Citrix SCOM Management Pack for NetScaler User Guide

Software version: 1.15
Release date: June 2016

This document provides installation, configuration, and usage instructions for Citrix SCOM Management Pack for NetScaler.

Legal notices
Copyright © 2016 Citrix Systems, Inc. All rights reserved.

Citrix, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309
United States of America

Disclaimers
This document is furnished "AS IS." Citrix, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix, Inc. and its licensors, and are furnished under a license from Citrix, Inc.

Citrix Systems, Inc., the Citrix logo, and NetScaler are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark office and in other countries. All other trademarks and registered trademarks are property of their respective owners.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
Contents

Chapter 1: Brief introduction ................................................................. 3
  About NetScaler Management Pack ..................................................... 3
  Product architecture ......................................................................... 6

Chapter 2: Installation and configuration ........................................... 8
  Preparing for the installation ............................................................. 8
  Configuring NetScaler for monitoring by NetScaler Management Pack ..... 10
  Installing the product on the SCOM management server computer ...... 16
  Configuring access to the shared folder for agent installation ............. 19
  Verifying the installation on the SCOM management server computer ... 20
  Installing the product on the SCOM resource pool members ............... 21
  Verifying the installation on the SCOM resource pool members .......... 22
  Manually importing included management packs into SCOM .......... 23
  Verifying the import of the included management packs .................. 24
  Configuring the NetScaler Appliance action account in SCOM .......... 26

Chapter 3: Uninstallation ....................................................................... 29
  Removing dependent management packs (customizations) .................. 29
  Removing included management packs .......................................... 29
  Uninstalling the product from the SCOM resource pool members ....... 31
  Uninstalling the product from the SCOM management server computer .. 31

Chapter 4: Usage ............................................................................... 32
  Optional configuration ................................................................... 32
  Customizing sealed management packs ....................................... 36

Chapter 5: Support ........................................................................... 36
  General support resources ............................................................... 36
  Contacting Citrix Customer Service ................................................. 36
Chapter 1: Brief introduction

About NetScaler Management Pack

Citrix SCOM Management Pack for NetScaler (NetScaler Management Pack) 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 NetScaler Management Pack 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

NetScaler Management Pack 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*

NetScaler Management Pack 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**

NetScaler Management Pack 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**

NetScaler Management Pack 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.

**Product architecture**

The following diagram shows how NetScaler Management Pack is deployed on SCOM management platform.
NetScaler Management Pack 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 NetScaler Management Pack Agent. It is designed to act as a layer between the management packs and the NetScaler instances in the monitoring process. All requests initiated by NetScaler Management Pack 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 instances, and collects and caches data from these instances. 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. NetScaler Management Pack Agent must reside on all members of a resource pool.

---

Chapter 2: Installation and configuration

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

**Preparing for the installation**

Before installing NetScaler Management Pack, make sure the following prerequisites are fulfilled:

- Your environment meets the software requirements.
  For software requirements, see the *Citrix SCOM Management Pack for NetScaler Compatibility Matrix*.
- A SCOM management server computer is chosen where the server side of NetScaler Management Pack will be installed. This computer is referred to as **SCOM management server computer**.
- A SCOM resource pool is chosen for NetScaler monitoring. For easier deployment of NetScaler Management Pack Agent and decreased SCOM resource usage, Citrix recommends that this is a custom resource pool (a resource pool designated to monitor NetScaler devices).
- A 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 NetScaler Management Pack 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 select 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
• All members of the SCOM resource pool that is designated for NetScaler device monitoring are configured to discover managed objects on other entities. Such configuration of a resource pool member requires that the **Allow this server to act as proxy and discover managed objects on other computers** option is selected for it. To check this, launch the SCOM Operations console and navigate to **Administration view > Device Management > Management Servers > Properties > Security** property page.

**Configuring NetScaler for monitoring by NetScaler Management Pack**

In order to access and communicate with NetScaler, NetScaler Management Pack needs a NetScaler user account with proper privileges. This 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.

