Citrix SCOM Management Pack 1.17 for NetScaler

May 21, 2017

Citrix SCOM Management Pack for NetScaler is an availability and performance management solution that extends end-to-end service monitoring capabilities of Microsoft System Center Operations Manager (SCOM) to include the Citrix NetScaler (NetScaler) infrastructure. It fully integrates topology, health, and performance data into SCOM, providing an end-to-end operations overview across the entire NetScaler estate and enabling delivery of effective business service management.

Some key benefits of Citrix SCOM Management Pack for NetScaler are:

- Agentless monitoring architecture
- Intuitive topology discovery of internal NetScaler components
- Deep monitoring of key virtual servers and services
- Enhanced infrastructure health
- Quick deployment and simple upgrades
- Functioning across physical and virtual NetScaler appliances
- Easy identification and resolution of network-specific issues
- Acceleration of problem resolution
- Scaling management responsibility across your infrastructure and organization
- Automation of routine administration to improve service levels, increase efficiencies, and achieve greater control of the IT environment

Topology discovery

Citrix SCOM Management Pack for NetScaler provides out-of-the-box discovery of the NetScaler configuration:

- Automatically discovers and visualizes the topology of NetScaler devices. The discovery and visualization are based on a defined NetScaler device model. The discovered devices are used as a base for NetScaler component discovery.
- Updates NetScaler topology in regular time intervals.

Discovered NetScaler appliance objects are divided into the following major components:

- System
  Shows system settings as well as licensed functionalities on NetScaler and memory pools.

- Network
  Provides details on IP addresses (IPv4 and IPv6), network interfaces, VLANs, channels, and bridge groups.

- Access Gateway
  Displays AG virtual servers and related authentication policies.

- Traffic Management
  Contains Load Balancing group which includes LB virtual servers, as well as LB services and service groups.

- SSL
  Covers SSL entities, namely policies, actions, and certificates.

- Authentication Authorization Auditing
  Divides authentication servers into three groups: LDAP, Radius, and TACACS.

- Cloud Bridge
  Contains information about Network Bridges that are configured.

Monitoring

Citrix SCOM Management Pack for NetScaler monitors many components out-of-the-box and is designed to be extendable to meet custom monitoring requirements. Some out-of-the-box monitoring capabilities are:

- Settings in detail, monitors per object as well as monitoring of configuration changes.
- Detection of unusual session behavior.
- Detection of NetScaler service failures.
- Identification of internal NetScaler issues and non-responding services.

Monitors are classified into the following groups:

- Appliance
  Includes hardware and system information monitoring:
  - CPU and memory usage
  - Temperature
  - Fan speed
  - Power supply
  - High availability node master state
    General statistics for:
  - Authentication, Authorization, and Auditing
  - Access Gateway
  - Protocols (IPv4, IPv6, SSL, TCP, UDP)
- Access Gateway Virtual Servers
  Related to a specific virtual server and includes monitoring of:
  - State
  - Number of current users
  - Requests rate
  - Activity in terms of requests and responses
- Load Balancing
  Monitors health states for LB related objects including:
  - Virtual Server
  - Service
  - Service group
- Authentication
  Detects the number of authentication failures in a given time interval for the following authentication protocols:
  - LDAP
  - Radius
  - TACACS
- Network
  Network-related monitors show:
  - State change for interfaces and channels
  - IP address conflicts for both IPv4 and IPv6
- SSL

SSL-specific monitors are used to monitor:

  - Impending SSL certificate expiry
  - Absence of SSL policy hits (no traffic to trigger the policy)

Views

Citrix SCOM Management Pack for NetScaler provides various out-of-the-box views that present alerts, the health state, tasks, and performance.

There are a number of performance collection views:

- Appliance
  The NetScaler appliance is the target.
  - Authentication, Authorization, and Auditing (general)
  - Access Gateway VPN (general)
  - Application Firewall
  - Integrated Cache
  - Compression
  - NetScaler Configuration Changes
  - CPU
  - Disk
  - Memory
  - HTTP Protocol
  - IP Protocol
  - SSL Protocol
  - TCP Protocol
  - UDP Protocol
  - Temperature
- Network
  One of the network components is the target.
  - Channel
  - Interface
- Access Gateway
  The Access Gateway virtual server is the target.
- Load Balancing
  Load Balancing service is the target.
- SSL
  SSL policies or SSL actions are the target.

Tasks

Citrix SCOM Management Pack for NetScaler provides some tasks that can be easily extended:

- Displays all NetScaler events.
- Displays a current list of system sessions.
- Displays a current list of ICA connections.
- Displays all SSL virtual servers.

Architecture

The following diagram shows how Citrix SCOM Management Pack for NetScaler is deployed on the SCOM management platform.

Increasing the queue size of the version store

The Microsoft Monitoring Agent Service stores records of unfinished transactions in a version store. Version store enables the Extensible Storage Engine (ESE) to track and manage current transactions. It contains a list of operations performed by active transactions maintained by the Health Service. This list is an in-memory list of modifications made to the Health Service store database.

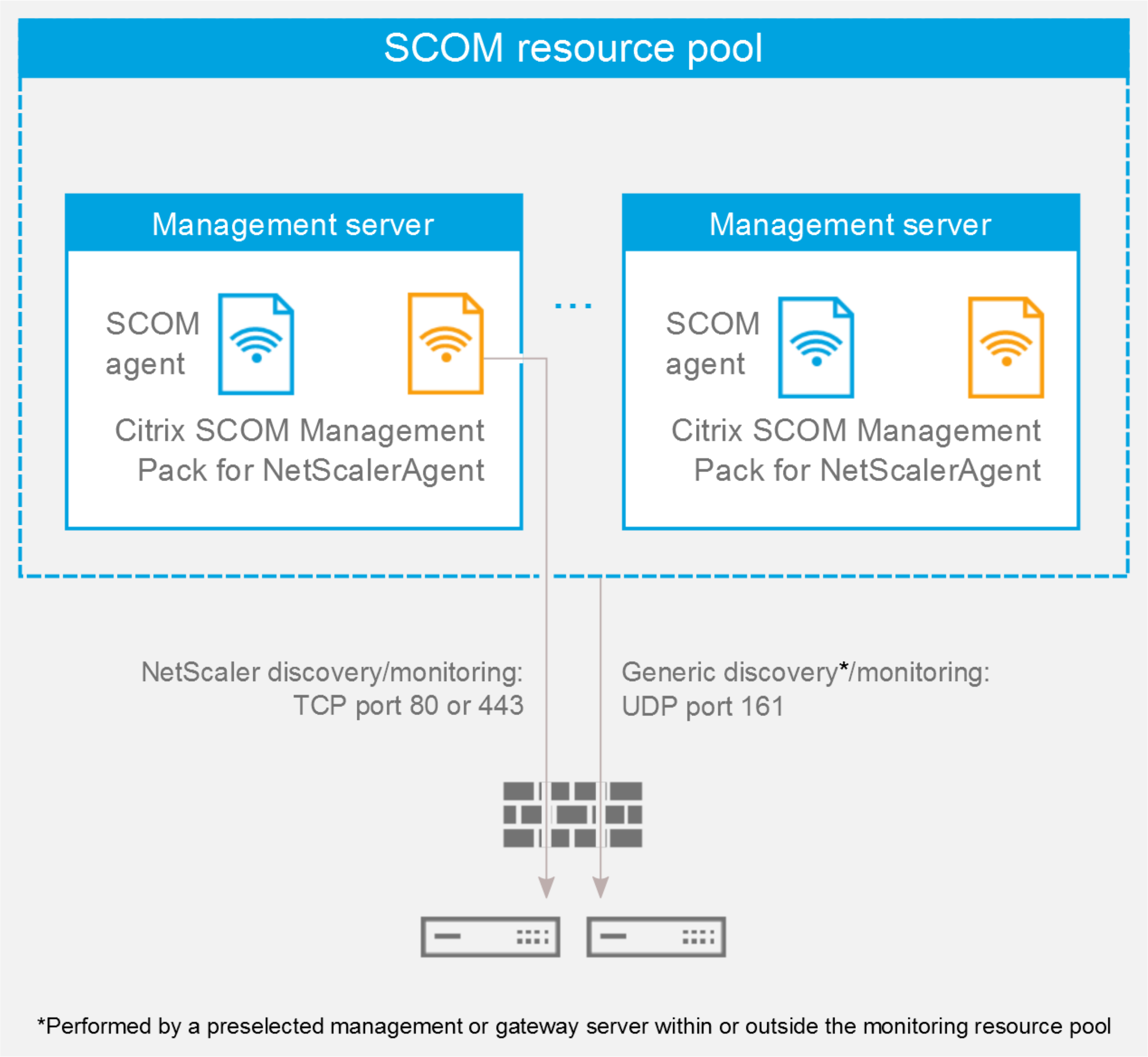
The default size of version store is 1,920 16-KB memory pages (30 MB) and is optimized for a typical installation of SCOM. A version store of this size is not sufficient to handle the high data flow in a large XenApp and XenDesktop environment.

To increase the queue size of the version store, do the following:

Caution: Using Registry Editor incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

1. In the Start menu, type **regedit** in the Search text box, and then click **Search**.
2. In the Results list, click **regedit** or **regedit.exe**.
3. In the User Account Control dialog box, click **Yes**.
4. In the Registry Editor window, navigate to **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Services** > **HealthService** > Parameters.
5. Right-click the **Persistence Version Store Maximum** value and click **Modify**.

Figure The **Persistence Version Store Maximum** value in Registry Editor


SCOM resource pool
Management server
SCOM agent
Citrix SCOM Management Pack for NetScalerAgent
...
Management server
SCOM agent
Citrix SCOM Management Pack for NetScalerAgent
NetScaler discovery/monitoring: TCP port 80 or 443
Generic discovery*/monitoring: UDP port 161
*Performed by a preselected management or gateway server within or outside the monitoring resource pool

Citrix SCOM Management Pack for NetScaler has two main parts:

- Server side (installed on one computer out of management server computers in the SCOM management group)
  The server side of the product contains management packs as well as agent installation packages. When management packs are imported into SCOM, all network devices are targeted and NetScaler devices discovery is based on the network device OID value. Other discovery and monitoring processes use the agent to communicate with NetScaler devices.

- Agent side (installed on each member of the SCOM resource pool dedicated to NetScaler device monitoring)
  The agent side of the product contains Citrix SCOM Management Pack for NetScaler Agent. It is designed to act as a layer between the management packs and the NetScaler appliances in the monitoring process. All requests initiated by Citrix SCOM Management Pack for NetScaler on the SCOM side flow though the agent. The agent is a proxy and data collector that optimizes the requests, optimizes sessions with the NetScaler appliances, and collects and caches data

from these appliances.

The agent is implemented as a Windows service. It uses AJAX technology to access the NetScaler appliances through the NITRO API. Credentials for accessing the NetScaler appliances are sent from SCOM. A single agent instance can monitor multiple NetScaler appliances.

The agent must be installed on all members in the chosen SCOM resource pool.

Note: Resource pools are a feature introduced in SCOM 2012. A resource pool is a collection of management servers or gateway servers used to distribute work amongst themselves and take over work from a failed member. Citrix SCOM Management Pack for NetScaler Agent must reside on all members of a resource pool.

What's new

May 21, 2017

Citrix SCOM Management Pack 1.17 for NetScaler introduces the following new or enhanced features:

- **Documentation in HTML format.** The documentation for the Citrix SCOM Management Pack 1.17 for NetScaler is available in HTML format. To access the documentation for earlier versions, see Citrix SCOM Management Pack for NetScaler.

- **FIPS Compliance.** Citrix SCOM Management Pack for NetScaler now uses FIPS (Federal Information Processing Standards) compliant algorithms and can monitor FIPS-compliant systems.

- **TLS 1.2 support**. Citrix SCOM Management Pack for NetScaler is enhanced to monitor Citrix NetScaler devices that have TLS (Transport Layer Security) protocol version 1.2 enabled.

Known issues

The following is a list of known issues in this product version.

- **Issue ID**: SCOM-420
  Symptom: After upgrading the product from the version 1.14 or 1.13, the **%ProgramData%\Comtrade** folder is left on the local system. This issue occurs on the SCOM management server computer as well as on the SCOM resource pool members.
  Action: Manually remove the residuary folder by using an operating system tool.

Fixed issues

The following issues have been fixed in this version:

- When the Citrix SCOM Management Pack Agent for NetScaler is deployed on an SCOM Gateway monitoring a large number of Load Balancing service groups, it does not discover the Load Balancing service groups.
  [SCOM-1259]

- The Citrix SCOM Management Pack for NetScaler stops monitoring when the debug option for the discovery of Load Balancing Service Group is enabled and the state of the Load Balancing Objects is not updated.
  [SCOM-1722, SCOM - 1259]

- A while after the Citrix SCOM Management Pack Agent for NetScaler is started, it starts timing out and stops discovering or monitoring objects.
  [SCOM-1725]

- Citrix SCOM Management Pack Agent for NetScaler in debug mode logs a **Session expired** error message even when a reconnection to the NetScaler device was successful.
  [SCOM-1227]

- The Citrix SCOM Management Pack Agent for NetScaler does not monitor any NetScaler objects or alerts on SCOM

2012 and SCOM 2012 SP1 systems.
[SCOM-1206]

- When the Citrix SCOM Management Pack Agent for NetScaler is installed on the SCOM Gateway, the management pack's support tasks do not function.
[SCOM-1193]

- The Citrix SCOM Management Pack Agent for NetScaler does not support TLS 1.2 communication protocol between the Citrix SCOM Management Pack for NetScaler and the NetScaler NSIP.
[SCOM-1760]

- Citrix SCOM Management Pack for NetScaler times out and stops monitoring you make the master NetScaler appliance node secondary.
[SCOM-1727]

Upgrading

Note: Product versions earlier than 1.14 were released under the name Comtrade Management Pack for Citrix NetScaler.

An upgrade is available only for the following versions 1.13 and later.

In-place upgrade is not supported in the Citrix SCOM Management Pack for NetScaler. Instead to do an upgrade, follow the steps as below:

1. Uninstall the current version of the management pack following the uninstallation instructions as per the documentation of your current version.
Note: Do not delete the %ProgramData%\Citrix\CitrixMPShare\NetScaler MP folder.
2. Your management pack customization is preserved. Install the new version of the Citrix SCOM Management Pack for NetScaler following the instructions in Install and Configure.
   - Install and verify the product (its server-side part) on the SCOM management server computer.
   - Manually import the management packs from the %ProgramFiles%\Citrix\NetScaler MP folder on the SCOM management server computer.
   - If you are upgrading from **version 1.13**, configure access to the shared folder for agent installation.
3. Uninstall the product from the SCOM resource pool members as per the documentation of your current version.
4. Install and verify the product (its agent-side part) on the SCOM resource pool members following the instructions in Install and Configure.

