

Slide 1 - ZCCP-IA



ZCCP-IA

Zscaler Nanolog Streaming Service (NSS)

©2019 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to the Zscaler Nanolog Streaming Service module.

Slide 2 - Navigating the eLearning Module



Slide notes

Here is a quick guide to navigating this eLearning module. There are various controls for playback including Play/Pause, Previous and Next Slide, and Fast Forward. You can also mute the Audio or enable Closed Captioning which will cause a transcript of the module to be displayed on the screen. Finally, you can click the "X" button if you wish to exit.

Slide 3 - Module Agenda

Module Agenda

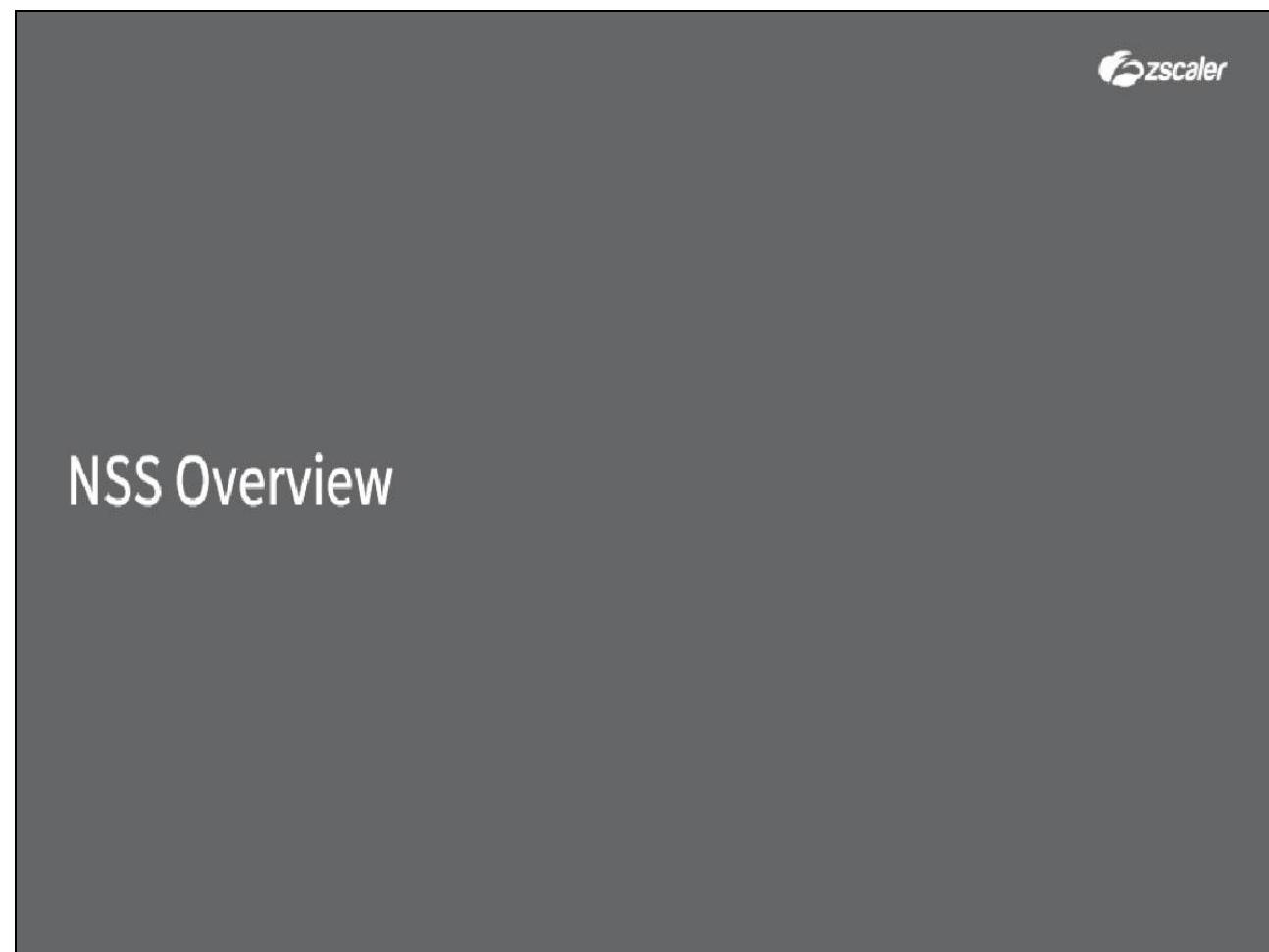


- NSS Overview
- NSS Requirements
- Deploying NSS
- Configuring NSS Feeds/Alerts
- Configuring Your SIEM

Slide notes

In this module we will cover: an overview of the Nanolog Streaming Service, Requirements for NSS, Deploying NSS, Configuring NSS Feeds and Alerts, and Configuring your SIEM.

Slide 4 - NSS Overview



Slide notes

Slide 5 - NSS Overview

NSS Overview



- Nanolog Streaming Service (NSS)
 - Service to stream Zscaler logs to the organization's SIEM
- Benefits:
 - ✓ Long term archival of logs
 - ✓ Real-time alerting by SIEM
 - ✓ Multiple streams
 - ✓ Correlation with other devices in your network
 - ✓ Flexible Log format and filtering
 - ✓ User obfuscation
 - ✓ Automatic updates

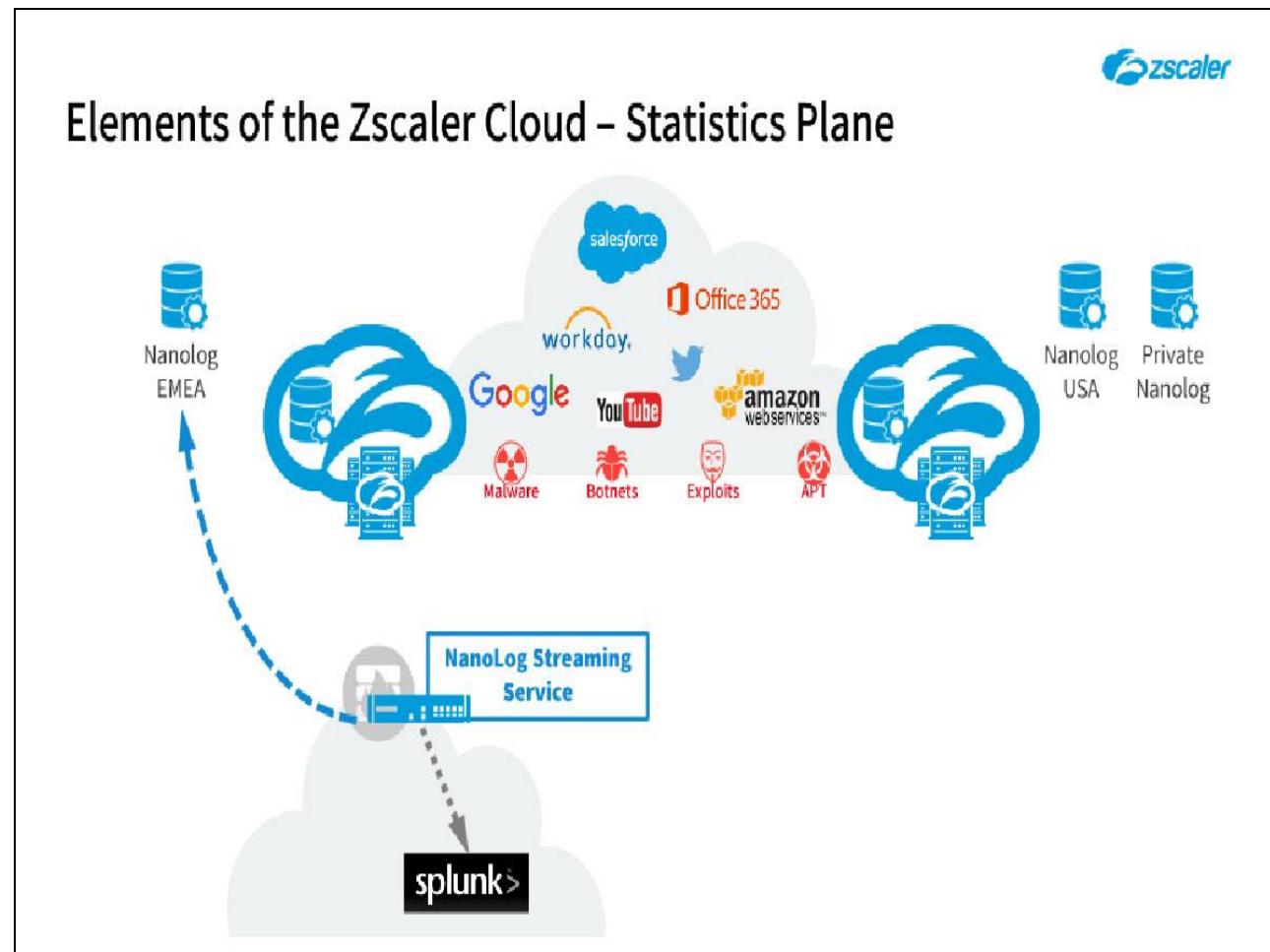
Slide notes

The Nanolog Streaming Service is a mechanism for streaming log data generated by Zscaler into your organization's SIEM. Some of the benefits include: Long term archiving of logs. Zscaler stores logs for a maximum of one year. If you wish to store logs beyond that time you will need NSS to deliver them into your organization where they can be stored locally.

NSS allows real-time alerting by your SIEM as well as allows event correlation with other devices in your network. NSS allows a great deal of control over which logs are sent to your SIEM and the format of those logs. NSS can be configured to deliver multiple streams for redundancy or to separate data like sending URL category violations to a different system than security alerts.

Depending on your regulatory and HR policies you can optionally obfuscate user identities. Finally, once the NSS is configured it is managed by Zscaler and any software updates are automatically applied.

Slide 6 - Elements of the Zscaler Cloud – Statistics Plane



Slide notes

The Nanolog Streaming Service is performed by a virtual machine that is installed inside your network or DMZ. A certificate-based TLS connection is made from the NSS virtual machine to a nanolog cluster. Then, when users are browsing through Zscaler, the logs that you specify are sent down that TLS tunnel into the NSS virtual machine and then on to your SIEM.

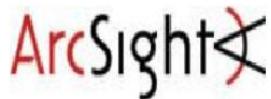
Slide 7 - SIEM Compatibility & Integration



SIEM Compatibility & Integration



- Partnered with IBM for QRadar integration
- Support for QRadar LEEF format
- Works with Zscaler DSM (Device Support Module) written by IBM



- Partnered with HP for Arcsight integration
- Support for Arcsight CEF format
- Works with Arcsight Connector to send logs into Arcsight ESM



- Partnered with Splunk for integration
- Support for CIM format for Splunk ESM integration
- Zscaler app on Splunkbase available for free



- Format flexibility -> to output logs in native format of SIEMs
- Logs can be sent as syslog
- Responsibility of NSS is to ensure that the logs reach the SIEM

Slide notes

Zscaler provides built-in support for a variety of SIEMs. Logs can also be sent as syslog, CSV, or tab separated

Slide 8 - Fault Tolerance

<h2>Fault Tolerance</h2>		
Multiple Redundancy Options	SIEM Connection Loss	NSS Connection Loss
<ul style="list-style-type: none">Up to 2 active NSS's for Active-Active SIEMsEach NSS can be deployed as Active/Passive	<ul style="list-style-type: none">NSS will buffer at least 1 hour of logs (can be increased with more RAM)Can resend logs for X minutes prior to connection loss detection	<ul style="list-style-type: none">Nanolog automatically sends any missed logs

Slide notes

Zscaler supports multiple redundancy options depending on your SIEM deployment. You can have up to 2 active NSS Virtual Machines at a time for when your SIEMs run Active-Active. You can also deploy additional NSS Virtual Machines as cold standbys by using the same TLS client certificate as the primary. Make sure you do not have both Virtual Machines active at the same time or lost logs may result.

