NetScaler Insight 1.0

2015-04-19 05:20:31 UTC

Contents

NetScaler Insight 1.0

NetScaler Insight provides an in-depth analysis of application performance. User friendly features help you to quickly notice potential problems. For example:

- Specifying a NetScaler appliance to be monitored by NetScaler Insight requires only a mouse click.
- A centralized Dashboard displays dynamic reports that provide application visibility.
- You can view the performance of applications historically, across different time-slots.
- Easy navigation across the Dashboard makes information readily available.

Quick Links

- Release Notes
- Frequently Asked Questions

Release notes

This Release note covers the bug fixes and known issues identified in the NetScaler Insight Release.

Bug Fixes

The following issues have been fixed in this release.

Configuration

- Issue ID 0362717: If a user enables AppFlow for any load balancing or content switching virtual server from NetScaler Insight interface, the -clientOnlyTraffic parameter is not reset to the default value of NO on the NetScaler appliance that manages the virtual server.
- Issue ID 0333503/ 0357524: On the NetScaler Insight Inventory Setup screen of a NetScaler appliance with more than 30 virtual servers, if you choose to view more than 25 virtual servers per page, NetScaler Insight displays the "Connection Limit to CFE Exceeded" error.
- Issue ID 0349525: If a NetScaler appliance monitored by NetScaler Insight has service groups configured, the Appflow records exported to NetScaler Insight might be incomplete.
- Issue ID 0356282: If a NetScaler appliance has more than 8 cores, the NetScaler Insight dashboard does not report any data for that appliance.

Dashboard

- Issue ID 0334256: When reports are viewed, the values displayed on the x-axis of the charts might overlap because of a problem with resolution.
- Issue ID 0333541: When using the bread-crumb navigation in the Dashboard, you might not be able to go to earlier report you viewed by clicking on the respective component on the bread-crumb.

Known Issues

The following known issues have been identified in this NetScaler Insight1.0 release.

Dashboard Issues

- Issue ID 0332872: If you minimize the Dashboard page and then maximize it, the reports might not be displayed clearly.

  Workaround: Refresh the browser and view the reports.

- Issue ID 0333224: The Dashboard page might sometimes display double scroll bars.

  Workaround: Refresh the browser.

- Issue ID 0333551: When using Internet Explorer version 8, the Dashboard page might display an JavaScript error. However, it does not affect the functionality. The table borders in the dashboard might not be displayed clearly.

- Issue ID 0333560: The charts in NetScaler Insight might display junk values collected from the AppFlow records generated by the NetScaler appliance.

Configuration Issues

- Issue ID 0329751: If a NetScaler appliance monitored by NetScaler Insight restarts at short intervals, NetScaler Insight might not collect the AppFlow data generated by that appliance after the restart. The reports for that appliance might not be displayed on the NetScaler Insight Dashboard.

  Workaround: Restart the NetScaler Insight appliance.

- Issue ID 0333555: After you enable AppFlow on the virtual server, the **Insight** column might not display **ENABLED**, even if the operation is successful.

  Workaround: Refresh the browser and view the status.

- Issue ID 0350977: When specifying the expression for generating traffic, if you manually type a complex expression in the text box, the expression might not be saved.

  Workaround: Type the expression in Notepad, then copy it, and paste it into the text box.

- Issue ID 0377447: On the NetScaler Insight Inventory Setup screen of a NetScaler appliance with more than 30 virtual servers, if more than 25 virtual servers are listed per page, NetScaler Insight displays the "Error in retrieving Virtual Servers" error.

  Workaround: Select the option for viewing 25 virtual servers per page.

- Issue ID 0378044: On the NetScaler Insight Inventory Setup page, at the top of the Application List, the value shown for number of applications displayed and total number of applications might be incorrect.

FAQs

Basic Information

What is NetScaler Insight?

NetScaler Insight is a reporting and monitoring tool that collects AppFlow traffic generated across NetScaler appliances, and generates reports.

What are the features supported by NetScaler Insight?

NetScaler Insight supports Web Insight (HTTP analytics) and HDX Insight (ICA visibility).

Is NetScaler Insight a hardware or a software?

NetScaler Insight is a virtual appliance that is designed to be installed on a XenServer hypervisor, whereas NetScaler Insight is currently available only as a XenServer XVA.

What are the configurations I have to verify on the XenApp and XenDesktop server?

On a XenApp or XenDesktop server running version 6.5, make sure that the **ICA round trip calculations for Idle Connections** option is enabled for NetScaler Insight. If the option is not enabled, enable it and execute the **gpupdate** command.

What type of report does NetScaler Insight generate?

NetScaler Insight generates analytical reports, from which users can view the performance of applications, identify problem areas, and intelligently troubleshoot issues with performance and access.

Is there any physical connection required between the NetScaler appliances to be monitored and the XenServer?

No.

How do I specify the NetScaler appliances to be monitored by NetScaler Insight?

You need to add the NetScaler appliances to the NetScaler Insight Inventory list. To do so, you have to specify the IP address, username and password of the NetScaler appliance.

After I add the NetScaler appliance, does NetScaler Insight start collecting information?

No. You must first enable AppFlow on the applications managed by that NetScaler appliance. When you enable AppFlow, you should specify the expression against which the NetScaler appliance will generate AppFlow records.

Should I access the individual NetScaler appliance for enabling AppFlow?

No. All configurations are done from the NetScaler Insight GUI. The list of virtual servers for a specific NetScaler appliance will be listed in the NetScaler Insight user interface. In

addition for HDX Insight, ICA ports can be configured at a global level so that traffic flowing to these ports will be inspected and Appflow records are generated

Are all virtual servers on a NetScaler appliance listed for enabling AppFlow?

Currently the Load Balancing, Content Switching, VPN virtual servers and Access Gateway virtual servers are listed in the NetScaler Insight GUI, for enabling AppFlow.

Should the virtual server be UP when you enable AppFlow on it?

Yes, the virtual server should be UP when you enable AppFlow on it. You can view the operational status of the virtual server on the NetScaler Insight user interface.

NetScaler Appliance Specifications

Is there any specification for a NetScaler appliance to be monitored?

Yes, only NetScaler nCore appliances, running build 9.3 or later can be monitored. In addition, for HDX Insight, only Netscaler appliances running build 10.1 versions can be monitored.

Can I add NetScaler appliances running different licenses?

Any nCore NetScaler appliance running build 9.3 or later can be monitored by NetScaler Insight. However, the full set of counters and reports are generated only for platinum licensed NetScaler 10 appliances.

Can an AGEE appliance be monitored by NetScaler Insight?

No. A standalone AGEE appliance license cannot be added to the NetScaler Insight inventory. You need to have a NetScaler license to monitor AGEE traffic.

I am not able to add a NetScaler appliance running build 10. What are the possible reasons?

Make sure that NetScaler appliance you add is UP or reachable when you add it to the Inventory. If the appliance is DOWN, or OUT-OF-SERVICE, you cannot add it to the Inventory.

General Information

The host name of the NetScaler appliance is changed. Will it be reflected on NetScaler Insight inventory and the Dashboard?

Yes. NetScaler Insight reflects the changes every 30 minutes.

The login credentials of my NetScaler appliance are changed. Should I update that information in NetScaler Insight?

Yes. When the login credentials of a NetScaler appliance change, after 15 seconds, NetScaler Insight inventory displays the state of the NetScaler appliance as "OUT-OF-SERVICE" and you can view the reports for the particular NetScaler appliance.

You must update the login credentials in the NetScaler Insight appliance to collect AppFlow records on the virtual servers managed by that NetScaler appliance.

If I update the login credentials, will the state of the NetScaler appliance be "UP" immediately?

The state of the NetScaler appliance in the NetScaler Insight inventory will change to "UP" after seven seconds.

My NetScaler appliance uses it's Subnet IP address (SNIP) as the source IP for management access. Does NetScaler Insight collect data from the NetScaler appliances?

Yes. NetScaler Insight collects data from the NetScaler appliance. When adding the NetScaler appliance to NetScaler Insight Inventory, specify the SNIP address as the IP address of the appliance.

Reports

How do I view the reports?

By default, the Dashboard page displays the performance chart of the NetScaler appliances monitored by NetScaler Insight. You can click on the chart to move to the next level of information.

Are reports generated for all NetScaler appliances added to the NetScaler Insight inventory?

No. Only if you enable AppFlow on at least one virtual server in the NetScaler appliance, or configure ICA ports globally after enabling Appflow feature NetScaler Insight collects data from that appliance and generates reports.

How are the reports organized?

You can view reports for devices, applications, URLs, Clients and Servers on the Web Insight node and reports for users, applications, desktop, gateway and licenses on the HDX Insight node by clicking on the respective data-point in the Dashboard. When you access the reports from one of these data points, you get a consolidated report for that respective data point. For example, when you click Applications, you view the performance chart of all applications (across all NetScaler appliances) monitored by NetScaler Insight .

How can I view the reports of applications managed by a specific NetScaler appliance?

In the Dashboard, click **Devices** data-point in the left pane. The performance report for the appliances is displayed. Click on the data chart of a NetScaler appliance. The performance report of applications managed by that specific appliance is displayed. Similarly, when you click on that data chart of a particular application, you can view the next level details.

What are the counters I can choose for which viewing the performance reports?

The following table displays the counters you can choose to view the performance of application at different levels.

Web Insight	Devices	Hits, Bandwidth
	Applications	Hits, Bandwidth, Response Time
	URLs	Hits, Load Time, Render Time
	Clients	Requests, render Time, Client Network Latency
	Servers	Hits, Bandwidth, Server processing Time, Server Network latency
HDX Insight	Users	Average Bandwidth, Average Client latency, Average Server latency, Average ICA RTT, Client Smooth RTT, Server Smooth RTT
	Applications	Total Session Launch Count, Average Launch duration
	Desktops	Average Bandwidth
	Gateways	Total Session Launch Count, Total Application Launch Count
	Licenses	Licenses in Use

What other information can I view?