System requirements

May 21, 2017

Before installing Citrix SCOM Management Pack for NetScaler, make sure that your environment meets the requirements listed in this section.

Software requirements

Citrix SCOM Management Pack for NetScaler requires a supported version of the following products that it integrates with:

- Citrix NetScaler
- Microsoft System Center Operations Manager

Note: Make sure that Microsoft .NET Framework 4.5.2 or later is available on the NetScaler device.

Supported platforms and versions of Citrix NetScaler

Citrix SCOM Management Pack for NetScaler is compatible with the following Citrix NetScaler platforms:

Product platform	Supported
Citrix NetScaler MPX	✔
Citrix NetScaler VPX	✔

Citrix SCOM Management Pack for NetScaler is compatible with the following Citrix NetScaler versions:

Product version	Supported
Citrix NetScaler 11.1	✔
Citrix NetScaler 11.0	✔
Citrix NetScaler 10.5	✔
Citrix NetScaler 10.1	✔
Citrix NetScaler 10.0	✔
Citrix NetScaler 9.3	✔

Supported versions of SCOM

Citrix SCOM Management Pack for NetScaler is compatible with the following SCOM versions:

Microsoft System Center Operations Manager version	Supported
Microsoft System Center Operations Manager 2016	✔
Microsoft System Center Operations Manager 2012 R2	✔
Microsoft System Center Operations Manager 2012[1]	✔

[1] This entry covers the following configurations: base release, base release + SP1 (Service Pack 1).

Language support

Citrix SCOM Management Pack for NetScaler can be deployed and operates correctly in environments with the following languages and locale settings:

Language	Locale identifier	Supported
English	en	✔
Spanish	es	✔

Performance overview

May 21, 2017

Generally speaking, Citrix SCOM Management Pack for NetScaler consists of two parts:

- A collection of SCOM management packs that are imported into SCOM (the server-side part)
- Citrix SCOM Management Pack for NetScaler Agent

The server-side part

Management packs included in this part are collections of discoveries, monitors, rules, and tasks for Citrix NetScaler (NetScaler). From the compute and memory perspectives, this part does not add to the basic resource requirements of the SCOM management server where they are imported.

Citrix SCOM Management Pack for NetScaler Agent

Performance and resource consumption of Citrix SCOM Management Pack for NetScaler Agent both primarily depend on the size of your NetScaler environment, specifically on the number of discovered and monitored NetScaler objects.

Configuration specifications

All figures in this document are valid for environments that:

- Are monitored with the specified product version of Citrix SCOM Management Pack for NetScaler
- Match the documented configuration specifications for NetScaler and SCOM
- Use the default configuration of management packs in terms of which rules and monitors are enabled (this applies to management packs included in NetScaler Management Pack and management packs bundled with SCOM)
- Use the default configuration of SCOM management servers and SCOM agents, without fine-tuning or any special adjustments

Note: Factors such as different hardware specifications and condition of your environment may cause divergence of your observed values from the documented values.

Validated Citrix SCOM Management Pack for NetScaler version

Validation of Citrix SCOM Management Pack for NetScaler was performed with the product version listed in the following table.

Product	Version
Citrix SCOM Management Pack for NetScaler	1.5

Citrix NetScaler configuration specification

Specification item	Value
Software version	Citrix NetScaler 11.0 and 10.5

Virtualization platform	XenServer 6.5
Instantiated packet engines (NetScaler 11.0)	1
Instantiated packet engines (NetScaler 10.5)	1
Appliance type	NetScaler VPX
NetScaler devices in the monitored environment	2

Microsoft System Center Operations Manager configuration specification

With this configuration, the SCOM database and data warehouse server is deployed outside the SCOM management server.

Resource pool configuration

Specification item	Value
SCOM resource pools	1
SCOM management servers in the resource pool	1

Computer: **SCOM management server**

Specification item	Value
Compute	four virtual CPUs; CPU clock speed of 2.67 GHz
Memory	8 GB of RAM
Software version	Microsoft System Center Operations Manager 2012 R2

Computer: **SCOM database and data warehouse server**

Specification item	Value

Compute	four virtual CPUs; CPU clock speed of 2.67 GHz
Memory	24 GB of RAM
Storage	100 GB of free storage space
Software version	Microsoft SQL Server 2014

Monitoring ability

The following table lists the lab set-up in which Citrix SCOM Management Pack for NetScaler was successfully validated with the specified NetScaler and SCOM configurations. NITRO API was used for monitoring during which data was gathered at the following intervals: 15 minutes for rules, 5 minutes for monitors, and 4 hours for object discovery.

Maximum number of monitored objects (for the specified configuration)

Item	Value
NetScaler objects discovered and monitored by Citrix SCOM Management Pack for NetScaler[1]	app. 14,000

[1] Refers to the total number of objects of any type in either validated environment (with one or two appliances). For examples of object type distribution, see the following table.

Object type distribution examples (with load balancing)

Object type[2]	Example A value	Example B value
Appliances	1	2
Virtual servers	3,750	4,550
Services	1,500	1,000
Service groups	4,350	3,850
Other object types[3]	app. 3,850	app. 4,600

[2] This table lists examples of object types that are monitored by Citrix SCOM Management Pack for NetScaler. Object type distribution examples A and B explain how the maximum number of monitored objects is calculated.

[3] Examples of other object types are Features, Global Settings, HTTP Settings, Interface, IPv4, Licenses, Memory Pool,

Modes, Other Settings, SSL Certificate, TCP Settings, Timeout Settings, Virtual LAN, Other Settings, and so on.

Resource consumption

Measuring of the product's resource consumption was performed on different validation sets. Windows Performance Monitor was used as the measuring tool. During validation, NetScaler objects were gradually (on a daily basis) added to the monitored environment.

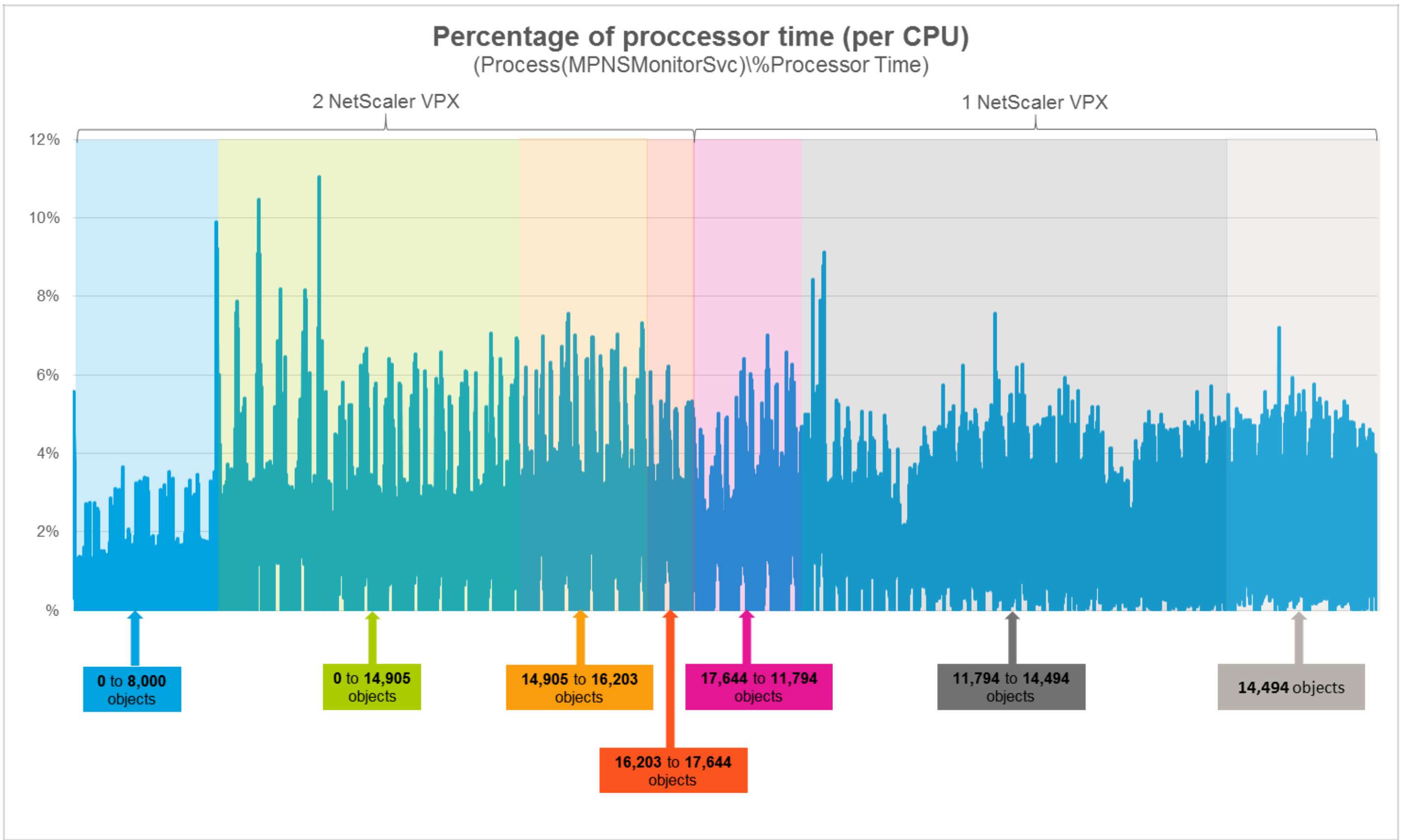
Average compute and memory consumption of the agents

The process of measuring average compute and memory consumption of the agents spanned a period of 26 days. Based on the measurement results, average percentage of processor time and average memory usage of both *MPNSMonitorSvc* and *HealthService* were determined.

Average consumption on a SCOM resource pool member (for app. 14,000 NetScaler objects)

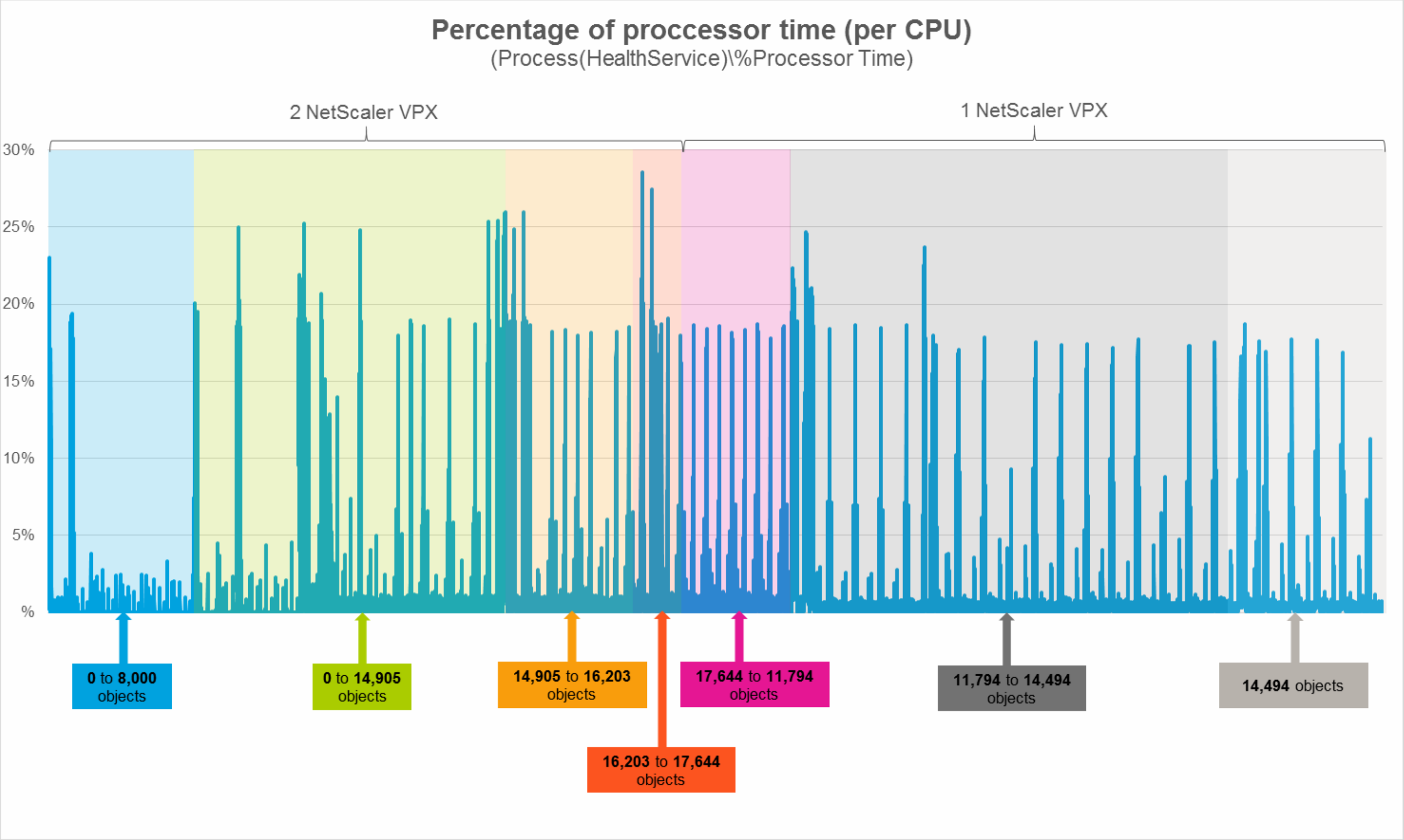
Item	Value
MPNSMonitorSvc percentage of processor time (per CPU)	1.19%
HealthService percentage of processor time (per CPU)	1.18%
MPNSMonitorSvc memory usage	331 MB
HealthService memory usage	659 MB

The following figure shows the percentage of processor time used by *MPNSMonitorSvc* through time, measured in seven different validation sets.



