

NetScaler Management and Analytics Service

Jun 29, 2017

NetScaler Management and Analytics Service (NetScaler MA Service) provides an easy and scalable solution to manage NetScaler deployments that include Citrix NetScaler MPX, Citrix NetScaler VPX, Citrix NetScaler Gateway, Citrix NetScaler SDX, Citrix NetScaler CPX, and Citrix NetScaler SD-WAN appliances that are deployed on-premises or on the cloud.

You can use this cloud solution to manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified, and centralized cloud based console.

NetScaler MA Service provides all the capabilities required to quickly set up, deploy, and manage application delivery in NetScaler deployments and with rich analytics of application health, performance, and security.

NetScaler MA Service provides the following benefits:

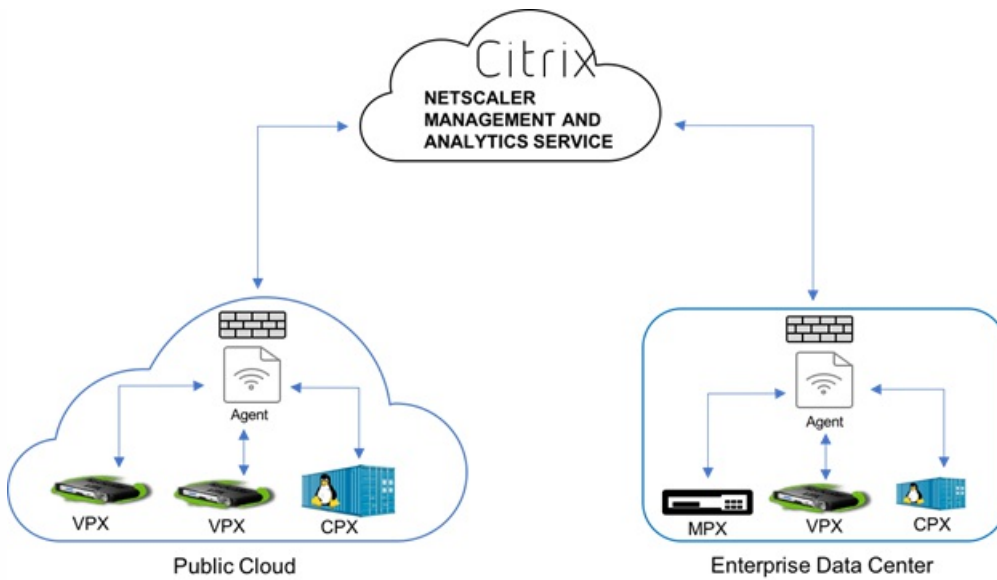
- **Agile** – Easy to operate, update, and consume. The service model of NetScaler MA Service is available over the cloud, making it is easy to operate, update, and use the features provided by NetScaler MA Service. The frequency of updates, combined with the automated update feature, quickly enhances your NetScaler deployment.
- **Faster time to value** – Quicker business goals achievement. Unlike with the traditional on-premises deployment, you can use your NetScaler MA Service with a few clicks. You not only save the installation and configuration time, but also avoid wasting time and resources on potential errors.
- **Multi-Site Management** – Single Pane of Glass for instances across Multi-Site data centers. With the NetScaler MA Service, you can manage and monitor NetScaler ADCs that are in various types of deployments. You have one-stop management for NetScaler ADCs deployed on premises and in the cloud.
- **Operational Efficiency** – Optimized and automated way to achieve higher operational productivity. With the NetScaler MA Service, your operational costs are reduced by saving your time, money, and resources on maintaining and upgrading the traditional hardware deployments.

How NetScaler MA Service Manages your Deployment

NetScaler MA Service is available as a service on the Citrix Cloud. After you sign up for Citrix cloud and start using this service, you have to install agents in your network environment, and then add the instances you want to manage to the service.

An agent enables communication between the NetScaler MA Service and the managed instances in your data center. The agent collects data from the managed instances in your network and sends it to the NetScaler MA Service. When you add an instance to NetScaler MA Service, the service implicitly adds itself as a trap destination for the instance and collects inventory of the instance. It collects instance details such as host name, software version, running and saved configuration, certificate details, entities configured on the instance, and so on. NetScaler MA Service periodically polls managed instances to collect information.

The following image illustrates the communication between the service, agents, and instances:



Documentation Guide

The NetScaler MA Service documentation includes information about how to get started with the service, list of features supported on the service, and configuration specific to this service solution. The NetScaler MAS documentation covers the latest on-premises release of NetScaler MAS and provides detailed information about all features. For details about using the features supported on NetScaler MA Service, see the articles under [NetScaler MAS 12.0](#).

Features and Solutions

Jun 29, 2017

NetScaler Management and Analytics Service (NetScaler MA Service) is compatible with most of the features that are available with the on-premises version of NetScaler MAS. This document describes the features that are supported on the service.

The following table describes the features that are available on NetScaler MA Service:

Feature	Description
Application Analytics and Management	<p>Application Analytics and Management feature of NetScaler MA Service strengthens the application-centric approach to help you address various application delivery challenges. This approach gives you visibility into the health scores of applications, helps you determine the security risks, and helps you detect anomalies in the application traffic flows and take corrective actions.</p> <ul style="list-style-type: none">• Application Performance Analytics: App Score is the product of a scoring system that defines how well an application is performing. It shows whether the application is performing well in terms of responsiveness, is not vulnerable to threats, and has all systems up and running.• Application Security Analytics: The App Security Dashboard provides a holistic view of the security status of your applications. For example, it shows key security metrics such as security violations, signature violations, threat indexes. App Security dashboard also displays attack related information such as SYN attacks, small window attacks, and DNS flood attacks for the discovered NetScaler instances.
StyleBooks	<p>StyleBooks simplify the task of managing complex NetScaler configurations for your applications. A StyleBook is a template that you can use to create and manage NetScaler configurations. You can create a StyleBook for configuring a specific feature of NetScaler, or you can design a StyleBook to create configurations for an enterprise application deployment such as Microsoft Exchange or Skype for Business.</p>
Instance Management	<p>Enables you to manage the NetScaler ADC, NetScaler Gateway, and NetScaler SD-WAN instances.</p> <p>Note: Currently, NetScaler MA Service supports only the WAN Optimization functionality for NetScaler SD-WAN instances.</p>
Event Management	<p>Events represent occurrences of events or errors on a managed NetScaler instance. For example, when there is a system failure or change in configuration, an event is generated and recorded on NetScaler MA Service. Following are the related features that you can configure or view by using NetScaler MA Service:</p> <ul style="list-style-type: none">• Creating Event Rules• Using NetScaler Management and Analytics Service to Export Syslog Messages
Certificate Management	<p>NetScaler MA Service streamlines every aspect of certificate management for you. Through a single console, you can establish automated policies to ensure the right issuer, key strength, and correct algorithms, while keeping close tabs on certificates that are unused or soon to expire.</p>
Configuration Management	<p>NetScaler MA Service allows you to create configuration jobs that help you perform configuration tasks, such as creating entities, configuring features, replication of configuration changes, system upgrades, and other maintenance activities with ease on multiple instances. Configuration jobs and templates simplify the most repetitive administrative tasks to a single task on NetScaler MA Service.</p>
Configuration Monitoring	<p>Enables you to monitor and identify anomalies in the configurations across your instances.</p>

Configuration Audit	Configuration Advice
	<ul style="list-style-type: none"> • Audit Template: Allows you to monitor the changes across a specific configuration.
Feature	Description
Network Reporting	You can optimize resource usage by monitoring your network reporting on NetScaler MA Service.
Analytics	<p>Provides an easy and scalable way to look in to the various insights of the NetScaler instances' data to describe, predict, and improve application performance. You can use one or more analytics features simultaneously.</p> <ul style="list-style-type: none"> • HDX Insight: Provides end-to end visibility for ICA traffic passing through NetScaler ADC. HDX Insight enables administrators to view real-time client and network latency metrics, historical reports, end-to-end performance data, and troubleshoot performance issues. • Gateway Insight: Provides visibility into the failures that users encounter when logging on, regardless of the access mode. You can view a list of users logged on at a given time, along with the number of active users, number of active sessions, and bytes and licenses used by all users at any given time. • Security Insight: Provides a single-pane solution to help you assess your application security status and take corrective actions to secure your applications.
Role Based Access Control	Role Based Access Control (RBAC) allows you to grant access permissions based on the roles of individual users within your enterprise. The first user of an organization who logs on with Citrix Cloud credentials has the super admin role who, by default, has all access permissions. The other users of that organization, who are later created by the admin, are granted non-admin roles.
Subscriptions	Provides a dashboard view of the subscriptions that you have purchased. While on trial period, every tenant by default has a license for 10 virtual IP addresses and 5GB storage.

The NetScaler MAS features that are currently not available on NetScaler MA Service are as follows:

- Deployment
 - Migrating from NetScaler Insight Center to NetScaler MA Service
 - Integrating NetScaler MA Service with Citrix XenDesktop Director
- Application Analytics and Management
 - Managing and Monitoring HAProxy Instances
 - Advanced Analytics
- Networks
 - Backup and Restore of NetScaler Instances
 - Physical downloads of backups from NetScaler instances
 - Physical download of SSL Cert/Key Download from NetScaler instances
 - Single sign-on to Instance GUI
 - Record & Play functionality in Configuration Jobs
 - NetScaler VPX CICO Licensing
 - NetScaler Pooled Capacity
- Analytics: Web Insight, SSL Insight, TCP Insight, Video Insight, and WAN Insight
- Limited System Settings
- Orchestration
 - Integration with OpenStack and VMware NSX Manager
 - NetScaler Automation in Cisco ACI's Hybrid Mode
 - Container Orchestration: Integration with Mesos/Marathon and Kubernetes

System Requirements

Jun 29, 2017

Before you begin using NetScaler Management and Analytics Service (NetScaler MA Service), you must review the software requirements, browser requirements, port information, license information, and limitations.

This document includes the following information:

- [Supported Browsers](#)
- [Agent Installation Requirements](#)
- [Ports](#)
- [Minimum NetScaler Versions Required](#)
- [Requirements for NetScaler SD-WAN Instance Management](#)
 - [Minimum NetScaler SD-WAN WO Versions Required](#)
 - [Inter-Operability Matrix of NetScaler SD-WAN Platform Editions and NetScaler MA Service Features](#)
 - [Thin Clients Supported for NetScaler SD-WAN Instances](#)
- [Requirements for NetScaler MA Service Analytics Solution](#)
 - [Minimum XenApp and XenDesktop Versions Required](#)
 - [Thin Clients Supported for HDX Insight](#)
 - [NetScaler Instance License Required for HDX Insight](#)
- [Supported Operating Systems and Receiver Versions](#)

Supported Browsers

To access NetScaler MA Service, your workstation must have a supported web browser.

The following browsers are supported.

Web Browser	Version
Internet Explorer	11.0 and later
Google Chrome	Chrome 19 and later
Safari	Safari 5.1.1 and later
Mozilla Firefox	Firefox 3.6.25 and later

Agent Installation Requirements

You have to install and configure an agent in your network environment to enable communication between the NetScaler MA Service and the managed instances in your data center. In your data center on premises, you can install an agent on Citrix XenServer, VMWare ESXi, Microsoft Hyper-V, and Linux KVM Server.

The following table lists the virtual computing resources that the hypervisor must provide for each NetScaler MA Service agent.

Component	Requirement
RAM	8 GB Note: Citrix recommends that you use 32 GB for better performance.
Virtual CPU	4 Note: Citrix recommends that you use 8 CPUs for better performance.
Storage Space	120 GB Note: Citrix recommends that you use 500 GB for better performance.
Virtual Network interfaces	1
Throughput	1 Gbps

Note

You can also install your agent on Microsoft Azure cloud or AWS cloud. The agent image is available on the respective cloud marketplace.

- For instructions about installing an agent on Microsoft Azure cloud, see [Installing NetScaler MA Service Agent on Microsoft Azure Cloud](#).
- For instructions about installing an agent on AWS, see [Installing NetScaler MA Service Agent on AWS](#).

Ports

Make sure the following ports are open for NetScaler MA Service agent to communicate with NetScaler and/or SD-WAN instances.

Type	Port	Details
TCP	80/443	For NITRO communication from NetScaler MA Service agent to NetScaler or NetScaler SD-WAN instances.
TCP	22	For SSH communication from NetScaler MA Service agent to NetScaler or NetScaler SD-WAN instances.
UDP	4739	For AppFlow communication from NetScaler or NetScaler SD-WAN instances to NetScaler MA Service agent
ICMP	No reserved port	To detect network reachability from NetScaler MA Service agent to NetScaler or NetScaler SD-WAN instances.
SNMP	161, 162	To receive SNMP events from NetScaler instance to NetScaler MA Service agent
Syslog	514	To receive syslog messages in NetScaler MA Service agent from NetScaler or NetScaler SD-WAN instances.
TCP	5557	For logstream communication from NetScaler instances to NetScaler MA Service agent

For communication between the NetScaler MA Service agent and the NetScaler MA Service, make sure the following port is open:

Type	Port	Details
TCP	443	For NITRO communication from the agent to NetScaler Management and Analytics Service.

Minimum NetScaler Versions Required

NetScaler Management and Analytics Service Feature	NetScaler Software Version
StyleBooks	10.5 and later
Monitoring/Reporting & Configuration using Jobs	10.5 and later
Analytics	

NetScaler Management and Analytics Service Feature	NetScaler Software Version
Gateway Insight	11.0.65.31 and later
Security Insight	11.0.65.31 and later

Requirements for NetScaler SD-WAN Instance Management

Minimum NetScaler SD-WAN WO Versions Required

NetScaler Management and Analytics Service Feature	CloudBridge / NetScaler SD-WAN WO
Monitoring/Reporting & Configuration using Jobs	CloudBridge 7.4.0 and later
Analytics	
HDX Insight	CloudBridge 7.4.0 and later
WAN Insight	CloudBridge 7.4.0 and later

Inter-Operability Matrix of NetScaler SD-WAN Platform Editions and NetScaler MA Service Features

Platform Editions	Discovery	Configuration	Monitoring	Reporting	Event Management (SNMP Traps)	HDX Insight and WAN Insight Analytics	Multi-Hop Insight
NetScaler SD-WAN WANOP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NetScaler SD-WAN Enterprise	Yes	No	No	No	No	No	Yes

Thin Clients Supported for NetScaler SD-WAN Instances

NetScaler Management and Analytics Service supports the following thin clients for monitoring NetScaler SD-WAN deployments:

- Dell Wyse WTOS Model R10L Rx0L Thin Client
- NComputing N400

- Dell Wyse WTOS Model CX0 C00X Xenith
- Dell Wyse WTOS Model TXO T00X Xenith2
- Dell Wyse WTOS Model CX0 C10LE
- Dell Wyse WTOS Model R00LX Rx0L HDX Thin Client
- Dell Wyse Enhanced Suse Linux Enterprise, Model Dx0D, D50D
- Dell Wyse ZX0 Z90D7 (WES7) Thin Client

Requirements for NetScaler MA Service Analytics Solution

Minimum XenApp and XenDesktop Versions Required

NetScaler Management and Analytics Service Feature	XenApp / XenDesktop Version
HDX Insight	XenAPP 6.5
HDX Insight	XenDesktop 7.0, build 3018

Note

The NetScaler Gateway feature (branded as Access Gateway Enterprise for versions 9.3 and 10.x) must be available on the NetScaler instance. NetScaler Management and Analytics Service does not support standalone Access Gateway Standard appliances.