If the NSS Virtual Machine loses connection with your SIEM, the NSS will automatically buffer logs until connectivity is reestablished. If you are using the minimum calculated amount of RAM for the Virtual Machine it will be able to buffer for at least 1 hours of logs. If you allocate more RAM to the Virtual Machine this time will be increased.

Once connectivity is reestablished, you can configure NSS to send logs starting with some number of minutes before the connectivity loss was detected. Each log has a unique record ID so your SIEM can eliminate duplicate logs. In the case that the NSS Virtual Machine loses connectivity with the Nanolog, any missed logs will be automatically sent when connectivity is reestablished.

Slide 9 - NSS Requirements



NSS Requirements

Slide notes

Slide 10 - NSS Requirements

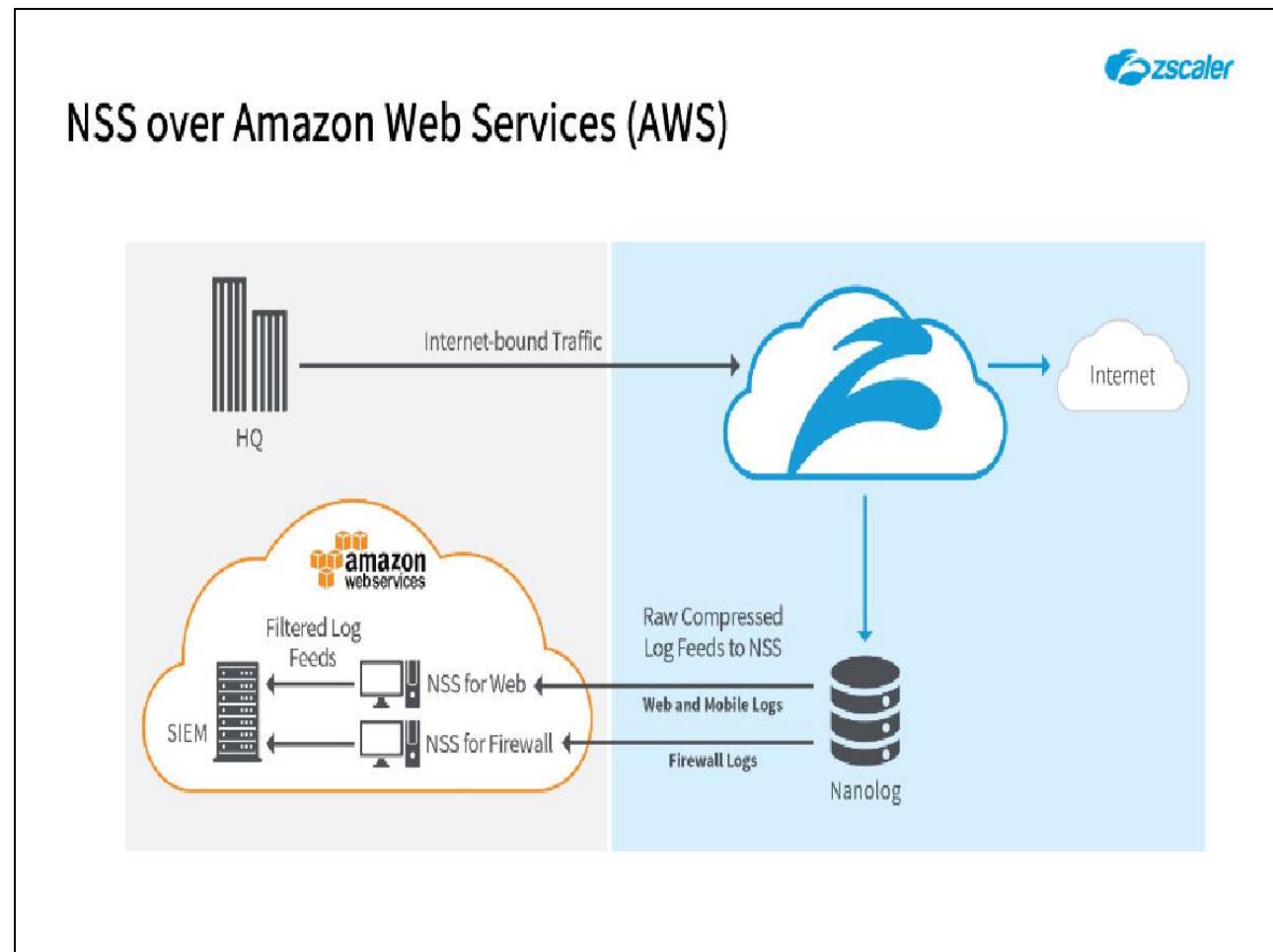
 NSS Requirements - on-prem VM		
VM Host	VM Specs	Network Specs
<ul style="list-style-type: none">• Vmware ESX/ESXi v5 or above• 64-bit Xeon or equivalent at least 2.0GHz• VMWare vSphere Client or vCenter	<ul style="list-style-type: none">• VM CPU: 2 cores<ul style="list-style-type: none">◦ 1 for control plane (OS)◦ 1 for data plane (NSS service)• VM Memory: Variable 8GB-32GB based on number of users/traffic• VM Disk Space: 500GB	<ul style="list-style-type: none">• 2 virtual NICs:<ul style="list-style-type: none">◦ 1 for management◦ 1 for data connection to Zscaler and SIEM• Bandwidth: Variable based on number of users/traffic• Outbound access:<ul style="list-style-type: none">◦ Access through firewall to Zscaler cloud IP, see: <a href="https://ips.<cloud name>.net">https://ips.<cloud name>.net◦ NAT is supported

Slide notes

Here are the basic requirements for the NSS virtual machine. The Zscaler Admin UI contains a calculator that will give you more specific recommendations for CPU, memory, disk storage, and bandwidth based on the number of users and expected peak transactions per hour.

We'll walk through that during the demo portion. For the network portion you will need to allocate 2 IP addresses and allow connectivity to the Zscaler Nanolog clusters. You can find a detailed list of IP addresses and ports needed at ips.<cloud name>.net

Slide 11 - NSS over Amazon Web Services (AWS)



Slide notes

Another option for deploying NSS is on an EC2 Instance on Amazon Web Services. One NSS instance is deployed for web and mobile logs and another NSS instance is deployed for firewall logs. The Nanolog then streams copies of the logs to each NSS in AWS in a highly compressed format to reduce bandwidth footprint. The original logs are retained on the Nanolog for 6 months.

Logs can be retained on the SIEM based on the organization's needs and SIEM configuration.

Slide 12 - NSS Requirements for AWS

NSS Requirements for AWS		
AWS	EC2 Instance	Network Specs
<ul style="list-style-type: none">An AWS account with access to an AWS Console	<ul style="list-style-type: none">EC2 CPU: dual-core instance<ul style="list-style-type: none">1 for control plane (OS)1 for data plane (NSS service)EC2 Memory:<ul style="list-style-type: none">8GB up to 15K users16GB up to 40K users32GB up to 100K usersEBS Storage Size: 500GB	<ul style="list-style-type: none">2 EC2 Network Interfaces:<ul style="list-style-type: none">1 for management1 for data connection to Zscaler and SIEM2 Elastic IPsBandwidth:<ul style="list-style-type: none">Variable based on number of users/traffic11Mbps per 10K usersOutbound access:<ul style="list-style-type: none">Access through firewall to Zscaler cloud IP, see: <a href="https://ips.<cloud name>.net">https://ips.<cloud name>.netNAT is supported

Slide notes

This slide lists the requirements for deploying an NSS instance on AWS. Press pause in the player to review and then press Play when you are ready.

Slide 13 - Optional : Enable SNMP management of NSS



Optional : Enable SNMP management of NSS

Slide notes

Slide 14 - Optional SNMP monitoring



Optional SNMP monitoring

- SNMP monitoring of NSS is available as an option
- The NSS MIB is downloaded from the NSS configuration page
- SNMP is disabled by default and is enabled via the NSS console using the command “`nss snmp-admin-configure`”
- The following tables can be monitored via your SNMP management application:

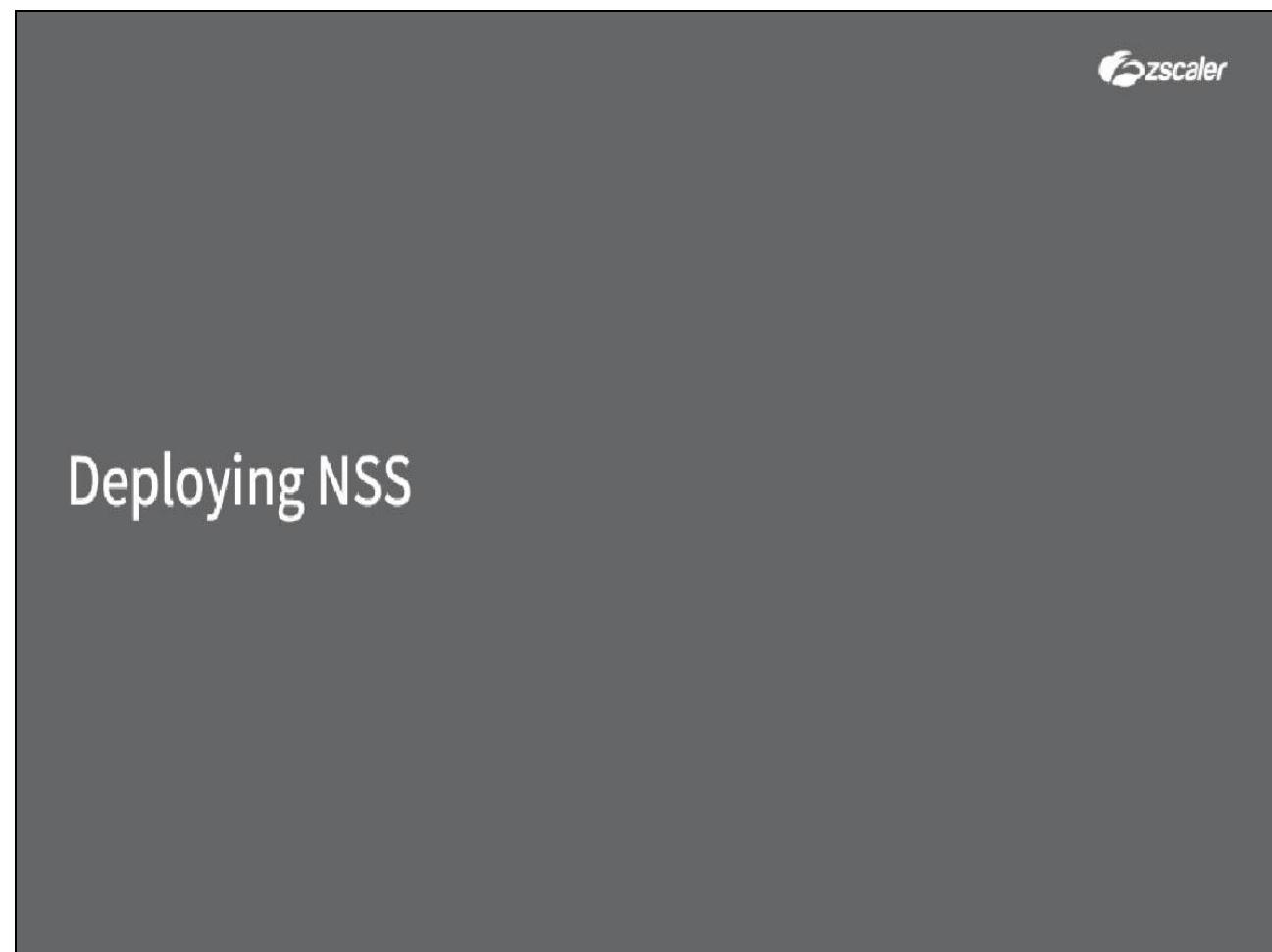
Zscaler MIB Files	Description
<code>ZSCALER-NSSFEED-MIB.mib</code>	This module describes information specific to NSS feeds.
<code>ZSCALER-NSS-MIB.mib</code>	This module describes information specific to the NSS instance.
<code>ZSCALER-OSNIC-MIB.mib</code>	This module describes the NIC devices managed by the OS. On a Zscaler system, there are NIC devices managed by the Zscaler instances and also by the base OS.
<code>ZSCALER-PROCESSHEALTH-MIB.mib</code>	This module describes health information for all watched processes in the Zscaler instance.
<code>ZSCALER-PROCESSWATCHDOG-MIB.mib</code>	This module describes the process watchdog information for each of the managed processes of a Zscaler instance. For example: For a SME type of instance, the watched processes are smme, smavd, smavd2, smcdisc, and sctimer.
<code>ZSCALER-ROLEHEALTH-MIB.mib</code>	This module describes the health information for a Zscaler instance. This includes many of the OS level information for the instance such as CPU, memory, and also some instance specific information. Example: current connections on SME.
<code>ZSCALER-SWAPINFO-MIB.mib</code>	This module describes the status of the swap devices present on the system.
<code>ZSCALER-ZSCALERNIC-MIB.mib</code>	This module describes the NIC devices managed by the Zscaler instance. On a Zscaler system, there are NIC devices managed by the Zscaler instances and also by the base OS.

Slide notes

Monitoring of the NSS Virtual Machine may be done via SNMP. A copy of the NSS MIB file can be downloaded from the NSS configuration page in the Zscaler Admin UI and then imported into your own SNMP manager application.

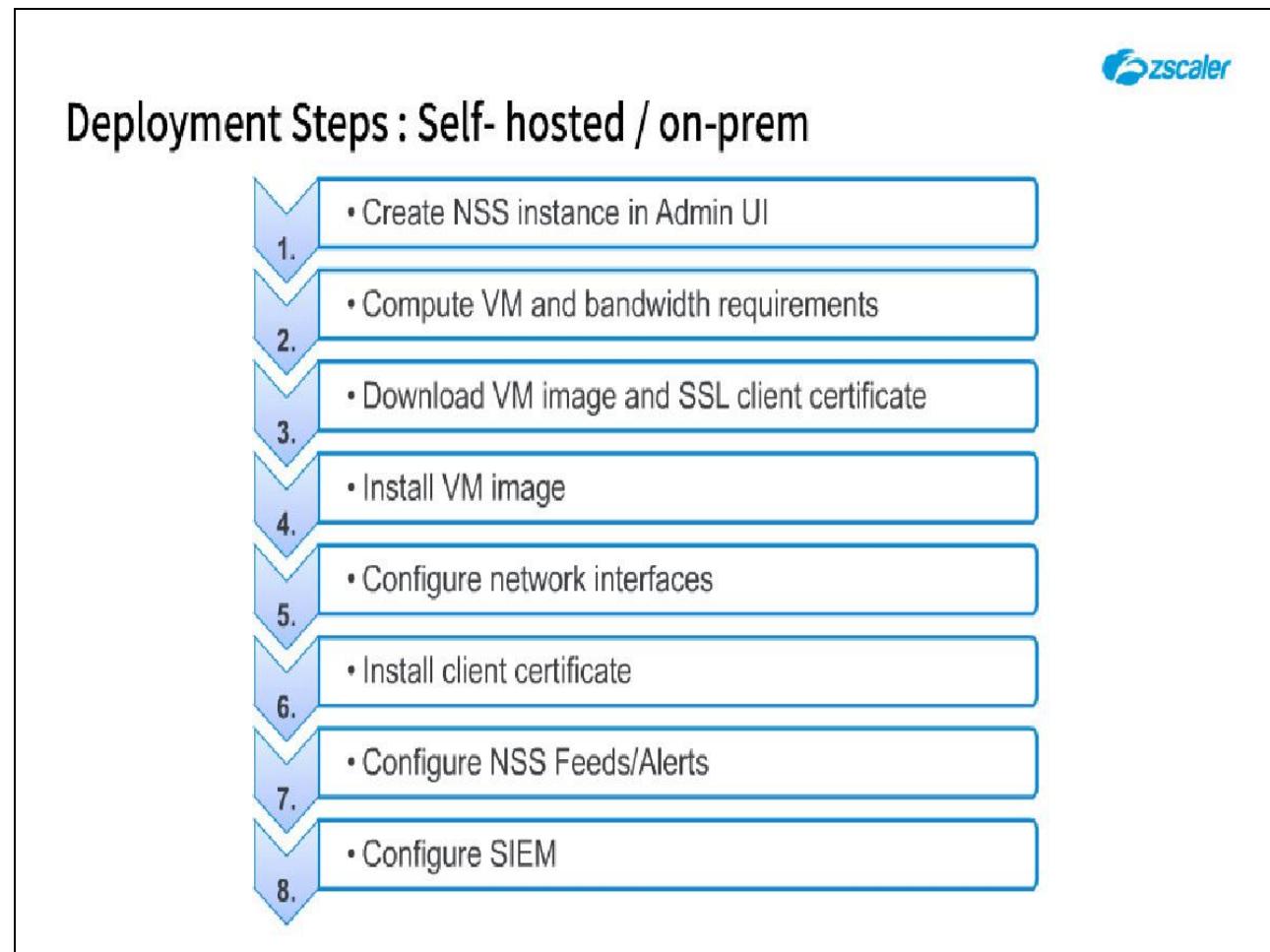
SNMP is disabled by default. It must be enabled from the NSS console using the command “`NSS snmp-admin-configure`” to configure the SNMP username, password, authentication type, and encryption type for the SNMP manager. Once enabled and configured you can monitor the NSS via your SNMP manager.

Slide 15 - Deploying NSS



Slide notes

Slide 16 - Deployment Steps



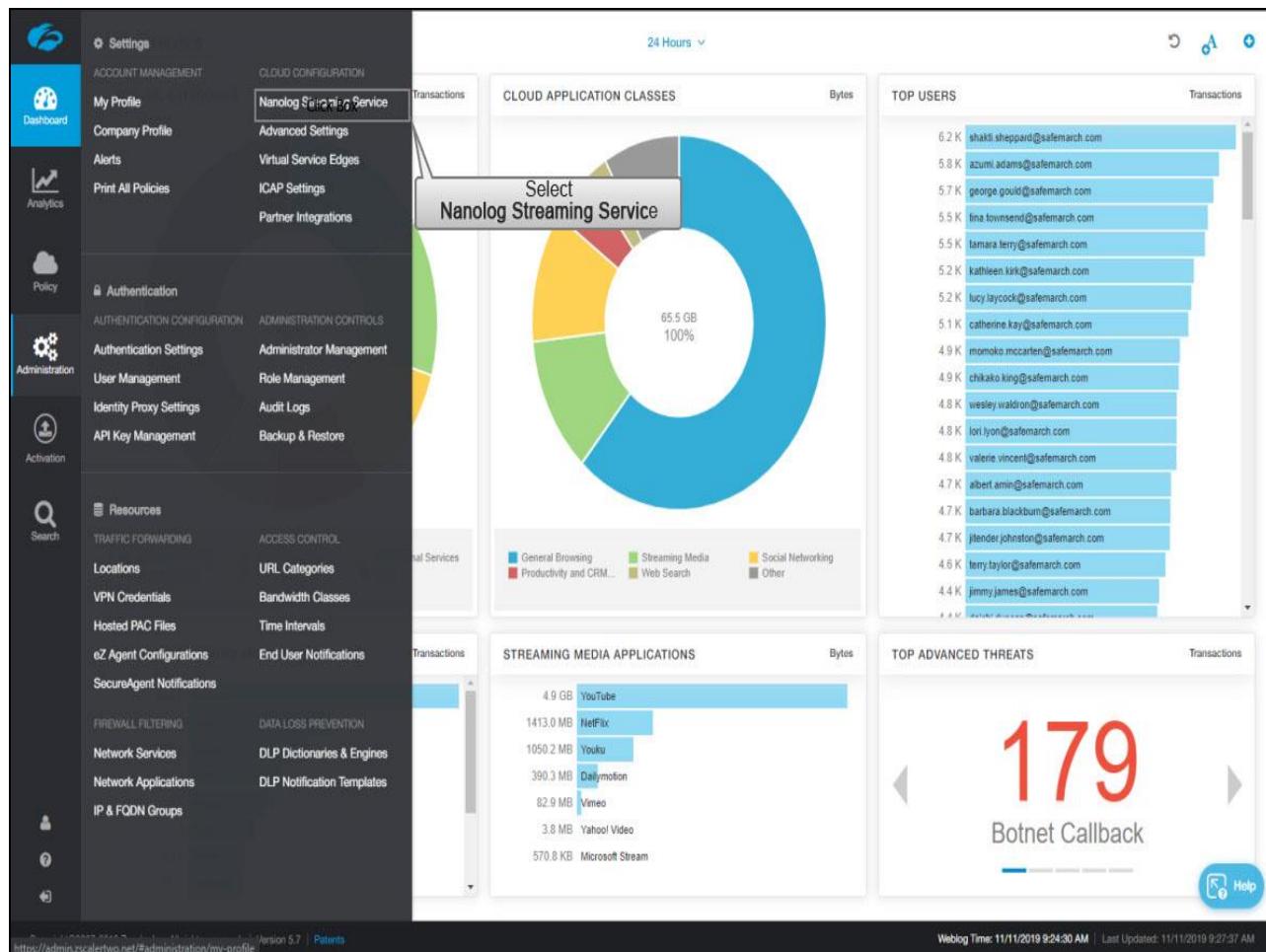
Slide notes

Here are the steps to Deploying NSS. Create an NSS instance in the Admin UI. Compute VM and bandwidth requirements. Download the VM image and SSL client certificate. Install the VM image. Configure network interfaces. Install the SSL client certificate. Configure NSS Feeds and Alerts in the Zscaler Admin UI. And finally, configure your SIEM to receive the logs.