You can view information of HTTP request methods, HTTP response status, operating system, and user agents with respect to devices, application, client, URL, or server on the Web Insight node.

Even when the Appflow is enabled, I do not see the reports in the Dashboard. What are the possible reasons?

Even if Appflow is enabled on the virtual servers, the services bound to the virtual servers might have **AppFlow logging** set to disabled. In that case, you might not see the reports in the dashboard. In the NetScaler appliance, enable **AppFlow logging** at the service level to view the reports.

How is NetScaler Insight different from the Reporting tool on the NetScaler appliance?

The following table explains the basic differences between the Reporting tool and NetScaler Insight:

NetScaler Reporting tool	NetScaler Insight
Web based interface accessed from the NetScaler appliance	A separate VM in XVA format running on a XenServer. Many NetScaler appliances can be connected to the VM.
Displays performance statistics of the NetScaler appliance on which it runs.	Displays L3-L7 performance statistics of all connected NetScaler instances.
Statistics are collected by the nscollect utility.	Statistics are collected from the AppFlow records generated by the NetScaler appliances. NetScaler Insight adds itself as an AppFlow collector on the NS appliance.

Licensing Information

The depth of data collected by the NetScaler Insight virtual appliance depends on the license of the NetScaler appliance being monitored. The following tables explains what data is collected for the NetScaler appliances running different builds and versions.

- Web Insight
- HDX Insight

Web Insight

The following table provides the list of Web Insight - NetScaler Appliances License Information:

Table 1. Web Insight - NetScaler Appliances License Information

Metrics		**Description**	**NS 10 Platinum edition,**	**, NS 10 (Standard and Enterprise editions, and NS 9.3 (All editions)**
Devices	Hits	Number of requests received on NetScaler.	Yes	Yes
	Bandwidth	Total bytes processed by NetScaler device.	Yes	Yes

Applications	Hits	Number of requests received on application.	Yes	Yes
	Bandwidth	Total bytes sent to the application.	Yes	Yes
	Response Time	Elapsed time, between the end of an enquiry and the beginning of a response from the application. Response time constitutes of Client Network Latency, Server Processing Time and Server Network Latency.	Yes	No

URLs	Hits	Number of requests received for a URL.	Yes	Yes
	Load time	Elapsed time, from when the browser starts to receive the first byte of a response until the user starts to interact with the page. At this stage, some of the page content might not yet have been loaded.	Yes	No
	Render Time	Elapsed time, from when the browser starts to receive the first byte of a response until either all page content has been rendered or the page load action has timed out.	Yes	No
Clients	Requests	Number of requests sent by the client.	Yes	Yes
	Render time	Elapsed time, from when the browser starts to receive the first byte of a response until either all page content has been rendered or the page load action has timed out.	Yes	No
	Client Network Latency	Latency caused by client side network.	Yes	Yes

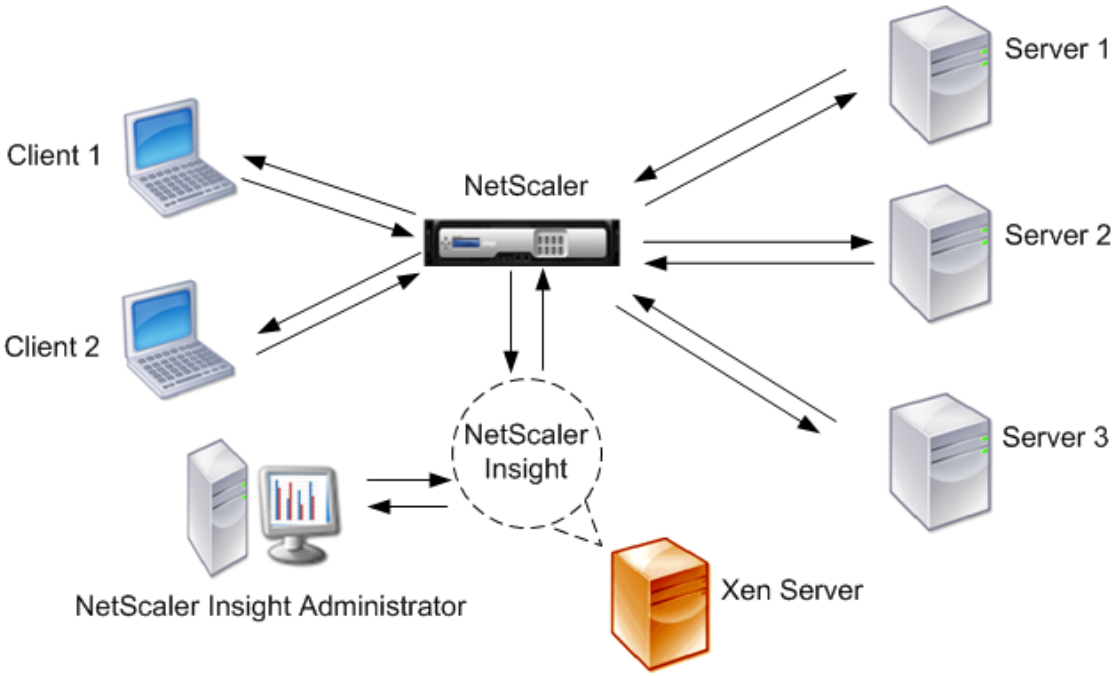
Servers	Hits	Number of requests received by the servers.	Yes	Yes
	Bandwidth	Total bytes received by the servers.	Yes	Yes
	Server Processing Time	Elapsed time, from when the server starts to receive the first byte of a request from the NetScaler appliance until the NetScaler appliance receives the first byte to response.	Yes	No
	Server Network Latency	Latency caused by server network.	Yes	Yes
HTTP Request Methods	Hits	Number of requests received distributed with respect to various request methods.	Yes	Yes
	Bandwidth	Total bytes received segregated across HTTP request methods.	Yes	Yes

HTTP Response Status	Hits	Number of response sent segregated with respect to HTTP response status.	Yes	Yes
	Bandwidth	Total bytes received segregated across the HTTP response status.	Yes	Yes
	Render Time	Average render time experienced by clients segregated across the HTTP status responses.	Yes	No
Operating Systems	Hits	Number of client requests received segregated across the user agents used.	Yes	Yes
	Bandwidth	Total bytes received from clients segregated across OS used.	Yes	Yes
	Render Time	Average Render time experienced by clients segregated across OS used.	Yes	No

User Agents	Hits	Number of client requests received segregated across the user agents used.	Yes	Yes
	Bandwidth	Total bytes received from clients segregated across user agents used.	Yes	Yes
	Render Time	Averaged Render time experienced by clients segregated across user agents used.	Yes	No
Waterfall Chart	-NA-		Yes	No

Where NetScaler Insight Fits in Network

NetScaler Insight is installed as a virtual machine on Citrix XenServer. Figure 1-1 shows the deployment scenario for NetScaler Insight. More than one NetScaler appliance can be connected to NetScaler Insight. Similarly, more than one instance of NetScaler Insight can be deployed on a XenServer. After adding the NetScaler appliances to the NetScaler Insight inventory, you must enable AppFlow on the virtual servers running on the NetScaler appliance.



When you enable AppFlow, you have to specify the rule or expression based on which the NetScaler appliance generates AppFlow records for the traffic passing through the virtual servers. Once AppFlow is enabled, the NetScaler appliance starts generating AppFlow records for the traffic generated by the virtual servers. NetScaler Insight collects that traffic information, and generates reports. Figure 1. NetScaler Insight Deployment

Benefits of using NetScaler Insight

- Because NetScaler Insight is installed on a XenServer server, it has no dependency on an external database and requires no additional hardware.
- On the NetScaler Insight Center Dashboard, you can:
  - Identify problem areas without accessing individual devices.
  - Identify user experience with respect to client-side parameters.
  - Know the top applications accessed by clients.
  - Track peak usage.
  - View the performance of applications in the last 5 minutes, 1 hour, 1 day, 1 week, and 1 month
- In addition, the Dashboard provides:
  - A waterfall chart to identify URL specific information: URL-level response time, render time, and load time.
  - Easy navigation. You can navigate from one report to another by clicking on the reports.
  - Bread-crumb navigation. You can readily identify the path by which you have navigated through the dashboard.

Installing NetScaler Insight

Before installing a NetScaler Insight virtual appliance, make sure that your XenServer installation and license files meet the minimum requirements. Use Citrix XenCenter to install NetScaler Insight on XenServer. Then, to activate the application's interface, you must specify the initial NetScaler appliance to be monitored.

Prerequisites for Installing NetScaler Insight

Before installing the NetScaler Insight virtual appliance, verify that the following requirements have been met.

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

XenServer Requirements for NetScaler Insight

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

Table 1. **Minimum Virtual Computing Resources Required for Running NetScaler Insight**

Component	Requirement
RAM	3 GB or more
Virtual CPU	2 or more
Storage space	120 GB, Recommended: 240 GB
Virtual Network Interfaces	2
Throughput	1 Gbps

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

On a XenApp or XenDesktop server running version 6.5, make sure that the **ICA round trip calculations for Idle Connections** option is enabled. If the option is not enabled, enable it and execute the gpupdate command. Also, the EUEM service must be running on the server.

Note: Verify that correct date, time, and time zone are configured on XenServer before NetScaler Insight is installed on the XenServer server.

For information about XenServer, see the documentation at http://support.citrix.com/product/xens/.

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 2. **Minimum System Requirements for XenCenter Installation**

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

Installing NetScaler Insight

After you have installed and configured XenServer and XenCenter, you can use XenCenter to install NetScaler Insight on XenServer. The number of NetScaler Insight instances that you can install depends on the amount of memory available on the hardware that is running XenServer.