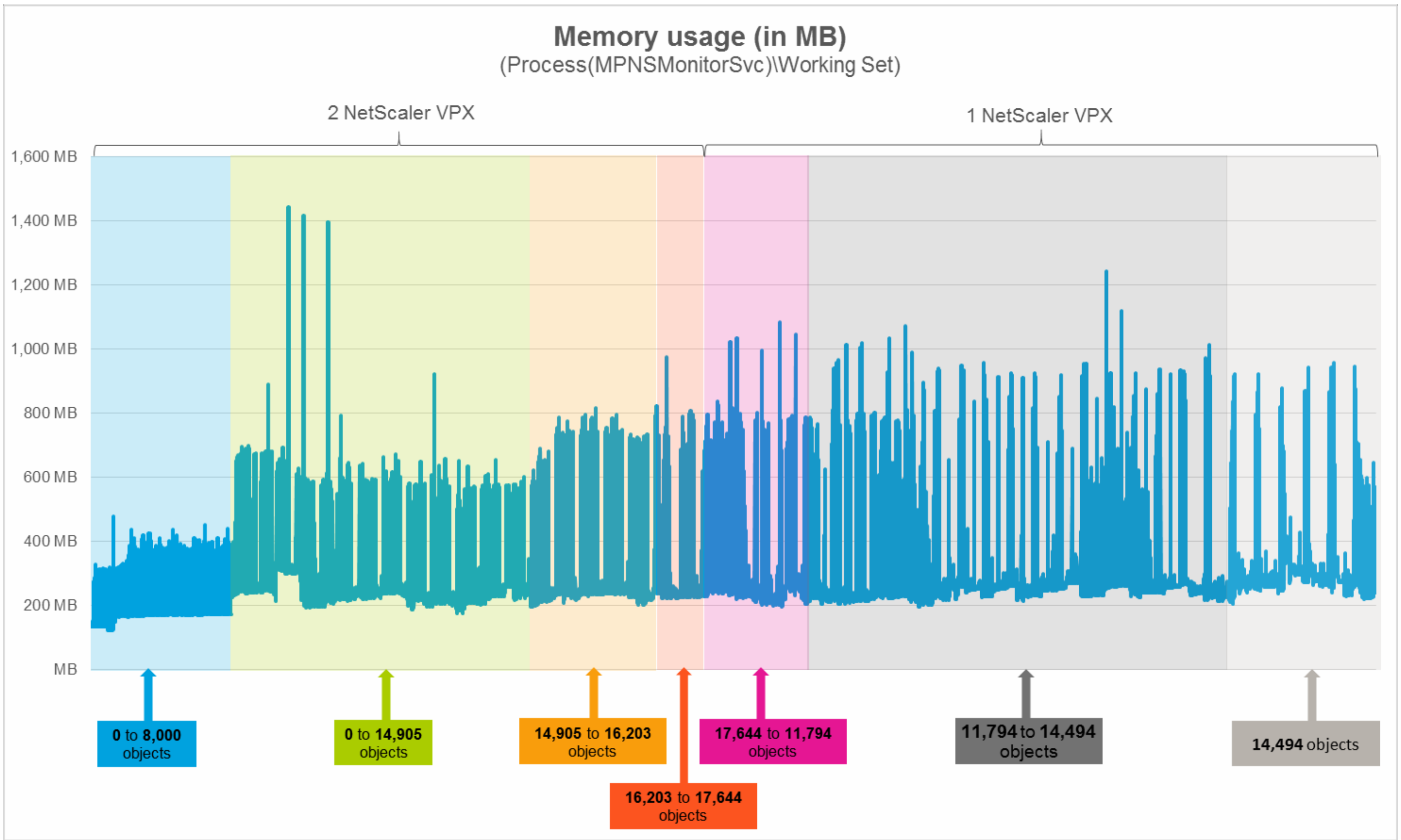
As the figure above shows, adding NetScaler objects has no significant impact on the percentage of processor time used by Citrix SCOM Management Pack for NetScaler Agent.

The following figure shows the percentage of processor time used by *HealthService* through time, measured in seven different validation sets.



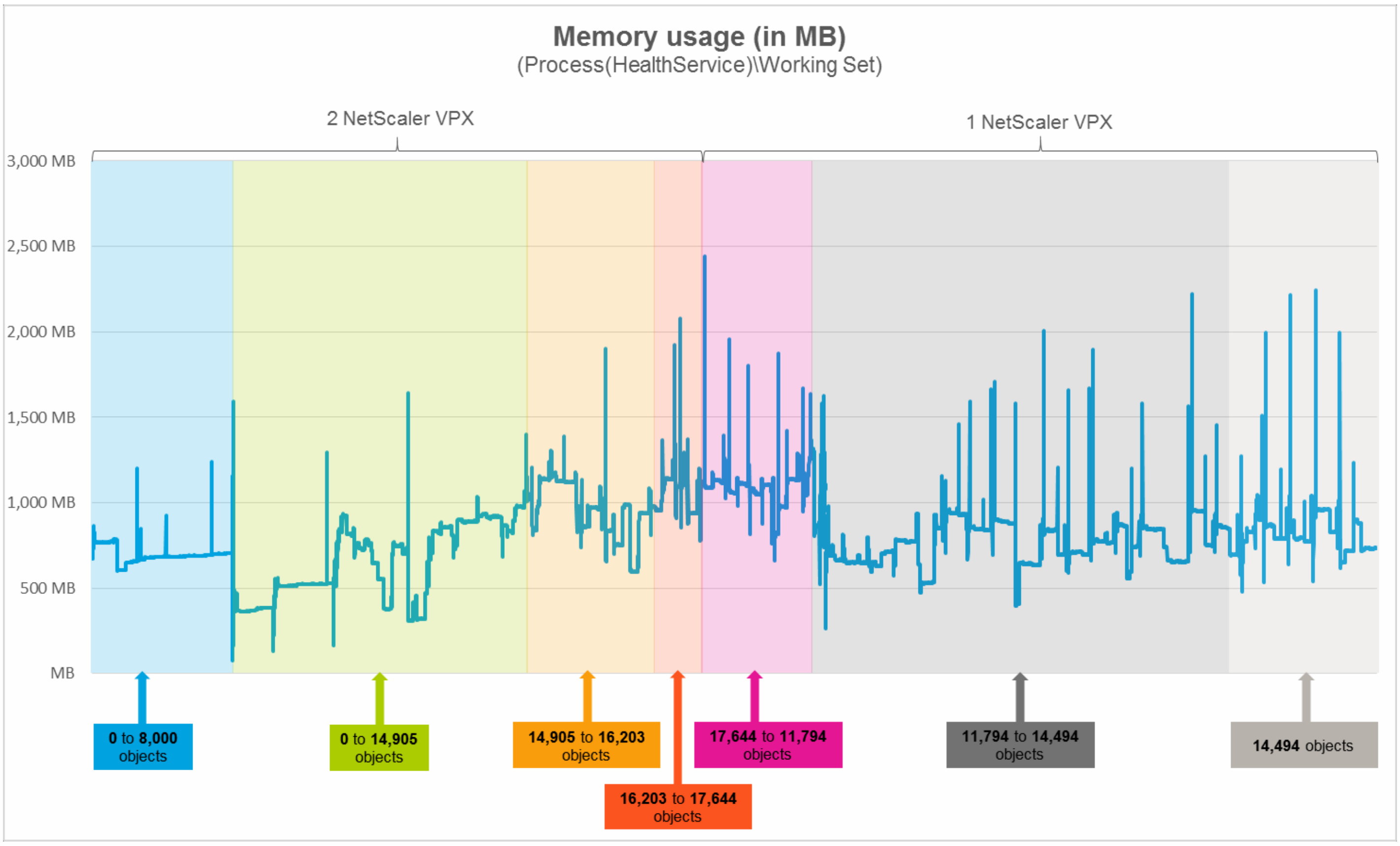
As the figure above shows, addition of objects also does not influence the percentage of processor time used by the SCOM agent (Operations Manager Agent, Microsoft Monitoring Agent).

The following figure shows the memory usage of *MPNSMonitorSvc* through time, measured in seven different validation sets.



As the figure above shows, on the SCOM management server, there should be approximately 1.4 GB of physical memory available for the needs of the *MPNSMonitorSvc* service.

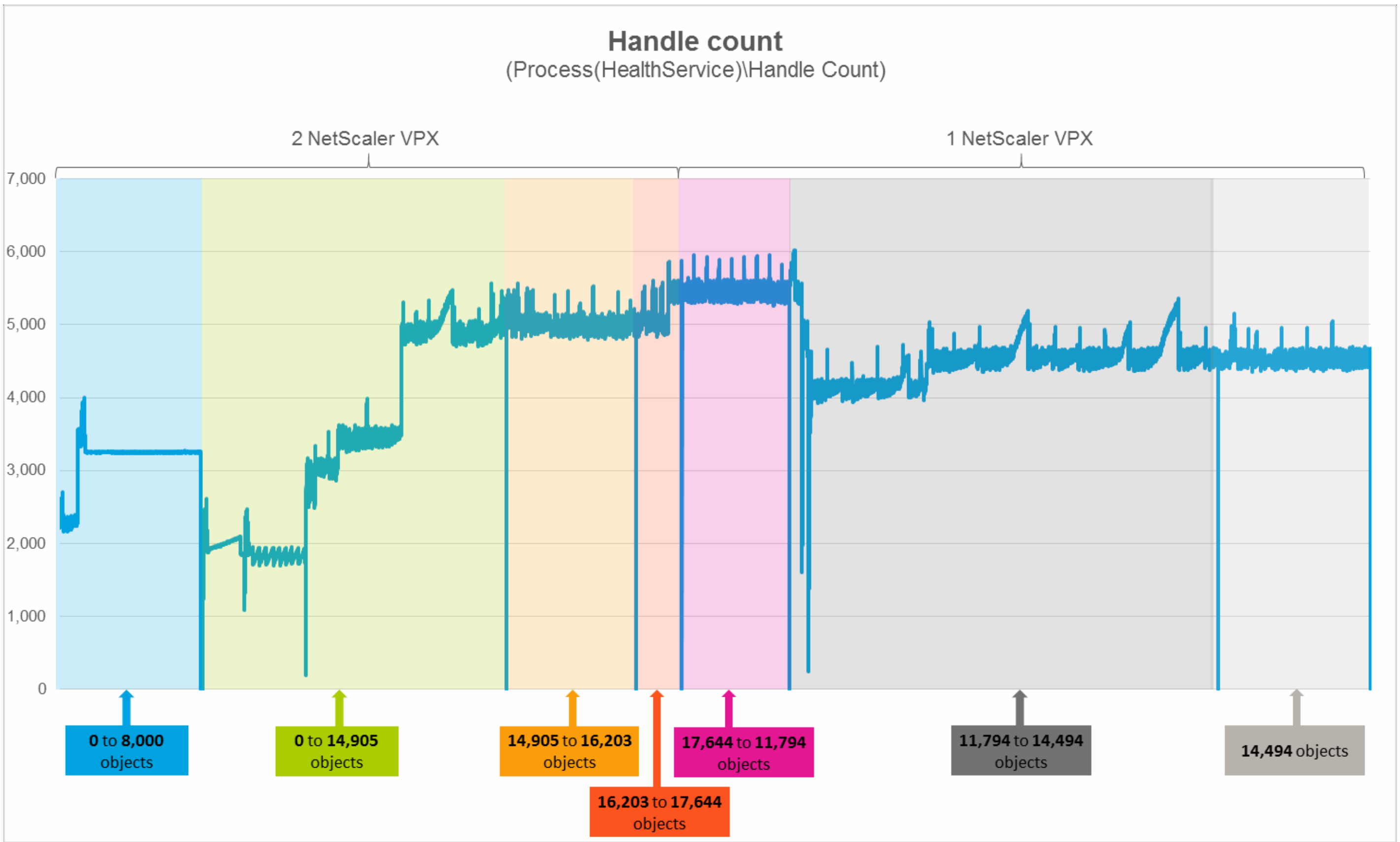
The following figure shows the memory usage of *HealthService* through time, measured in seven different validation sets.



As the figure above shows, on the SCOM management server, there should be approximately 1.6 GB of physical memory available for the needs of the *HealthService* service.

Detailed analysis of the sampled data reveals that Citrix SCOM Management Pack for NetScaler has no significant impact on the compute and memory requirements for the SCOM resource pool members.

The following figure shows the handle count of *HealthService* through time, measured in seven different validation sets.

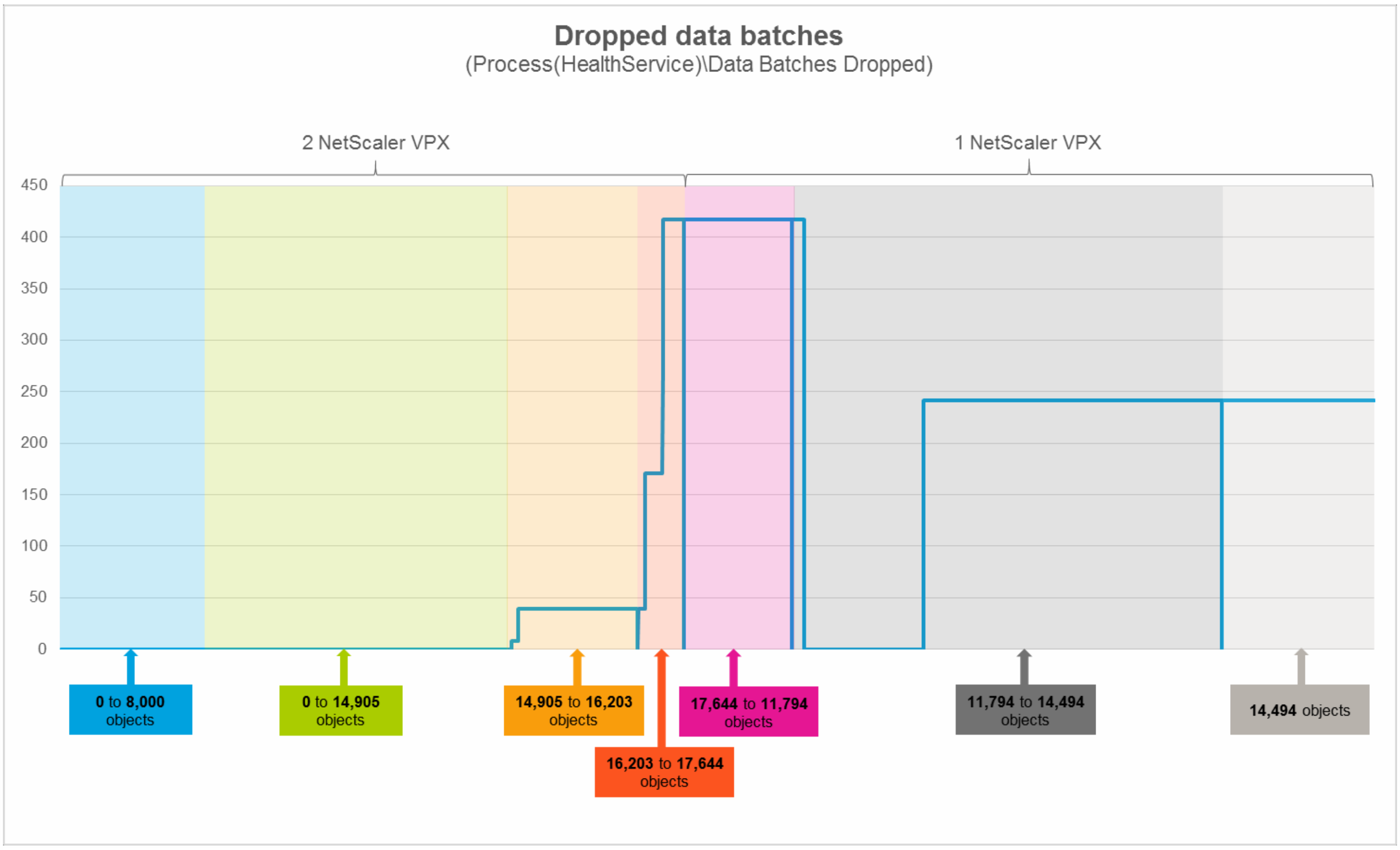


The data analysis also helped estimate potential load on the *HealthService* service during workflow execution on individual validation sets. The following table lists handle count averages for different validation sets.