**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 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:

   ```bash
   add system cmdPolicy polNetScalerMonitoring ALLOW
   (^show\s+system\s+\s+\s+)\|\(^show\s+system\s+\s+\s+s+.*)\|\(^show\s+configstatus\s+.*)\|\(^show\s+configstat\s+\s+.*)\|\(^show\s+configstatus\s+.*)\|\(^shell\s+nsconmsg\s+-K\s+s+\s+.*)
   ``

   For higher security, run the following command instead:

   ```bash
   add system cmdPolicy polNetScalerMonitoring ALLOW
   (^show\s+system\s+\s+\s+)\|\(^show\s+system\s+\s+\s+s+.*)\|\(^show\s+configstatus\s+.*)\|\(^show\s+configstat\s+\s+.*)\|\(^shell\s+nsconmsg\s+-K\s+s+\s+.*)\|\(^shell\s+nsconmsg\s+-K\s+/var/nslog/newnslog\s+-d\s+\s+sconmsg\s+-d\s+grep\s+-E\s+'IP\s+address\s+conflict\|current\s+time')
   ``

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

   ```bash
   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 messages)(!\!techsupport).*)|(^stat.*)
```

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 10.1. 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.
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:

   \(^\text{show}\{s+system\{s+}\}\{s+\}\)\|(\^\text{show}\{s+system\{s+\}\{s+\}\{s+\}\})\|(\^\text{show}\{s+configstatus\}\{s+\})\|(\^\text{show}\{s+configstatus\}\{s+\})\|(\^\text{shell}\{s+nsconmsg\}\{s+-K\{s+\}\{s+\}\})\|(\^\text{shell}\{s+nsconmsg\}\{s+-K\{s+/\}\{s+\}\{s+\}\{s+\}\})

   For higher security, use the following regular expression:

   \(^\text{show}\{s+system\{s+\}\}\{s+\}\)\|(\^\text{show}\{s+system\{s+\}\{s+\}\{s+\}\})\|(\^\text{show}\{s+configstatus\}\{s+\})\|(\^\text{show}\{s+configstatus\}\{s+\})\|(\^\text{shell}\{s+nsconmsg\}\{s+-K\{s+/\}\{s+\}\{s+\}\})\|(\^\text{shell}\{s+nsconmsg\}\{s+-K\{s+/\}\{s+\}\{s+\}\{s+\}\})\|(\^\text{grep}\{s+IP\{s+address\}\{s+conflict\}\{s+\}current\{s+\}time\})

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

6. Click **Close** to close the Create Command Policy dialog box.

   *Important* Steps 7 to 13 apply only in case of a non-LDAP authentication. Steps 14 to 16 apply only in case of the LDAP authentication.

7. From the **System [User Administration]** menu select the **Users** node.

8. Click **Add** to open the Create System User dialog.

9. Type the user name and password for the user account.

10. In the Command Policies section, insert or select the command policy created in the previous steps as well as the read-only policy. The **read-only** command policy should be present in NetScaler by default. If the **read-only** policy is missing, go back to step 3, create the **read-only** command policy and allow the following permissions:
Figure 2.3  Creating a system user in NetScaler

Figure 2.4  The Insert Command Policies dialog box
11. In the Create System User dialog set the **Priority** for the required command policies to 1.