Slide notes

Log into the Zscaler Admin UI and click on the “Administration” tab.



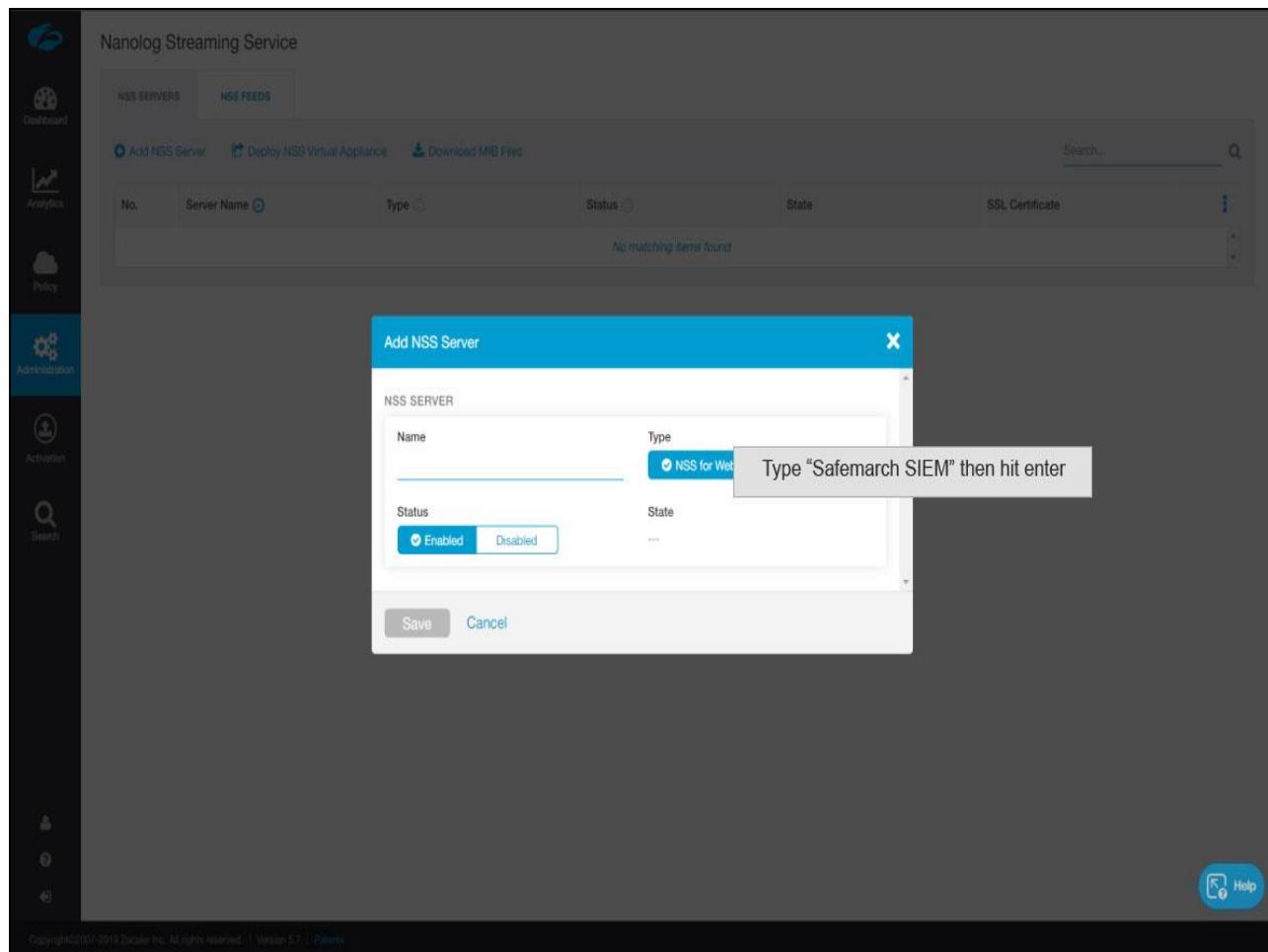
Slide notes

Click on Nanolog Streaming Service.

The screenshot shows the Zscaler Nanolog Streaming Service interface. On the left, there's a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration (which is selected), Activation, and Search. The main area is titled "Nanolog Streaming Service" and has tabs for "NSS SERVERS" (selected) and "NSS FEEDS". Below the tabs are buttons for "Click Box" (with a tooltip "Click Box over"), "Deploy NSS Virtual Appliance", and "Download MIB Files". A search bar with placeholder "Search..." and a magnifying glass icon is also present. The main content area displays a table with columns: No., Server Name (with a tooltip "Select Add NSS Server" highlighted with a red box), Type, Status, State, and SSL Certificate. A message at the bottom of the table says "No matching items found". At the bottom right of the main area is a "Help" button with a gear icon.

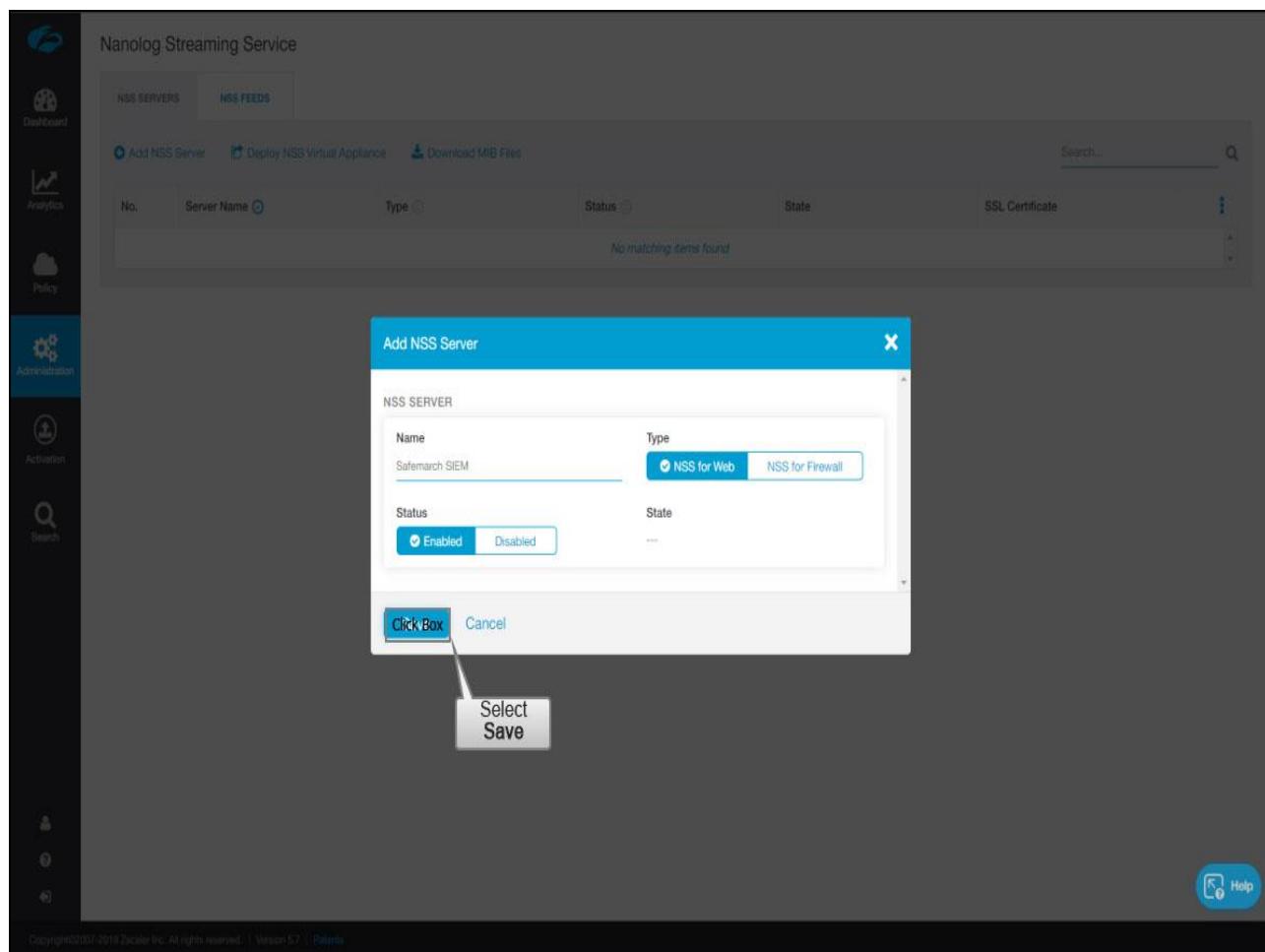
Slide notes

Click Add NSS Server



Slide notes

Name this NSS instance



Slide notes

and click “Save”.

The screenshot shows the Zscaler Nanolog Streaming Service interface. The main window displays the 'NSS SERVERS' tab, which lists a single server named 'Safemarch SIEM'. The server details are as follows:

No.	Server Name	Type	Status	State	SSL Certificate
1	Safemarch SIEM	NSS for Web	Enabled	---	Download

A callout box with the text 'Select Activation' points to the 'Activation' button in the left sidebar. The sidebar also includes icons for Dashboard, Analytics, Policy, Administration, Click Protection, and Search. A message at the top of the main window says 'All changes have been saved.'

Slide notes

Then **Activate** your changes.

The screenshot shows the Zscaler Activation interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation (which is selected and highlighted in blue), and Search. The main area has a title bar with 'MY ACTIVATION STATUS' and 'Editing'. It shows 'CURRENTLY EDITING (1)' and 'admin@training1.zsclearn.com'. Below this is a table with columns: Type, Status, State, and SSL Certificate. One row is visible: 'NSS for Web' with 'Enabled' status and '---' state. There are 'Download' and 'Edit' buttons for this row. A blue box highlights the 'Force Activate' checkbox under the 'Type' column. A callout bubble points to this box with the text 'Select Activate'.

Type	Status	State	SSL Certificate
NSS for Web	Enabled	---	Download Edit

Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents

Slide notes

The screenshot shows the Nanolog Streaming Service interface. On the left, there is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Nanolog Streaming Service" and has a message "Activation Completed!" at the top. It features two tabs: "NSS SERVERS" (selected) and "NSS FEEDS". Below the tabs are three buttons: "Add NSS Server", "Deploy NSS Virtual Appliance", and "Download MIB Files". A search bar with placeholder text "Search..." is also present. The main content area displays a table with one row of data:

No.	Server Name	Type	Status	State	SSL Certificate
1	Safemarch SIEM	NSS for Web	Enabled	---	Download

At the bottom right of the main area is a "Help" button. At the very bottom of the screen, there is a footer bar with the text "Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents".

Slide notes

The screenshot shows the Zscaler Admin UI interface for the Nanolog Streaming Service. The main content area displays the NSS SERVERS tab, showing a table with one row of data:

No.	Server Name	Type	Status	State	SSL Certificate
1	Search SIEM	NSS for Web	Enabled	---	Download

The sidebar on the left contains several tabs: Dashboard, ClickBox, Analytics (which is highlighted), Policy, Administration, Activation, and Search. A callout box with the text "Select Analytics" points to the Analytics tab. At the bottom of the screen, there is a copyright notice: "Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents".