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

Thin Clients Supported for HDX Insight

NetScaler MA Service supports the following thin clients for monitoring NetScaler instances running on software version 11.0 Build 65.31 and later:

- WYSE Windows based Thin Clients
- WYSE Linux based Thin Clients
- WYSE ThinOS based Thin Clients
- 10Zig Ubuntu based Thin Clients

NetScaler Instance License Required for HDX Insight

The data collected by NetScaler MA Service for HDX Insight depends on the version and the installed licenses of the

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

NetScaler License/Duration	5 minutes	1 Hour	1 Day	1 Week	> 1 Month
Standard	✗	✗	✗	✗	✗
Enterprise	✓	✓	✗	✗	✗
Platinum	✓	✓	✓	✓	✓

Supported Operating Systems and Receiver Versions

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

Operating System	Receiver Version
Windows	4.0 Standard Edition
Linux	13.0.265571 and later
Mac	11.8, build 238301 and later
HTML5	1.5*
ChromeApp	1.5*

* Applicable with CloudBridge release 7.4 and later.

Getting Started

Jun 29, 2017

This document walks you through how to get started with onboarding and setting up NetScaler Management and Analytics Service (NetScaler MA Service) for the first time. This document is intended for network and application administrators who manage Citrix network devices (NetScaler, SD-WAN WO, NetScaler Gateway, and so on). You must follow the steps in this document irrespective of the type of device you plan to manage using NetScaler MA Service.

The following image illustrates the steps you have to perform to get started.



Before you begin onboarding, make sure you review the [browser requirements](#), the [agent installation requirements](#), and the [port requirements](#).


Step 1: Sign Up for Citrix Cloud

To start using NetScaler MA Service, you must first create a new Citrix Cloud company account or join an existing one that has been created by someone else in your company. For detailed processes and instructions on how to proceed, see [Signing Up for Citrix Cloud](#).

Step 2: Request a NetScaler MA Service Trial

After you log on to Citrix Cloud, a screen similar to the following appears. In the **Available Services** section, on the **NetScaler Management and Analytics Service** tile, click **Request Trial**.


Available Services (2)



Citrix App Layering
App and Image Management on-premises and in the cloud.

[Request Trial](#)

[How to Buy](#)
[Learn more](#)




NetScaler Management and Analytics Service
Management and Analytics for NetScaler on-premises and cloud.

[Request Trial](#)

[How to Buy](#)
[Learn more](#)


Labs Services (5)



Citrix Launch for Microsoft Access
Transform your Access reports into a secure web apps.

[Try It](#)


[Learn more](#)



Citrix Provisioning for Microsoft Office 365
Assign Office 365 subscription licenses.

[Try It](#)


[Learn more](#)



IoT Automation
Integrate and automate devices, services, and people.

[Try It](#)

[Learn more](#)



Session Manager
Pre-launch anonymous apps for faster access.

[Try It](#)

[Learn more](#)

The **NetScaler Management and Analytics Service** tile moves to the **My Services** section, and the button then changes to **View Trial Status**. You will receive an email to notify you when your trial becomes available. It might take a few minutes. After you are authorized to access the trial, the button on the tile changes to **Manage**. Click **Manage** to log on to the NetScaler MA Service GUI.

Note

Citrix assigns permissions to you to access the NetScaler Management and Analytics Service for a 30-day trial period. For information about trial subscriptions and how to buy, see <https://www.citrix.com/products/citrix-cloud/subscriptions.html>.

The following image shows the NetScaler MA Service GUI screen. Click **Get Started** to begin setting up the service for the first time.



NetScaler Management and Analytics Service

Manage your NetScaler deployment and gain real-time visibility into network and application performance and security across hybrid cloud and traditional environments.

To get started with NetScaler Management and Analytics Service, first set up an agent, and then add instances to your service.



Set Up Agent

Install an agent that can work as an intermediary between the service and the managed instances.



Add Instances

Add network devices that you want to discover, manage, and monitor from the service.

[Get Started](#)

[Getting Started Guide](#)

Step 3: Download and Install the NetScaler MA Service Agent

You must install and configure the NetScaler MA Service agent in your network environment to enable communication between the NetScaler MA Service and the managed instances in your data center or cloud.

You can install an agent on any one of the following hypervisors in your enterprise data center: Citrix XenServer, VMWare ESXi, Microsoft Hyper-V, and Linux KVM Server.

On the **Set Up Agent** page, select the hypervisor and click **Download Image** to download the agent image to your local system.

Set Up Agent

You have to install and configure an agent in your network environment to enable communication between the NetScaler Management and Analytics service and the managed instances in your data center. [Learn More](#)

Step 1: Select the type of hypervisor where you want to install the agent.	Step 2: Download the agent image to your local system and copy the activation code.	Step 3: Install the agent on the hypervisor and register it with the service.	Step 4: Log back on to the service and verify whether the agent is discovered.	Step 5: Add the network instances you want to manage and monitor.
---	--	--	---	--

Minimum System Requirements for Agent Installation: 8 GB RAM, 4 Virtual CPUs, 120 GB Storage Space, 1 Virtual Network Interface, 1 Gbps Throughput

Select the type of hypervisor ↓ [Download Image](#) [Generate Activation Code](#)

[Cancel](#) [Add Instances](#) [Done](#)

A service URL and an activation code are generated and displayed on the GUI. Copy both because you have to enter the service URL and the activation code while installing the agent on your hypervisor. The agent uses the service URL to locate the service and the activation code to register with the service.

For instructions about installing an agent on your on-premises hypervisor, see [Installing NetScaler MA Service Agent on Premises](#).

Note

You can also install a NetScaler MA Service agent on Microsoft Azure cloud or AWS cloud.

To install the agent on the cloud, you do not have to download the agent image from the **Set Up Agent** page. The agent image is available on the respective cloud marketplace.


You must, however, generate the service URL and the activation code by clicking **Generate Activation Code**, and then copy and save them to use during agent installation.

- For instructions about installing an agent on Microsoft Azure cloud, see [Installing NetScaler MA Service Agent on Microsoft Azure Cloud](#)
- For instructions about installing an agent on AWS, see [Installing NetScaler MA Service Agent on AWS](#)

Step 4: Add Instances to NetScaler MA Service

NetScaler instances are NetScaler network appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler MA Service. To manage and monitor these instances, you must add the instances to the service.

After you have successfully installed and registered the agent, it is displayed on the NetScaler MA Service GUI. When the agent status is in the UP state denoted by a green dot next to it, click **Add Instances** to start adding instances to the service.

Discovered Agents 

After agent installation is complete, verify the agent status on this page.

Host Name	IP Address	Instances
maasservice	10.102.29.98	0

On the **Add Instances** screen, specify values for **Agent**, **Instance Type**, **IP Address**, and **Profile Name**, and then click **OK**.

Add Instances ×

Instances are network appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler Management and Analytics service. To manage and monitor these instances, you must add these instances to the service.

Agent*
 >

Instance Type*


Enter Instance IP Address Import from File

IP Address*

Profile Name*
 + ✎

Adding instances might take some time depending on the number of instances being added.

After the instances are added, you can view the number of instances that have been successfully discovered. Click the number to view details of these instances.

Discovered Agents 

After agent installation is complete, verify the agent status on this page.

Host Name	IP Address	Instances
maasservice	10.102.29.98	2

Click **Done** to complete your initial setup and start managing your deployment.

Note

If you do not want to add instances during the initial setup, you can click **Done** to complete the setup and add the instances at a later time. For instructions about how to add instances at a later time to NetScaler MA Service, see [Adding Instances](#).

Installing NetScaler MA Service Agent on Premises

Jun 29, 2017

The agent works as an intermediary between the NetScaler Management and Analytics Service (NetScaler MA Service) and the discovered instances in the data center. This document describes how to install the NetScaler MA Service agent on your hypervisor in your on-premises network environment.

Before you begin installing the agent, make sure that you have the required virtual computing resources that the hypervisor must provide for each agent.

Component	Requirement
RAM	8 GB Note: Citrix recommends that you use 32 GB for better performance.
Virtual CPU	4 Note: Citrix recommends that you use 8 CPUs for better performance.
Storage space	120 GB Note: Citrix recommends that you use 500 GB for better performance.
Virtual Network Interfaces	1
Throughput	1 Gbps

To install the NetScaler Management and Analytics Service agent

1. Download the agent image as instructed in [Getting Started](#).
2. Import the agent image file to your hypervisor, and from the Console tab configure the initial network configuration options as shown in the following example.

```
NetScaler MAS initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
-----
1. NetScaler MAS Host Name [maasservice]:
2. NetScaler MAS IPv4 address [10.102.29.98]:
3. Netmask [255.255.255.0]:
4. Gateway IPv4 address [10.102.29.1]:
5. DNS IPv4 Address [10.140.50.5]:
6. Cancel and quit.
7. Save and quit.
Select a menu item from 1 to 7 [?]:
```

Note

Make sure that you configure your DNS to allow Internet access to your NetScaler MA Service agent.

3. Enter the **Service URL** and the **Activation Code** that you saved when you had downloaded the agent image. The agent uses the service URL to locate the service and the activation code to register with the service.

```
-----  
NetScaler MAS Agent Configuration. This menu allows you to specify a cloud url and obtain an instance ID for your device.  
-----  
Enter Service URL: agent.netscalermgmt.net  
Enter Activation Code : c56ba264-e6c0-4c2d-8daa-bc34493bd4e5
```

4. After agent registration is successful, the agent restarts to complete the installation process.

After the agent has restarted, access the NetScaler MA service GUI and on the **Set Up Agent** page, under **Discovered Agents**, verify the status of the agent.

Installing NetScaler MA Service Agent on Microsoft Azure Cloud

Jun 29, 2017

The agent works as an intermediary between the NetScaler Management and Analytics Service (NetScaler MA Service) and the managed instances in the enterprise data center, or on the cloud.

To install the NetScaler MA Service agent on Microsoft Azure cloud, you have to create an instance of the agent in the virtual network. Obtain the NetScaler MA Service agent image from the Azure marketplace, and then use the Azure Resource Manager portal to create the agent.

Before you begin creating the NetScaler MA Service agent instance, make sure that you have created a virtual network with required subnets where the instance will reside. You can create virtual networks during VM provisioning, but without the flexibility to create different subnets. For information about creating virtual networks, see <http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network>.

Configure DNS server and VPN connectivity that allows a virtual machine to access Internet resources.

Prerequisites

Make sure that you have the following:

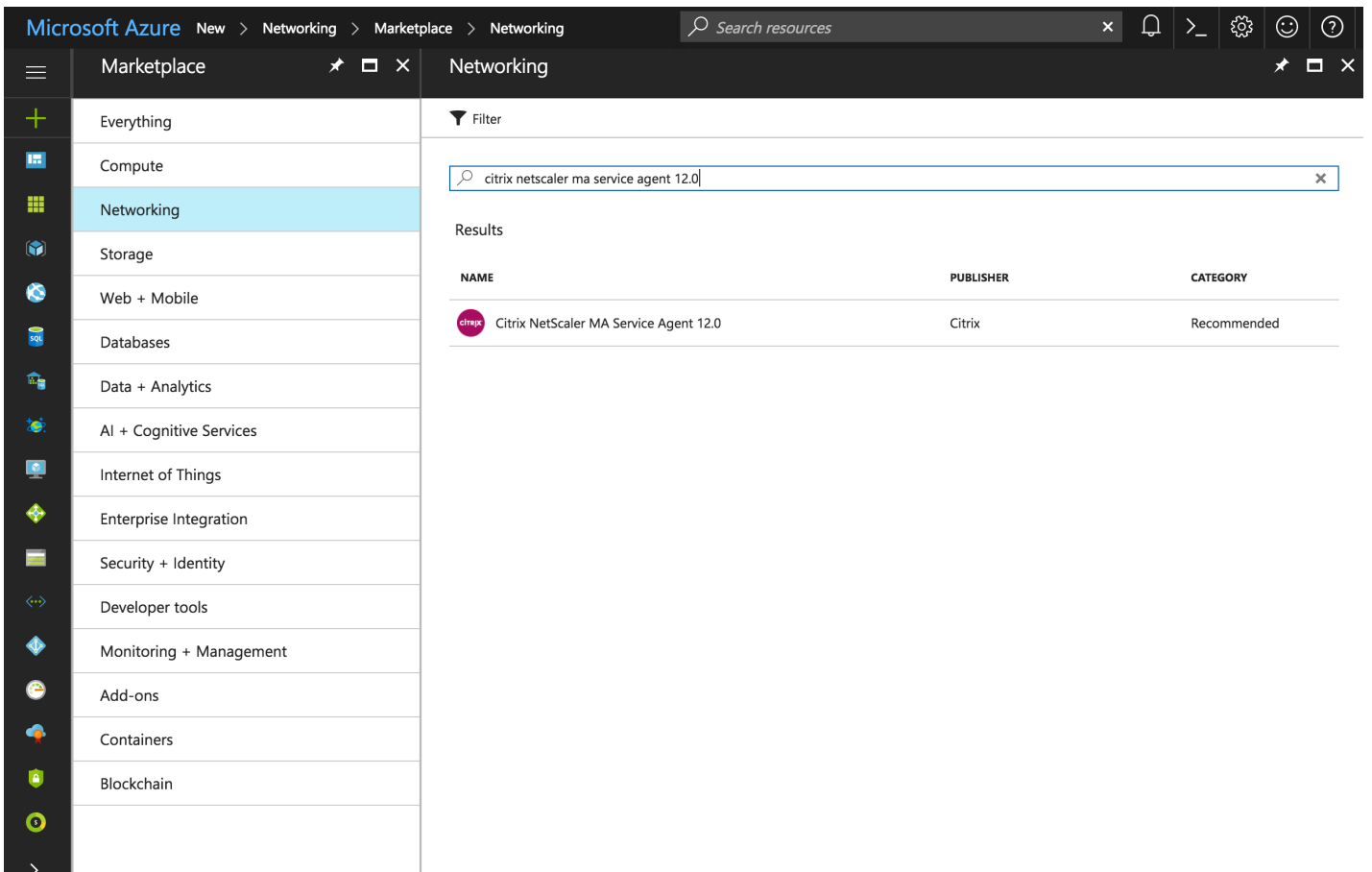
- A Microsoft Azure user account
- Access to Microsoft Azure Resource Manager