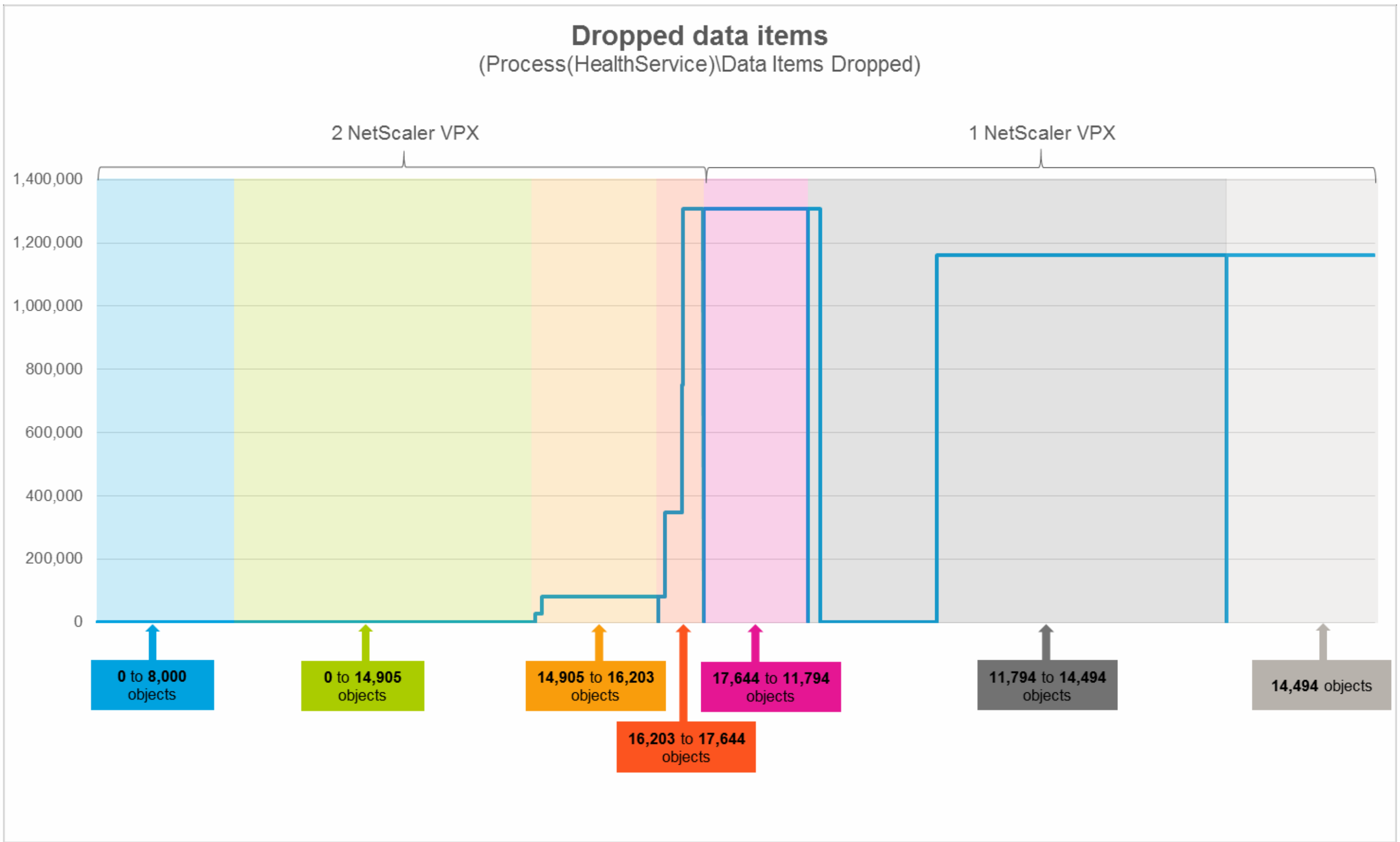
Number of objects	From	0	0	14,905	16,203	17,644	11,794	14,494
	To	8,000	14,905	16,203	17,644	11,794	14,494	
Average handle count		3,143	3,392	5,014	5,198	5,472	4,491	4,538

For validation sets that contained more than 14,000 NetScaler objects, the *HealthService* service started dropping data. This was caused by a very large amount of workflows on the SCOM management server computer that *HealthService* could not process. The following two figures show the number of dropped data batches and data items for different validation sets.

The following figure shows the data batches dropped by *HealthService* through time, measured in seven different validation sets.



The following figure shows the data items dropped by *HealthService* through time, measured in seven different validation sets.



Storage consumption of the SCOM database server

Storage consumption of the SCOM database server was measured in an environment with two NetScaler VPX appliances. The measurement process spanned a period of 30 days. During it, NetScaler objects were added to the monitored environment at different intervals of one or three days. Based on the results, maximum consumption of SCOM database (*OperationsManager*) and consumption growth of SCOM data warehouse (*OperationsManagerDW*) were determined.

Maximum consumption of the SCOM database

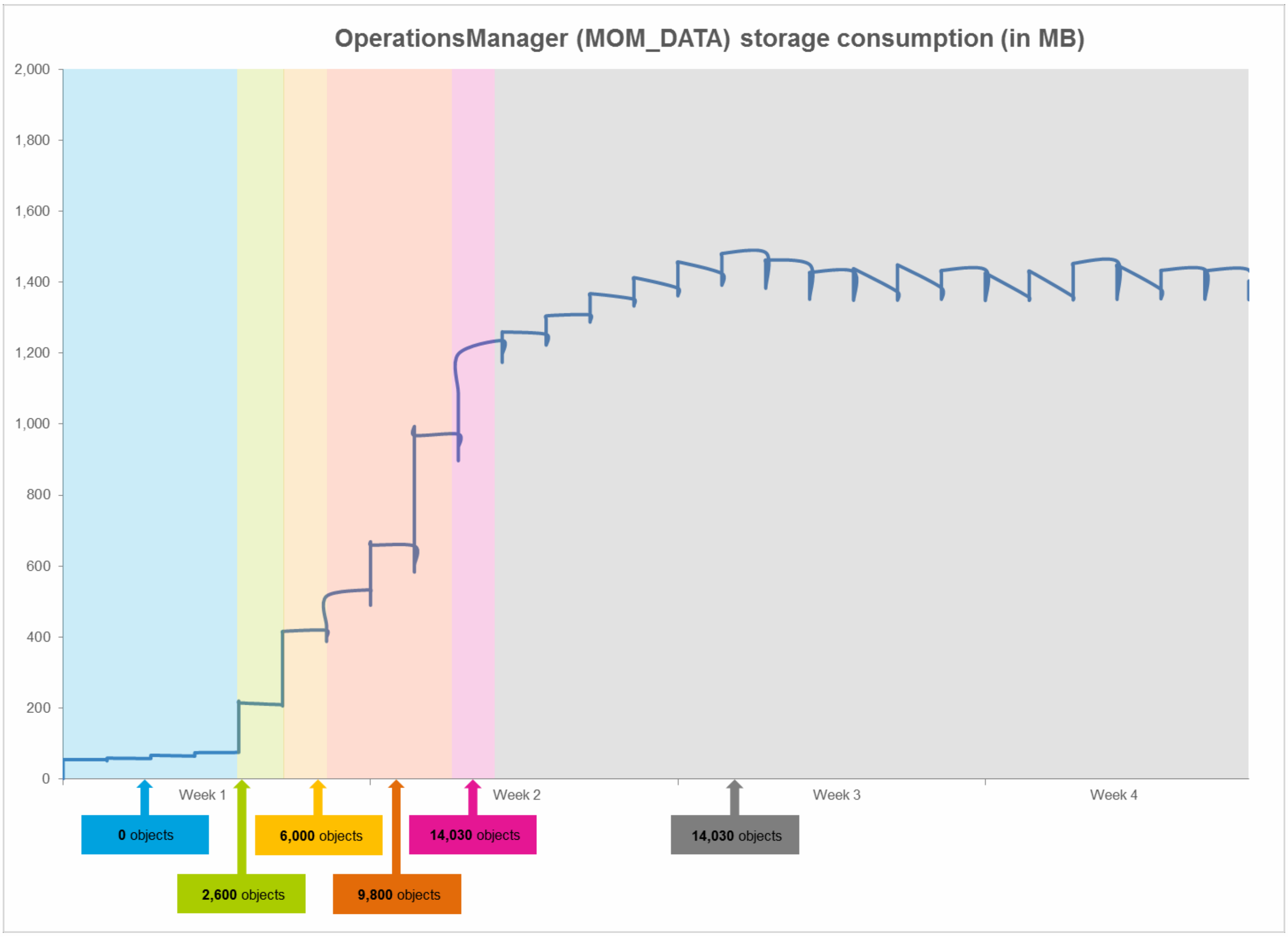
SQL Server database	Database filename	Monitored objects	Maximum storage consumption
OperationsManager	MOM_DATA	2,600	0.25 GB (237 MB)
		6,000	0.42 GB (433 MB)
		9,800	0.97 GB (994 MB)
		14,000	1.45 GB (1,483 MB)

Consumption growth of the SCOM data warehouse

SQL Server database	Database filename	Monitored objects	Consumption growth		
			Per day (in MB)	Per week[4] (in MB)	Per month[4] (in GB)
OperationsManagerDW	MOM_DATA	2,600	29	203	0.85
		6,000	49	344	1.44
		9,800	86	601	2.51
		14,000	197	1,377	5.76

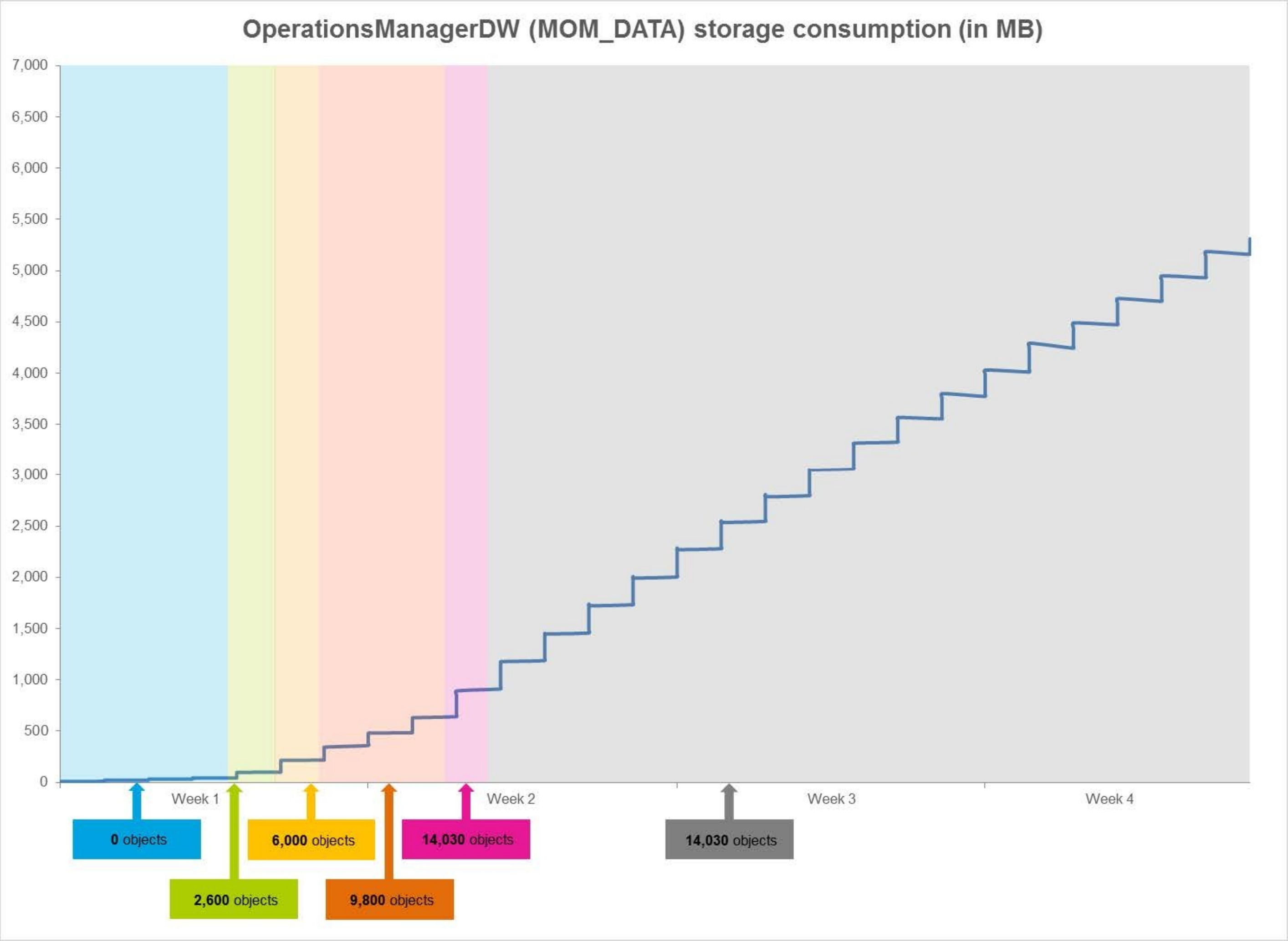
[4] A projection.