Slide notes

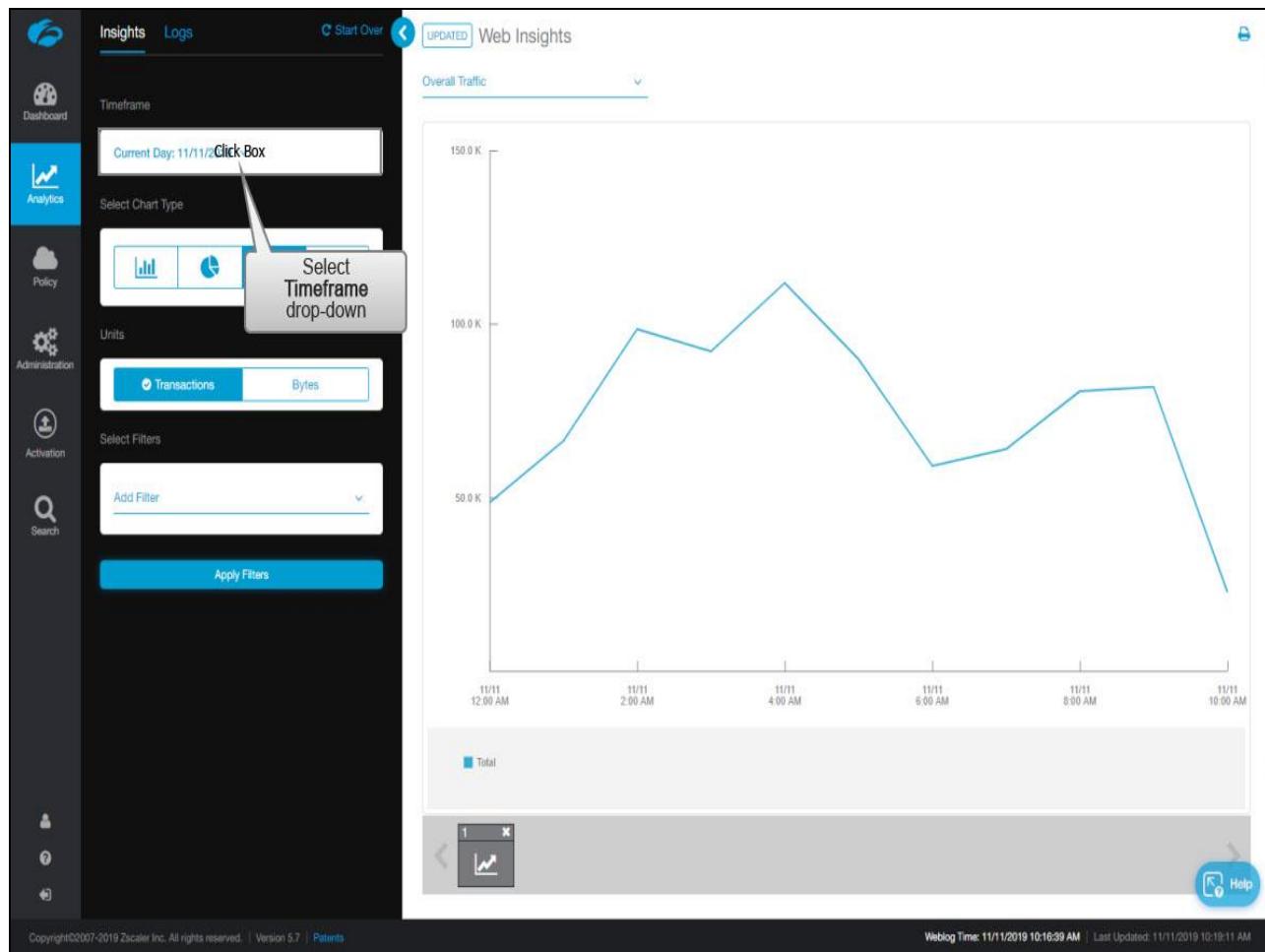
Our next step is to download the VM image. But before we do that, we need to have two data points to correctly size the VM. You will need your number of users and your peak transactions per hour. The first one is pretty straightforward. For the second you can use the Zscaler Admin UI itself to give you the number. Click the Analytics Tab

The screenshot shows the Zscaler NSS interface. On the left, there's a sidebar with various navigation options: Reporting, Interactive Reports, Executive Reports, Scheduled Reports, Company Risk Score Report (marked as NEW), Industry Peer Comparison, System Audit Report, Security Policy Audit Report, Sandbox Activity Report (marked as NEW), Activation, Search, and several user-related icons. The main content area has tabs for 'REPORTING' and 'INSIGHTS'. Under 'INSIGHTS', there are several options: Web Insights (highlighted with a red box and a 'Select Web Insights' callout), Mobile Insights, Firewall Insights, DNS Insights, Threat Insights (marked as NEW), and Tunnel Insights. At the top right of the main area, there are buttons for 'NSS Virtual Appliance', 'Download MIB Files', and a search bar. Below the search bar is a table with columns: Type, Status, State, and SSL Certificate. A single row is shown: Type is 'NSS for Web', Status is 'Enabled', State is 'Unhealthy', and there's a 'Download' button. At the bottom of the interface, there's a footer with the URL 'https://admin.zscaler.net/reports' and the text 'rights reserved. | Version 5.7 | Patents'.

Slide notes

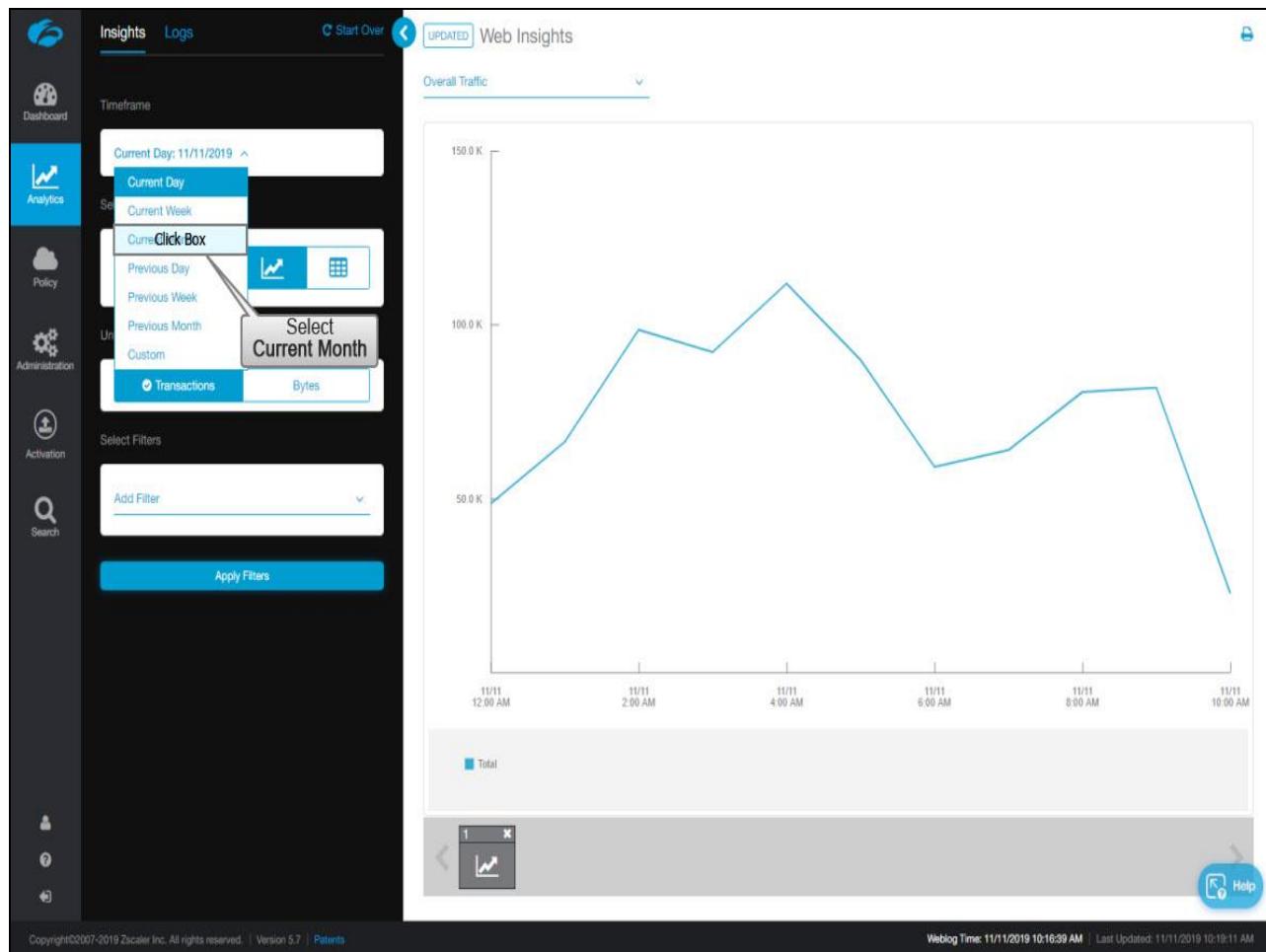
and then click “Web Insights”.