12. Click **Create** to create the user account.

13. Click **Close** to close the dialog box.

**Important**  Steps 14 to 16 apply only in case of the LDAP authentication.

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

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

15. 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):

```plaintext
add system group NetScalerActiveDirectoryUserGroup
```
16. 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 \
polNetScalerMonitorin
```

**Installing the product on the SCOM management server computer**

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

To install NetScaler Management Pack 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**.

![Initial Setup Wizard page of NetScaler Management Pack](image)
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**.

**Figure 2.7** The License Agreement page


   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:
     a. Click **Change**.
     b. In the Browse For Folder dialog box, browse to a 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 about how to import or reimimport 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 is displayed.
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, click Finish to close the Setup Wizard.

Configuring access to the shared folder for agent installation

**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 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 Management Pack agent to managed computers.

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

Verifying the installation on the SCOM management server computer
To verify that the NetScaler Management Pack 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**, click **Programs**, and then click **Programs and Features**.

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):
   
   **Command:**
   
   net share | findstr -i CitrixMPShare

   **Command output:**
   
   `CitrixMPShare $ProgramData%\Citrix\CitrixMPShare`

   **Command:**
   
   net use \\<ManagementServerHostName>\CitrixMPShare /USER:<DomainName>\<UserName>

   **Command output:**
   
   The command completed successfully

   **Command:**
   
   dir \\<ManagementServerHostName>\CitrixMPShare

   **Command output:**
   
   `<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 communication between the management server and the agent-managed computers during installation of the agent.

**Installing the product on the SCOM resource pool members**

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

To install the product on the members of a resource pool, 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.

   **Figure 2.10** NetScaler network devices in the SCOM Operations console

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.

Verifying the installation on the SCOM resource pool members
To verify that the NetScaler Management Pack 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, click Programs, and then click Programs and Features.

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.
In the Name column of the Services window, locate the **Citrix MPNS Agent** service, and make sure that its status is to **Started**.

---

**Manually importing included management packs into SCOM**

For general instructions about how to import management packs into SCOM, see the [How to Import an Operations Manager Management Pack](https://technet.microsoft.com/en-us/library/qq442866.aspx) 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.Library.mp

8. Click **Install**.

---
Verifying the import of the included management packs

To verify that the import of the sealed management packs included in NetScaler Management Pack 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.

Figure 2.12 Elements of NetScaler Management Pack, as seen in the SCOM Operations console (part 1)
Figure 2.13 Elements of NetScaler Management Pack, as seen in the SCOM Operations console (part 2)
Configuring the NetScaler Appliance action account in SCOM

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 NetScaler Management Pack” 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 assign 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 middle 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](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/xqkbz8v6) 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 all specified computers. 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:

    a. Under More-secure Run As accounts, click the Run As account.

    b. In the Run As Account Properties dialog box, review the Selected computers list.

    c. 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:
a. In the **Administration** view, in the left pane, expand **Run As Configuration**, and then click **Accounts**.

b. In the middle pane, in the Name column, double-click the Run As account.

c. Click the **Distribution** tab.

d. Click **Add**.

e. 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.
Chapter 3: Uninstallation

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

Removing dependent management packs (customizations)

**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, click **Management Packs**.
3. In the middle 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:
   a. Back up the management pack file.
   b. Right-click it and then click **Delete**.
   c. On the message stating that deleting the management pack might affect the scoping of some user roles, click **Yes**.

Removing included management packs

To remove 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, click **Management Packs**.
3. Remove references to the included management packs from the Microsoft.SystemCenter.SecureReferenceOverride management pack. To do this perform the following steps:
a. 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.

b. 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.