The following figure shows the storage requirements of SCOM database (*OperationsManager*) through time, measured in six different validation sets.



In the figure above, you can see a strong correlation between the number of monitored NetScaler objects and storage consumption of SCOM database. In stable circumstances, the SCOM database storage consumption (mean value) increases linearly with addition of new objects. The consumption then stabilizes when objects cease to be added.

The following figure shows the storage requirements of SCOM data warehouse (*OperationsManagerDW*) through time, measured in six different validation sets.



In the figure above, you can see a linear growth of the SCOM data warehouse through the validation period. Increase in the storage consumption happens regardless of whether new objects are added to the monitored environment or not; it persists after the object count no longer changes. Depending on how many objects are added in each interval, the storage consumption growth may be either steeper or more gradual.

Install and configure

May 21, 2017

This chapter contains instructions that you must follow to install and configure Citrix SCOM Management Pack for NetScaler. Perform all procedures in the documented order of precedence.

Before installing Citrix SCOM Management Pack for NetScaler, make sure that the following prerequisites are fulfilled:

- Your environment meets the software requirements. For software requirements, see the System requirements.
- A computer is chosen on which an SCOM management server resides and where the server side of Citrix SCOM Management Pack for NetScaler will be installed. This computer is referred to as the **SCOM Management Server.**
- A SCOM resource pool is chosen for NetScaler monitoring. For easier deployment of Citrix SCOM Management Pack for NetScaler Agent and decreased SCOM resource usage, Citrix recommends that this is a custom resource pool (a resource pool designated to monitor NetScaler devices).
- An SNMP version is chosen that will be used for monitoring. Additionally, all required SNMP configuration parameters are defined and accounts for SNMP-based monitoring are configured in SCOM.
- All NetScaler appliances that you plan to monitor by using Citrix SCOM Management Pack for NetScaler are discovered by SCOM. For general instructions on network device discovery, see the How to Discover Network Devices in Operations Manager webpage on the Microsoft TechNet website.
  To discover network devices by using SNMPv1 or SNMPv2, do the following:

1. Log on to NetScaler with an existing administrator account and by using an SSH client, for example, PuTTY.
2. Run the following command to configure the SNMP community:
   add snmp community <CommunityString> <Permission>
   In the above instances, *<CommunityString>* is the community name and *<Permission>* is the associated SNMP query type.
   Citrix recommends that you use the *ALL* query type only in the event that you are unable to discover devices by using some other query type. In this case, revert the NetScaler configuration to accept a more restrictive query type immediately after the discovery completes.
3. Log on to the management server computer and launch the SCOM Operations console.
4. In the **Administration** view, expand **Network Management**, and then click **Discovery Rules**. In the Tasks pane, expand **Actions**, and then click **Discover Network Devices**.
5. In the Network Devices Discovery Wizard, in the Name text box, type a name. From the **Available servers** drop-down list, select a discovery server, and from the **Available pools** drop-down list, select a resource pool.
   Note: Citrix recommends that you use a custom resource pool that you have created in advance specifically for the needs of NetScaler monitoring.
   Click **Next**.
6. In the Discovery Method page, leave the **Explicit discovery** option selected, and then click **Next**.
7. In the Default Accounts page, select a preconfigured account for SNMP-based monitoring. Click **Next**.
8. In the Devices page, click **Add** to open the Add a Device dialog box. In the Add a Device dialog box, enter the required data. Pay attention to select the appropriate account from the SNMP V1 or V2 Run As account drop-down list, to associate it with the device. Click **OK** to close the dialog box.
9. Repeat step 8 for each additional NetScaler device you plan to monitor. Click **Next**.
10. In the Schedule Discovery page, define a schedule for the discovery rule or choose to run the rule manually. Click **Next**.
11. In the Summary page, verify your settings, click **Create**, and then wait for the discovery rule to be created.

12. In the Completion page, click **Close** to close the wizard.

Once the devices are discovered, their entries appear at two locations in the SCOM operations console: in the Administration view in the Network Management > Network Devices context and in the Monitoring view in the Network Monitoring > Network Devices context.

To discover network devices by using SNMPv3, do the following:

1. Perform the necessary steps on the NetScaler devices. For instructions, see the Configuring the NetScaler for SNMPv3 Queries webpage (or a corresponding webpage for your NetScaler product version).
2. Perform the necessary steps in the SCOM Operations console. For instructions, see the How to Discover Network Devices in Operations Manager webpage. Pay attention to the SNMP version.

- All members of the SCOM resource pool that is designated for NetScaler device monitoring can access NetScaler devices through the following ports:
  - UDB port 161 — for generic discovery and monitoring provided by SCOM
  - TCP port 80 (HTTP) or 443 (HTTPS) — for NetScaler-specific discovery and monitoring

In order to access and communicate with NetScaler, Citrix SCOM Management Pack for NetScaler needs a NetScaler user account configured with proper privileges. This configuration step requires administrative access to NetScaler either through the SSH command-line interface (preferred) or through the NetScaler GUI. Depending on your choice, perform only one of the two procedures that follow. For better guidance, see also Citrix NetScaler documentation.

Set up the NetScaler Management Pack user account by using the NetScaler CLI

To set up the user account through the NetScaler CLI, do the following (the assumption is that the user account name is *usrNetScalerMonitoring* and the corresponding command policy is *polNetScalerMonitoring*):

1. Log on to NetScaler with an existing administrator account and by using an SSH client, for example PuTTY.
2. Run the following command to create a new command policy with proper permissions for NetScaler monitoring:

```
add system cmdPolicy polNetScalerMonitoring ALLOW (^show\s+system\s+\S+)|(^show\s+system\s+\S+\s+.*)|(^show\s+configstatus)|(^
```

For higher security, run the following command instead:

```
add system cmdPolicy polNetScalerMonitoring ALLOW (^show\s+system\s+\S+)|(^show\s+system\s+\S+\s+.*)|(^show\s+configstatus)|(^
```

3. Run the following command to verify existence and allowed actions of the *read-only* policy:

```
show cmdPolicy read-only
```

The command should generate an output similar to the following:

```
Command policy: read-only    Action: ALLOW

cmdspec: (^man.*)|(^show\s+(?!system)(?!configstatus)(?!ns ns\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gslb runningConfig)(?!audit

Done
```

If the *read-only* policy does not exist, create one with the previously listed permissions. To update the command policy, use the *set system cmdPolicy* command.

4. Run the following command to create a new system user:

```
add system user usrNetScalerMonitoring
```

5. Run the following commands to associate the user with the command policies:

```
bind system user usrNetScalerMonitoring read-only 1

bind system user usrNetScalerMonitoring polNetScalerMonitoring 1
```

6. Run the following command to verify configuration of the user account:

```
show system user usrNetScalerMonitoring
```

The command should generate an output similar to the following:

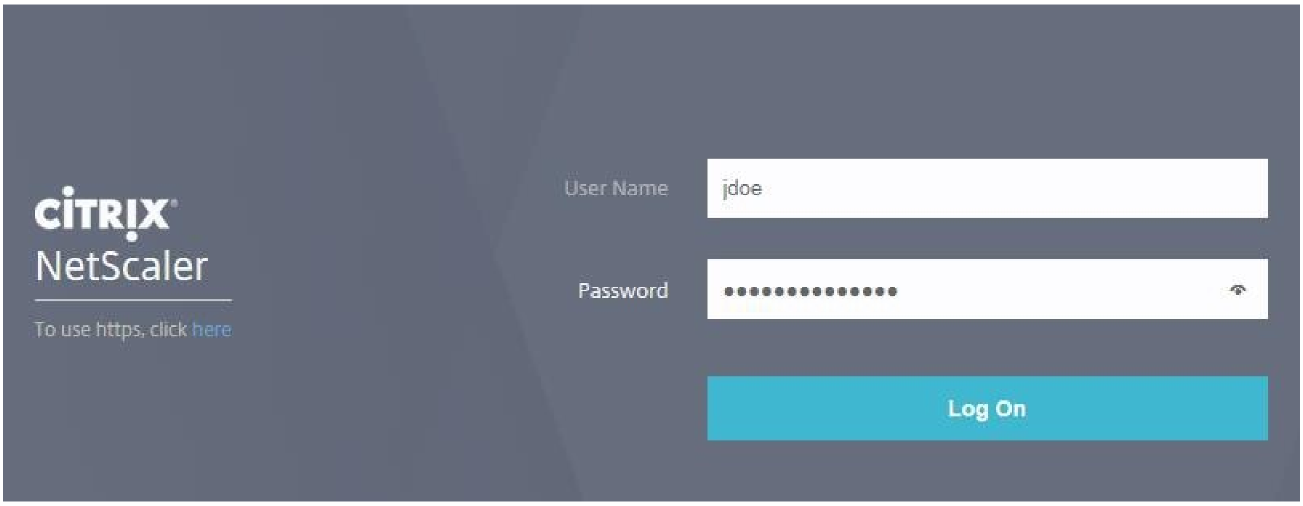
```
User name: usrNetScalerMonitoring

Command Policy: read-only Priority:1

Command Policy: polNetScalerMonitoring Priority:1

Done
```

Set up the NetScaler Management Pack user account by using the NetScaler GUI

Note: Figures in this section reflect the GUI of NetScaler 11.1. GUI appearance in other NetScaler versions may be different.

To set up the user account through the NetScaler GUI, do the following:

1. Launch a web browser and go to the NetScaler management host (host name or IP address). The login screen appears.



User Name: jdoe

Password: ••••••••••••••

2. Log in with credentials of an existing administrator account.
3. In the NetScaler GUI, navigate to **Configuration** > **System** > **User Administration** > **Command Policies**.

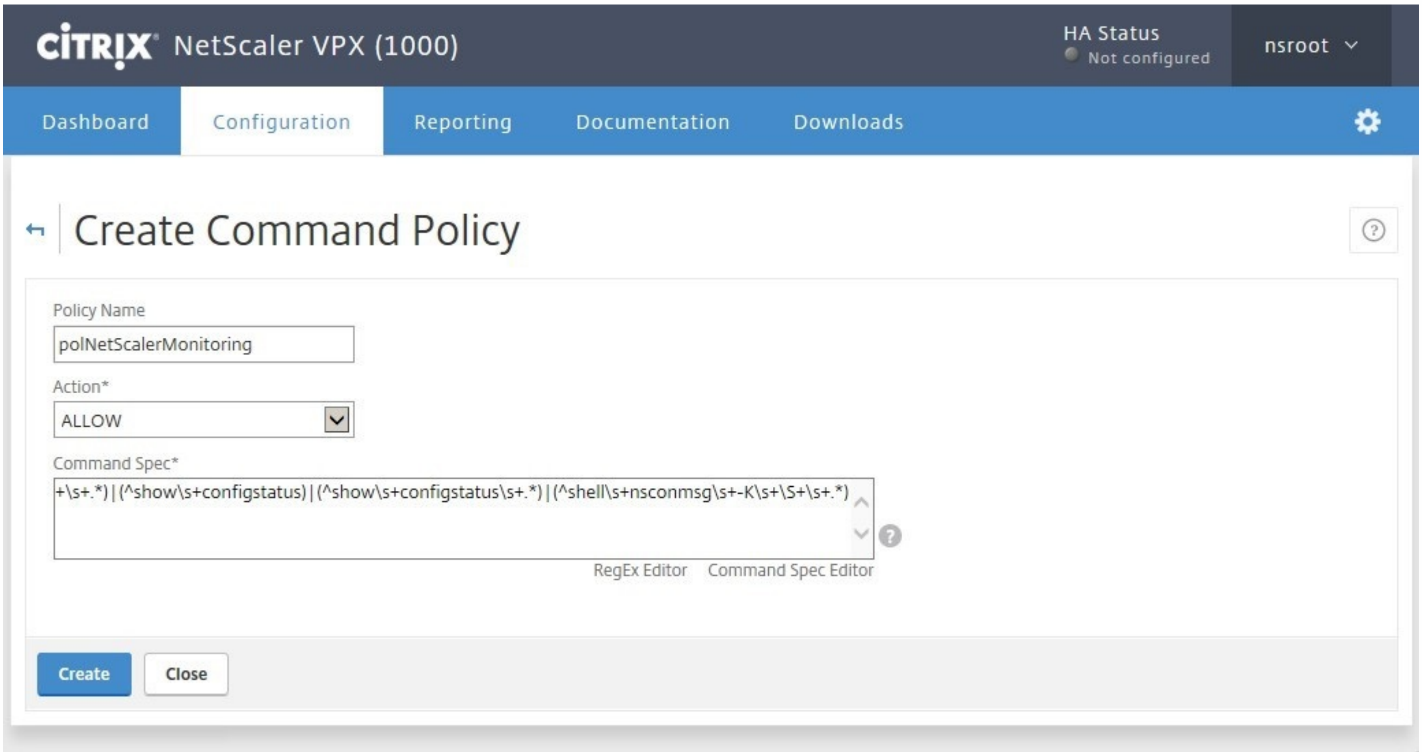
4. Add a new command policy with the following Command Spec regular expression:

```
(^show\s+system\s+\S+)|(^show\s+system\s+\S+\s+.*)|(^show\s+configstatus)|(^show\s+configstatus\s+.*)|(^shell\s+nsconmsg\s+-K\
```

For higher security, use the following regular expression:

```
(^show\s+system\s+\S+)|(^show\s+system\s+\S+\s+.*)|(^show\s+configstatus)|(^show\s+configstatus\s+.*)|(^shell\s+nsconmsg\s+-K\
```

This command policy grants permissions to execute some *show* commands as well as the *shell nsconmsg -K* command to access the console message log on the NetScaler. The permissions are read-only.