Slide 32 - Slide 32



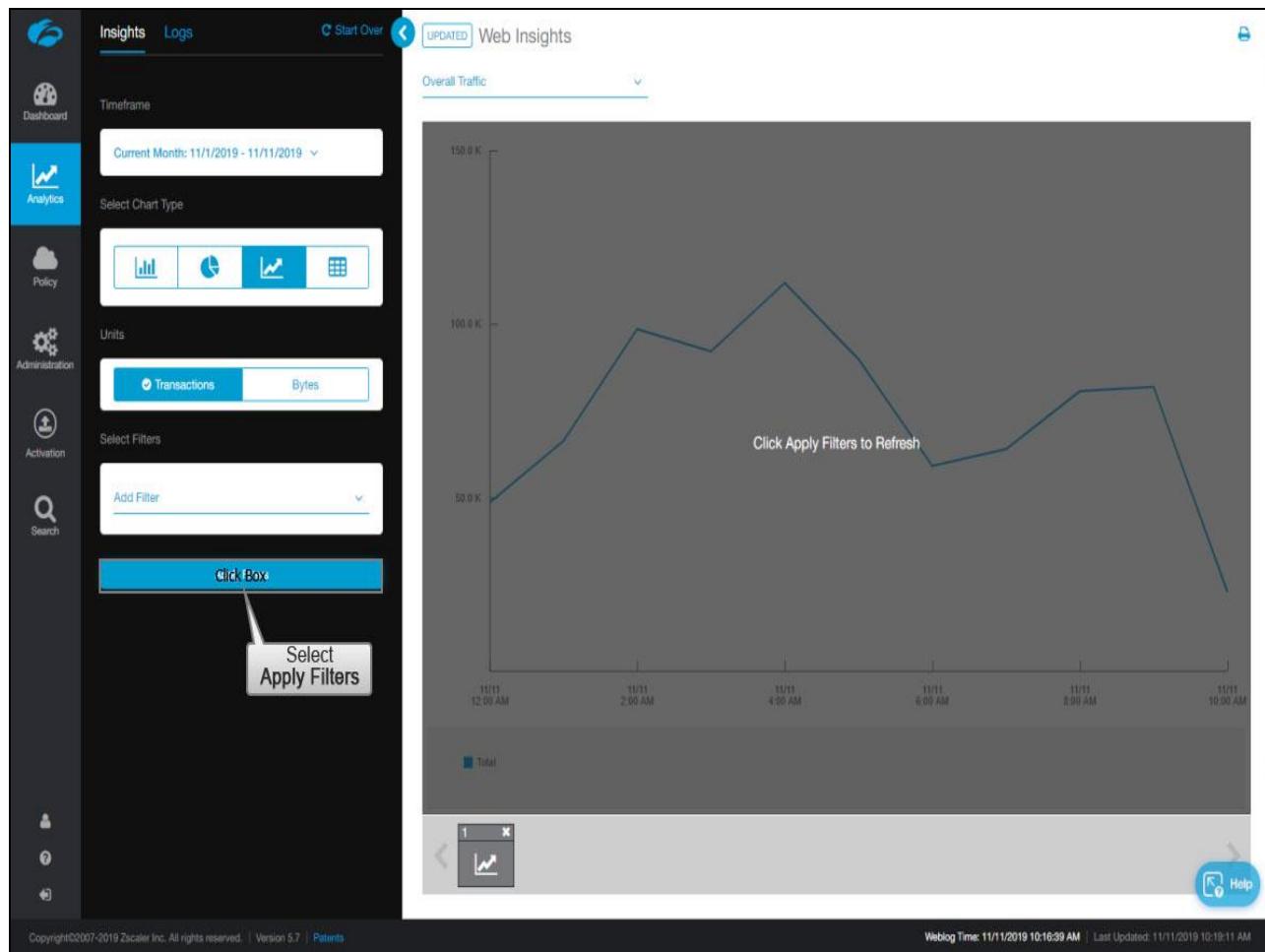
Slide notes

Try a variety of timeframes and note the peaks. You don't need to be super exact – you're basically looking for orders of magnitude; are you going 500,000 or 5,000,000 transactions per hour?



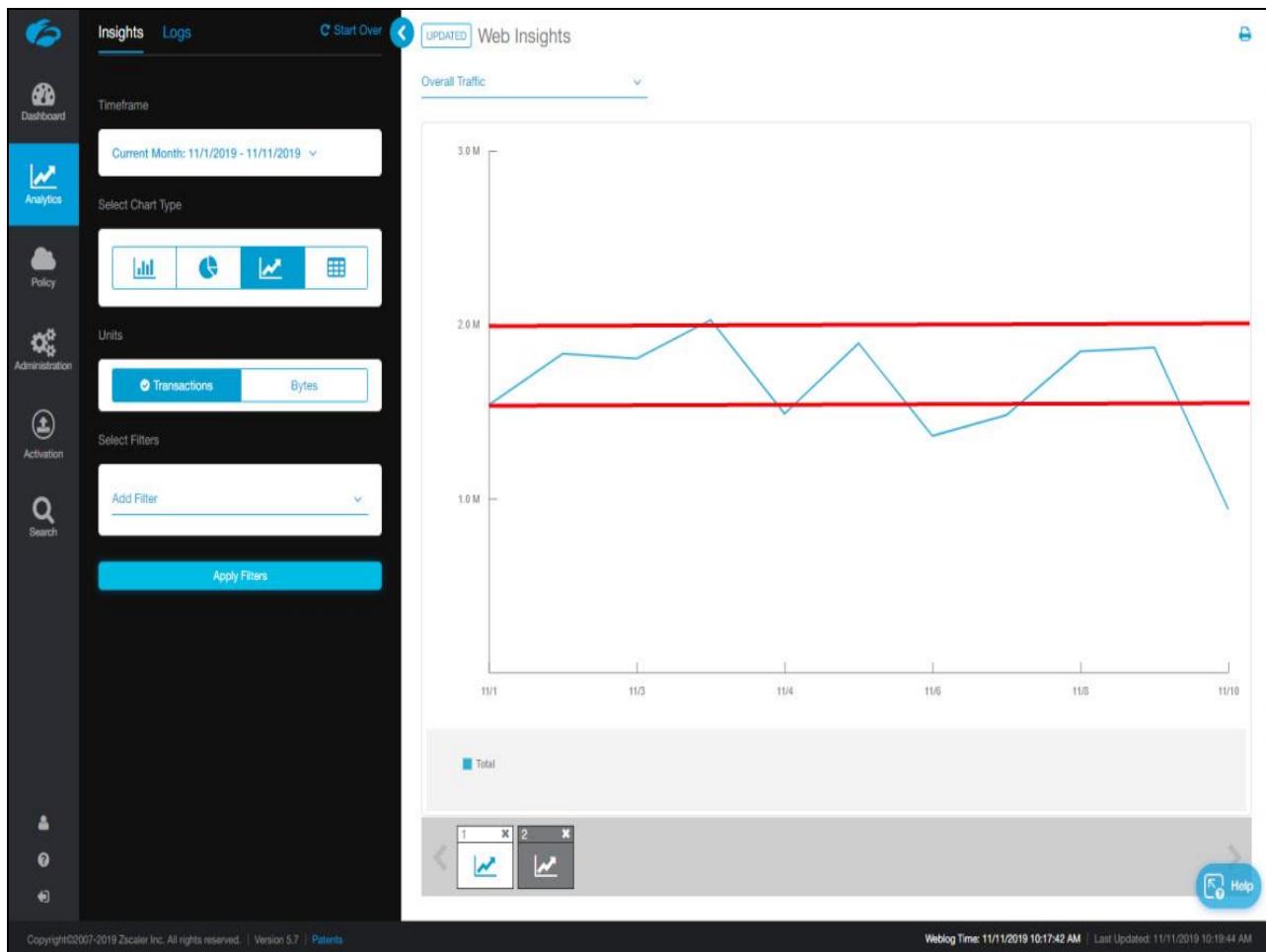
Slide notes

Click on “Current Month”.



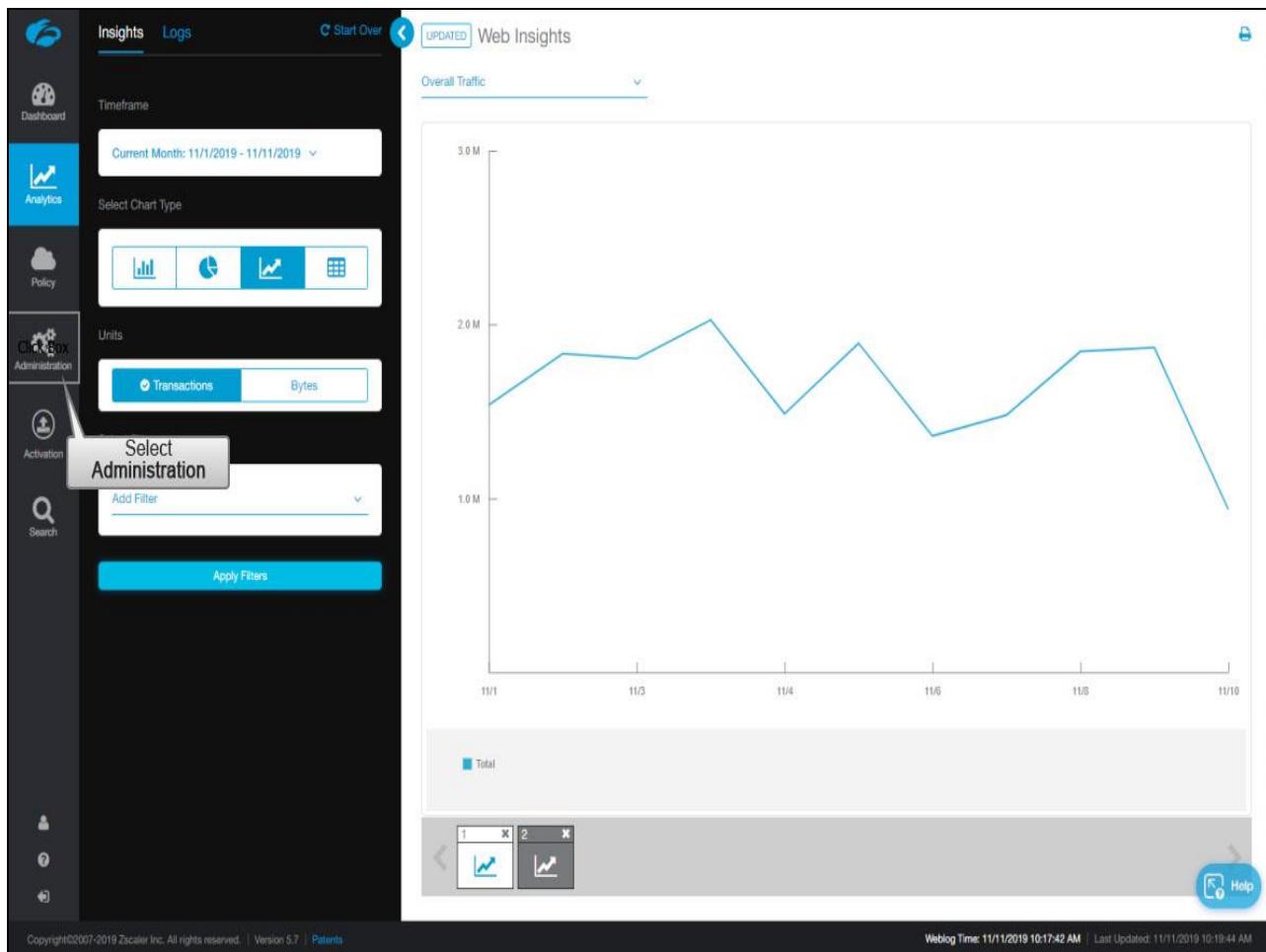
Slide notes

Then click “Apply Filters”.