Note: Before installing NetScaler Insight, verify that the correct date, time, and time zone are configured on XenServer.

To install NetScaler Insight on XenServer by using XenCenter

1. Start XenCenter on your workstation.
2. On the Server menu, click Add.
3. In the Add New Server dialog box, in the Hostname text box, type the IP address or DNS name of the XenServer that you want to connect to.
4. In the User Name and Password text boxes, type the administrator credentials, and then click Connect. The XenServer name appears in the navigation pane with a green circle, which indicates that the XenServer is connected.
5. In the navigation pane, right-click the name of the XenServer server on which you want to install NetScaler Insight and click Import.
6. In the Import dialog box, in Import file, browse to the location at which you saved the NetScaler Insight .xva image file. Make sure that the Exported VM option is selected, and then click Next.
7. Select the XenServer server on which you want to install the virtual appliance, and then click Next.
8. Select the local storage repository in which to store the virtual appliance, and then click Import to begin the import process.
9. You can add, modify, or delete virtual network interfaces as required. When finished, click Next.
10. Click Finish to complete the import process.

    Note: To view the status of the import process, click the **Log** tab.

    Once the import is complete, the kernel reboots. Select the **Console** tab to display the NetScaler Insight Initial Network Configuration options for specifying the initial IPv4 address, Netmask, and Gateway IP address for the NetScaler Insight virtual server.
11. Specify the NetScaler Insight IP address, Netmask and Gateway IP address by selecting the respective options.

    Note:

- To access the NetScaler Insight configuration utility, use the default user name (nsroot) and password (nsroot) to log on.

- In case the wizard closes and you want to update the network details, then run the command networkconfig on the command line interface.

12. If you want to install another NetScaler Insight virtual appliance, repeat steps 5 through 12.

Accessing NetScaler Insight

After installing the NetScaler Insight virtual appliance, you can access it through its user interface. To access the user interface, in the address bar of a browser, type the IP address that you specified when installing NetScaler Insight. NetScaler Insight is supported on the browsers listed in the following table.

Table 1. Browser Support

Browser	Version
Internet Explorer	IE8, and later
Google Chrome	Chrome 19, and later
Safari	Safari 5.1.1, and later
Mozilla Firefox	Mozilla Firefox 3.6.25, and later

Specifying the initial NetScaler Appliance to be Monitored

The first time you type the IP address of NetScaler Insight in the address bar of the browser, the application page appears. Enter the NetScaler Insight login credentials (username and password), that you specified when you installed the application. When the login credentials are validated, a Welcome Screen appears. Before you can view the dashboard or configure NetScaler Insight features, you have to add a NetScaler appliance to NetScaler Insight.

To add the initial NetScaler appliance:

1. On the Welcome Screen, Click Get Started.
2. On the NetScaler Insight Setup page, in the **NetScaler IP** field, enter the IP address of the NetScaler appliance to be added to NetScaler Insight. Make sure that the appliance meets the following conditions:

   - Must be **UP** when you add it to the Inventory.
   - Must be running nCore build with version 9.3 or later.
   - Should not be a standalone NetScaler AGEE appliance.

   Note: If the NetScaler appliance uses it's Subnet IP address (SNIP) for management access, specify the SNIP address as the IP address of the appliance.
3. Enter the user name and password for the NetScaler appliance in the UserName and Password fields, respectively.
4. Click Add to save the configuration and proceed to the Inventory list. To return to the Welcome Screen, click Cancel.

   The Inventory list, which is on the Configuration tab, displays the IP address, host name, and current operational state of the appliance that you added.

Enabling Data Collection

The landing page on the Configuration tab is the Inventory list, which lists the NetScaler appliances monitored by NetScaler Insight. The inventory list displays the IP address, host name, and operational state of each NetScaler appliance that has been added to the NetScaler Insight inventory. If an appliance is down or out-of-service, you cannot enable data collection on the virtual servers running on that appliance.

Enabling Data Collection on Virtual Servers

This topic enables data collection for web applications.

NetScaler Insight does not start collecting traffic information from the appliances in the Inventory list until you enable data collection on the virtual servers configured on those appliances. When enabling data collection on the virtual server, you can specify an expression describing the traffic about which to collect data for that virtual server. NetScaler appliance then generates AppFlow records for traffic that matches the expression. See Expressions for information on constructing expressions.

If you want to use NTP server time on NetScaler Insight, make sure that you configure NTP before enabling AppFlow on the virtual servers.

Note: When you enable AppFlow, NetScaler Insight adds itself as an AppFlow Collector on that NetScaler appliance. If you have enabled AppFlow on more than one NetScaler Insight virtual appliance, the appliance for which you most recently enabled data collection has the highest priority for collecting AppFlow information from the virtual server.

To enable data collection on a virtual server

1. On the **Configuration** tab, click **Inventory** (unless the Inventory list is already displayed).
2. From the Inventory list, click the IP address of the appliance on which you want to enable data collection.
3. On the AppFlow Setup screen, in the Applications pane, from the **View** drop-down list, select the type of virtual server (Load Balancing, Content Switching, or VPN). The virtual servers of the specified type populate a table that includes the following information:
   - IP Address—IP address of the virtual server
   - Name—Name of the virtual server
   - State—Current operational state of the virtual server. Can be UP or DOWN.
   - Type—Service type of the virtual server.
   - Insight—Data-collection status of the virtual server (ENABLED or DISABLED).
4. Select a virtual server for which to enable data collection.

   Note: You can enable data collection on a virtual server only if the operational state of the virtual server is UP.
5. Click Enable AppFlow in the task pane..

6. In The **Enable AppFlow** window, select an **Analytics expression** from the drop-down list, or type an expression.

   Note: The expressions listed in drop-down list are for the reference of the users. The users can select expressions from the list or construct their own expressions. If you do not specify an expression, you cannot enable AppFlow on the selected virtual server.

7. Click Enable to save the configuration. If data collection is enabled, the Insight column in the Application Lists table for that virtual server will show **Enabled**.

   Note:

   - You cannot enable AppFlow when the NetScaler appliance on which this virtual server is configured has already reached the limit (four) for the number of collectors.

   - If AppFlow logging is not enabled for the respective services on the NetScaler appliance, the NetScaler Insight dashboard will not display the records, even if the Insight column shows Enabled.

8. To return to the Inventory list, click Return to Inventory listfrom the Action list, select Return to Inventory list.

Disabling Data Collection on the Virtual Servers

When data collection is disabled for a virtual server, the NetScaler appliance stops sending AppFlow records for the traffic generated by that virtual server. If you want to disable data collection on specific virtual servers, select the NetScaler device on which the virtual server is hosted from the **Inventory** list.

To disable data collection on a virtual server:

1. On the AppFlow setup screen, from the Applications List , select the virtual server or virtual servers for which you want to disable data collection.
2. Click Disable AppFlow.
3. In the confirmation message, click **Yes**. The **Insight** column for the virtual server displays **DISABLED.**
4. To return to the Inventory list, click Return to Inventory list.

Editing the Expression for Generating Traffic

After you have enabled data collection on a virtual server, you can edit the expression which specifies which data to collect. You can also create a new expression. Select the virtual server for which you want to edit the expression, and then click Edit AppFlow expression. The Edit AppFlow Expression dialog box appears displaying the current expression.

1. Select a new expression from the list, or edit the existing expression.
2. Click OK to save the changes. To exit without changing the expression, click Cancel.

   Note: If data-collection has been recently enabled by another instance of NetScaler Insight, the expressions defined in that instance take priority.

Managing NetScaler Appliances

The Configuration tab provides the interface through which you can add or delete NetScaler appliances from which to collect AppFlow information, enable AppFlow data collection on the virtual servers managed by the appliances in the Inventory list, view the properties of managed appliances, and perform other management tasks.

In addition to adding and deleting NetScaler appliances, you can update NetScaler login credentials, that have changed.

Adding NetScaler Appliances to Inventory

After you add the first NetScaler appliance to be monitored by NetScaler Insight, you can add additional appliances.

Note: Before adding the appliance, make sure that it is:

- An nCore appliance running version 9.3 or later
- Not a standalone NetScaler Gateway appliance
- In the UP state

To add a NetScaler appliance to the Inventory

1. On the Configuration tab, in the navigation pane, select Inventory, and then Click Add.
2. On the NetScaler Insight Inventory Setup screen, enter the IP address, user name, and password for the appliance that you want to add to the Inventory list.

   Note: If the NetScaler appliance uses it's Subnet IP address (SNIP) as the source IP for management access, specify the SNIP address as the IP address of the appliance.
3. Click Add to save the changes, or click Cancel, to return to the Inventory list without adding the appliance. If the appliance is added, information about the appliance appears in the Inventory list.

Viewing properties of a NetScaler Appliance

To view the properties of an appliance in the Inventory list, click the show/hide details button (a small triangle) to the left of the appliance's IP address.

The following information appears:

Netmask

Subnet mask for the appliance’s IP address.

Gateway

IP address of the default gateway, which is the router that forwards traffic out of the subnet in which the appliance resides.

Up Since

Date and time since the appliance has been continuously in the UP state.

Version

Release number, build date, and time, of the NetScaler software currently running on the appliance.

Host Name

Host name of the appliance.

Peer IP address

IP address of the appliance's peer in a high availability setup.

HA Master State

State of the device, indicating whether it is in a standalone or a high availability (HA) setup. In an HA setup, the state also indicates whether the appliance is the primary or the secondary node.

HA Sync Status

Status of HA synchronization (enabled or disabled).

Description

Description entered while provisioning the appliance.

Status

Status of the operations being performed on the appliance, such as whether an inventory of the instance is completed or whether a reboot is in progress.