d. Make a copy of the file you exported the management pack to.

e. 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.

f. Import back the altered Microsoft.SystemCenter.SecureReferenceOverride management pack from the modified file.

4. In the SCOM Operations console, in the middle 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**.

**Uninstalling the product from the SCOM resource pool members**

To uninstall NetScaler Management Pack 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**, click **Programs**, and then click **Programs and Features**.

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.

**Uninstalling the product from the SCOM management server computer**

To uninstall NetScaler Management Pack 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](https://docs.microsoft.com/en-us/sysinternals/downloads/handle) webpage on the Microsoft TechNet website).

4. Go to **Start > Control Panel**, click **Programs**, and then click **Programs and Features**.

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. Check if other Citrix SCOM Management Pack products are installed on the management server computer. If none of them is installed, follow the steps:

   a. Stop sharing the **CitrixMPShare** shared folder.

   b. Delete the $ProgramData$\Citrix\CitrixMPShare folder.

   __Caution__ This action permanently deletes the Agent configuration data. You will be unable to reuse it at a later time.

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

---

**Chapter 4: Usage**

**Optional configuration**

_Tuning thresholds for performance monitors and rules_

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 baseline the relevant performance counters, and then adjust the threshold by overriding them.

In the *Citrix SCOM Management Pack for NetScaler Reference Guide*, which you can find in the Citrix_MPNS_ReferenceGuide.html file, you can find details about the following items:

- Discoveries
- Monitors
- Roll-up Monitors
- Rules
- Tasks
- Scripts
- Enabled and disabled items by default
Discovering objects

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 NetScaler Management Pack discovers in the managed environment.

Table 4.1 Discovered NetScaler object types

<table>
<thead>
<tr>
<th>Object type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>An Action object.</td>
</tr>
<tr>
<td>Authentication Server</td>
<td>An Authentication Server object.</td>
</tr>
<tr>
<td>Bridge</td>
<td>A Bridge object.</td>
</tr>
<tr>
<td>Channel</td>
<td>A Channel object.</td>
</tr>
<tr>
<td>Cloud Bridge</td>
<td>A group of NetBridge objects.</td>
</tr>
<tr>
<td>Group</td>
<td>A group of related objects.</td>
</tr>
<tr>
<td>Object</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Interface</td>
<td>An Interface object.</td>
</tr>
<tr>
<td>IP</td>
<td>A group of IPv4 and IPv6 objects.</td>
</tr>
<tr>
<td>LDAP Policy</td>
<td>A LDAP Policy object.</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>A LDAP Server object.</td>
</tr>
<tr>
<td>License</td>
<td>A License object.</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>The root object for Load Balancing.</td>
</tr>
<tr>
<td>Load Balancing Virtual Server</td>
<td>A Load Balancing Virtual Server object.</td>
</tr>
<tr>
<td>Memory Pool</td>
<td>A Memory Pool object.</td>
</tr>
<tr>
<td>NetBridge</td>
<td>A Network Bridge object.</td>
</tr>
<tr>
<td>NetScaler Appliance</td>
<td>The root object for topology of NetScaler appliance.</td>
</tr>
<tr>
<td>Network</td>
<td>A Network object.</td>
</tr>
<tr>
<td>Policy</td>
<td>A Policy object.</td>
</tr>
<tr>
<td>Radius Policy</td>
<td>A RADIUS Policy object.</td>
</tr>
<tr>
<td>Object</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Radius Server</td>
<td>A RADIUS Server object.</td>
</tr>
<tr>
<td>Service</td>
<td>A Service object.</td>
</tr>
<tr>
<td>Service Group</td>
<td>A Service Group object.</td>
</tr>
<tr>
<td>Settings</td>
<td>HTTP, Global, Timeout, Feature, Modes, TCP, and other settings.</td>
</tr>
<tr>
<td>SSL</td>
<td>An SSL object.</td>
</tr>
<tr>
<td>SSL Action</td>
<td>An SSL Action object.</td>
</tr>
<tr>
<td>SSL Certificate</td>
<td>An SSL Certificate object.</td>
</tr>
<tr>
<td>SSL Policy</td>
<td>An SSL Policy object.</td>
</tr>
<tr>
<td>System</td>
<td>A System object.</td>
</tr>
<tr>
<td>TACACS Policy</td>
<td>A TACACS Policy object.</td>
</tr>
<tr>
<td>Traffic Management</td>
<td>The Root object for Traffic Management.</td>
</tr>
<tr>
<td>VLAN</td>
<td>A Virtual LAN object.</td>
</tr>
</tbody>
</table>
Customizing sealed management packs
Similarly to customizing the default SCOM management pack, you can customize the sealed management packs that NetScaler Management pack 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.

Chapter 5: Support

General support resources
Citrix® offers a variety of resources for support with your Citrix environment, including the following:

- The Knowledge Center is a self-service, Web-based technical support database that contains thousands of technical solutions, including access to the latest hotfixes, service packs, and security bulletins.
- Technical Support Programs for both software support and appliance maintenance are available at a variety of support levels.
- The Subscription Advantage program is a one-year membership that gives you an easy way to stay current with the latest product version upgrades and enhancements.
- Citrix Education provides official training and certification programs on virtually all Citrix products and technologies.

For more information about Citrix services and support, see the Citrix Support Services and Resources website.

You can also participate in and follow technical discussions offered by the experts on various Citrix products at the Welcome to the Citrix Community, Citrix Discussions, and Citrix Services websites.

Contacting Citrix Customer Service
To contact Citrix Customer Service, see the Contact Support website.