Note

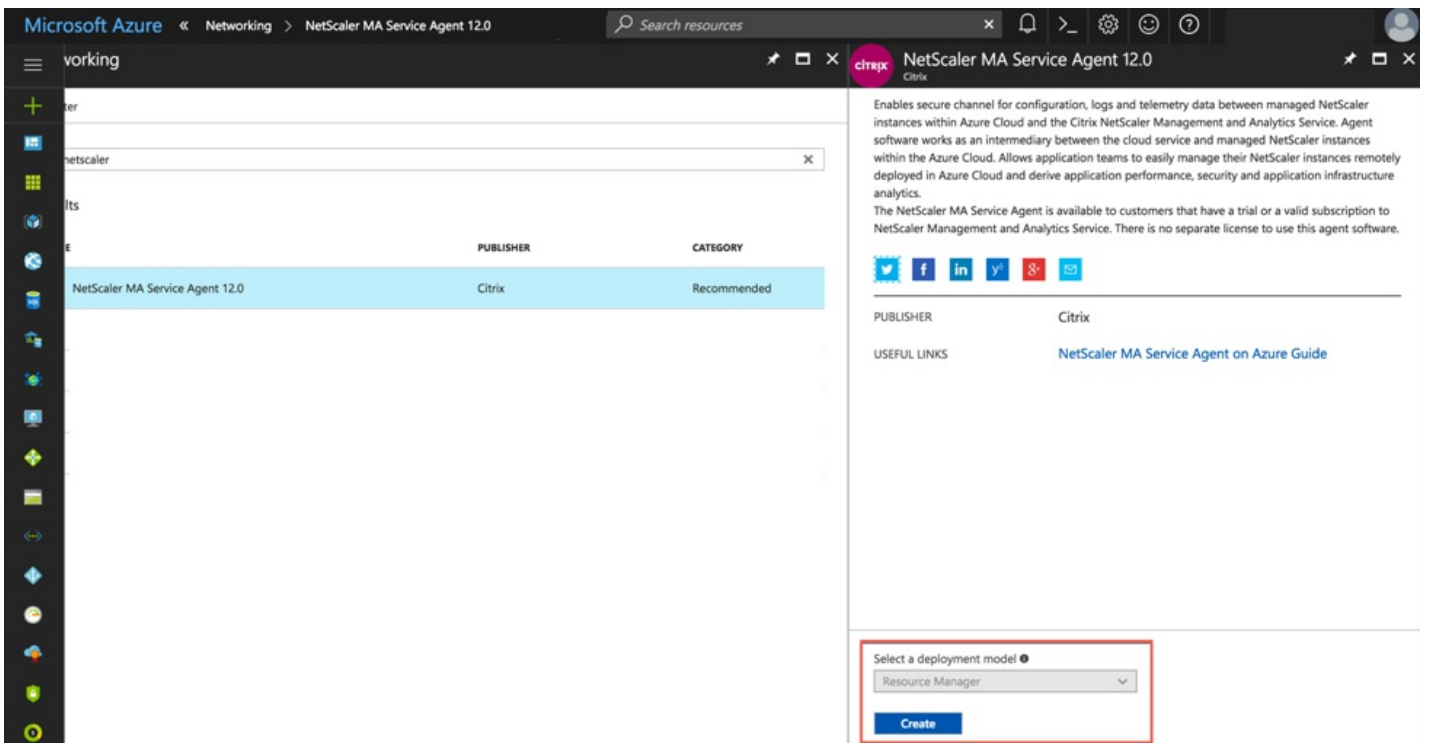
- Citrix recommends that you create resource group, network security group, virtual network, and other entities before you provision the NetScaler MA Service agent virtual machine, so that the network information is available during provisioning.
- For NetScaler MA Service agent to communicate with NetScaler MA Service and the NetScaler instances, ensure that the recommended ports are open. For complete details about the port requirements for NetScaler MA Service agent, see [Ports](#).

To install the NetScaler Management and Analytics Service agent on Microsoft Azure Cloud

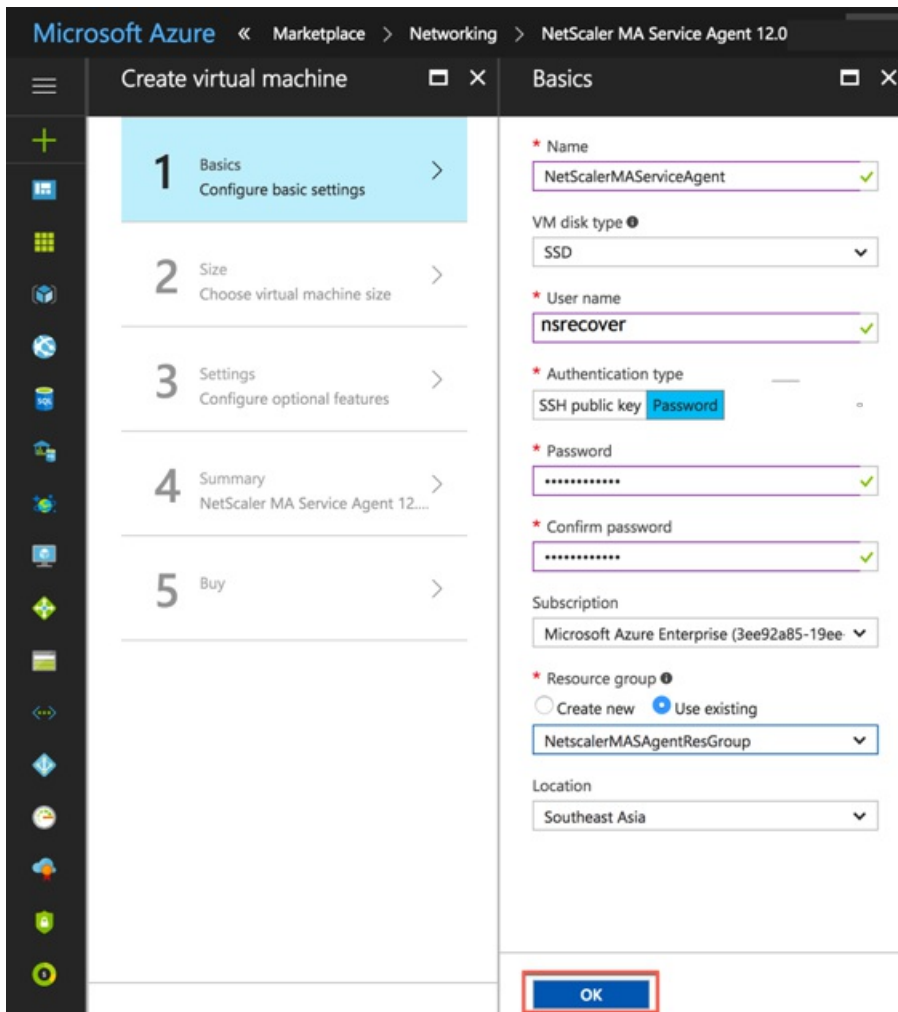
1. Log on to the Azure portal (<https://portal.azure.com>) by using your Microsoft Azure credentials.
2. Click **+New**.
3. Click **See All** and in the **Networking** pane, type Citrix NetScaler MA Service Agent 12.0 in the Azure Marketplace search box and press **Enter**.



4. On the **NetScaler MA Service Agent** page, from the drop-down list, select **Resource Manager** and click **Create**.



5. In the **Create virtual machine** pane, specify the required values in each section to create a virtual machine. Click **OK** in each section to save your configuration.

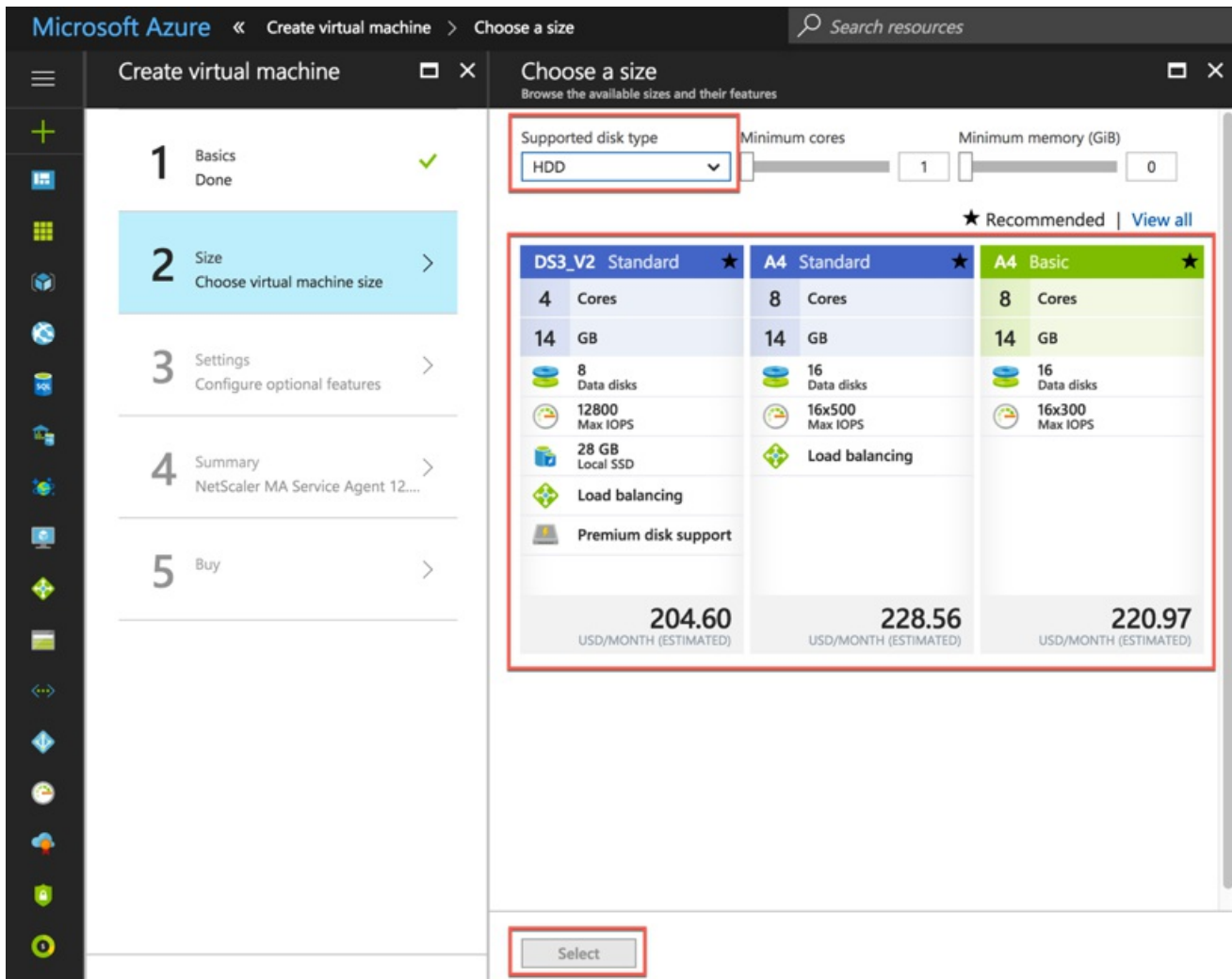


Basics

- **Name** – Specify a name for the NetScaler Management and Analytics Service agent instance.
- **VM disk type** - Select the virtual disk type.
- **User name and Password** – Specify a user name and password to access the resources in the resource group that you have created.
Note: You must use the username as **nsrecover** for all the agents that you install in Microsoft Azure.
- **Authentication Type** – Select Password.
- **Resource group** – Select the resource group you have created from the drop-down list.
Note: You can create a resource group at this point, but Citrix recommends that you create a resource group from Resource groups in Azure Resource Manager and then select the group from the drop-down list.

Size

In the **Size** menu, you can choose the type and size of the virtual disk for deploying your NetScaler MA Service agent.