Updating Login Credentials of NetScaler Appliances

If the login credentials of a NetScaler appliance change, NetScaler Insight cannot connect to the appliance. To indicate this condition, the **State** column in the Inventory list turns yellow or red. Though there can be many reasons for the state change, a change in the login credentials is one of them. You have to manually acquire information about the change from the NetScaler administrator. You can then update the credentials in the NetScaler Insight configuration utility.

To update login credentials for the NetScaler appliance

1. On the Configuration tab, in the navigation pane, select Inventory.
2. Select the appliance by clicking to the right of its IP address.
3. Click Update Login Credentials.
4. On the NetScaler Insight Inventory Setup screen, enter the new credentials for logging in to the appliance.
5. Click Change to save the changes or, to return to the inventory list without updating the login credentials, click Cancel.

Deleting a NetScaler Appliance from the Inventory List

You can delete a single NetScaler appliance or multiple appliances from the Inventory list.

Note: If you delete the entire list, the Welcome Screen appears the next time you login. To access the Inventory list, click Get Started and add an appliance.

To delete a NetScaler instance from the Inventory

1. In the Inventory list, select the row that lists the NetScaler to be deleted. (Do not click the IP address. Click the space to the right of the address.) Or, you can select multiple rows (Press **Ctrl** and select multiple rows).

2. Click Delete in the task pane.

3. At the confirmation prompt, click Yes.

Viewing the Reports

When you enable data-collection on the virtual servers of the appliances in the Inventory list, NetScaler Insight starts collecting traffic data from those virtual servers. It analyzes the collected data and presents it as charts and tables. On the Dashboard tab, you can compare the performance of the applications managed by the appliances. You can get an insight to all the components that affect the application performance. The charts and tables also help you identify the reasons for fault or slow performance.

When you enable data collection, NetScaler Insight starts collecting traffic data, analyzes the collected data and presents it as charts and tables in the NetScaler Insight Dashboard.

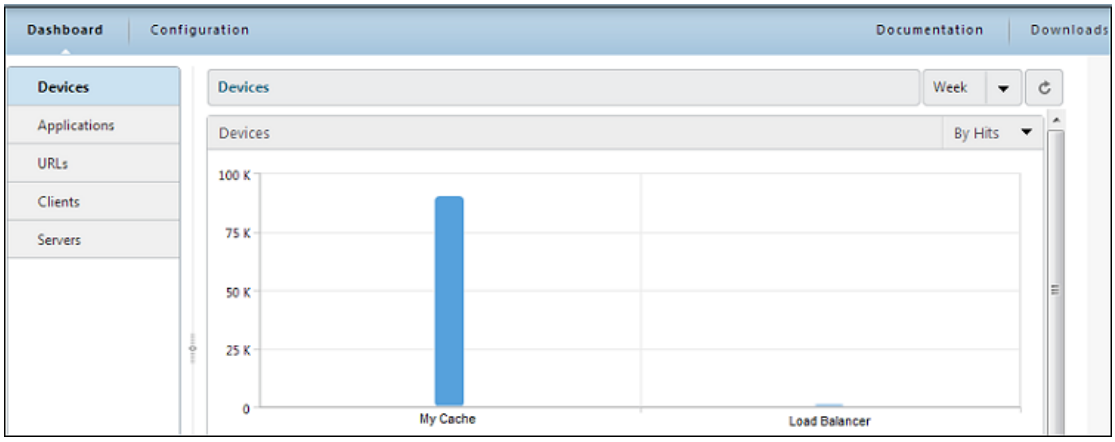
Note: To view the list of reports generated by NetScaler Insightfor NetScaler appliances with different licenses, see Licensing Information.

Overview of Dashboard

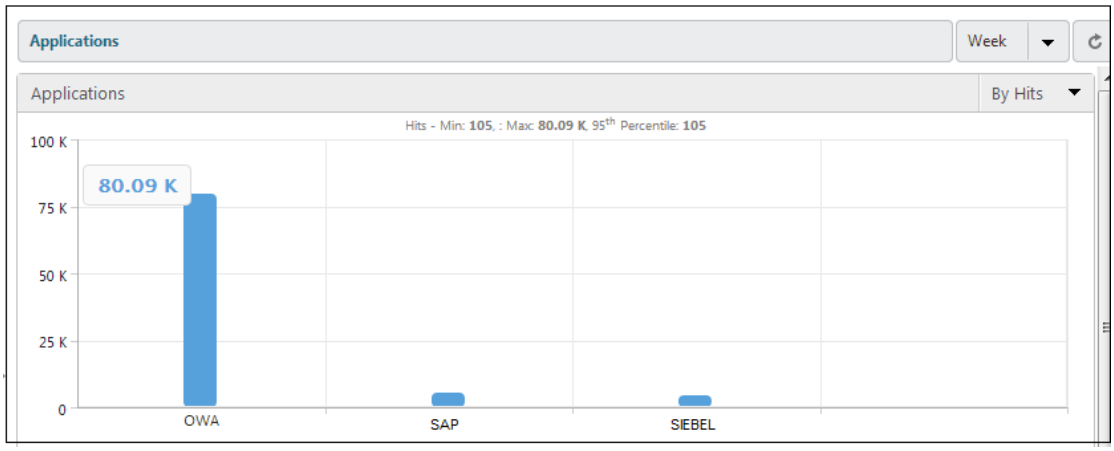
The left pane of the Dashboard displays Devices, Applications, URL, Client, and Servers, tabs, each of which provides a different type of report. For example you can select Applications to display a performance chart for applications managed by all the appliances in the Inventory list. two nodes: Web Insight and HDX Insight, which contain the nodes for displaying the Web Insight and HDX Insight reports respectively.

The right pane of the Dashboard displays the reports as charts and tables. The collected data is aggregated every 5 minutes and every 1 hour, 1 day, 1 week, and 1 month. You can view the performance information for a selected time-slot. The performance of the application over a week, based on the number of hits is displayed as shown in the following illustration.

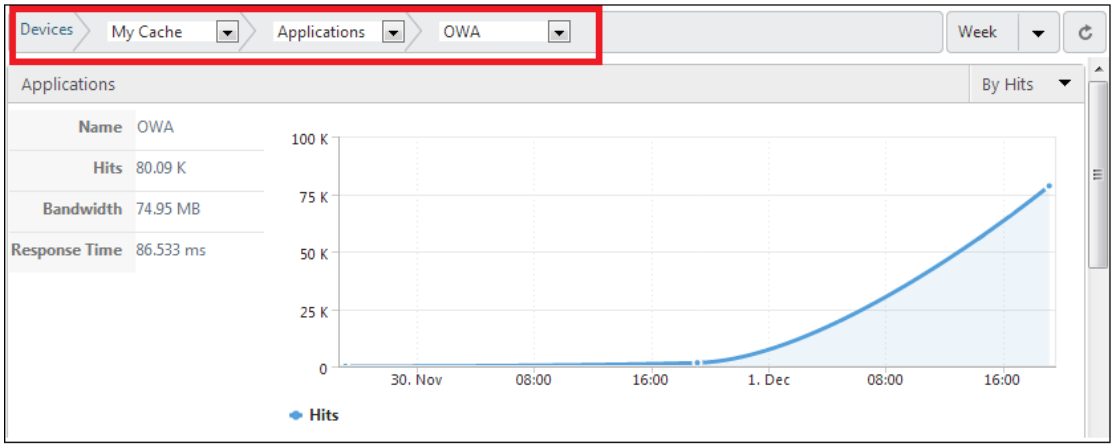
Figure 1. Application Performance-By Hits



By default, the dashboard displays a performance chart for the NetScaler appliances based on the number of hits. To view more details of the appliance performance, click on the host name of the appliance, or click on the chart. All the components that affect the performance of the device are displayed as charts.

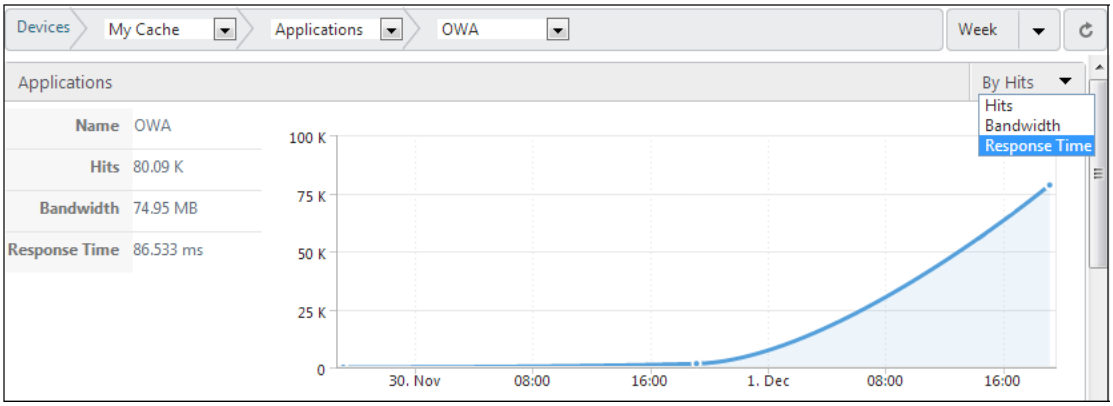


If you hover your mouse over any chart that is displayed, the maximum, minimum and the percentile value of the selected metrics is populated on the top of the chart. Figure 2. Report - Mouseover



The Dashboard provides bread-crumb navigation; the users can know their path of navigation. For example, if the user starts with Device level information, and then views the performance of applications managed by that device, and then the Client details, the user can at any time know for which application and device the client information is being accessed. Figure 3. Bread-crumb navigation

Performance Metrics



The following table lists the various reports you can generate, by choosing the performance metrics, to view the performance of the applications. You can choose the performance metrics from the list displayed in the right corner of every chart. Figure 4. Performance Metrics

Table 1. Performance Metrics

	Performance Metrics
Device	Hits, Bandwidth
Applications	Hits, Bandwidth, Response Time
URLs	Hits, Load Time, Render Time
Clients	Requests, Client Network Latency, Render Time
Servers	Hits, Bandwidth, Server Processing Time, Server Network Latency

In addition to this, NetScaler Insight application collects information of the following components in the web-traffic, and displays them as charts:

- HTTP Request Methods
- HTTP Response Status
- Operating System
- User Agents
- Waterfall Chart

Note: The performance metrics are displayed based on the license of the NetScaler appliance you are monitoring. For standard and enterprise licenses, certain performance metrics is not generated by the NetScaler Insight application. For NetScaler appliances running version 10.0 with platinum license, all the performance metrics are displayed.