Create Command Policy

Policy Name
polNetScalerMonitoring

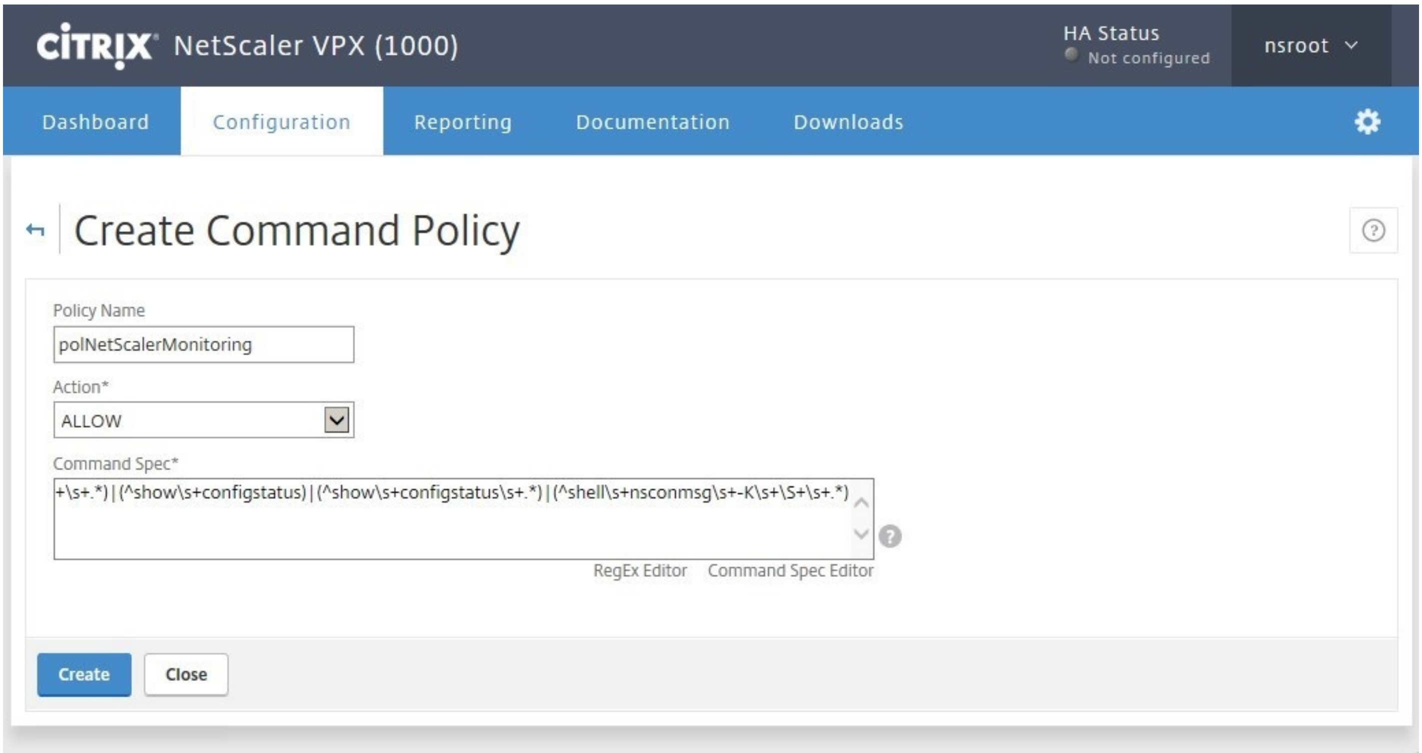
Action*
ALLOW

Command Spec*
+\s+.*)|(^show\s+configstatus)|(^show\s+configstatus\s+.*)|(^shell\s+nsconmsg\s+-K\s+\S+\s+.*)

5. Click **Create** to create the command policy.

Important: Steps 6 to 19 apply only in case of a non-LDAP authentication. Steps 20 to apply only in case of the LDAP authentication.

6. In the **System** > **User Administration** context, click **Users**.
7. Click **Add** to open the Add System User dialog.



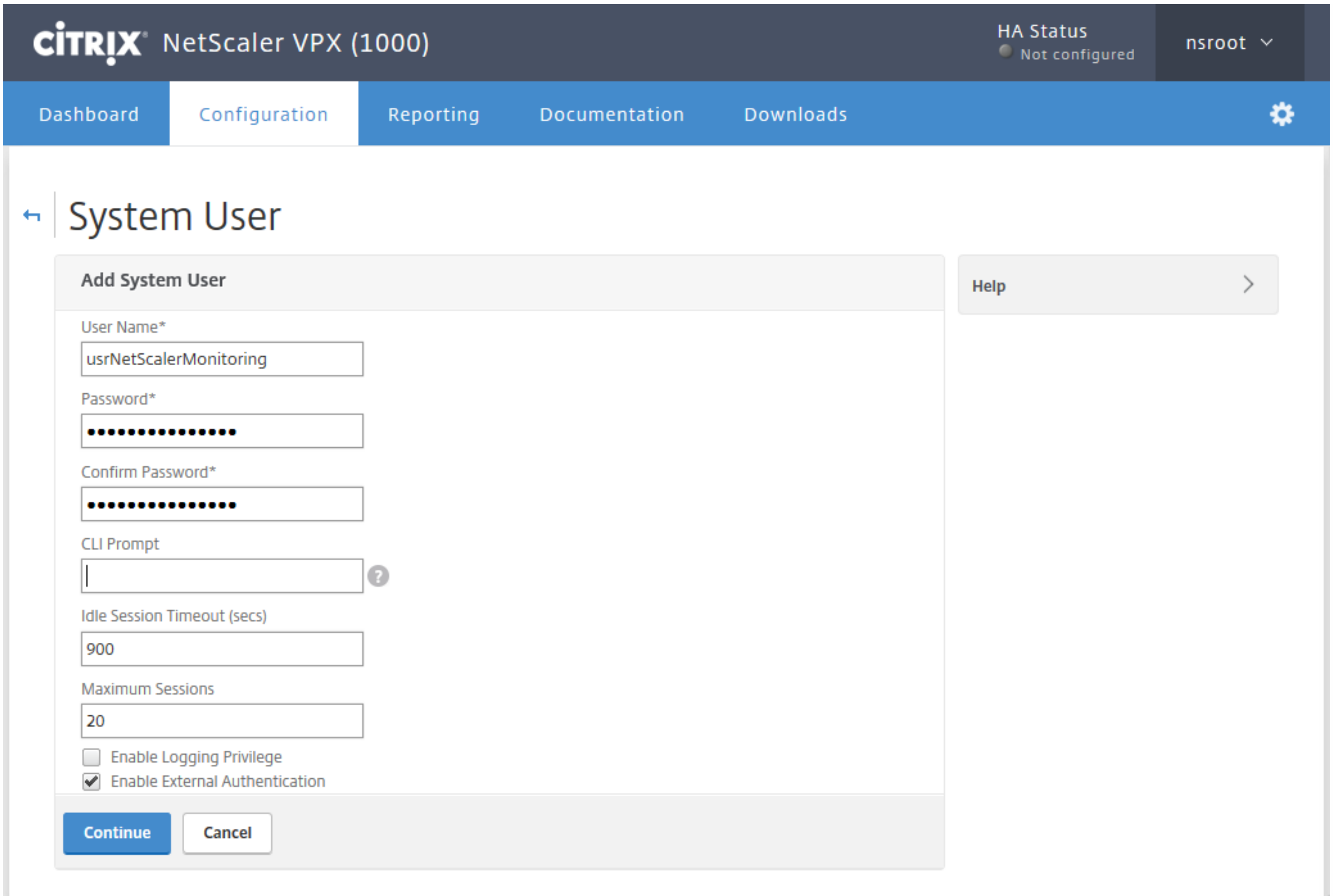
Policy Name
polNetScalerMonitoring

Action*
ALLOW

Command Spec*

```
+\s+.*)|(^show\s+configstatus)|(^show\s+configstatus\s+.*)|(^shell\s+nsconmsg\s+-K\s+\S+\s+.*)
```

8. Type the user name and password for the user account, and click **Continue**.
9. In the Bindings pane, expand **System Command Policy**.
10. In the User Command Policy Binding dialog, click **>**.



Add System User

User Name* usrNetScalerMonitoring

Password* ••••••••••••••••

Confirm Password* ••••••••••••••••

CLI Prompt

Idle Session Timeout (secs) 900

Maximum Sessions 20

☐ Enable Logging Privilege

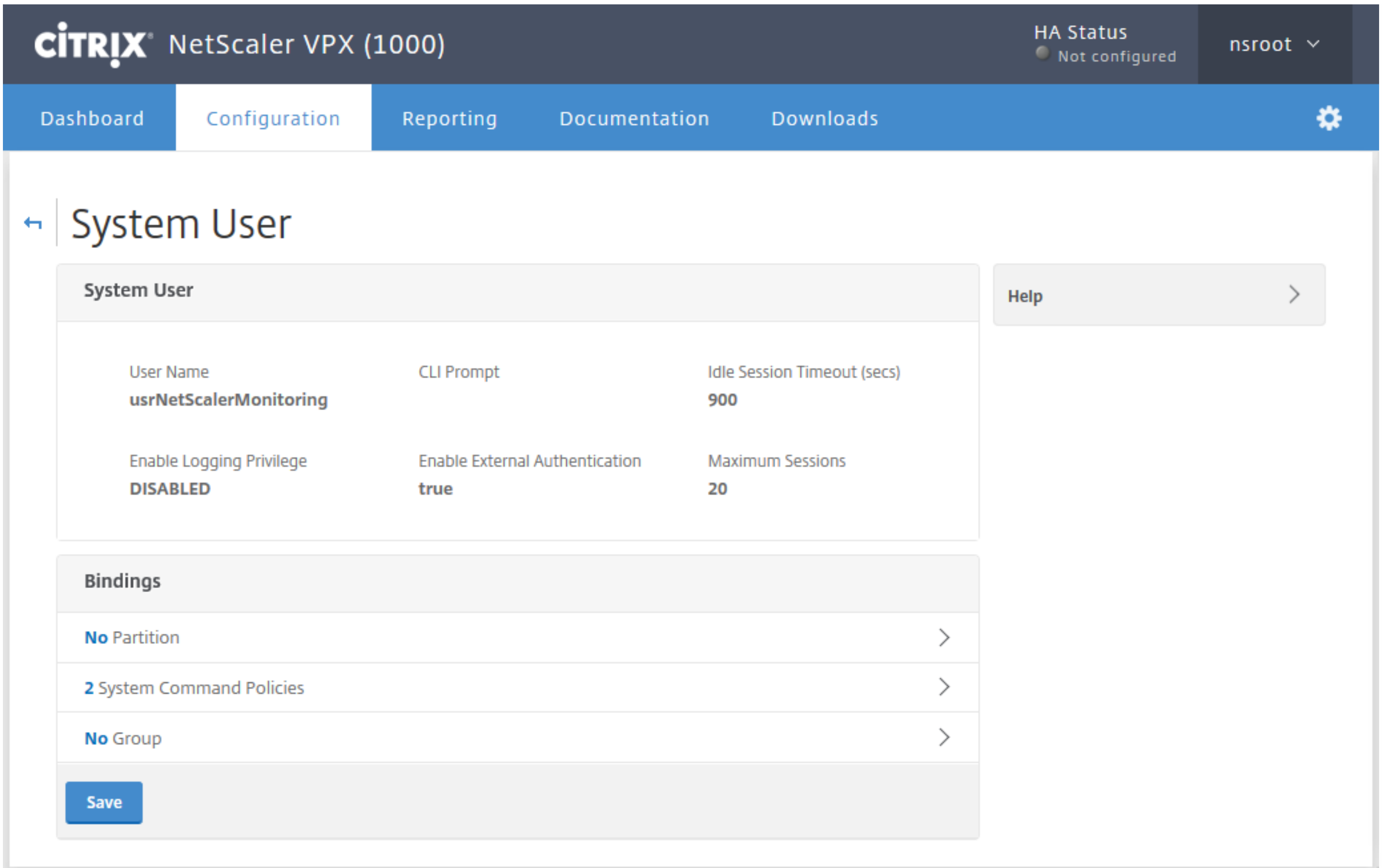
☑ Enable External Authentication

11. In the Command Policies dialog, select the command policy created in the previous steps, then click **Select**.
12. In the User Command Policy Binding dialog, set the **Priority** for the required command policies to *1*.
13. Click **Bind**.
14. In the System User dialog, in the Bindings pane, expand **System Command Policy**.
15. In the User Command Policy Binding dialog, click **Add Binding**, and then click **>**.
16. In the Command Policies dialog, select the *read-only* policy.

    The *read-only* command policy should be present in NetScaler by default. If the policy is missing, go back to step 3, create the *read-only* command policy and allow the following permissions:

```
(^man.*)|(^show\s+(?!system)(?!configstatus)(?!ns ns\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gslb runningConfig)(?!audit messages
```

17. In the User Command Policy Binding dialog, set the **Priority** for the required command policies to *1*.
18. Click **Bind**.
19. Click **Close** to close the dialog box, then click **Save** to save configuration of the new system user.



System User

System User

User Name: usrNetScalerMonitoring

CLI Prompt:

Idle Session Timeout (secs): 900

Enable Logging Privilege: DISABLED

Enable External Authentication: true

Maximum Sessions: 20

Important: Steps 20 to 22 apply only in case of the LDAP authentication.

20. Run the following command to create necessary authentication policy and perform global binding (the assumption is that the policy is named *Policy_LDAP*):

```
bind system global Policy_LDAP -priority 100
```

21. Run the following command to create a user group with the same name as the user group in your Active Directory (as an example, if the Active Directory user account for NetScaler monitoring belongs to the *NetScalerActiveDirectoryUserGroup* group, add the system group *NetScalerActiveDirectoryUserGroup* to NetScaler. The group must therefore exist on both sides: in NetScaler and in Active Directory Users and Computers):

```
add system group NetScalerActiveDirectoryUserGroup
```

22. Run the following commands to bind the same command policies to the group as described for the NetScaler user account:

```
bind system group NetScalerActiveDirectoryUserGroup -policy read-only 1

bind system group NetScalerActiveDirectoryUserGroup -policy polNetScalerMonitoring 1
```

The server-side part of Citrix SCOM Management Pack for NetScaler must be installed on the SCOM management server computer.

To install Citrix SCOM Management Pack for NetScaler on the SCOM management server computer, do the following:

1. Log on to the management server computer. Use a user account that has local administrative privileges and SCOM administrative privileges.
2. In Windows Explorer, locate the *Citrix_SCOM_Management_Pack_for_NetScaler_<Version>.exe* file (where *<Version>* is the current software version), and double-click it to invoke the installation process. Wait for the Setup Wizard to appear.
3. In the Welcome page of the Setup Wizard, click **Next**.

4. In the View Relevant Product Configuration page, click **Next**.
5. In the License Agreement page of the Setup Wizard, carefully read the end user license agreement. If you accept the terms of the agreement, click **Next**.