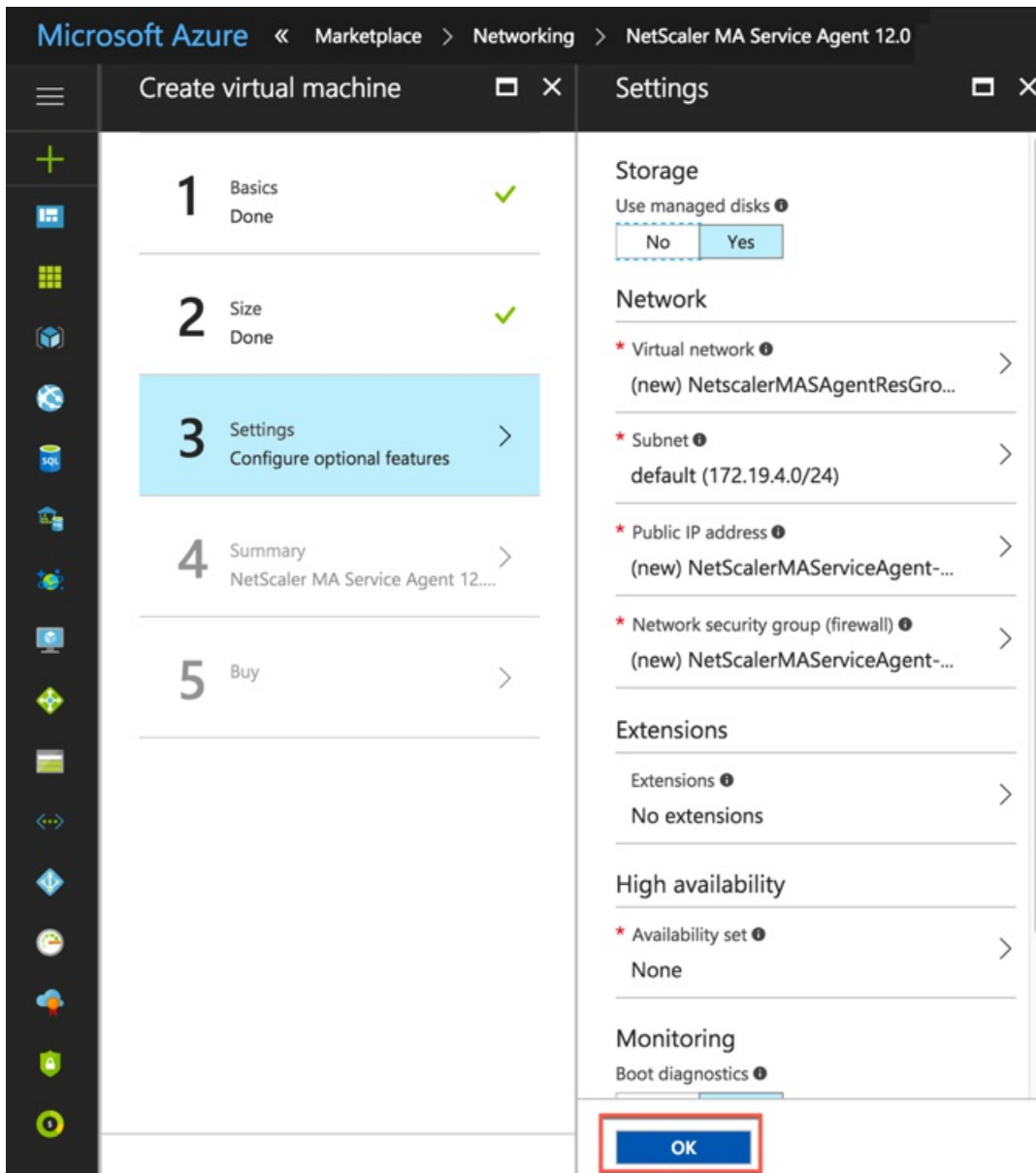


To select the virtual disk size

- From the Supported disk type drop-down, select the type (**HDD** or **SSD**) of the virtual disk.
- Select one of the available sizes for deploying NetScaler MA Service agent.
- Click **Select**.

Settings

In the **Settings** menu, most of the options are set by default. You can make changes to the default configuration as required.



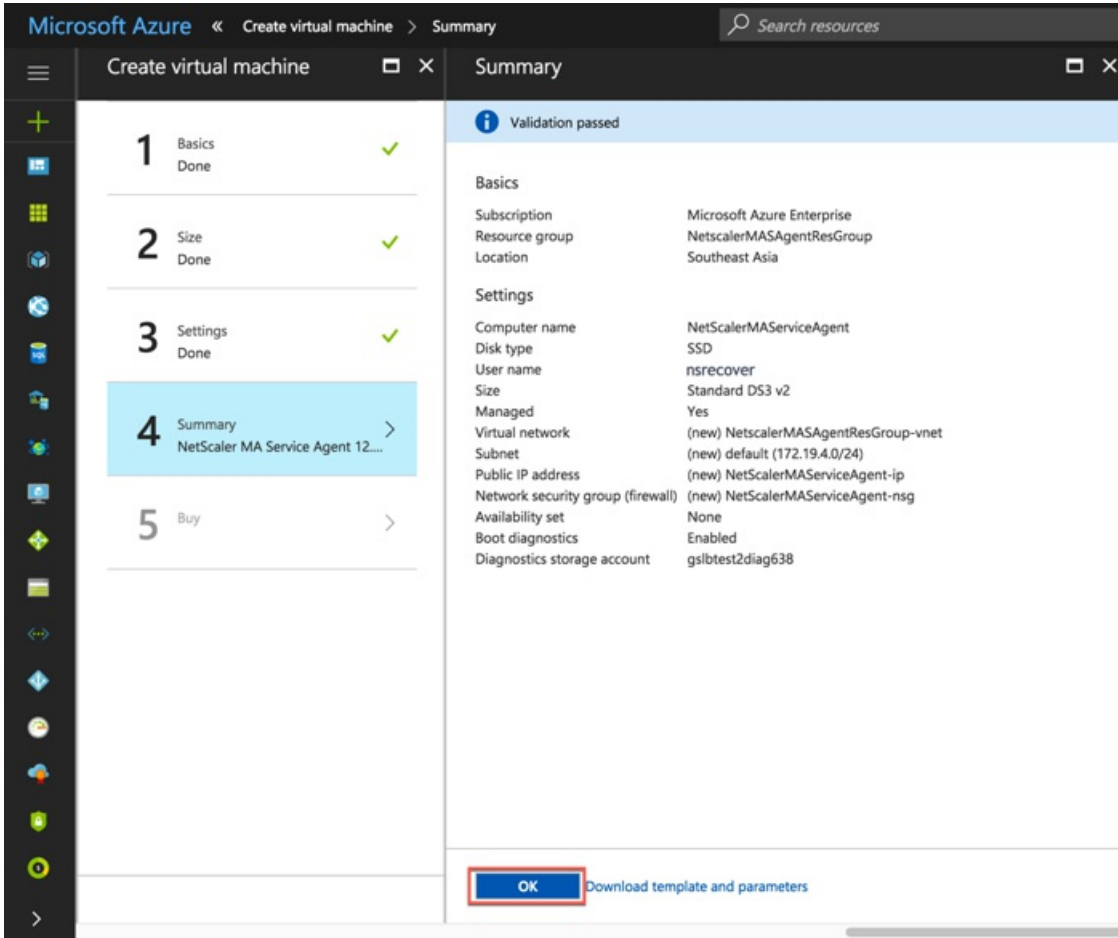
- **Virtual network** – Select the virtual network.
- **Subnet** – Set the subnet address.
- **Public IP address** – Select the IP address.
- **Network security group** – Select the security group that you have created. Ensure that inbound and outbound rules are configured in the security group.
For more details, see Prerequisites.
- **Availability Set** – Select the availability set from the drop-down box.

Summary

The configuration settings are validated and the Summary page displays the result of the validation.

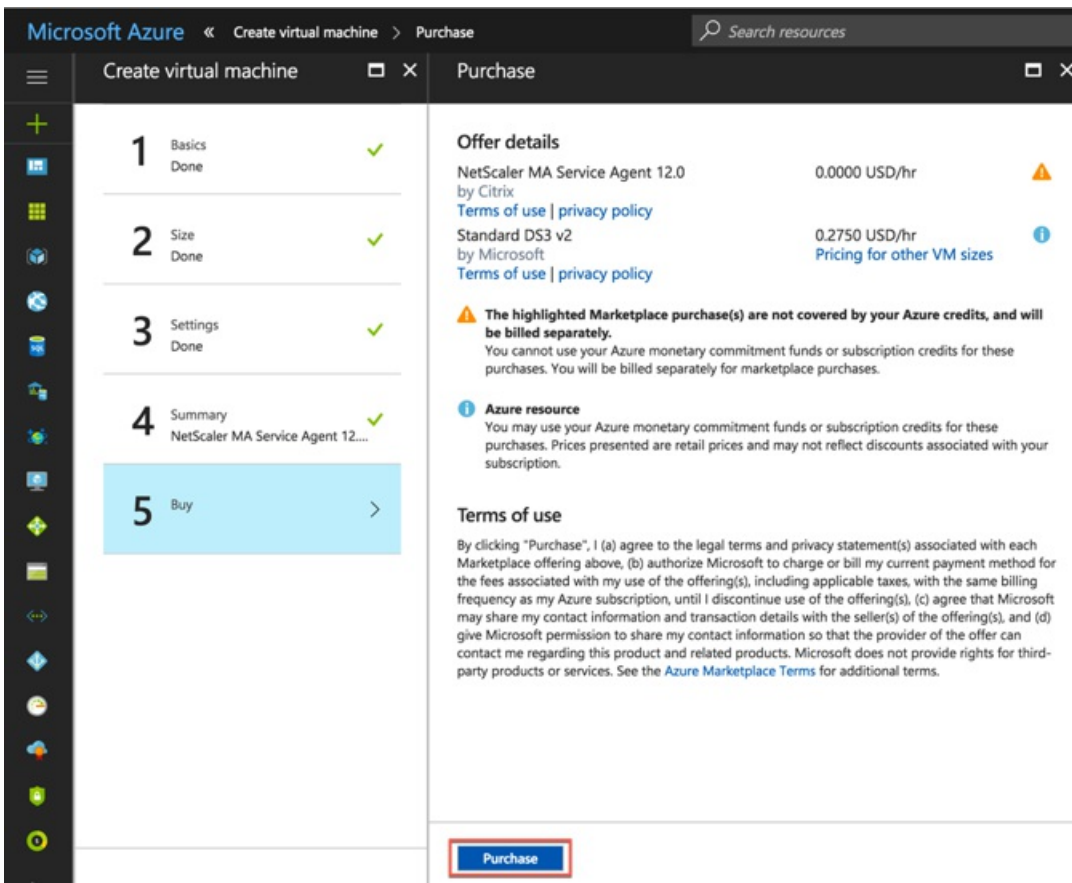
- If the validation fails, the Summary page displays the reason for the failure. Go back to the particular section and make changes as required.

- If the validation passes, click **OK**.

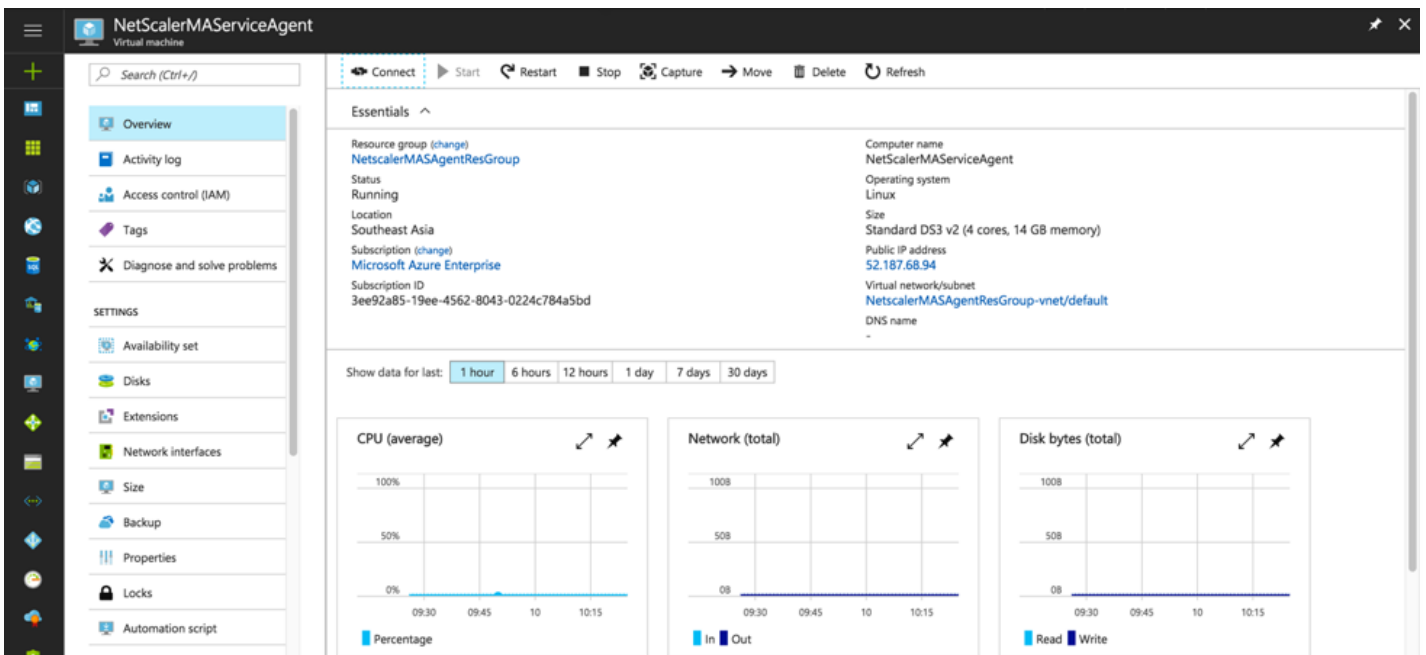


Buy

Review the offer details and legal terms on the Purchase page, and click **Purchase**.



Once the purchase is confirmed, Microsoft Azure will deploy the agent. The deployment process might take approximately 10-15 minutes. Once the deployment is successfully completed, you can view your NetScaler MA Service agent virtual machine in your Microsoft Azure account.



6. Once the agent is up and running, using an SSH client, log on to your NetScaler MA Service agent using the **Public IP**

address.

Note

- Use the default NetScaler MA Service agent credentials (**nsrecover/nsroot**) to log on to the virtual machine.
- Citrix recommends that you change your default password after the first logon. To change the password, at shell type: **passwd nsroot**.

7. Enter the following command to invoke the deployment screen:

deployment_type.py

8. Enter the **Service-URL** and the **Activation code** that you had copied and saved from the **Set Up Agents** page in NetScaler MA Service as instructed in [Getting Started](#). The agent uses the service URL to locate the service and the activation code to register with the service.

```
-----  
NetScaler MAS Agent Configuration. This menu allows you to specify a cloud url and obtain an instance ID for your device.  
-----  
Enter Service URL: agent.netscalermgmt.net  
Enter Activation Code : c56ba264-e6c0-4c2d-8daa-bc34493bd4e5
```

After agent registration is successful, the agent restarts to complete the installation process.

After the agent has restarted, access NetScaler MA Service and on the **Set Up Agent** page, under **Discovered Agents**, verify the status of the agent.

Installing NetScaler MA Service Agent on AWS

Jun 29, 2017

The NetScaler Management and Analytics Service agent (NetScaler MA Service) works as an intermediary between the NetScaler MA Service and the discovered instances in the data center or on the cloud.

Prerequisites

To launch a NetScaler MA Service agent AMI within an Amazon Web Services (AWS) Virtual Private Cloud (VPC) by using the Amazon GUI, you need:

- An AWS account
- An AWS Virtual Private cloud (VPC)
- An IAM account

Note

- Citrix recommends that you create security group, virtual private network, key pair, subnet, and other entities before you provision the NetScaler MA Service agent virtual machine, so that the network information is available during provisioning.
- For NetScaler MA Service agent to communicate with the NetScaler MA Service, and the NetScaler instances, ensure that the recommended ports are open. For complete details about the port requirements for NetScaler MA Service agent, see [Ports](#).