Terminologies used in the Reports

- Response Time - Elapsed time, between the end of an enquiry and the beginning of a response from the application.
- Load Time - Elapsed time, from when the browser starts to receive the first byte of a response until the user starts to interact with the page. At this stage, some of the page content might not yet have been loaded.
- Render Time - Elapsed time, from when the browser starts to receive the first byte of a response until either all page content has been rendered or the page load action has timed out.
- Server Processing Time - Elapsed time, from when the server starts to receive the first byte of a request from the NetScaler appliance until the NetScaler appliance receives the first byte to response.

Managing the NetScaler Insight Virtual Appliance

The Configuration tab provides the interface through which you can manage the NetScaler Insight virtual appliance. You can perform the following management activities by using the options on the Configuration tab:

- Install and manage SSL files.
- Manage users and sessions.
- Upgrade, or reboot NetScaler Insight
- Manage the documentation and software key files.
- Configure clock synchronization.

Installing an SSL Certificate on the NetScaler Insight Virtual Appliance

Before installing an SSL certificate, you must upload it to NetScaler Insight and then install the certificate. See Uploading SSL files for instructions on uploading the SSL files to NetScaler Insight. Installing an SSL certificate terminates all current client sessions with the NetScaler Insight, so you have to log back for any additional configuration tasks.

To install an SSL certificate on NetScaler Insight

1. On the Configuration tab, in the navigation pane, click System.
2. In the System pane, in **Setup NetScaler Insight,** click Install SSL Certificate.
3. In the Install SSL Certificate dialog box, set the following parameters:
   - Certificate File*—The file name of a valid certificate. The certificate file must be present on the NetScaler Insight virtual appliance.
   - Key File—The file name of the private-key used to create the certificate. The key file must be present on the NetScaler Insight virtual appliance.
   - Password—The pass-phrase that was used to encrypt the private-key. This option can be used to load encrypted private-keys. Max length: 32.

     Note: Password protected private key is supported only for the PEM format.

   * A required parameter
4. Click OK, and then click Close.

Uploading SSL files to the NetScaler Insight Virtual Appliance

For any SSL transaction, the server needs a valid certificate and the corresponding private and public key pair. The certificate file must be present on the NetScaler Insight virtual appliance when you install the SSL certificate on NetScaler Insight. You can also download the SSL Certificate and key files to a local computer as a backup.

To upload SSL certificate files to

1. On the Configuration tab, expand NetScaler Insight Center, and then click SSL Certificate Files.
2. In the SSL Certificates pane, click Upload.
3. In the Upload SSL Certificate dialog box, click Choose File and select the certificate file that you want to upload.
4. Click Upload. The certificate file appears in the SSL Certificates pane.

To create a backup for an SSL certificate file

1. On the SSL Certificates pane, select the file that you want to download, and then click Download.
2. In the message box, from the Save list, select Save as.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

To upload SSL key files to NetScaler Insight

1. In the Configuration tab, expand NetScaler Insight Center , and then click SSL Certificate Files.
2. In the SSL Certificate pane, on the SSL Keys tab, click Upload.
3. In the Upload SSL Key File dialog box, click Browse and select the key file that you want to upload.
4. Click Upload to upload the key file to the NetScaler Insight application. The key file appears in the SSL Keys pane.

To create a backup for an SSL key file

1. In the SSL Certificate pane, on the SSL Keys tab, select the file that you want to download, and then clickDownload.

2. In the message box, from the Save list, select Save as.

3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

Viewing SSL Certificate details

The NetScaler Insight virtual appliance uses an SSL certificate for secure client connections. After installing the certificate, you can view details such as certificate's validity status, issuer, subject, days to expiration, valid from and to dates, version, and serial number.

To view the SSL certificate on NetScaler Insight

1. In the navigation pane, click System.
2. In the System pane, under Setup NetScaler Insight, click View SSL Certificate. The certificate details appear.

Upgrading the NetScaler Insight Virtual Appliance to a Later Version

For upgrading the NetScaler Insight build, you must first upload the latest software image and documentation files to the NetScaler Insight application. Refer to Uploading the NetScaler InSight Build and Documentation Files for instruction on uploading the build files. You can use this image to upgrade the version of the NetScaler Insight.

To upgrade NetScaler Insight

1. In the navigation pane, click System.
2. In the System pane, under System Administration, click Upgrade NetScaler InSight.
3. In the Upgrade NetScaler InSight dialog box, in Software Image, select the file of the build to which you want to upgradeNetScaler Insight.
4. In Documentation File, select the documentation file that you want to use for the upgrade.
5. Click OK.

Uploading the NetScaler Insight Build and Documentation Files

You can upload the NetScaler Insight build and documentation files from a client computer to theNetScaler Insight virtual appliance. You can also download the build and documentation files to a local computer as a backup.

To upload the NetScaler Insight build file

1. In the Configuration tab, expand NetScaler Insight, and then click Software Images.
2. In the Software Images pane, click Upload.
3. In the Upload NetScaler Insight Software Image dialog box, click Browse, navigate to the folder that contains the build file, and then double-click the build file.
4. Click Upload.

To create a backup for the NetScaler Insight build file

1. In the Software Images pane, select the file you want to download, and then click Download.
2. In the message box, from the Save list, select Save as.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

To upload the NetScaler Insight documentation file

1. In the Configuration tab, expand NetScaler Insight, and then click Software Images.
2. In the Software Images pane, on the Documentation Files tab, click Upload.
3. In the Upload NetScaler Insight Documentation File Upload NetScaler Insight Center Documentation File dialog box, click Browse, navigate to the folder that contains the documentation file, and then double-click the file.
4. Click Upload.

To create a backup for the NetScaler Insight documentation file

1. In the Software Images pane, select the file you want to download, click Download.
2. In the message box, from the Save list, select Save as.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

Configuring Clock Synchronization

You can configure your NetScaler Insight virtual appliance to synchronize its local clock with a Network Time Protocol (NTP) server. NetScaler Insight has the same date and time settings as the other servers on your network. The clock synchronization configuration does not change if the appliance is restarted, upgraded, or downgraded.

The clock is synchronized immediately if you add a new NTP server or change any of the authentication parameters. You can also explicitly enable and disable NTP synchronization.

Note: If you do not have a local NTP server, you can find a list of public, open access, NTP servers at the official NTP site, http://www.ntp.org. Before configuring your NetScaler to use a public NTP server, be sure to read the Rules of Engagement page (link included on all Public Time Servers pages).

To configure an NTP server

1. In the navigation pane, expand System, and then click NTP Servers.
2. In the details pane, do one of the following:
   - To add a new NTP server, click Add.
   - To modify settings for an existing NTP server, select the NTP server, and then click Open.
3. In the Add NTP Server or Configure NTP Server dialog box, set the following parameters:
   - Server Name/IP Address*—The domain name of the NTP server or the IP address of the NTP server. The name or IP address cannot be changed for an existing NTP server.
   - Minimum Poll Interval—The minimum number of seconds after which the NTP server must poll the NTP messages, expressed as a power of 2. Minimum value: 4 (2^4=16 seconds). Maximum value: 6 (2^6=64 seconds). Default: 6 (2^6=64 seconds).
   - Maximum Poll Interval—The maximum number of seconds after which the NTP server must poll the NTP messages, expressed as a power of 2. Minimum value: 10 (2^10=1024 seconds). Maximum value: 17 (2^17=36 hours). Default : 10 (2^10=1024 seconds).
   - Key Identifier—The key to be used for the specified server. This key identifier should be added to the list of Trusted Key IDs in the authentication parameters. Minimum value: 1. Maximum value: 65534.

     Note: Do not add if Autokey is selected.
   - Autokey—Use the Autokey protocol for the specified server.
   - Preferred—Synchronize with this server first. Applicable if more than one server is configured.

   *A required parameter
4. Click Add, and then click Close.
5. In the details pane, verify that the settings displayed for the NTP server that you just created are correct.

To enable NTP synchronization

1. In the navigation pane, expand System, and then click NTP Servers.
2. In the details pane, click NTP Synchronization.
3. In the NTP Synchronization dialog box, select Enable NTP Sync.
4. Click OK.

To modify Authentication options

1. In the navigation pane, expand System, and then click NTP Servers.
2. In the details pane, click Authentication Parameters.
3. In the Modify Authentication Options dialog box, set the following parameters:
   - Authentication—Enable NTP authentication. Possible values: YES, NO. Default: YES.
   - Trusted Key IDs—The trusted key IDs. While adding an NTP server, you select a key identifier from this list. Minimum value: 1. Maximum value: 65534.
   - Revoke Interval—The interval between re-randomization of certain cryptographic values used by the Autokey scheme, as a power of 2, in seconds. Default value: 17 (2^17=36 hours).
   - Automax Interval—The interval between regeneration of the session key list used with the Autokey protocol, as a power of 2, in seconds. Default value: 12 (2^12=1.1 hours).
4. Click OK.

Modifying the Time Zone of the NetScaler Insight Virtual Appliance

You can modify the time zone used by the NetScaler Insight virtual appliance's clock. The default time zone is UTC.

To modify the time zone

1. On the Configuration tab, in the navigation pane, click System.
2. In the System pane, under System Settings, click Change Time Zone.
3. In the Modify Time Zone dialog box, select a time zone from the list, and then click OK.