6. In the Destination Folder page, define the Citrix SCOM Management Pack for NetScaler installation folder. Citrix recommends that you install Citrix SCOM Management Pack for NetScaler to the default folder.
Proceed as follows:

- To install the product to the default folder listed in the Setup Wizard, no special actions are required.
- To install the product to a different folder, follow the substeps:
  1. Click **Change**.
  2. In the Browse For Folder dialog box, browse to the desired installation folder, select it, and click **OK**.

Click **Next**.
7. In the Configure Post-Install Actions page of the Setup Wizard, decide whether the Setup Wizard should automatically import the included management packs into SCOM.

To let the Setup Wizard import the management packs, select the **Automatically import the Management Pack** option.

To import the management packs into SCOM manually at a later time, leave the **Automatically import the Management Pack** option unselected. For instructions on how to import or reimport the management packs, see Manually importing included management packs into SCOM.

8. Click **Install**. The Setup Wizard displays the Installing the product page and starts copying the installation files.

9. After the installation completes, the installation completion page appears.

   If you let the Setup Wizard to automatically import the management packs, click **Next**. In the opposite case, click **Finish** to close the Setup Wizard, and skip the remaining steps of this procedure.

10. If you let the Setup Wizard to automatically import the management packs, it displays the Executing post-install actions page. Attend the import process.
11. In the post-installation completion page, if you let the Setup Wizard to automatically import the management packs, review the management packs import log. Click **Finish** to close the Setup Wizard.

Note: Steps of this procedure must be followed only once on a SCOM management server computer. In case you previously installed any Citrix SCOM Management Pack product (except Citrix SCOM Management Pack for License Server or Citrix SCOM Management Pack for XenServer) on the same computer, you do not need to repeat the steps.

To configure access to the shared folder for agent installation, do the following:

1. Log on to the SCOM management server computer. Use a user account that has local administrative privileges.
2. Choose a local user account (local to the computer with the shared folder) or a domain user account that will have access to the shared folder, for the purpose of agent deployment and configuration.

   Important: Citrix recommends creating a new, dedicated user account that you will use only for deployment of the Citrix SCOM Management Pack for NetScaler Agent to SCOM resource pool members.

3. Using an operating system administrative tool, add the user account to the local *CitrixMPShareUsers* user group.

To verify that the Citrix SCOM Management Pack for NetScaler installation on the SCOM management server computer is correct, do the following:

1. Log on to the management server computer.
2. Go to **Start** > **Control Panel** and click **Programs and Features** (actions of this step may differ on operating systems earlier than Windows Server 2016).
3. Check for the presence of the following entry in the Name column:
   Citrix SCOM Management Pack for NetScaler
4. To check if the *CitrixMPShare* shared folder is correctly configured, open a Command Prompt window and run the following commands in sequence (their outputs in case of success are also shown):

```
net share | findstr -i CitrixMPShare
```

```
CitrixMPShare

          %ProgramData%\Citrix\CitrixMPShare
```

```
net use \\<ManagementServerHostName>\CitrixMPShare

  /USER:<DomainName>\<UserName>
```

```
The command completed successfully
```

```
dir \\<ManagementServerHostName>\CitrixMPShare
```

```
<FolderContents>
```

In these instances, *%ProgramData%* refers to the actual value of this operating system variable. *<ManagementServerHostName>* is the name of the SCOM management server computer. *<DomainName>* is the domain or computer name and *<UserName>* is the name of the user account that you chose in step 2 of the procedure documented in “Configuring access to the shared folder for agent installation”. *<FolderContents>* is the list of the contents of the *CitrixMPShare* folder.

Note: The shared folder is vital for installation of the Citrix SCOM Management Pack for NetScaler Agent and deployment of its configuration to the SCOM resource pool members.

On each member of the SCOM resource pool that is chosen for NetScaler monitoring, SCOM agent must be configured to act as a proxy agent. This configuration enables the agent to relay or forward information from or about other computes and network devices to the SCOM management server.

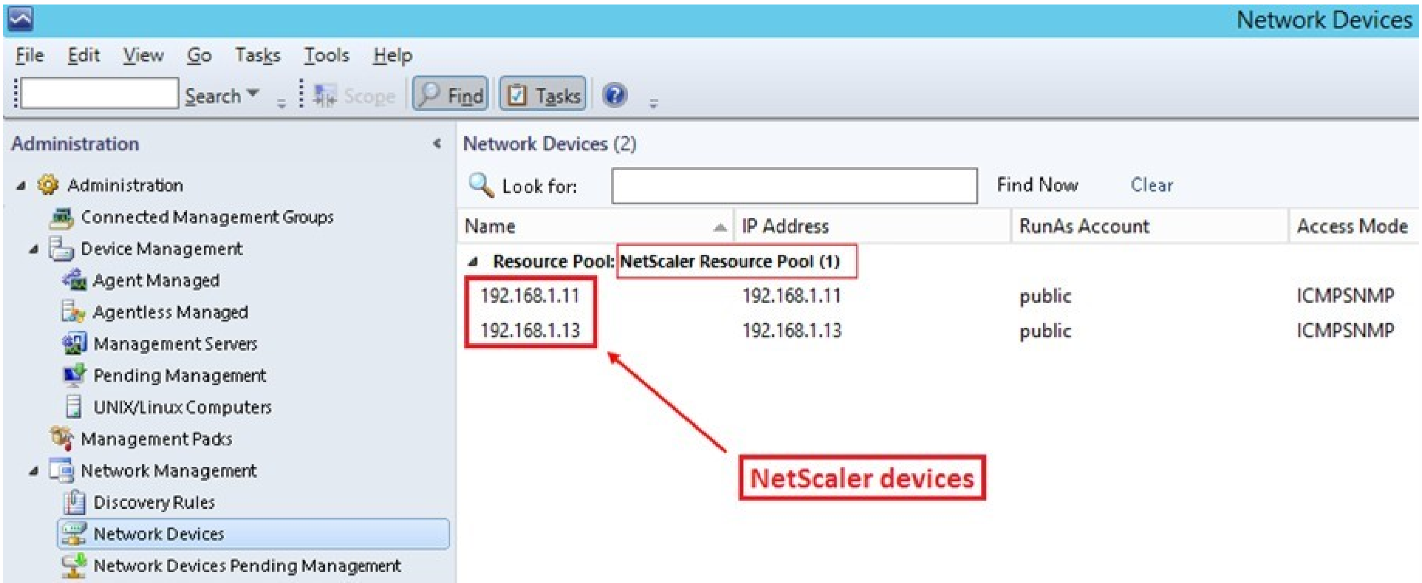
To configure the SCOM agent instances to act as proxy agents, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Administration** view, expand **Device Management**, and then click **Management Servers**.
3. For each management server computer, follow the steps:
   1. Right-click the host name, and select **Properties**.
   2. Click the **Security** tab.
   3. Select the **Allow this agent to act as proxy and discover managed objects on other computers** option.
   4. Click **OK**.

On all members of the SCOM resource pool that is chosen for NetScaler monitoring, Citrix SCOM Management Pack for NetScaler Agent must be installed.

To find the members of a resource pool and install Citrix SCOM Management Pack for NetScaler Agent on them, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Administration** view, expand **Device Management** > **Network Management**, and then click **Network Devices**.
3. Identify discovered NetScaler network devices and the corresponding resource pool names.



Network Devices (2)

Name	IP Address	RunAs Account	Access Mode
Resource Pool: NetScaler Resource Pool (1)			
192.168.1.11	192.168.1.11	public	ICMPSNMP
192.168.1.13	192.168.1.13	public	ICMPSNMP

NetScaler devices

4. For the identified resource pool, find out its members.

5. Log on to a member of the resource pool. Use a user account that has local administrative privileges.

6. Copy the *MPNSAgent.exe* file from the \\<*ManagementServeHostName*>*CitrixMPShare**NetScaler MP* shared folder to a location on the pool member.
7. In Windows Explorer, locate the *MPNSAgent.exe* file, and double-click it to invoke the installation process.
8. Follow instructions of the Setup Wizard.
9. Repeat steps 5 to 8 for each additional resource pool member.

To verify that the Citrix SCOM Management Pack for NetScaler Agent installation on a SCOM resource pool member is correct, do the following:

1. Log on to the SCOM resource member computer.
2. Go to **Start** > **Control Panel** and click **Programs and Features** (actions of this step may differ on operating systems earlier than Windows Server 2016).
3. Check for the presence of the following entry in the Name column:

   Citrix SCOM Management Pack Agent for NetScaler

4. Go to **Start** > **Administrative Tools** and double-click **Services**.
5. In the Name column of the Services window, locate the *Citrix MPNS Agent* service, and make sure that its status is to *Started*.

Tip: You can use Windows PowerShell to perform the verification. For example, to check if the program is correctly installed, run the following command:

```
Get-WmiObject -Class Win32_product | ? {$_.Name -match "NetScaler" -and $_.Name -match "Agent"}
```

For general instructions about how to import management packs into SCOM, see the How to Import an Operations Manager Management Pack webpage on the Microsoft TechNet website.

To import the sealed management packs for NetScaler, do the following:

1. Log on to the management server computer.
2. Launch the SCOM Operations console.
3. In the Administration view, click **Management Packs**.
4. In the Tasks pane, expand **Actions**, and then click **Import Management Packs**.
5. In the Import Management Packs dialog box, click **Add**, and then select **Add from disk**.
6. In the Online Catalog Connection dialog box, click **No**.
7. In the Select Management Packs to import dialog box, browse to the *%ProgramFiles%**Citrix**NetScaler MP* folder, select the following management pack files, and then click **Open**.

- Comtrade.Citrix.Library.mp
- Comtrade.Citrix.NetScaler.Appliance.9.Discovery.mp

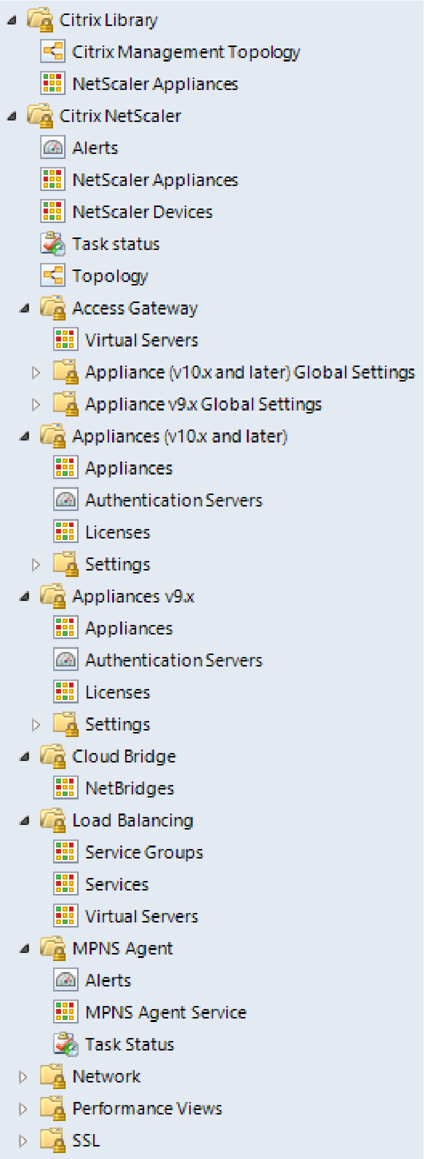
- Comtrade.Citrix.NetScaler.Appliance.9.Library.mp
- Comtrade.Citrix.NetScaler.Appliance.10.Discovery.mp
- Comtrade.Citrix.NetScaler.Appliance.10.Library.mp
- Comtrade.Citrix.NetScaler.Appliance.10.Monitoring.mp
- Comtrade.Citrix.NetScaler.Device.mp
- Comtrade.Citrix.NetScaler.Library.mp
- Comtrade.Citrix.NetScaler.Modules.mpb
- Comtrade.Citrix.NetScaler.Monitoring.mp

8. Click **Install**.

To verify that the import of the sealed management packs included in Citrix SCOM Management Pack for NetScaler was successful, do the following:

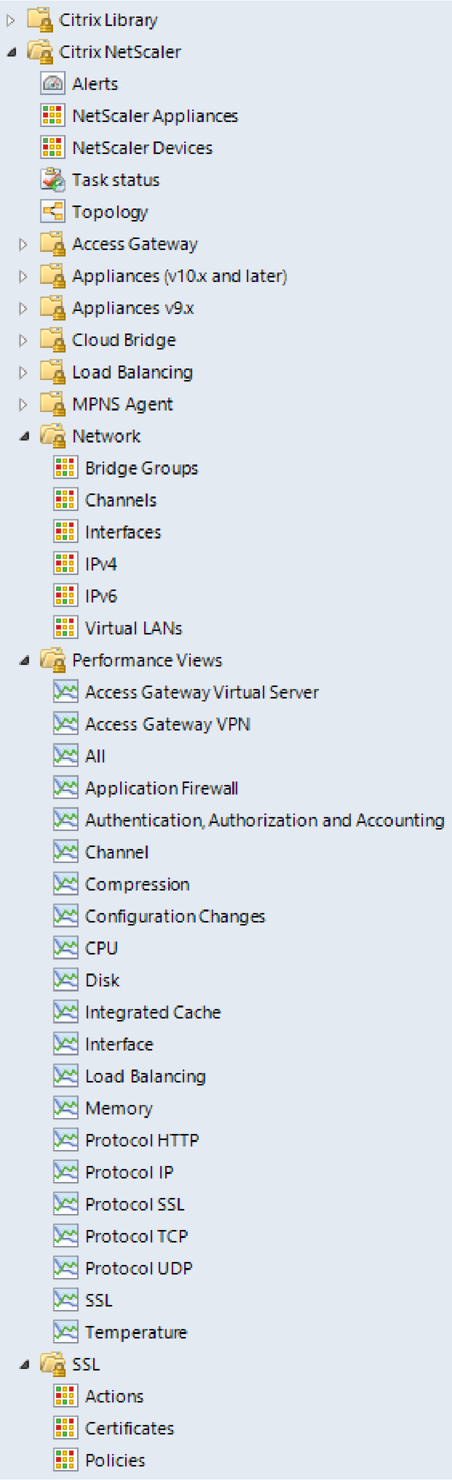
1. Launch the SCOM Operations console and connect to the management server.
2. In the **Monitoring** view, expand the items in the left pane until they match the following figure.