To install the NetScaler Management and Analytics Service agent on AWS

1. Log on to the AWS marketplace (<https://aws.amazon.com/marketplace>) by using your Amazon AWS credentials.
2. In the search field, type NetScaler MA Service Agent 12.0 to search for the NetScaler MA Service agent AMI, and click **Go**.
3. On the search result page, click the Citrix NetScaler MA Service agent AMI from the available list.
4. On the **Citrix NetScaler MA Service Agent AMI** page, click **Continue**.



Citrix NetScaler MA Service Agent AMI

Sold by: Citrix

AMI for the Citrix NetScaler Management and Analytics Service agent software that facilitates the secure remote management of NetScaler instances deployed within the AWS VPC via the NetScaler Management and Analytics Service.

Customer Rating ★★★★★ (0 Customer Reviews)

Latest Version 12.0

Operating System Linux/Unix, FreeBSD Other Linux

Delivery Method 64-bit Amazon Machine Image (AMI) ([Read more](#))

Support [See details below](#)

AWS Services Required Amazon EC2, Amazon EBS

- Highlights**
- Agent software works as an intermediary between the cloud service and managed NetScaler instances within the AWS VPC.
 - Enables secure channel for configuration, logs and telemetry data between managed NetScaler instances within AWS and the Citrix NetScaler Management and Analytics Service.

Product Description

AMI for the Citrix NetScaler Management and Analytics Service agent software that facilitates the secure remote management of NetScaler instances deployed within the AWS VPC via the NetScaler Management and Analytics Service.

Product Details

Version: 12.0

Available on AWS Marketplace Since: 06/28/2017

Resources

[How it Works](#)

Usage Instructions

To access the instance via SSH, please use the username: nsrecover and the <instance-id> as the password. Please go through our Docs available at <http://docs.citrix.com/en-us/netScaler-management-and-analytics-service-agent.html>

Continue

You will have an opportunity to review your order before launching or being charged.

Pricing Information

Use the Region dropdown selector to see software and infrastructure pricing information for the chosen AWS region.

For Region

US East (N. Virginia)

Pricing Details

Software pricing is based on your chosen options, such as subscription term and AWS region. Infrastructure prices are estimates only. Final prices will be calculated according to actual usage and reflected on your monthly report.

1 Software Pricing

The data below shows pricing per instance for services hosted in US East (N. Virginia).

Citrix NetScaler MA Service Agent AMI - Hourly			
EC2 Instance Type	Software /hr	EC2 /hr	Total /hr
m3.xlarge	\$0.00	\$0.266	\$0.266
m3.2xlarge	\$0.00	\$0.532	\$0.532
m4.xlarge	\$0.00	\$0.20	\$0.20
m4.2xlarge	\$0.00	\$0.40	\$0.40
m4.4xlarge	\$0.00	\$0.80	\$0.80

2 Infrastructure Pricing

Total hourly price will vary by instance type and EC2 region. [Click here for full EC2 pricing](#)

5. Select **1-Click Launch** tab and specify values for the following fields:

- Version** - Version of the NetScaler MA Service agent.
 - Region** - Specify the region.
 - EC2 Instance type** - Type of the instance. Select one of the available instance types from the available list.
 - VPC Settings** - Select the VPC and the subnet as required.
 - Security Group** - Security groups define the inbound and out bound traffic to your NetScaler MA Service agent.
- Note:** For recommended settings and for the list of ports to be opened for your NetScaler MA Service agent,

see [Ports](#).

f. **Key Pair** – You can select the key pair to login to your NetScaler MA Service agent.

6. Click **Launch with 1-Click**.

Launch on EC2: Citrix NetScaler MA Service Agent AMI

1-Click Launch
Review, modify and launch

Manual Launch
With EC2 Console, API or CLI

Click "Launch with 1-Click" to launch this software with the settings below

The default settings are provided by the software seller and AWS Marketplace.

- Version**
12.0, released 06/28/2017
- Region**
US East (N. Virginia)
- EC2 Instance Type**
m4.xlarge
- VPC Settings**
Will launch into: subnet-87229
- Security Group**
Create new based on seller settings
- Key Pair**
mas_8722

Price for your Selections:

- \$0.20 / hour**
\$0.20 m4.xlarge EC2 Instance usage fees +
\$0.00 hourly software fee
- \$0.10 per GB-month of provisioned storage**
EBS General Purpose (SSD) volumes

Launch with 1-click

You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#) and your use of AWS services is subject to the [AWS Customer Agreement](#).

Cost Estimator

- \$144.00 / month**
m4.xlarge EC2 Instance usage fees
Assumes 24 hour use over 30 days

Software Charges
\$0.00 / month
\$0.00 monthly software fees for m4.xlarge

AWS Infrastructure Charges
\$144.00 / month
Cost varies for storage fees
\$144.00 monthly EC2 instance fees for m4.xlarge
[Varied EBS Storage and data transfer fees](#)

Once the purchase is confirmed, Amazon AWS deploys the agent, and displays the confirmation summary.



Thank you for launching Citrix NetScaler MA Service Agent AMI

An instance of this software is now deploying on EC2.

You can check the status of this instance on [EC2 Console](#). You can also view all instances on [Your Software](#) page.

Software and AWS hourly usage fees apply when the instance is running and will appear on your monthly bill.



Next Steps:

- The software will be ready in a few minutes.

Software Installation Details

Product	Citrix NetScaler MA Service Agent AMI
Version	12.0
Region	us-east-1
EC2 Instance Type	m4.xlarge
VPC	vpc-cb2
Subnet	subnet-cb
Security Group	Create new security group based on seller settings
Key Pair	mas

[Return to Launch Page](#)

Related Links

[AWS Management Console](#)
[Your Software](#)
[Continue shopping on AWS Marketplace](#)

Service Catalog

Click [here](#) for instructions to deploy Marketplace products in [AWS Service Catalog](#).

[AWS Marketplace on Twitter](#)

[AWS Marketplace Blog](#)

[RSS Feed](#)

[Software Infrastructure](#)

[Business Software](#)

[Sell in AWS Marketplace](#)

[Featured Categories](#)

[AWS Marketplace is hiring!](#)

Note: The deployment process might take approximately 10-15 minutes. After the deployment is successfully completed, you can view your NetScaler MA Service agent virtual machine on your Amazon AWS account.

7. Once the agent is deployed, assign a name for your NetScaler MA Service agent.

8. Once the agent is up and running, assign an elastic IP address for your NetScaler MA Service agent.

Note: Elastic IP enables NetScaler MA Service agent to communicate with NetScaler MA Service.

9. Using a SSH client, login to your NetScaler MA Service agent using the public IP address.

Note: Use the NetScaler MA Service agent credentials as **(nsrecover/<instance id>)** to login to the agent virtual machine for the first time.

10. Enter the following command to invoke the deployment screen:

deployment_type.py

11. Enter the **Service-URL** and the **Activation code** that you had copied and saved from the **Set Up Agents** page in NetScaler MA Service as instructed in [Getting Started](#). The agent uses the service URL to locate the service and the

activation code to register with the service.

```
-----  
NetScaler MAS Agent Configuration. This menu allows you to specify a cloud url and obtain an instance ID for your device.  
-----
```

```
Enter Service URL: agent.netscalermgmt.net  
Enter Activation Code : c56ba264-e6c0-4c2d-8daa-bc34493bd4e5
```

After agent registration is successful, the agent restarts to complete the installation process.

After the agent has restarted, access NetScaler MA service and on the **Set Up Agent** page, under **Discovered Agents**, verify the status of the agent.

Note

Once the agent is registered with the NetScaler MA Service, to log on to the agent virtual machine, you can SSH to the agent virtual machine using the key based authentication and nsroot as the username.

Managing Subscriptions

Jun 29, 2017

NetScaler Management and Analytics Service (NetScaler MA Service) requires a verified license to manage and monitor Citrix NetScaler instances. You can manage and monitor any number of instances when you are on the trial period or when you have subscribed to a valid license. However, you can manage the discovered applications on the App Dashboard, view analytics data, and monitor network functions and network reports only for the number of virtual servers for which you have purchased licenses. During trial period, you can monitor only 10 virtual servers or applications.

With each installed license, you will receive a limited amount of data and capacity to manage certain virtual servers. However, you can also purchase and apply data-only licenses to top-up your data storage.

Note

After the trial period expires, you must purchase a valid license to continue to use any feature in NetScaler MA Service.

For information and instructions about buying and upgrading your NetScaler Management and Analytics Service licenses, see <https://www.citrix.com/products/citrix-cloud/subscriptions.html>.

You can view the licenses installed on your NetScaler MA Service by navigating to **Settings > Subscriptions**. You can also view the license summary such as the type of license subscribed to, the entitled data subscription and consumed data subscription, and the allowed and managed virtual servers in the **Summary** section.

Summary			
Type	Allowed Virtual Servers	Managed Virtual Servers	Storage
Trial	10	10	<i>Entitled: 5 GB</i> <i>Consumed: 151.94 MB</i>

The following table lists the NetScaler licenses that are required to use some of the NetScaler Management and Analytics Service features.

NetScaler Management and Analytics Service Features	NetScaler License Requirement

NetScaler Management and Analytics Service		Platinum (reporting = Unlimited)	
Features	Security Insight	NetScaler License Requirement	
Analytics		Platinum (or)	
	Gateway Insight	Enterprise with App Firewall license	
		Enterprise (reporting < 1 hour)	
		Platinum (reporting = Unlimited)	
		<p>NetScaler Web App Firewall related information on App dashboard, and app security dashboard needs Platinum (or) Enterprise with App Firewall license</p>	
Applications	Application Statistics (App Dashboard, App Security Dashboard)	N/A	
	Stylebooks		
	Inventory Management – Infrastructure Dashboard, Instance groups, Instance dashboards & Sites		
	Event Management & Syslog		
	Configuration Jobs, Configuration Audit & Configuration Advice		
	Network reporting (Instance level)		
	Network reporting (virtual server level)		
	Network Functions (Plain visibility & Management of virtual servers, services, service groups, server)		
	SSL certificate management (Instance level)		
	SSL certificate management (virtual server level)		

(instance level)			
NetScaler Management and Analytics Service Features	RBAC & External Authentication (virtual server level)	NetScaler License Requirements	N/A

Selecting the Virtual Servers to Manage

You can select the virtual servers you want to manage and monitor through NetScaler MA Service.

Points to Note

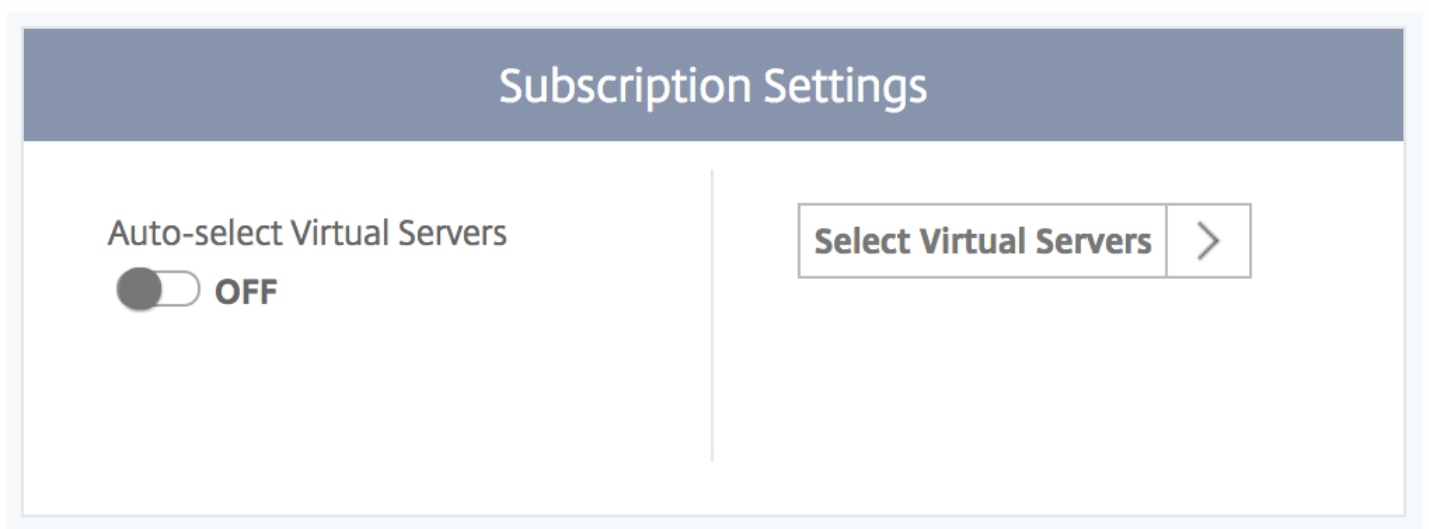
- By default, NetScaler MA Service automatically licenses the virtual servers randomly after each virtual server poll cycle.
- If the total number of virtual servers discovered in your NetScaler MA Service is lower than the number of installed virtual server licenses, NetScaler MA Service, by default, licenses all the virtual servers.

To select the virtual servers manually, or to restrict licensing to limited virtual servers, you have to first disable auto licensing the virtual servers, and then select the virtual servers you want to manage.

1. Log on to NetScaler Management and Analytics Service using a supported web browser.
2. Navigate to **Settings > Subscriptions**.

The dashboard displays the virtual server licenses available, the managed virtual servers along with the virtual server type, and license expiry information

3. In **Subscription Settings**, disable Auto-select Virtual servers.



4. Click **Select Virtual Servers**.
5. In the **Choose Virtual Servers** screen, select the type of virtual servers by clicking the relevant tab.