Modifying the Network Configuration of the NetScaler Insight Virtual Appliance

You can modify the network configuration details that you provided for the NetScaler Insight appliance during initial configuration.

To modify the network configuration of NetScaler Insight

1. On the Configuration tab, in the navigation pane, click System.
2. In the System pane, under Setup NetScaler Insight, click Network Configuration.
3. In the Modify Network Configuration dialog box, set the following parameters:
   - NetScaler Insight IP Address*—The IP address of the NetScaler Insight.
   - Netmask*—The subnet mask for the subnet in which the NetScaler Insight is located.
   - Gateway*—The default gateway for the network.

   * A required parameter
4. Click OK.

Configuring User Accounts

To allow a user to access NetScaler Insight virtual appliance, you must create a user account on NetScaler Insight for that user. Users are authenticated locally, on the virtual appliance.

To configure a user account

1. On the Configuration tab, in the navigation pane, expand System, and then click Users. The Users pane displays a list of existing user accounts, with their permissions.

2. In the Users pane, do one of the following:

   - To create a user account, click Add.

   - To modify a user account, select the user, and then click Modify.

3. In the Create System User or Modify System User dialog box, set the following parameters:

   - Name*—The user name of the account. The following characters are allowed in the name: letters a through z and A through Z, numbers 0 through 9, period (.), space ( ), and underscore (_). Maximum length: 128. You cannot change the name after the account is created.

   - Password*—The password for logging on to the NetScaler Insight virtual appliance.

   - Confirm Password*—The password.

   - Permission*—The user's privileges on the appliance. Possible values:

     - Superuser—The user can perform all administration tasks related to the NetScaler Insight.

     - Readonly—The user can only monitor the system and change the password of the account.

     Default: superuser.

   *A required parameter

4. Click Create or OK, and then click Close. The user account that you created is listed in the details pane.

Modifying System Security Settings

For security reasons, you can specify that all communication between NetScaler Insight and the NetScaler appliance must be over a secure channel. You can also specify HTTPS-only access to NetScaler Insight user interface.

To modify system settings

1. On the Configuration tab, in the navigation pane, click System.
2. In the System pane, under System Settings, click Change System Settings.
3. In the Modify System Settings NetScaler Insight Center to NetScaler Communication*dialog box, select **https** from the list.
4. To specify secure-only access to NetScaler Insight, select Secure Access only.
5. Click OK.

Managing Client Sessions

A client session is created when a user logs on to the NetScaler Insight virtual appliance. You can view all the client sessions on the appliance in the Sessions pane.

To view client sessions, on the Configuration tab, in the navigation pane, expand System, and then click Sessions.

In the Sessions pane, you can view the following details:

User Name

The user account that is being used for the session.

IP Address

The IP address of the client from which the session has been created.

Port

The port being used for the session.

Login Time

The time at which the current session was created on NetScaler Insight.

Last Activity Time

The time at which user activity was last detected in the session.

Session Expires In

Time left for session expiry.

To end a client session, in the Sessions pane, click the session that you want to remove, and then click End Session.

Note: You cannot end a session from the client that initiated that session.

Rebooting the NetScaler Insight Virtual Appliance

You can restart NetScaler Insight from the System pane. Restarting does not affect the working of the NetScaler appliances monitored by NetScaler Insight. The NetScaler instances continue to function during the Restart process.

To restart NetScaler Insight

1. On the Configuration tab, in the navigation pane, click System.
2. In the System pane, under System Administration, click Reboot NetScaler Insight.Reboot NetScaler Insight Center.
3. At the confirmation prompt, Click Yes.

Monitoring the NetScaler Insight Virtual Appliance

You can use audit and task logs to monitor the operations performed on the NetScaler Insight virtual appliance and on the NetScaler instances.

Viewing Audit Logs

All operations performed in the NetScaler Insight virtual appliance are logged in the XenServer database. In the audit logs, you can view the operations the user has performed, the date and time of each operation, and the success or failure status of the operation. You can also sort the details by user, operation, audit time, status, and so on by clicking the appropriate column heading.

Pagination is supported in the Audit Log pane. Select the number of records to display on a page. By default, a page displays 25 records.

To view audit logs

1. In the navigation pane, expand System, and then click Audit.
2. In the Audit Log pane, you can view the following details:

   User Name

   The NetScaler Insight user who performed the operation.

   IP Address

   IP address of the system on which the operation was performed.

   Port

   Port at which the system was sending and receiving data when the operation was performed.

   Resource Type

   Type of resource used to perform the operation.

   Resource Name

   Name of the resource used to perform the operation, and the user name used to log in.

   Audit Time

   Time when the audit log was generated.

   Operation

   Task that was performed, such as add, delete, or log out.

   Status

   Status of the audit, such as Success or Failed.

   Message

   Message describing the cause of failure, if the operation failed, and the status of the task, such as Done, if the operation was successful.
3. To sort the logs by a particular field, click the heading of the column.

Viewing Task Logs

Use task logs to view and track tasks, such as upgrading instances and installing SSL certificates, that are executed by NetScaler Insight on the NetScaler appliances. The task log shows whether a task is in progress or has failed or succeeded.

Pagination is supported in the Task Log pane. Select the number of records to display on a page. By default, the page displays 25 records.

To view the task log

1. On the Configuration tab, expand Diagnostics, and then click Task Log.
2. In the Task Log pane, you can view the following details.

   ID

   Auto-generated ID assigned to a task. For a task performed on multiple instances, such as installing an SSL certificate or upgrading instances, a single unique ID is generated in the task log.

   Name

   Name of the task that is being executed or has already been executed.

   Status

   Status of the task, such as In progress, Completed, or Failed.

   Executed By

   NetScaler Insight user who performed the operation.

   Start Time

   Time at which the task started.

   End Time

   Time at which the task ended.
3. To sort the logs by a particular field, click the heading of the column.

Viewing Task Device Logs

Use task device logs to view and track tasks being performed on each NetScaler appliance. The task device log shows whether a task is in progress or has failed or succeeded. It also displays the IP address of the applaince on which the task is performed.

To view the task device log

1. On the Configuration tab, expand Diagnostics, and then click Task Log.
2. In the Task Log pane, double-click the task to view the task device details.
3. In the Task Device Log pane, to sort the logs by a particular field, click the heading of the column.

Viewing Task Command Logs

Use task command logs to view the status of each command of a task executed on a NetScaler appliance. The task command log shows the commands that were attempted. It also shows which commands succeeded, which failed, and the reasons for the failures.

To view the task command log

1. On the Configuration tab, expand Diagnostics, and then click Task Log.
2. In the Task Log pane, double-click the task to view the task device details.
3. In the Task Device Log pane, double-click the task to view the task command details.
4. In the Task Command Log pane, to sort the logs by a particular field, click the heading of the column.

Generating a Tar Archive for Technical Support

You can use the Technical Support option to generate a tar archive of data and statistics for submission to Citrix technical support. After generating the file, you can download it to your local system and send it to Citrix technical support.

To generate the tar archive for technical support

1. On the Configuration tab, in the left pane, expand Diagnostics, and then click Technical Support.
2. In the Technical Support pane, click Generate Technical Support File.
3. In the Generate Technical Support File dialog box, in Mode, select NetScaler Insight .
4. Click OK.

To download the tar archive for technical support

1. In the Technical Support pane, select the technical support file that you want to download, click Download.
2. In the File Download message box, click Save.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

NITRO API

With the NetScaler Insight NITRO protocol, you can configure and monitor the NetScaler Insight Center virtual appliance programmatically.

NITRO exposes its functionality through Representational State Transfer (REST) interfaces. Therefore, NITRO applications can be developed in any programming language. Additionally, for applications that must be developed in Java or .NET, NITRO APIs are exposed through Java and .NET libraries that are packaged as separate Software Development Kits (SDKs).

Note: You must have a basic understanding of NetScaler Insight before using the NITRO protocol.

To use the NITRO protocol, the client application needs only the following:

- Access to a NetScaler Insight virtual appliance.
- To use REST interfaces, you must have a system that can generate HTTP or HTTPS requests (payload in JSON format) to the NetScaler Insight virtual appliance. You can use any programming language or tool.
- For Java clients, you must have a system on which Java Development Kit (JDK) 1.5 or later is available. The JDK can be downloaded from http://www.oracle.com/technetwork/java/javase/downloads/index.html.
- For .NET clients, you must have a system on which .NET framework 3.5 or later installed. The .NET framework can be downloaded from http://www.microsoft.com/downloads/en/default.aspx.

Obtaining the NITRO Package

The NITRO package is available as a tar file on the Downloads page of the NetScaler Insight Center virtual appliance's configuration utility. You must download and un-tar the file to a folder on your local system. This folder is referred to as <NITRO_SDK_HOME> in this documentation.

The folder contains the NITRO libraries (JARs for Java and DLLs for .NET) in the lib subfolder. The libraries must be added to the client application classpath to access NITRO functionality. The <NITRO_SDK_HOME> folder also provides samples and documentation that can help you understand the NITRO SDK.

Note: The REST package contains only documentation for using the REST interfaces.

How NITRO Works

The NITRO infrastructure consists of a client application and the NITRO Web service, which runs on a NetScaler Insight virtual appliance. The communication between the client application and the NITRO web service is based on REST architecture and uses HTTP or HTTPS.