Elements of Citrix SCOM Management Pack for NetScaler, as seen in the SCOM Operations console (part 1)



- Citrix Library
  - Citrix Management Topology
  - NetScaler Appliances
- Citrix NetScaler
  - Alerts
  - NetScaler Appliances
  - NetScaler Devices
  - Task status
  - Topology
  - Access Gateway
    - Virtual Servers
    - Appliance (v10.x and later) Global Settings
    - Appliance v9.x Global Settings
  - Appliances (v10.x and later)
    - Appliances
    - Authentication Servers
    - Licenses
    - Settings
  - Appliances v9.x
    - Appliances
    - Authentication Servers
    - Licenses
    - Settings
  - Cloud Bridge
    - NetBridges
  - Load Balancing
    - Service Groups
    - Services
    - Virtual Servers
  - MPNS Agent
    - Alerts
    - MPNS Agent Service
    - Task Status
  - Network
  - Performance Views
  - SSL

Elements of Citrix SCOM Management Pack for NetScaler, as seen in the SCOM Operations console (part 2)



- Citrix Library
- Citrix NetScaler
  - Alerts
  - NetScaler Appliances
  - NetScaler Devices
  - Task status
  - Topology
  - Access Gateway
  - Appliances (v10.x and later)
  - Appliances v9.x
  - Cloud Bridge
  - Load Balancing
  - MPNS Agent
  - Network
    - Bridge Groups
    - Channels
    - Interfaces
    - IPv4
    - IPv6
    - Virtual LANs
  - Performance Views
    - Access Gateway Virtual Server
    - Access Gateway VPN
    - All
    - Application Firewall
    - Authentication, Authorization and Accounting
    - Channel
    - Compression
    - Configuration Changes
    - CPU
    - Disk
    - Integrated Cache
    - Interface
    - Load Balancing
    - Memory
    - Protocol HTTP
    - Protocol IP
    - Protocol SSL
    - Protocol TCP
    - Protocol UDP
    - SSL
    - Temperature
  - SSL
    - Actions
    - Certificates
    - Policies

3. In the **Administration** view, expand **Administration** > **Management Packs** and click **Installed Management Packs** (the navigation pane structure may differ in SCOM versions earlier than 2016).

4. Verify the following management pack versions are listed in the results pane:

Citrix Management Pack Library	1.0.32.0
Citrix NetScaler Appliance (v10.x and later) Component Library	1.17.87.0

Citrix NetScaler Appliance (v10.x and later) Discovery Library	1.17.87.0
Citrix NetScaler Appliance (v10.x and later) Monitoring Library	1.17.87.0
Citrix NetScaler Appliance (v9.x) Discovery Library	1.17.87.0
Citrix NetScaler Appliance (v9.x) Component Library	1.17.87.0
Citrix NetScaler Appliance Component Library	1.17.87.0
Citrix NetScaler Device Discovery Library	1.17.87.0
Citrix NetScaler Module Library	1.17.87.0
Citrix NetScaler Monitoring Library	1.17.87.0

To configure Run As account in SCOM, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Administration** view, in the left pane, expand **Run As Configuration**, and then click **Accounts**.
3. In the Tasks pane, expand **Actions**, and then click **Create Run As Account**.
4. In the Create Run As Account Wizard window, click **Next**.
5. In the General Properties page, from the **Run As account type** drop-down list, select **Basic Authentication**, **Simple Authentication**, or **Windows**. If you are using LDAP, select **Windows**.
6. In the **Display name** text box, type a name that the SCOM Operations console will use to refer to the newly created SCOM user account. Click **Next**.
7. In the Credentials page, type credentials of the user account that you used in Configuring NetScaler for monitoring by Citrix SCOM Management Pack for NetScaler in the respective text boxes. Click **Next**.
8. In the Distribution Security page, select a distribution security option. Citrix recommends that you select the **More secure** option.
9. Click **Create** to save configuration data of the new account.
10. Click **Close** to close the wizard.

To distribute the configured Run As account to NetScaler devices, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Administration** view, in the left pane, expand **Run As Configuration**, and then click **Profiles**.
3. In the results pane, in the Name column, double-click **Citrix NetScaler Appliance Action Account**.
4. In the Run As Profile Wizard window, click **Next** twice.
5. In the Run As Accounts page, click **Add**.
6. In the Add a Run as Account dialog box, from the Run As account drop-down list, select the display name of the newly

created Run As account.

7. Select either the **All targeted objects** (less secure) or **A selected class, group, or object** (more secure) option. For general information on the distribution methods, see the Distribution and Targeting for Run As Accounts and Profiles webpage on the Microsoft TechNet website.
   Note: The remaining steps of this procedure apply to the more secure distribution method.
8. Click **Select** and then select either **Class**, **Group**, or **Object**. The most appropriate choice depends on your NetScaler infrastructure.
   Note: The following few steps apply to the scenario when you select **Object**.
9. In the Object Search dialog box, from the Look for drop-down list, select **Node** and then click **Search**.
10. In the Available items list, select a NetScaler network device, and then click **Add**.
11. Repeat step 10 for each additional NetScaler network device that you plan to monitor.
12. Click **OK** to close the dialog box.
13. Click **OK** to close the Add a Run As Account dialog box.
14. Click **Save** to save the changes.
    Note: After saving the updated Run As profile, it may take some time for the updated configuration to become active on the targets. The required time depends on the state of the SCOM agent (*HealthService*) instances and overall load on the SCOM infrastructure.
15. If you selected the **More secure** option in step 9 of the previous procedure, validate the Run As account distribution:
    1. Under More-secure Run As accounts, click the Run As account.
    2. In the Run As Account Properties dialog box, review the Selected computers list.
    3. Click **OK** to close the dialog box.
16. Click **Close** to close the Run As Profile Wizard window.
17. If you selected the **More secure** option in step 9 of the previous procedure, do the following:
    1. In the **Administration** view, in the left pane, expand **Run As Configuration**, and then click **Accounts**.
    2. In the results pane, in the Name column, double-click the Run As account.
    3. Click the **Distribution** tab.
    4. Click **Add**.
    5. Decide which of the following to distribute the Run As account to:
       - All members of the resource pool that is designated for NetScaler device monitoring
       - The designated resource pool itself

       Citrix recommends that you choose the resource pool itself.

    f. In the Computer Search dialog box, from the Option drop-down list, select either **Show management servers** (for distribution to individual resource pool members) or **Search by resource pool name** (for distribution to the entire resource pool), and then click **Search**.

    g. Under Available items, select either all management servers of the designated resource pool (for distribution to individual resource pool members) or the resource pool itself (for distribution to the entire resource pool), and then click **Add**.

    h. Click **OK** to close the dialog box.

    i. Click **OK** to close the Run As Account Properties dialog box and save your changes.

For more information on Run As accounts and Run As profiles, see the Managing Run As Accounts and Profiles and How to Associate a Run As Account to a Run As Profile webpages on the Microsoft TechNet website.

Uninstall

This chapter contains instructions that you must follow to effectively uninstall Citrix SCOM Management Pack for NetScaler. Perform all procedures in the documented order of precedence.

Important: Perform this procedure only if you have customized the management packs included in the product.

To remove the customizations that you made to the management packs included in NetScaler Management Pack, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Administration** view, expand **Administration** > **Management Packs** and click **Installed Management Packs** (the navigation pane structure may differ in SCOM versions earlier than 2016).
3. In the results pane, locate the management packs that depend on the management packs included in NetScaler Management Pack.
4. For each such dependent management pack (except for *Microsoft.SystemCenter.SecureReferenceOverride*), follow the steps:
   1. Back up the management pack file.
   2. Right-click it and then click **Delete**.
   3. On the message stating that deleting the management pack might affect the scoping of some user roles, click **Yes**.

To remove the management packs included in Citrix SCOM Management Pack for NetScaler, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Administration** view, expand **Administration** > **Management Packs** and click **Installed Management Packs** (the navigation pane structure may differ in SCOM versions earlier than 2016).
3. Remove references to the included management packs from the *Microsoft.SystemCenter.SecureReferenceOverride* management pack. To do this, perform the following steps:
   1. Identify which included management packs are referenced. In the **Administration** > **Management Packs** context of the SCOM Operations console, right-click **Microsoft.SystemCenter.SecureReferenceOverride** and select **Properties**. In the dialog box, click the **Dependencies** tab.
   2. For each such referenced management pack, find out its ID. Right-click the referenced management pack. In the dialog box, take note of the value in the ID text box on the General tab.
   3. Export the *Microsoft.SystemCenter.SecureReferenceOverride* management pack.
   4. Make a copy of the file you exported the management pack to.
   5. Edit the originally exported file to remove all dependencies to the management packs from the **Manifest** > **References** context (the *Reference* elements) and the **Monitoring** > **Overrides** context (the *SecureReferenceOverride* elements), and then save the changes.
      Tip: For better tracking, increase the management pack version by adjusting the value of the *Version* element within the *Identity* element.
   6. Import back the altered *Microsoft.SystemCenter.SecureReferenceOverride* management pack from the modified file.

4. In the SCOM Operations console, in the results pane, right-click **Citrix NetScaler Appliance (v10.x and later) Monitoring Library**.
5. On the message stating that deleting the management pack might affect the scoping of some user roles, click **Yes**.
6. Repeat steps 4 and 5 with the following management packs (in the presented order of precedence):

- Citrix NetScaler Appliance (v10.x and later) Discovery Library

- Citrix NetScaler Appliance (v10.x and later) Monitoring Library
- Citrix NetScaler Appliance (v9.x) Discovery Library
- Citrix NetScaler Appliance (v10.x and later) Component Library
- Citrix NetScaler Appliance (v9.x) Component Library
- Citrix NetScaler Monitoring Library
- Citrix NetScaler Appliance Component Library
- Citrix NetScaler Device Discovery Library
- Citrix NetScaler Module Library

7. Check if other Citrix SCOM Management Pack products are installed on the management server computer. If none of them is installed, repeat steps 4 and 5 with **Citrix Management Pack Library**.

To uninstall Citrix SCOM Management Pack for NetScaler Agent from a member of a resource pool, do the following:

1. Log on to the member of the resource pool. Use a user account that has local administrative privileges.
2. Make sure no product folders or files are in use by any user.
3. Go to **Start** > **Control Panel** and click **Programs and Features** (actions of this step may differ on operating systems earlier than Windows Server 2016).
4. Right-click **Citrix SCOM Management Pack Agent for NetScaler** and select **Uninstall**.
5. In the Programs and Features dialog box, click **Yes** to confirm uninstallation.

To uninstall Citrix SCOM Management Pack for NetScaler from the SCOM management server computer, do the following:

1. Log on to the management server computer. Use a user account that has local administrative privileges and SCOM administrative privileges.
2. Make sure no product folders or files are in use by any user.
3. Check if the *.mpb* file that was installed by the product is locked by any program, for example, SCOM Operations console or Windows PowerShell. This includes programs in both active and disconnected sessions. If the file is locked, exit the locking program, for example, exit the SCOM Operations console or close the Windows PowerShell window.
   Tip: To check if a file is locked, try renaming it and then reverting to its original file name. Inability to rename the file indicates a locking program. You can identify it by using the Handle utility of Sysinternals Suite (see the Handle webpage on the Microsoft TechNet website).
4. Go to **Start** > **Control Panel** and click **Programs and Features** (actions of this step may differ on operating systems earlier than Windows Server 2016).
5. Right-click **Citrix SCOM Management Pack for NetScaler** and select **Uninstall**. Wait for the Setup Wizard to appear.
6. In the Welcome page of the Setup Wizard, click **Uninstall**.
7. In the Uninstalling the product page, the Setup Wizard reports the uninstallation progress.
8. In the Completion page of the Setup Wizard, click **Finish**.
9. Delete the *%ProgramData%\Citrix\CitrixMPShare\NetScaler MP* folder.
   Caution: This action permanently deletes the Agent configuration data. You will be unable to reuse it at a later time.
10. Check if other Citrix SCOM Management Pack products are installed on the management server computer. If none of them is installed, follow the steps:
    1. Stop sharing the *CitrixMPShare* shared folder.
    2. Delete the *%ProgramData%\Citrix\CitrixMPShare* folder.

3. Using an operating system administrative tool, delete the local *CitrixMPShareUsers* user group.

Optimize

May 21, 2017

Optional configuration

Some monitors and rules have default thresholds that might need additional tuning to suit your environment. You should evaluate monitors and rules to determine whether the default thresholds are appropriate for your environment. If a default threshold is not appropriate for your environment, you should adjust the threshold by overriding it.

In the Citrix SCOM Management Pack for NetScaler Reference Guide, you can find details about the following items:

- Discoveries
- Monitors
- Roll-up Monitors
- Rules
- Tasks
- Scripts
- Defaults with regard to enabled and disabled items
- Adjustable parameters and their default values

For general information about discovering objects in SCOM, see the “Object Discoveries” section of the What Is in an Operations Manager Management Pack? webpage on the Microsoft TechNet website.

The following table lists the object types that Citrix SCOM Management Pack for NetScaler discovers in the monitored environment.

Object type	Description
AAA	An Authentication Authorization Auditing object.
Access Gateway	The root object for Access Gateway.
Access Gateway Virtual Server	The Access Gateway Virtual Server object.
Action	An Action object.
Authentication Server	An Authentication Server object.
Bridge	A Bridge object.

Channel	A Channel object.
Cloud Bridge	A group of NetBridge objects.
Group	A group of related objects.
Interface	An Interface object.
IP	A group of IPv4 and IPv6 objects.
LDAP Policy	A LDAP Policy object.
LDAP Server	A LDAP Server object.
License	A License object.
Load Balancing	The root object for Load Balancing.
Load Balancing Virtual Server	A Load Balancing Virtual Server object.
Memory Pool	A Memory Pool object.
NetBridge	A Network Bridge object.
NetScaler Appliance	The root object for topology of NetScaler appliance.
Network	A Network object.
Policy	A Policy object.
Radius Policy	A RADIUS Policy object.
Radius Server	A RADIUS Server object.
Service	A Service object.
Service Group	A Service Group object.

Settings	HTTP, Global, Timeout, Feature, Modes, TCP, and other settings.
SSL	An SSL object.
SSL Action	An SSL Action object.
SSL Certificate	An SSL Certificate object.
SSL Policy	An SSL Policy object.
System	A System object.
TACACS Policy	A TACACS Policy object.
Traffic Management	The Root object for Traffic Management.
VLAN	A Virtual LAN object.

Customizing sealed management packs

Similarly to customizing the default SCOM management pack, you can customize the sealed management packs that Citrix SCOM Management Pack for NetScaler provides. For details, see the Microsoft TechNet website:

- For general information about customization of management packs, see the Customizing Management Packs webpage.
- For instructions on how to customize a management pack, see the Create a New Management Pack for Customizations webpage.