← Choose Virtual Servers

LB Virtual Servers | CS Virtual Servers | CR Virtual Servers | Authentication Virtual Servers | GSLB Virtual Servers | NetScaler Gateway

Add the Load Balancing Virtual Servers that you want to manage

Add Virtual Servers | Mark Unlicensed | Search | ⚙️

<input type="checkbox"/>	Instance	Host Name	Name	IP Address	Effective State
<input type="checkbox"/>	10.102.29.160	-NA-	mysqlsvr	2.22.2.222	● DOWN
<input type="checkbox"/>	10.102.29.160	-NA-	testssl	3.4.6.9	● DOWN
<input type="checkbox"/>	10.102.29.160	-NA-	vhhttp1	10.102.29.162	● UP
<input type="checkbox"/>	10.102.60.27	-NA-	REPUTATION_TEST	10.102.60.243	● UP
<input type="checkbox"/>	10.102.60.27	-NA-	OWA_web_test	10.102.60.248	● UP
<input type="checkbox"/>	10.102.29.160	-NA-	trace	0.0.0.0	● UP

6. Select the virtual servers to be licensed from the available list.

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

LB Virtual Servers | CS Virtual Servers | CR Virtual Servers | Authentication Virtual Servers | GSLB Virtual Servers | NetScaler Gateway

Add the Load Balancing Virtual Servers that you want to manage

Add Virtual Servers | Mark Unlicensed | Search | ⚙️

<input type="checkbox"/>	Instance	Host Name	Name	IP Address	Effective State
<input type="checkbox"/>	10.102.29.160	-NA-	mysqlsvr	2.22.2.222	● DOWN
<input type="checkbox"/>	10.102.29.160	-NA-	testssl	3.4.6.9	● DOWN
<input type="checkbox"/>	10.102.29.160	-NA-	vhhttp1	10.102.29.162	● UP
<input checked="" type="checkbox"/>	10.102.60.27	-NA-	REPUTATION_TEST	10.102.60.243	● UP
<input type="checkbox"/>	10.102.60.27	-NA-	OWA_web_test	10.102.60.248	● UP
<input checked="" type="checkbox"/>	10.102.29.160	-NA-	trace	0.0.0.0	● UP
<input type="checkbox"/>	10.102.29.160	-NA-	vhhttp1234	10.102.2.3	● DOWN
<input type="checkbox"/>	10.102.29.140	-NA-	app_0_Applicationstest	0.0.0.0	● DOWN
<input type="checkbox"/>	10.102.29.140	-NA-	app_u_testvideos	0.0.0.0	● DOWN
<input type="checkbox"/>	10.102.29.140	-NA-	microsoft-skype-application-sfb-dir-http-lb	10.10.10.30	● DOWN

Cancel | Next → | Save and Exit

Expiry Checks for Virtual Server Subscriptions

You can view the status of installed licenses with the expiry and the allowed storage limit to the licenses in NetScaler Management and Analytics Service.

To view the status of the licenses

1. Navigate to **Settings > Subscriptions**.
2. In the **Subscription Expiry Information** section, you can view the details of licensed virtual servers and the days to expiry:

- **Allowed Virtual Servers:** Number of virtual servers that are being managed with the license.
- **Allowed Storage:** Storage limit of the license.
- **Days to expiry:** Number of days remaining before the license expiry.

Subscription Expiry Information		
Allowed Virtual Servers	Allowed Storage	Days To Expiry
10	5 GB	29

Setting Up

Jun 29, 2017

After your initial setup is complete, you have to configure certain settings to start managing your deployment completely.

- [Adding Multiple Agents](#). The number of agents to be installed depends on the number of managed instances in a data center or cloud and the total throughput. Citrix recommends that you install at least one agent for every data center.
- [Adding Instances](#). You can add instances either while setting up the NetScaler Management and Analytics Service for the [first time](#) or at a later time. You have to add instances to the service to start managing and monitoring them. After you install multiple agents, you have to add instances and associate them with the agents.
- [Enabling Analytics](#). To view analytics data for your application traffic flow, you must enable the Analytics feature on the virtual servers that receive traffic for the specific applications.
- [Configuring Syslog on Instances](#). You can monitor the syslog events generated on your NetScaler instances if you have configured your device to redirect all syslog messages to NetScaler Management and Analytics Service. To monitor syslog events, you need to first configure NetScaler MA Service as the syslog server for your NetScaler instance.
- [Configuring Role-Based Access Control](#). NetScaler MA Service provides fine-grained, role based access control (RBAC) with which you can grant access permissions based on the roles of individual users within your enterprise.
- [Configuring Analytics Settings](#). You can configure certain settings to ensure optimal experience with the Analytics feature. For example, you can specify the duration you want to store historical analytics data, and you can also set thresholds and alerts to monitor the desired analytics metrics.

Adding Multiple Agents

Jun 29, 2017




The number of agents to be installed depends on the number of managed instances in a data center and the total throughput. Citrix recommends that you install at least one agent for every data center.

You can install only one agent when you log on to the service for the first time. To add multiple agents, first complete the initial setup, and then navigate to **Settings > Setup Agents**.

Download the image for the required hypervisor and install the agent by following the instructions in [Installing NetScaler MA Service Agent on Premises](#). Make sure you copy the service URL and the activation code displayed on the screen because you have to enter the service URL and the activation code while installing the agent on your hypervisor. The agent uses the service URL to locate the service and the activation code to register with the service.

You can use the same image to install multiple agents in your hypervisor. However, you cannot use the same activation code on multiple agents. After you install one agent, generate the activation code again for the next agent. You can generate a new activation code by navigating to **Settings > Generate Activation Code**.

After the agent is successfully installed and registered, verify the agent status on the service GUI and add instances to it.

Discovered Agents 		
After agent installation is complete, verify the agent status on this page.		
 Host Name maasagent4	IP Address 10.102.29.96	Instances 14
 Host Name maasagent3	IP Address 10.102.29.94	Instances 6

Note

You can also install NetScaler MA Service agent on Microsoft Azure cloud or AWS cloud. The agent image is available on the respective cloud marketplace.

- For instructions about installing an agent on Microsoft Azure cloud, see [Installing NetScaler MA Service Agent on Microsoft Azure Cloud](#).
- For instructions about installing an agent on AWS, see [Installing NetScaler MA Service Agent on AWS](#).

Adding Instances

Jun 29, 2017

You can add instances either while setting up the NetScaler Management and Analytics Service (NetScaler MA Service) for the [first time](#) or at a later time.

Instances are Citrix appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler MA Service. You can add the following Citrix appliances and virtual appliances to NetScaler MA Service:

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

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

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

Note

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

To add an instance to NetScaler MA Service

1. Navigate to **Networks > Dashboard** and click **All Instances**. On the **Instances** page, click **New** at the top right corner of the page. On the **Add Instance** page, from **Instance Type**, select the type of instance you want to add.

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

2. Select one of the following options:

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

want to add.

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

Note

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

4. From **Agent**, select the agent with which you want to associate the instances, and then click **OK**.

While adding the instances, if there is only one agent configured on your NetScaler MA Service, by default, that agent is selected.

Add Instance

Instance Type*

NetScaler

Enter Instance IP Address Import from file

Enter one or more hostnames, IP addresses , and/or a range of IP addresses (for example, 10.102.40.30-10.102.40.45) using a comma separator.

IP Address*

10.102.42.25

Profile Name*

ns_nsroot_profile



Agent*

10.221.42.83



OK

Close

Enabling Analytics

Jun 29, 2017

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

To enable Analytics on NetScaler Management and Analytics Service

1. In a supported web browser, logon to your NetScaler Management and Analytics Service.
2. Navigate to **Networks > Instances**, and select the NetScaler instance on which you want to enable analytics.
3. From the **Action** drop-down, select **Enable/Disable Insight**.
4. Select the **virtual servers**, and click **Enable AppFlow**.
5. To enable Security Insight on your HTTP virtual server, in the **Enable AppFlow field**, type **true**, and select the **Security Insight** check box.


Enable AppFlow

Select Expression *

Load Balancing

Transport Mode IPFIX Logstream

Security Insight

 If the AppFlow for a virtual server is enabled on more than one NetScaler Management and Analytics Service appliance, then the appliance on which the AppFlow is enabled most recently has the highest priority for collecting the information.

To enable **HDX Insight** and **Gateway Insight**, while clicking **Enable AppFlow**, select VPN virtual server configured on your NetScaler instance, and then in the **Enable AppFlow** dialog box, select **ICA** or **HTTP** check boxes accordingly.

Enable AppFlow

Select Expression *

VPN

Transport Mode IPFIX Logstream ICA

TCP

HTTP



If the AppFlow for a virtual server is enabled on more than one NetScaler Management and Analytics System appliance, then the appliance on which the AppFlow is enabled most recently has the highest priority for collecting the information.

OK

Cancel

Note

For information about HDX Insight, Gateway Insight, and Security Insight, see:

- [HDX Insight](#)
- [Gateway Insight](#)
- [Security Insight](#)

Configuring Syslog on Instances

Jun 29, 2017

The syslog protocol provides a transport to allow the NetScaler instances to send event notification messages to NetScaler Management and Analytics Service (NetScaler MA Service), which is configured as a collector or the syslog server for these messages.

You can monitor the syslog events generated on your NetScaler instances if you have configured your device to redirect all syslog messages to NetScaler MA Service. To monitor syslog events, you need to first configure NetScaler MA Service as the syslog server for your NetScaler instance. After the instance is configured, all the syslog messages are redirected to NetScaler MA Service, so that these logs can be displayed to the user in a structured manner.

Syslog uses the User Datagram Protocol (UDP), port 514, for communication, and because UDP is a connectionless protocol it does not provide any acknowledgment back to the instances. The syslog packet size is limited to 1024 bytes and carries the following information:

- Facility
- Severity
- Hostname
- Timestamp
- Message

In NetScaler MA Service, you must configure facility and log severity levels on the instances.

- **Facility** - Syslog messages are broadly categorized on the basis of the sources that generate them. These sources can be the operating system, the process, or an application. These categories are called facilities and are represented by integers. For example, 0 is used by kernel messages, 1 is used by user-level messages, 2 is used by the mail system, and so on. The local use facilities (from local0 to local7) are not reserved and are available for general use. Hence, the processes and applications that do not have pre-assigned facility values can be directed to any of the eight local use facilities.
- **Severity** - The source or facility that generates the syslog message also specifies the severity of the message using a single-digit integer, as shown below:

1 - Emergency: System is unusable.

2 - Alert: Action must be taken immediately.

3 - Critical: Critical conditions.

4 - Error: Error conditions.

5 - Warning: Warning conditions.

6 - Notice: Normal but significant condition.

7 - Informational: Informational messages.

8 - Debug: Debug-level messages.

To configure syslog on NetScaler instances

1. In NetScaler MA Service, navigate to **Networks > Instances**.

2. Select the NetScaler instance from which you want the syslog messages to be collected and displayed in NetScaler MA Service.
3. In the **Action** drop-down list, select **Configure Syslog**.
4. Click **Enable**.
5. In the **Facility** drop-down list, select a local or user-level facility.
6. Select the required log level for the syslog messages.
7. Click **OK**.

This configures all the syslog commands in the NetScaler instance, and NetScaler MA Service starts receiving the syslog messages. You can view the messages by navigating to **Networks > Events > Audit Log Messages**.

Configuring Role-Based Access Control

Jun 29, 2017

NetScaler Management and Analytics Service (NetScaler MA Service) provides fine-grained, role based access control (RBAC) with which you can grant access permissions based on the roles of individual users within your enterprise. In this context, access is the ability to perform a specific task, such as view, create, modify, or delete a file. Roles are defined according to the authority and responsibility of the users within the enterprise. For example, one user might be allowed to perform all network operations, while another user can observe the traffic flow in applications and assist in creating configuration templates.

Roles are determined by policies. After creating policies, you can create roles, bind each role to one or more policies, and assign roles to users. You can also assign roles to groups of users. A group is a collection of users who have permissions in common.

For example, users who are managing a particular data center can be assigned to a group. A role is an identity granted to users by adding them to specific groups on the basis of specific conditions. In NetScaler Management and Analytics Service, creating roles and policies is specific to the RBAC feature in NetScaler. Roles and policies can be easily created, changed, or discontinued as the needs of the enterprise evolve, without having to individually update the privileges for every user.

In NetScaler Management and Analytics Service, all users are created in Citrix cloud. As the first user of your organization, you must first create a new account in Citrix Cloud and then log on to the NetScaler MA Service GUI with the Citrix cloud credentials. You are granted the super admin role, and by default, you have all access permissions in NetScaler Management and Analytics Service. Later you can create other users in your organization in Citrix cloud, and these users are granted non-admin roles. These non-admin users have all permissions in NetScaler MA Service GUI except accessing the Systems node, though it is possible for you to grant admin permissions to these non-admin users as well.

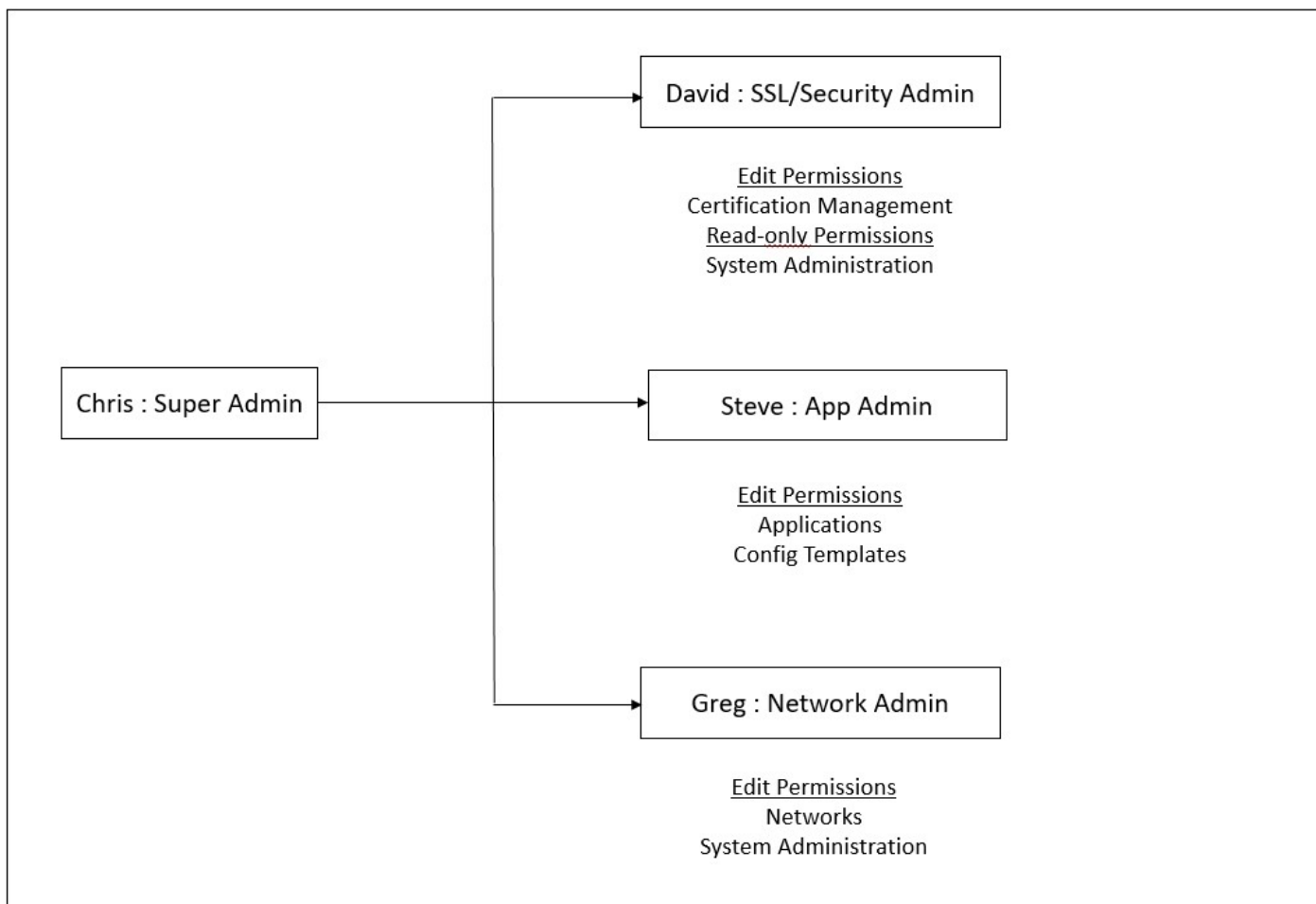
Roles can be feature based or resource based. For example, consider an SSL/security administrator and an application administrator. An SSL/security administrator must have complete access to SSL Certificate management and monitoring features, but should have read-only access for system administration operations. Application administrators should be able to access only the resources within their scope.