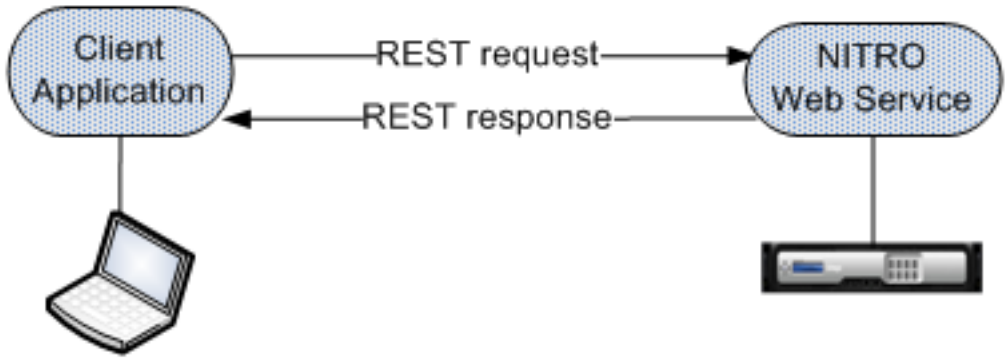


Figure 1. NITRO execution flow

As shown in the above figure, a NITRO request is executed as follows:

1. The client application sends a REST request message to the NITRO web service. With a Java or .NET SDK, an API call is translated into the appropriate REST request message.

2. The web service processes the REST request message.

3. The NITRO web service returns the corresponding REST response message to the client application. For a client using a Java or .NET SDK, the REST response message is translated into the appropriate response for the API call.

To minimize network traffic, you retrieve the whole state of a resource from the server, modify the state of the resource locally, and then upload it back to the server in one network transaction.

Note: Local operations on a resource (changing its properties) do not affect its state on the server until the state of the object is explicitly uploaded.

NITRO APIs are synchronous in nature. The client application waits for a response from the NITRO web service before executing another NITRO API.

Java SDK

You can use NetScaler Insight NITRO APIs to programmatically register a NetScaler appliance with the NetScaler Insight virtual appliance, gather performance data, and generate a report on this data. You can also troubleshoot NITRO operations by using the nitro_exception class.

Logging on to the NetScaler Insight Appliance

The first step toward using NITRO is to establish a session with the NetScaler Insight virtual appliance and then authenticate the session by using the administrator's credentials.

On the client system, create an object of the com.citrix.insight.nitro.service.nitro_service class by specifying the IP address of the NetScaler Insight Center virtual appliance and the protocol for connecting to the virtual appliance (HTTP or HTTPS). You then use this object to log on to the appliance.

Note: You cannot log on to a NetScaler Insight virtual appliance unless you have a user account on the virtual appliance. The configuration operations that you perform are limited by the administrative roles assigned to your account.

The following sample code establishes an HTTPs session with a NetScaler Insight virtual appliance with IP address 10.102.126.213:

```
//Specify the NetScaler Insight appliance IP address and protocol
nitro_service ns_insight_session = new nitro_service("10.102.126.213","https");

//Specify the login credentials
ns_insight_session.login("admin","verysecret");
```

Note: You must use the nitro_service object in all further NITRO operations on the appliance.

Note: By default, the connection to the appliance expires after 30 minutes of inactivity. You can modify the timeout period by specifying a new timeout period (in seconds) in the `login` method. For example, to modify the timeout period to 60 minutes:

```
ns_insight_session.login("admin","verysecret",3600);
```

Registering a NetScaler Appliance

The com.citrix.insight.nitro.resource.config.mps.managed_device class provides APIs to register a NetScaler appliance with the NetScaler Insight Center virtual appliance. You must specify the NetScaler IP (NSIP) address, the user name, and the password of the NetScaler appliance.

The following sample code registers a NetScaler appliance with IP address 10.102.29.60:

```
managed_device obj = new managed_device();

obj.set_ip_address("10.102.29.60");
obj.set_profile_username("admin");
obj.set_profile_password("verysecret");
obj.set_type("ns");

managed_device managed_device_result = managed_device.add(ns_insight_session, obj);
```

Updating a NetScaler Appliance's Login Credentials

If the login credentials of a NetScaler appliance are updated after it is registered to a NetScaler Insight virtual appliance, they have to be updated on the virtual appliance.

The following sample code updates the credentials of a NetScaler appliance:

```
managed_device device[] = managed_device.get(ns_insight_session);
device_profile result[] = device_profile.get_filtered(ns_insight_session,"name:"+ device[1].get_profile_name
device_profile obj = result[0];
obj.set_username("admin");
obj.set_password("newverysecretpassword");
device_profile.update(ns_insight_session, obj);
```

Gathering Performance Data about an Application

To gather performance data from applications (virtual servers) available on NetScaler appliances that are registered with the NetScaler Insight appliance, you must:

1. Identify the application (virtual server) from which you want to collect information.
2. Specify the expression on which the virtual server information must be filtered.
3. Enable AppFlow on that application.

The appliance starts gathering performance data for the application. To display the performance data, see Generating Performance Reports.

The following sample code gets the list of all the available load balancing virtual servers that are available on the NetScaler appliance 10.102.29.60 and enables appflow on a load balancing virtual server named http_test:

```
// Get the list of all load balancing virtual servers
String filter = "ns_ip_address:10.102.20.60,type:lb";
ns_vserver_appflow_config result[] = ns_vserver_appflow_config.get_filtered(client, filter);
for (int i = 0; i < result.length; i++)
{
   System.out.println("Name: " + result[i].get_name() + ", IP Address: " + result[i].get_ip_address() + ", Type:
}

// Enable appflow on one of the virtual servers
ns_vserver_appflow_config new_obj = new ns_vserver_appflow_config();
new_obj.set_ns_ip_address("10.102.29.60");
new_obj.set_type("lb");

//Virtual server whose performance data must be gathered
new_obj.set_name("http_test");
new_obj.set_servicetype("http");

// Policy rule
new_obj.set_appflow_policy_rule("true");

// Enable appflow data collection log
new_obj.set_appflowlog("enabled");

// Enable client side data collection log
new_obj.set_es4nslog("enabled");

ns_vserver_appflow_config ns_vserver_appflow_config_result = ns_vserver_appflow_config.add(client, new_
```

Note: To stop gathering data, disable AppFlow on the application.

Generating Performance Reports

The com.citrix.insight.nitro.resource.config.af.device class provides the APIs to generate and view reports about applications. You must retrieve the details of the application and specify the period for which you want the details.

The following sample code generates a report for a load balancing virtual server named `http_test`:

```
device device_obj = new device();

options option_obj =  new options();
option.set_duration("last_1_month");
option.set_pageno(1);
option.set_pagesize(25);
option.set_args("app_unit_name:http_test");

device.get_with_options(ns_insight_session, option);

for (int i = 0; i < result.length; i++)
{
   System.out.println("Application: " + result[i].get_name() + ", Total requests: " + result[i].get_total_reques
}
```

Exception Handling

The status of a NITRO request is captured in the com.citrix.insight.nitro.exception.nitro_exception class. This class provides the following details about the exception:

- **Session ID.** The session in which the exception occurred.
- **Error code.** The status of the NITRO request. An error code of 0 indicates that the NITRO request is successful. A non-zero error code indicates an error in processing the NITRO request.
- **Error message.** A brief description of the exception.

Note: For a list of error codes, see the errorlisting.html file available in the <NITRO_SDK_HOME>/doc/api_reference folder.

.NET SDK

You can use NetScaler Insight NITRO APIs to programmatically register a NetScaler appliance with the NetScaler Insight virtual appliance, gather performance data, and generate a report on this data. You can also troubleshoot NITRO operations by using the nitro_exception class.

Logging on to the NetScaler Insight Appliance

The first step toward using NITRO is to establish a session with the NetScaler Insight virtual appliance and then authenticate the session by using the administrator's credentials.

On the client system, create an object of the com.citrix.insight.nitro.service.nitro_service class by specifying the IP address of the NetScaler Insight Center virtual appliance and the protocol for connecting to the virtual appliance (HTTP or HTTPS). You then use this object to log on to the appliance.

Note: You cannot log on to a NetScaler Insight virtual appliance unless you have a user account on the virtual appliance. The configuration operations that you perform are limited by the administrative roles assigned to your account.

The following sample code establishes an HTTPs session with a NetScaler Insight virtual appliance with IP address 10.102.126.213:

```
//Specify the NetScaler Insight appliance IP address and protocol
nitro_service ns_insight_session = new nitro_service("10.102.126.213","https");

//Specify the login credentials
ns_insight_session.login("admin","verysecret");
```

Note: You must use the nitro_service object in all further NITRO operations on the appliance.

Note: By default, the connection to the appliance expires after 30 minutes of inactivity. You can modify the timeout period by specifying a new timeout period (in seconds) in the `login` method. For example, to modify the timeout period to 60 minutes:

```
ns_insight_session.login("admin","verysecret",3600);
```

Registering a NetScaler Appliance

The com.citrix.insight.nitro.resource.config.mps.managed_device class provides APIs to register a NetScaler appliance with the NetScaler Insight appliance. You must specify the NetScaler IP (NSIP) address, the user name, and the password of the NetScaler appliance.

The following sample code registers a NetScaler appliance with IP address 10.102.29.60:

```
managed_device obj = new managed_device();

obj.ip_address = "10.102.29.60";
obj.profile_username = "admin";
obj.profile_password = "verysecret";
obj.type = "ns";

managed_device managed_device_result = managed_device.add(ns_insight_session, obj);
```

Updating NetScaler Appliance's Logon Credentials

If the login credentials of a NetScaler appliance are updated after it is registered to a NetScaler Insight appliance, they have to be updated in the Insight appliance.

The following sample code updates the credentials of a NetScaler appliance:

```
managed_device device[] = managed_device.get(ns_insight_session);
device_profile result[] = device_profile.get_filtered(ns_insight_session,"name:"+ device[1].profile_name);
device_profile obj = result[0];
obj.username = "admin";
obj.password = "newverysecretpassword";
device_profile.update(ns_insight_session, obj);
```

Gathering Performance Data about an Application

To gather performance data from applications (virtual servers) available on NetScaler appliances that are registered with the NetScaler Insight appliance, you must:

1. Identify the application (virtual server) from which you want to collect information.
2. Specify the expression with which to filter the virtual server information.
3. Enable AppFlow on the virtual server.

