResponse: 
HTTP/1.1 200 OK
Date: Fri, 06 Jan 2017 19:18:34 GMT
Server: Apache
Content-Length: 1874
Content-Type: application/json; charset=utf-8
```

To assign a license to the NetScaler VPX appliance

1. Set the request type to Post.
2. Set the path to `/nitro/v1/config/nscapacity`.
3. Set the payload as follows:
   ```
   content-type: application/x-www-form-urlencoded
   
   nscapacity: { "platform": "VE8000" }
   ```

NetScaler MAS responds to the request. The following sample response shows success.
HTTP/1.1 200 OK
Date: Fri, 06 Jan 2017 18:16:21 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Type: application/json; charset=utf-8

{"errorcode":0,"message":"Done","severity":"NONE"}
finished.