Example

Chris, the ADC group head, is the super administrator of NetScaler MA Service in his organization. He creates three administrator roles: security administrator, application administrator, and network administrator.

- David, the security admin, must have complete access for SSL Certificate management and monitoring but should have read-only access for system administration operations.
- Steve, an application admin, needs access to only specific applications and only specific configuration templates.
- Greg, a network admin, needs access to system and network administration.
- Chris also must provide RBAC for all users, irrespective of the fact that they are local or a multi-tenant.

The following image shows the permissions that the administrators and other users have and their roles in the organization.



To provide role based access control to his users, Chris must first add users in Citrix cloud and only after that he can see the users in NetScaler Management and Analytics Service. Chris must create access policies for each of the users depending on their role. Access policies are tightly bound to roles. So, Chris must create roles and then create groups as roles can be assigned to groups and not to individual users.

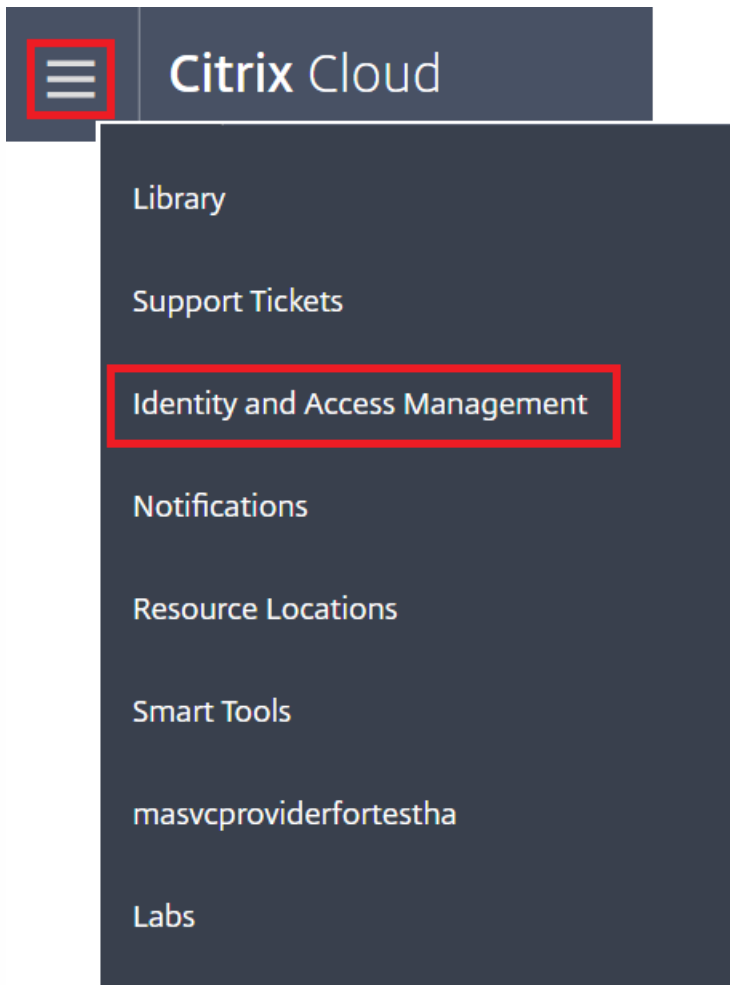
Therefore, in your role as Chris, the super admin, perform the following example tasks in NetScaler Management and Analytics Service to configure access policies, roles, and user groups for David who is the security admin in your organization:

Configuring Users on NetScaler Management and Analytics Service

As a super admin, you can create additional users by configuring accounts for them in Citrix cloud and not in NetScaler Management and Analytics Service. When the new users are added to NetScaler MA Service, you can only define their permissions by assigning the appropriate groups to the user.

To add new users in Citrix Cloud

1. In NetScaler MA Service GUI, click the Hamburger icon at the top left, and select **Identity and Access Management**.



2. On the Identity and Access Management page, select **Administrators** tab.

This tab lists the users that are created in Citrix cloud.

3. Type the email address of the user that you want to add in NetScaler MA Service and click **Invite**.

Identity and Access Management

Authentication **Administrators** API Access Domains

maasdoc+DavidT@gmail.com

Invite

Note

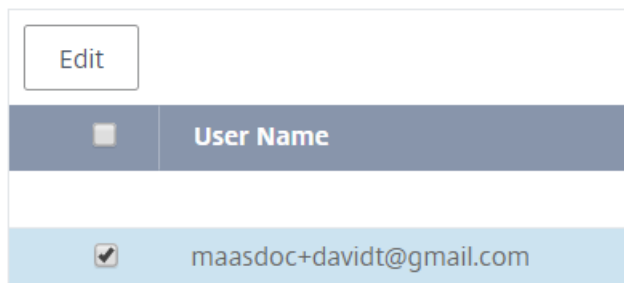
The user receives an email invite from Citrix cloud. The user must click the link provided in the email to complete the registration process by providing their full name and password, and later log on to NetScaler Management and Analytics Service using their credentials.

4. As an admin, you see the new user in NetScaler MA Service Users list only after the user logs on to NetScaler Management and Analytics Service.

To Configure Users in NetScaler Management and Analytics Service

1. In NetScaler MA Service GUI, navigate to **Settings > User Administration > Users**.
2. The user is displayed in the **Users** page.

Users



3. You can edit the privileges provided to the user by selecting the user and clicking **Edit**. You can also edit group permissions on Groups page under Settings node.

Note

Your users are added in NetScaler Management and Analytics Service from the Citrix cloud only. Therefore, even though you have admin permissions, you cannot add or delete users in NetScaler Management and Analytics Service GUI. You can only edit the group permissions. Users can be added or deleted from Citrix cloud.

Note

The user details appear on the service GUI only after the user has logged on to the NetScaler MA Service at least once.

Configuring Access Policies on NetScaler Management and Analytics Service

Access policies define permissions. A policy can be applied to a single user or group, or to multiple users and multiple groups.

NetScaler Management and Analytics Service provides five predefined access policies:

- **admin_policy**. Grants access to all NetScaler MA Service features. The user has both view and edit permissions, can view all NetScaler MA Service content, and can perform all edit operations. That is, the user can perform add, modify, and delete operations on the resources.
- **adminExceptSystem_policy**. Grants access to all non-admin users, except access to the Settings node in NetScaler MA Service GUI.
- **readonly_policy**. Grants read-only permissions. The user can view all content on NetScaler MA Service, but is not authorized to perform any operations.
- **appadmin_policy**. Grants administrative permissions for accessing the application features in NetScaler MA Service. A user bound to this policy can add, modify, and delete custom applications, and can enable or disable the services, service groups, and the various virtual servers, such as content switching, cache redirection, and HAProxy virtual servers.
- **appreadonly_policy**. Grants read-only permission for application features. A user bound to this policy can view the applications, but cannot perform any add, modify, or delete, enable, or disable operations.

Though you cannot edit the predefined policies, you can create your own (user-defined) policies.

To create user-defined access policies

1. In NetScaler MA Service GUI, navigate to **Settings > User Administration > Access Policies**.
2. Click **Add**.
3. On the **Create Access Policies** page, in the **Policy Name** field, enter the name of the policy, and enter the description in the **Policy Description** field.



← Create Access Policies

Policy Name*

Policy Description

Permissions

- All
 - Applications
 - Dashboard
 - App Security Dashboard
 - Configuration
 - Networks
 - Sites and IP Blocks
 - Configuration
 - Events
 - Network Functions
 - Certificate Management
 - Instance Groups
 - Network Dashboard
 - Instances
 - Agents
 - Configuration Audit
 - Network Reporting
 - API
 - System
 - User Administration
 - System Configuration
 - Analytics Settings
 - Subscriptions
 - Auditing
 - Analytics

Create

Close

Note

Selecting **Edit** might internally assign dependent permissions that are not shown as enabled in the Permissions section. For example, when you enable edit permissions for fault management, NetScaler Management and Analytics Service internally provides

permission for configuring a mail profile or for creating SMTP server setups, so that the user can send the report as a mail.

4. Click **Create**.

The **Permissions** section lists of all NetScaler MA Service features, with options for specifying read-only or edit access. Click the (+) icon to expand each feature group into multiple features. You must select the check box next to the feature name to give the users either the View or Edit permissions. The Edit option includes permission to view. Select **View** for read-only, or **Edit** for full access.

Configuring Roles on NetScaler Management and Analytics Service

In NetScaler Management and Analytics Service, each role is bound to one or more access policies. You can define one-to-one, one-to-many, and many-to-many relationships between policies and roles. You can bind one role to multiple policies, and you can bind multiple roles to one policy.

For example, a role might be bound to two policies, with one policy defining access permissions for one feature and the other policy defining access permissions for another feature. One policy might grant permission to add NetScaler instances in NetScaler Management and Analytics Service, and the other policy might grant permission to create and deploy StyleBooks and to configure NetScaler instances.

When multiple policies define edit and read-only permissions for a single feature, the edit permissions have priority over read-only permissions.

NetScaler Management and Analytics Service provides five predefined roles:

- **admin_role**. Has access to all NetScaler Management and Analytics Service features. (This role is bound to adminpolicy.)
- **adminExceptSystem_role**. Has access to the NetScaler Management and Analytics Service GUI except the Settings permissions. (This role is bound to adminExceptSystem_policy)
- **readonly_role**. Has read-only access. (This role is bound to readonlypolicy.)
- **appAdmin_role**. Has administrative access to only the application features in NetScaler Management and Analytics Service. (This role is bound to appAdminPolicy).
- **appReadonly_role**. Has read-only access to the application features. (This role is bound to appReadOnlyPolicy.)

Though you cannot edit the predefined roles, you can create your own (user-defined) roles.

To create roles and assign policies to them

1. In NetScaler MA Service GUI, navigate to **Settings > User Administration > Roles**.
2. Click **Add**.
3. On **Create Roles** page, in the **Role Name** field, enter the name of the role, and provide the description in the **Role Description** field (optional.)
4. In the **Policies** section, add move one or more policies to the **Configured** list.

Note

The policies are pre-fixed with a tenant ID (for example, maasdocfour) that is unique to all tenants.

← Create Roles

Role Name*

Role Description

Policies*

Available (5) [Select All](#)

maasdocfour_readonly_policy	+
maasdocfour_appadmin_policy	+
maasdocfour_admin_policy	+
maasdocfour_adminExceptSystem...	+
maasdocfour_appreadonly_policy	+

[New](#) | [Edit](#)

Configured (1) [Remove All](#)

Security-Admin-policy	-
-----------------------	---

→
←

[Create](#)

Note

You can create a new access policy by clicking **New**, or you can navigate to **Settings > User Administration > Access Policies**, and create new policies.

5. Click **Create**.

Configuring Groups on NetScaler Management and Analytics Service

In NetScaler Management and Analytics Service, a group can have both feature-level and resource-level access. For

example, one group of users might have access to only selected NetScaler instances; another group to only a selected few applications, and so on. When you create a group, you can assign roles to the group, provide application level access to the group, and assign users to the group. All users in that group are assigned the same access rights in NetScaler Management and Analytics Service.

To Create User Groups and Assign Roles to User Groups

1. In NetScaler MA Service GUI, navigate to **Settings > User Administration > Groups**.
2. Click **Add**.
3. On the **Create System Group** page, in the **Group Name** field, enter the name of the group.
4. In the **Roles** section, move one or more roles to the **Configured** list.

Note

The roles are pre-fixed with a tenant ID (for example, maasdocfour) that is unique to all tenants.

5. Under the **Available** list, you can click **New** or **Edit** and create or modify roles. Alternatively, you can navigate to **System > User Administration > Users**, and create or modify users.
6. Optionally, clear the **All Instances** check box and select specific instances. By default, this check box is selected, allowing the users to view and configure all NetScaler instances. You can clear the check box and select only those NetScaler instances that you want the users to access.

← Create System Group

Group Settings Applications and Templates Select Users

Group Name*

Roles*

Available (5) [Select All](#)

maasdocfour_readonly_role	+
maasdocfour_appReadonly_role	+
maasdocfour_admin_role	+
maasdocfour_appAdmin_role	+
maasdocfour_adminExceptSystem...	+

[New](#) | [Edit](#)

Configured (1) [Remove All](#)

Security-Admin-Role	-
---------------------	---




All Instances

Note

You can create a new role by clicking **New**, or you can navigate to **Settings > User Administration > Roles**, and create new roles.

7. Click **Next**. On the screen that appears, you can clear the **All Applications** and **All Configuration templates** checkboxes, and select only the required applications and templates. Or, to allow access to all applications and templates, leave these check boxes selected.

← Create System Group

 Group Settings  **Applications and Templates**  Select Users

All Applications

Add Applications Delete

<input type="checkbox"/>	Name
<input checked="" type="checkbox"/>	asd2_10.102.29.60_lb

All Configuration templates

Add Configuration Template Delete

<input type="checkbox"/>	Name
<input checked="" type="checkbox"/>	AddUserAdvancedPlatform
<input checked="" type="checkbox"/>	AddUser

Cancel ← Back Next →

8. Click **Next**.

9. In the **Users** section, select the user in the **Available** list, and add the user to the **Configured** list.

Note

You can also add new users by clicking **New**.