The appliance starts gathering performance data about the application. To display the performance data, see Generating Performance Reports.

The following sample code gets the list of all the available load balancing virtual servers that are available on the NetScaler appliance 10.102.29.60 and enables appflow on a load balancing virtual server named http_test:

```
// Get the list of all load balancing virtual servers
String filter = "ns_ip_address:10.102.20.60,type:lb";
ns_vserver_appflow_config result[] = ns_vserver_appflow_config.get_filtered(client, filter);
for (int i = 0; i < result.length; i++)
{
   Console.WriteLine("Name: " + result[i].name + ", IP Address: " + result[i].ip_address + ", Type: " + result[i]
}

// Enable appflow on one of the virtual servers
ns_vserver_appflow_config new_obj = new ns_vserver_appflow_config();
new_obj.ns_ip_address = "10.102.29.60";
new_obj.type = "lb";

//Virtual server whose performance data must be gathered
new_obj.name = "http_test";
new_obj.servicetype = "http";

// Policy rule
new_obj.appflow_policy_rule = "true";

// Enable appflow data collection log
new_obj.appflowlog = "enabled";

// Enable client side data collection log
new_obj.es4nslog = "enabled";

ns_vserver_appflow_config ns_vserver_appflow_config_result = ns_vserver_appflow_config.add(client, new_
```

Note: To stop gathering data, disable AppFlow on the application.

Generating Performance Reports

The com.citrix.insight.nitro.resource.config.af.device class provides the APIs to generate and view reports of applications. You must retrieve the details and specify the period for which you want the details.

The following sample code generates a report for a load balancing virtual server named `http_test`:

```
device device_obj = new device();

options option_obj =  new options();
option.duration = "last_1_month";
option.pageno = 1;
option.pagesize = 25;
option.args = "app_unit_name:http_test";

device.get_with_options(ns_insight_session, option);

for (int i = 0; i < result.length; i++)
{
   Console.WriteLine("Application: " + result[i].name + ", Total requests: " + result[i].total_requests + ", Tota
}
```

Exception Handling

The status of a NITRO request is captured in the com.citrix.insight.nitro.exception.nitro_exception class. This class provides the following details about the exception:

- **Session ID.** The session in which the exception occurred.
- **Error code.** The status of the NITRO request. An error code of 0 indicates that the NITRO request is successful. A non-zero error code indicates an error in processing the NITRO request.
- **Error message.** A brief description of the exception.

Note: For a list of error codes, see the errorlisting.html file available in the <NITRO_SDK_HOME>/doc/ folder.

REST Web Service

REST (REpresentational State Transfer) is an architectural style based on simple HTTP requests and responses between the client and the server. REST is used to query or change the state of objects on the server side. In REST, the server side is modeled as a set of entities where each entity is identified by a unique URL.

Each resource also has a state on which the following operations can be performed:

- **Create.** Clients can create new server-side resources on a "container" resource. You can think of container resources as folders, and child resources as files or subfolders. The calling client provides the state for the resource to be created. The state can be specified in the request by using XML or JSON format. The client can also specify the unique URL that identifies the new object. Alternatively, the server can choose and return a unique URL identifying the created object. The HTTP method used for Create requests is POST.

- **Read.** Clients can retrieve the state of a resource by specifying its URL with the HTTP GET method. The response message contains the resource state, expressed in JSON format.

- **Update.** You can update the state of an existing resource by specifying the URL that identifies that object and its new state in JSON or XML, using the PUT HTTP method.

- **Delete.** You can destroy a resource that exists on the server-side by using the DELETE HTTP method and the URL identifying the resource to be removed.

In addition to these four CRUD operations (Create, Read, Update, and Delete), resources can support other operations or actions. These operations use the HTTP POST method, with the request body in JSON specifying the operation to be performed and parameters for that operation.

Logging on to the NetScaler Insight Appliance

The first step toward using NITRO is to establish a session with the NetScaler Insight virtual appliance and then authenticate the session by using the administrator's credentials. You must specify the username and password in the `login` object. The session ID that is created must be specified in the request header of all further operations in the session.

Note: You cannot log on to the NetScaler Insight virtual appliance unless you have a user account on the appliance. The configuration operations that you can perform are limited by the administrative roles assigned to your account.

To connect to a NetScaler Insight virtual appliance with IP address 10.102.126.213 by using the HTTPS protocol:

- **URL.** https://10.102.126.213/nitro/v1/config/login/
- **HTTP Method.** POST
- **Request Payload**

```
object=
{
   "login":
   {
      "username":"admin",
      "password":"verysecret"
   }
}
```

- **Response Payload.**

```
{
   "errorcode":0,
   "message":"Done",
   "sessionid":"%23%2354B9.."
}
```

Note: You must use the session ID in all further NITRO operations on the virtual appliance.

Note: By default, the connection to the virtual appliance expires after 30 minutes of inactivity. You can modify the timeout period by specifying a new timeout period (in seconds) in the login object. For example, to modify the timeout period to 60 minutes, the request payload is:

```
object=
{
   "login":
   {
```

```
        "username":"admin",
        "password":"verysecret",
        "timeout":3600
    }
}
```

To disconnect from the virtual appliance, use the DELETE method:

- **URL.** https://10.102.126.213/nitro/v1/config/login
- **HTTP Method.** DELETE
- **Cookie.** SESSID=%23%2354B9...

Registering a NetScaler Appliance

To register a NetScaler appliance with the NetScaler Insight appliance, you must specify the NetScaler IP (NSIP) address, the user name, and the password of the NetScaler appliance in the managed_device object.

To register a NetScaler appliance with NSIP address 10.102.29.60:

- **URL.** https://10.102.126.213/nitro/v1/config/managed_device/
- **HTTP Method.** POST
- **Cookie.** SESSID=%23%2354B9...
- **Request Payload.**

```
object=
{
   "managed_device":
   {
      "ip_address":"10.102.29.60",
      "profile_username":"admin",
      "profile_password":"verysecret",
      "type":"ns"
   }
}
```

To retrieve a list of NetScaler appliances configured on an Insight appliance:

- **URL.** http://10.102.126.213/nitro/v1/config/managed_device/
- **HTTP Method.** GET
- **Cookie.** SESSID=%23%2354B9...

Among other parameters, the response payload provides an identity for each NetScaler appliance. You must use this ID to identify a NetScaler in further operations.

Updating NetScaler Appliance's Login Credentials

If the login credentials of a NetScaler appliance are updated after it is registered to a NetScaler Insight appliance, they have to be updated on the Insight appliance.

To update the password of a NetScaler appliance with IP address 10.102.29.60:

- **URL.** https://10.102.126.213/nitro/v1/config/device_profile
- **HTTP Method.** PUT
- **Cookie.** SESSID=%23%2354B9...
- **Request Payload.**

```
{
   "device_profile":
   {
      "username":"admin",
      "password":"verysecret-new",
      "id":"507be920475294e414f90889"
   }
}
```

Note: The ID of the NetScaler appliance must be obtained by using the GET HTTP method on the http://10.102.126.213/nitro/v1/config/managed_device/ URL.

Gathering Performance Data about an Application

To gather performance data from an appliance, you must select the virtual server, specify the filter condition, and then enable Appflow on the appliance in the ns_vserver_appflow_config object. The appliance then starts gathering performance data for the applications (services) bound to the virtual server.

Note: This operation gathers the performance dat but does not display.

To gather performance data of an application linked to virtual server with name "http_test":

- **URL.** http://10.102.126.213/nitro/v1/config/ns_vserver_appflow_config
- **HTTP Method.** PUT
- **Cookie.** SESSID=%23%2354B9...
- **Request Payload.**

```
{
   "ns_vserver_appflow_config":
   {
      "appflow_policy_rule":"TRUE",
      "appflowlog":"enabled",
      "es4nslog":"enabled",
      "name":"http_test",
      "state":"UP",
      "ns_ip_address":"10.102.29.60",
      "ip_address":"10.102.126.237",
      "type":"lb",
      "servicetype":"HTTP"
   }
}
```

Generating Performance Reports

To generate a report of the performance data of an application (a virtual server), you must specify the period for which you want the data in the URL.

To generate a report of the performance data for a device with IP address 10.102.71.201, for the past one month:

- **URL.** http://10.102.60.45/nitro/v1/appflow/user_agent?args=device_ip_address:10.102.71.201&asc=no&order_by=total_requests&pagesize=25&type=total_requests&duration=last_1_month

  where,

  - asc=no: Displays records in descending order.
  - order_by=total_requests: Orders records on the basis of the total requests.
  - pagesize=25: Displays 25 records per page.
  - type=total_requests: Total requests to be displayed.
  - duration=last_1_month: Records of the last one month must be displayed.
- **HTTP Method.** GET
- **Response Payload.**


```
{
   "errorcode": 0,
   "message": "Done",
   "user_agent":
   [
      {
         "__count": "-1",
         "http_resp_status_name": "",
         "server_ip_address": "",
         "name": "Chrome",
         "http_req_method_name": "",
         "rpt_sample_time": "-1",
         "total_bytes": "16644969",
         "device_ip_address": "10.102.71.201",
         "uri_url": "",
         "max_transaction_time": "-1",
         "app_unit_name": "",
         "render_time": "14",
         "client_ip_address": "",
         "id": "",
         "app_unit_ip_address": "",
         "total_requests": "245",
         "operating_system_name": ""
      },
```

```
        {
            "__count": "-1",
            "http_resp_status_name": "",
            "server_ip_address": "",
            "name": "Unknown",
            ...
            ...
        }
    ]
}
```

Exception Handling

The response payload of any operation, specifies the error code and error message. For a more detailed description of the error codes, see the API reference available in the <NITRO_SDK_HOME>/doc folder.