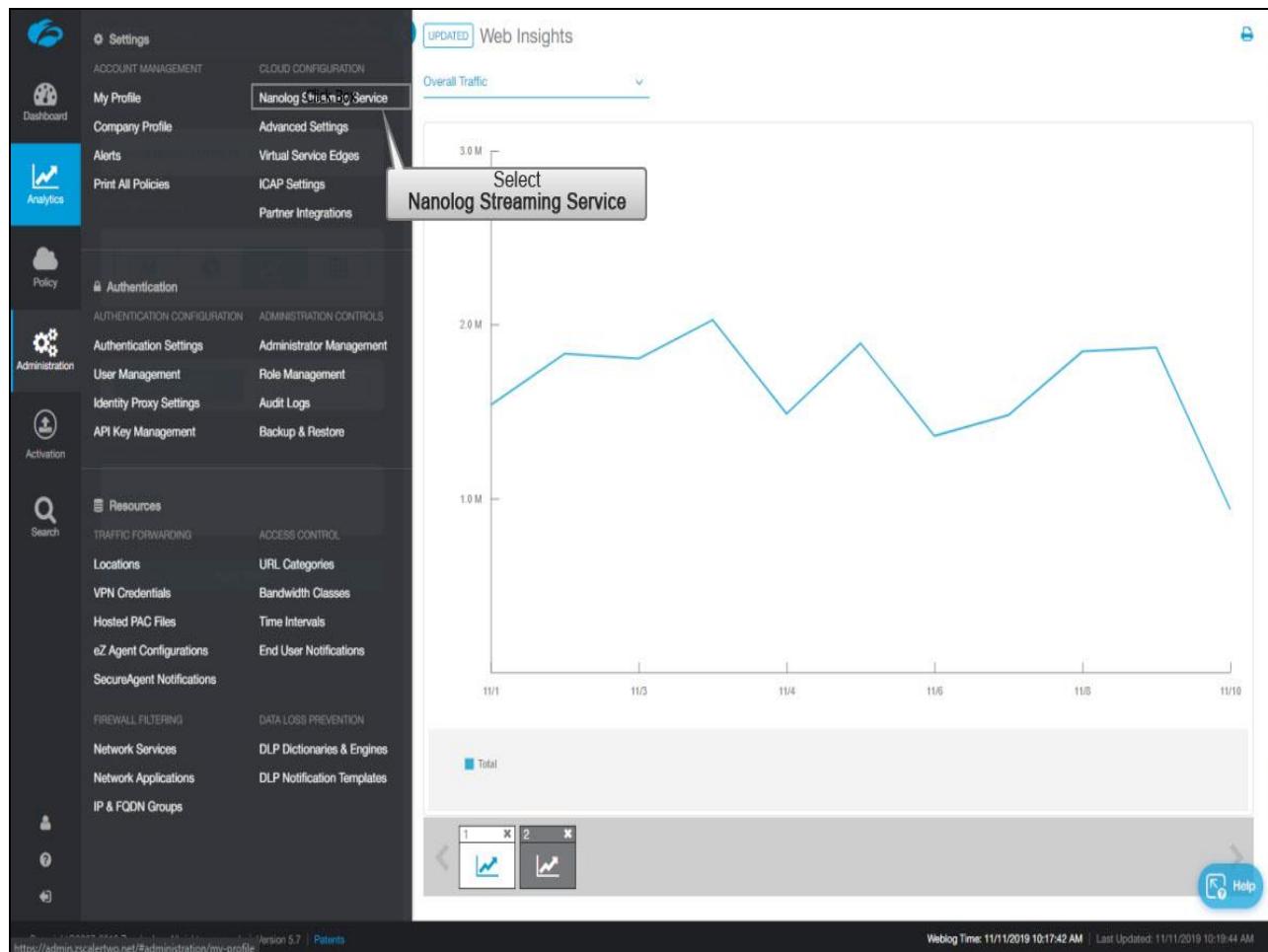
Slide notes

Note that your average number of transactions over the past month was around one and a half million with a peak of around 2 million. Note down 2 million for this example.



Slide notes

Let's head back over to the NSS page.



Slide notes

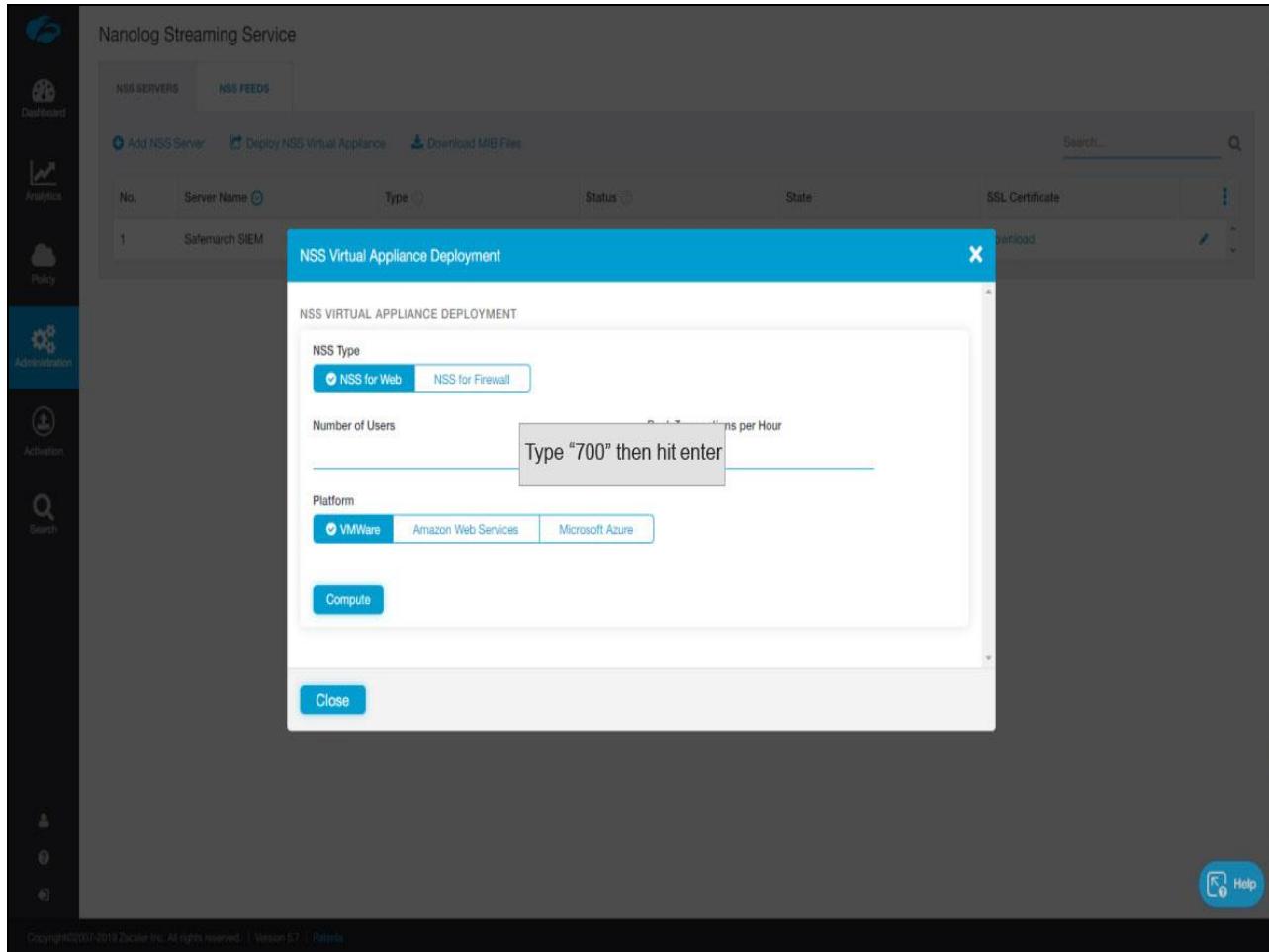
The screenshot shows the 'Nanolog Streaming Service' interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'NSS SERVERS' and contains a table with one row:

No.	Server Name	Type	Status	State	SSL Certificate
1	Safemarch SIEM	NSS	Unhealthy	Download	

A callout box with the text 'Select Deploy NSS Virtual Appliance' points to the 'Deploy' button in the top navigation bar. The URL in the address bar is <https://zscaler-nanolog-streaming-service.zscaler.net/nanolog/nsservers>.

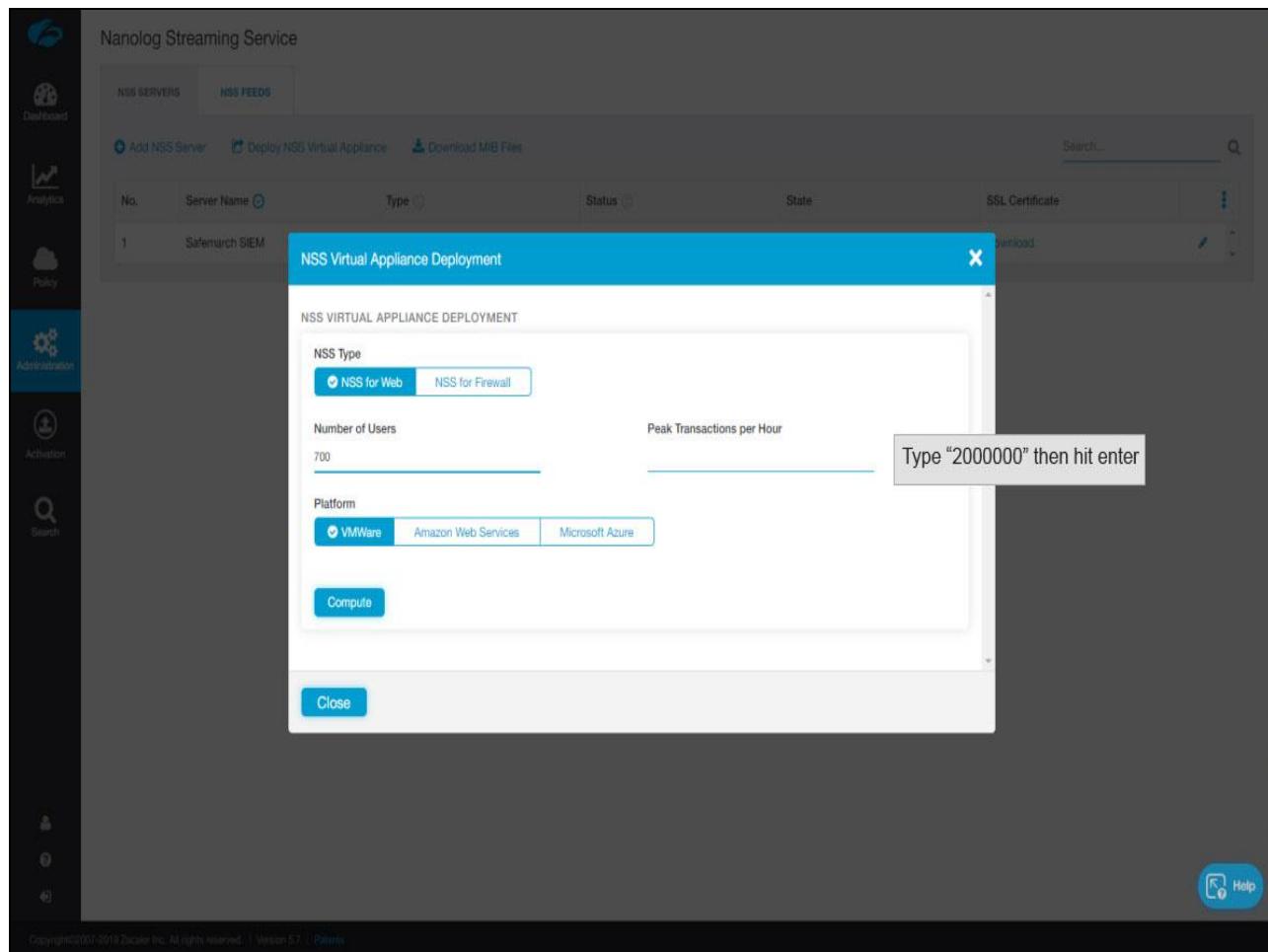
Slide notes

Click Deploy NSS Virtual Appliance.