← Create System Group

The screenshot shows the 'Select Users' step of the 'Create System Group' wizard. At the top, there are three tabs: 'Group Settings', 'Applications and Templates', and 'Select Users'. Below the tabs, the 'Users' section is divided into two panels. The left panel, titled 'Available (5)', contains a search box and a 'Select All' link. Below the search box, the email address 'maasdoc+five@gmail.com' is listed with a plus sign to its right. The right panel, titled 'Configured (1)', also has a search box and a 'Remove All' link. Below the search box, the email address 'maasdoc+davidt@gmail.com' is listed with a minus sign to its right. Between the two panels are two arrow buttons: a right-pointing arrow on top and a left-pointing arrow on the bottom. At the bottom of the wizard, there are three buttons: 'Cancel', '← Back', and 'Finish'.

10. Click **Finish**.

Limitations

RBAC is not fully supported for the following NetScaler Management and Analytics Service features:

- Analytics - RBAC is not supported fully in the analytics modules. RBAC support is limited to instance level, and it is not applicable at application level in the Gateway Insight, HDX Insight, and Security Insight analytics modules.
 - Example 1: Instance based RBAC (Supported). An administrator who has been assigned a few instances can see only those instances under HDX Insight > Devices, and only the corresponding virtual servers under HDX Insight > Applications, because RBAC is supported at instance level.
 - Example 2: Application based RBAC (Not Supported). An administrator who has been assigned a few applications can see all virtual servers under HDX Insight > Applications but cannot access them, because RBAC is not supported at applications level.
- StyleBooks – RBAC is not fully supported for StyleBooks.
 - In NetScaler MA Service, Stylebooks and configuration packs are considered as separate resources. Access permissions, either view, edit, or both, can be provided for Stylebook and configuration packs separately or concurrently. A view or edit permission on configuration packs implicitly allows the user to view the StyleBooks, which is essential for getting the configpack details and creating new configuration packs.
 - Access permission for specific Stylebook or configuration packs is not supported
Example: If there is already a configpack on the instance, users can modify the configuration on a target NetScaler instance even if they do not have access to that instance.

Configuring Analytics Settings

Jun 29, 2017

Before you start using the Analytics feature on NetScaler Management and Analytics Service (NetScaler MA Service) to gain visibility into your instance and application data, it is recommended that you configure a few analytics settings to ensure optimal experience with this feature.

Configuring Database Summarization for Analytics

Configure Database Summarization feature in NetScaler MA Service allows you to customize the duration for which you want to store the historical analytics data of your NetScaler instances. You can choose the following database summarization types:

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

To Configure Database Summarization

1. In a supported web browser, logon to your NetScaler MA Service.
2. Navigate to **Settings > Analytics Settings > Database Summarization**.
3. Click the name of the Insight type for which you want to configure database summarization. For example, if you want to configure database summarization for Gateway Insight, click **GatewayInsight**.

[Analytics Settings](#) / Database Summarization Configuration

Database Summarization Configuration



<input type="checkbox"/>	Insight Name	Hours to persist minutely data	Days to persist hourly data	Days to persist daily data
<input type="checkbox"/>	GatewayInsight	2 Hours	1 Days	31 Days
<input type="checkbox"/>	HDXInsight	2 Hours	1 Days	31 Days
<input type="checkbox"/>	SecurityInsight	2 Hours	1 Days	31 Days

4. Specify the duration for which you want to retain Insight data on NetScaler MA Service, and then click **OK**. For example, for Gateway Insight, you can store your analytics' minutely historical data for 2 hours, or hourly data for 1 day.

← Gateway Insight

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

Hours to persist minutely data

Days to persist hourly data

Days to persist daily data

Creating Thresholds and Alerts for Analytics

You can set thresholds and alerts to monitor the analytics' metrics of the managed virtual servers configured on the discovered instances. When the value of a metrics exceeds the threshold, NetScaler Management and Analytics Service (NetScaler MA Service) generates an event to signify a threshold breach.

You can also associate actions with the set thresholds. Actions include displaying an alert on the GUI, sending Email, or SMS notifications, as configured.

For example, you can set a threshold to generate an event for HDX insight if any user's ICA RTT value exceeds 1 second. You can also enable alerts for the generated event, and send the threshold breach information to a configured Email or SMS distribution list.

To create thresholds and alerts for analytics

1. In a supported web browser, logon to your NetScaler MA Service.
2. Navigate to **Settings > Analytics Settings > Thresholds**.
3. On the **Thresholds** screen, click **Add** to add a new threshold and configure alerts for the set thresholds.
4. On the **Create Thresholds and Alerts** page, specify the following details:
 - **Name** – Name for configuring the threshold.
 - **Traffic Type** – Type of analytics traffic for which you want to configure the threshold. For example: HDX Insight, Security Insight.
 - **Entity** – Category or resource type for which you want to configure the threshold.
 - **Reference Key** – Automatically generated value based on the selected traffic type and entity.
 - **Duration** - Interval for which you want to configure the threshold.
5. To configure alerts, such as emails notifications and SMS notifications, select the appropriate check boxes for the set thresholds.

6. In the **Rules** section, specify the following:

- **Metric** – Metric for the selected Traffic type to configure the threshold.
- **Comparator** – Comparator to the selected metric (for example: <, >=).
- **Value** – Value for the metric to set the threshold, and invoke alerts.

7. Click **Create**.

← Create Threshold and Alerts

Name*

Traffic Type*

Entity*

Reference Key

Duration*

Enable Alert
 Notify through Email
 Notify through SMS

Rule

Metric* <input type="text" value="Total Session Launch Co"/>	Comparator* <input type="text" value=">"/>	Value* <input type="text" value="90000"/>
---	--	--

How-to Articles

Jun 29, 2017

NetScaler Management and Analytics Service (NetScaler MA Service) "How-to Articles" are simple, relevant, and easy to implement articles on the features available with the service. These articles contain information about some of the popular NetScaler MA Service features such as instance management, configuration management, event management, application management, StyleBooks, and certificate management.

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

Instance Management	Configuration Management	Certificate Management
Application Management	StyleBooks	Event Management

Instance Management

- [How to Monitor Globally Distributed Sites](#)
- [How to Manage Admin Partitions of NetScaler Instances](#)
- [How to Add Instances to NetScaler MA Service](#)
- [How to Create Instance Groups on NetScaler MA Service](#)
- [How to Configure Sites for Geomaps in NetScaler MA Service](#)
- [How to Force a Failover to the Secondary NetScaler Instance](#)
- [How to Force a Secondary NetScaler Instance to Stay Secondary](#)

Configuration Management

- [How to Use SCP \(put\) Command in Configuration Jobs](#)
- [How to Upgrade NetScaler SDX Instances by Using NetScaler MA Service](#)
- [How to Schedule Jobs Created by Using Built-in Templates in NetScaler MA Service](#)
- [How to Reschedule Jobs That Were Configured by Using Built-in Templates in NetScaler MA Service](#)
- [How to Reuse Executed Configuration Jobs](#)
- [How to Upgrade NetScaler Instances using NetScaler MA Service](#)
- [How to Create a Configuration Job on NetScaler MA Service](#)
- [How to Use Variables in Configuration Jobs on NetScaler MA Service](#)
- [How to Use Configuration Templates to Create Audit Templates on NetScaler MA Service](#)
- [How to Create Configuration Jobs from Corrective Commands on NetScaler MA Service](#)

[How to Replicate Running and Saved Configuration Commands from One NetScaler Instance to Another on NetScaler MA Service](#)

[How to Create Configuration Jobs for NetScaler SD-WAN WO Instances in NetScaler MA Service](#)

[How to Use Configuration Jobs to Replicate Configuration from One Instance to Multiple Instances](#)

[How to Use the Master Configuration Template on NetScaler MA Service](#)

Certificate Management

[How to Configure an Enterprise Policy on NetScaler MA Service](#)

[How to Install SSL Certificates on a NetScaler Instance from NetScaler MA Service](#)

[How to Update an Installed Certificate from NetScaler MA Service](#)

[How to Link and Unlink SSL Certificates by Using NetScaler MA Service](#)

[How to Create a Certificate Signing Request \(CSR\) by Using NetScaler MA Service](#)

[How to Set Up Notifications for SSL Certificate Expiry from NetScaler MA Service](#)

[How to Use the SSL Dashboard on NetScaler MA Service](#)

Application Management

[How to Search for Entities in NetScaler MA Service](#)

[How to Disable Entities in NetScaler MA Service](#)

[How to View the Effective State of a Virtual Server on NetScaler MA Service](#)

[How to Create an Application Definition in NetScaler MA Service](#)

[How to Create Load Balancing Support through Application Dashboard in NetScaler MA Service](#)

StyleBooks

[How to Use StyleBooks Shipped with NetScaler MA Service](#)

[How to Create Your Own StyleBooks](#)

[How to Use User-Defined StyleBooks in NetScaler MA Service](#)

[How to Use API to Create Configurations from StyleBooks](#)

[How to Enable Analytics and Configure Alarms on a Virtual Server Defined in a StyleBook](#)

[How to Create a StyleBook to Upload SSL Certificate and Certificate Key Files to NetScaler MA Service](#)

[How to Use Microsoft Skype for Business StyleBook in Business Enterprises](#)

[How to Use Microsoft Exchange StyleBook in Business Enterprises](#)

[How to Use Microsoft SharePoint StyleBook in Business Enterprises](#)

Event Management

[How to Set Event Age for Events on NetScaler MA Service](#)

[How to Schedule an Event Filter by Using NetScaler MA Service](#)

[How to Set Repeated Email Notifications for Events from NetScaler MA Service](#)

[How to Suppress Events by Using NetScaler MA Service](#)

[How to Use the Events Dashboard to Monitor Events](#)

[How to Create Event Rules on NetScaler MA Service](#)

[How to Modify the Reported Severity of Events that Occur on NetScaler Instances](#)

[How to View the Events Summary in NetScaler MA Service](#)

[How to Display Event Severities and Skews of SNMP Traps on NetScaler MA Service](#)

[How to Export Syslog Messages using NetScaler MA Service](#)

Known Issues

Jun 29, 2017

The known issues and their workarounds that exist in the NetScaler Management and Analytics Service (NetScaler MA Service), wherever applicable, are listed as follows:

Analytics

- Exporting reports to PDF/JPEG/PNG is not working in NetScaler MA Service. [# 683778]
- When you enable Insight from NetScaler MA Service, you cannot see the check mark against AppFlow as enabled, but the configuration to enable AppFlow is pushed to NetScaler instances. [# 688309]

Application Analytics and Management

- When you use Safari browser on Microsoft Windows operating system, App Dashboard and Security Analytics Dashboard do not load. You can see other features of NetScaler MA Service. [# 688617]
- Application Dashboard in NetScaler MA Service shows incorrect security metrics for custom-defined applications. [# 689041]

Networks

- If control proxy is not available during agent start up process, the agent is not able to retrieve the SNMP trap settings from NetScaler Management and Analytics Service and all the traps received from NetScaler instances are dropped.
Workaround: Run "masd restart" on agent when connectivity to NetScaler Management and Analytics Service has been established. [# 687027]
- You cannot upload a command file while creating a configuration job, though **Networks > Configuration Jobs > Create Job** displays the option to upload a file. [# 688967]
- When you configure a rule to monitor specific events in NetScaler MA Service, emails are not sent for the events that match the filter criteria. [# 688985]
- When you configure a rule to monitor specific events in NetScaler MA Service, job is not executed for the events that match the filter criteria that you have specified. [# 688986]
- When you configure a rule to monitor specific events in NetScaler MA Service, events are not suppressed for the configured time period. [# 688988]
- When you configure a rule to monitor specific events in NetScaler MA Service, SNMP traps are not sent to external trap destinations. [# 689018]
- Upgrade NetScaler feature in Maintenance Tasks is not supported in NetScaler MA Service. But, you can still view the option in the GUI. [# 689068]

Settings

- While using NetScaler MA Service, the storage data consumption might be displayed as more than the entitled storage limit of 5GB. [# 689330]
- While using NetScaler MA Service, you might get logged out abruptly.
Workaround: Log on to NetScaler MA Service again. [# 689012]
- When you delete the users from Citrix Cloud, the deleted user names are displayed in NetScaler MA Service in **Settings > User Administration > Users**. [# 686581]

Note: [# XXXXXXX] labels are internal tracking IDs used by the Citrix NetScaler team.

FAQs

Jun 29, 2017

The number of agents depends on the number of managed instances in a data center and the total throughput. Citrix recommends that you install at least one agent for every data center.

You can install only one agent when you log on to the service for the first time. To add multiple agents, first complete the initial setup, and then navigate to **Settings > Setup Agents**.

If you are onboarding for the first time, access the service GUI, navigate to the **Set Up Agent** screen, and click **Generate Activation Code**.

While trying to install a second agent, to generate a new activation code, navigate to **Settings > Generate Activation Code**.

Default credentials for NetScaler MA Service agent is nsrecover/nsroot. This logs you on to the shell prompt of the agent.

Minimum requirements: 8 GB RAM, 4 Virtual CPU, 120 GB Storage, 1 Virtual Network Interfaces, 1 Gbps Throughput

Recommended requirements: 32 GB RAM, 8 Virtual CPU, 500 GB Storage, 1 Virtual Network Interfaces, 1 Gbps Throughput

No, you cannot.

No, you do not have to add an additional disk. The agent is used only as an intermediary between the NetScaler MA Service and the instances in your enterprise data center or on the cloud. It does not store inventory or analytics data that would require an additional disk.

No, you cannot.

Access the agent console on your hypervisor, log on to the shell prompt by using the credentials nsrecover/nsroot, and then run the command "networkconfig".

- Make sure your agent has access to the Internet (configure DNS).
- Make sure you have copied the activation code correctly.
- Make sure you have entered the service URL correctly.
- Make sure you have the required ports open.

After the agent is successfully registered, access NetScaler MA Service and navigate to the **Set Up Agent** screen. You can see the discovered agent on the screen. If the agent is running fine, the status is indicated by a green icon. If it is not running, the state is indicated by a red icon.

You have to enable Insight on your virtual servers to be able to see the Analytics Reports. For details, see [Enabling Analytics](#).

For management and monitoring features, NetScaler instances running 10.5 and later are supported. Some features are only supported on certain NetScaler versions. For details, see [System Requirements](#).