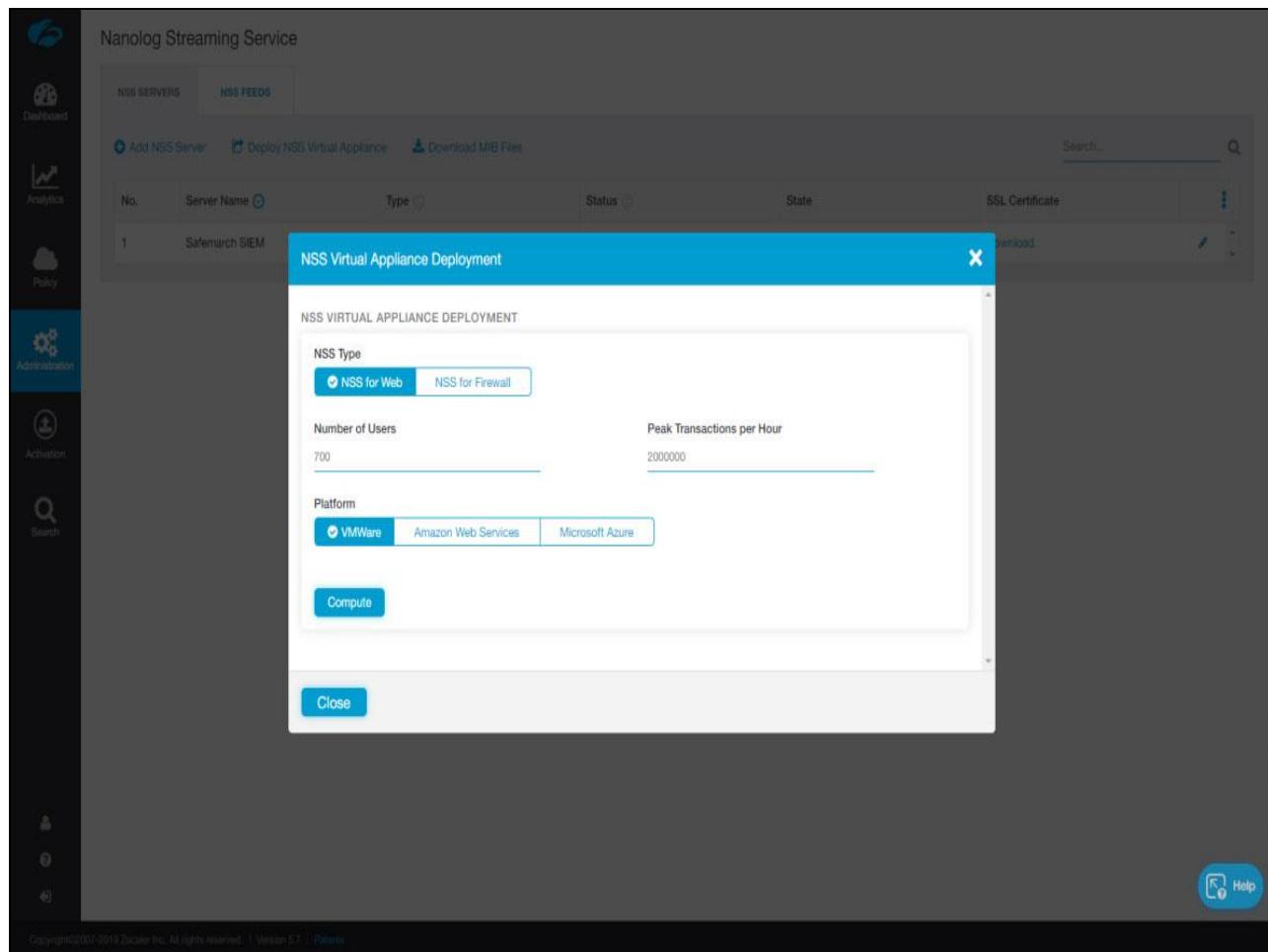
Slide notes

Let's assume that we are protecting 700 users in this organization. Enter 700 in the "Number of Users" field.



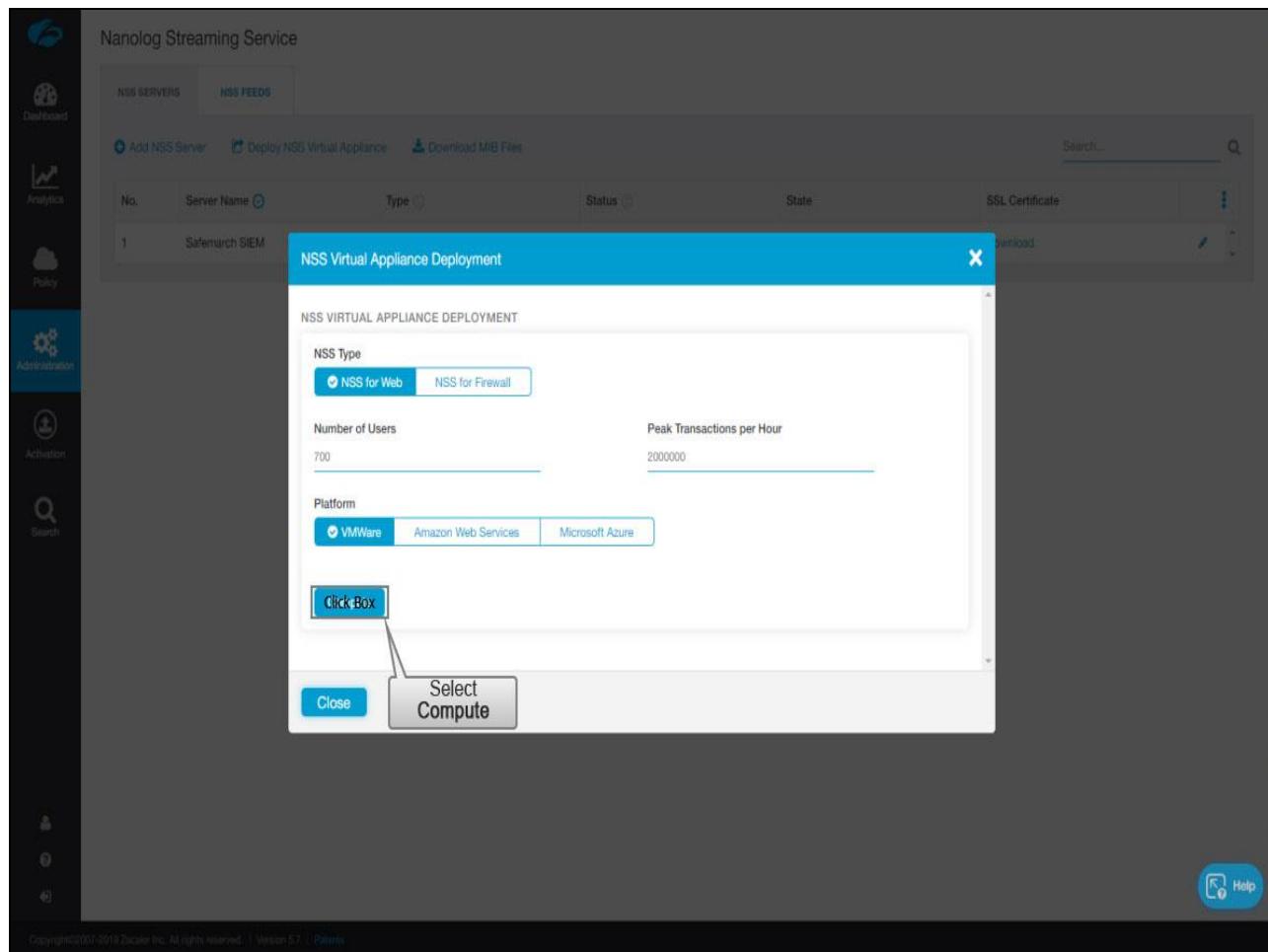
Slide notes

and 2,000,000 transactions.



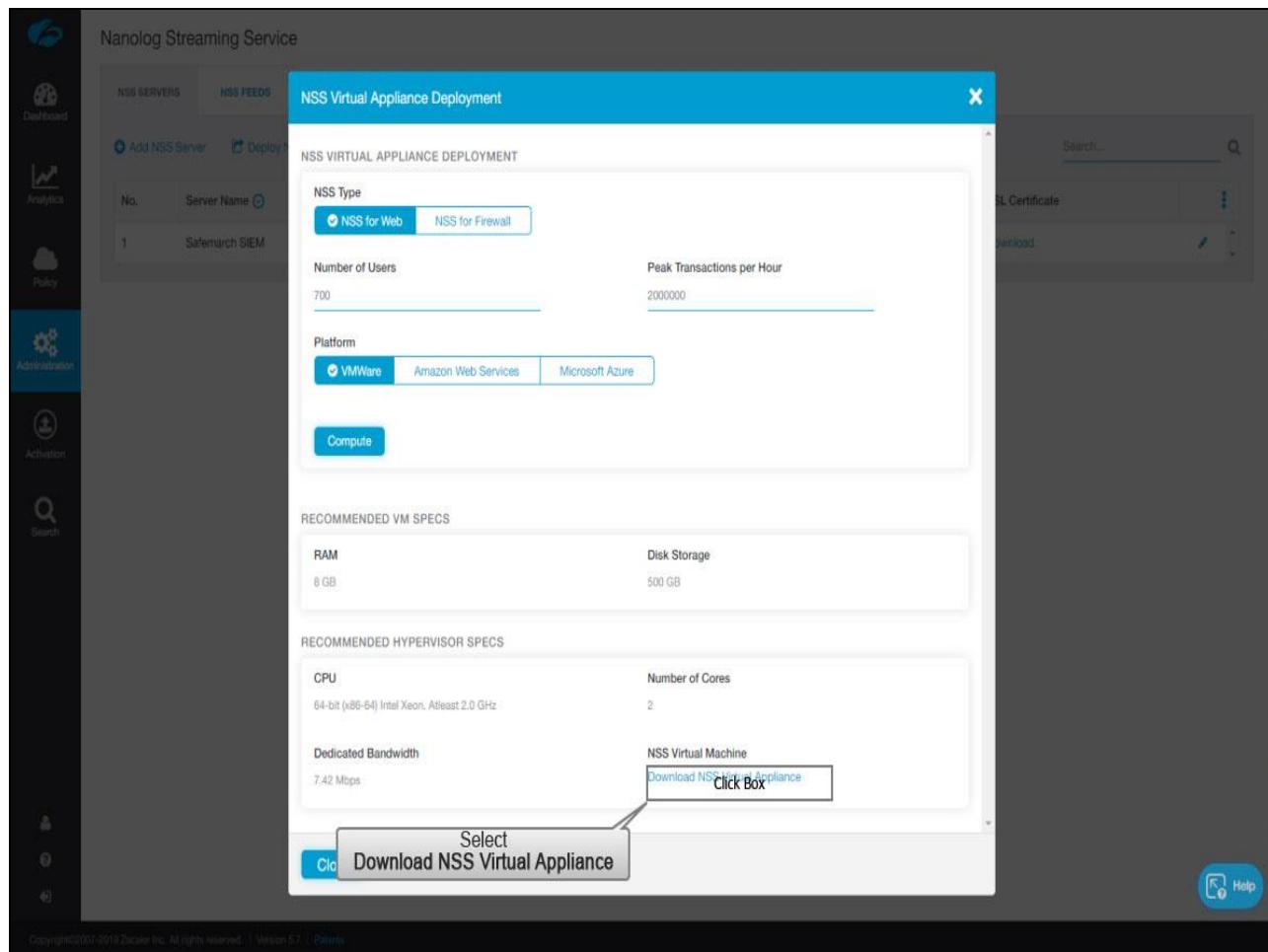
Slide notes

You can select between deploying an on-premise VM instance, in AWS, or in Microsoft Azure. For this demo, we will use VMWare.



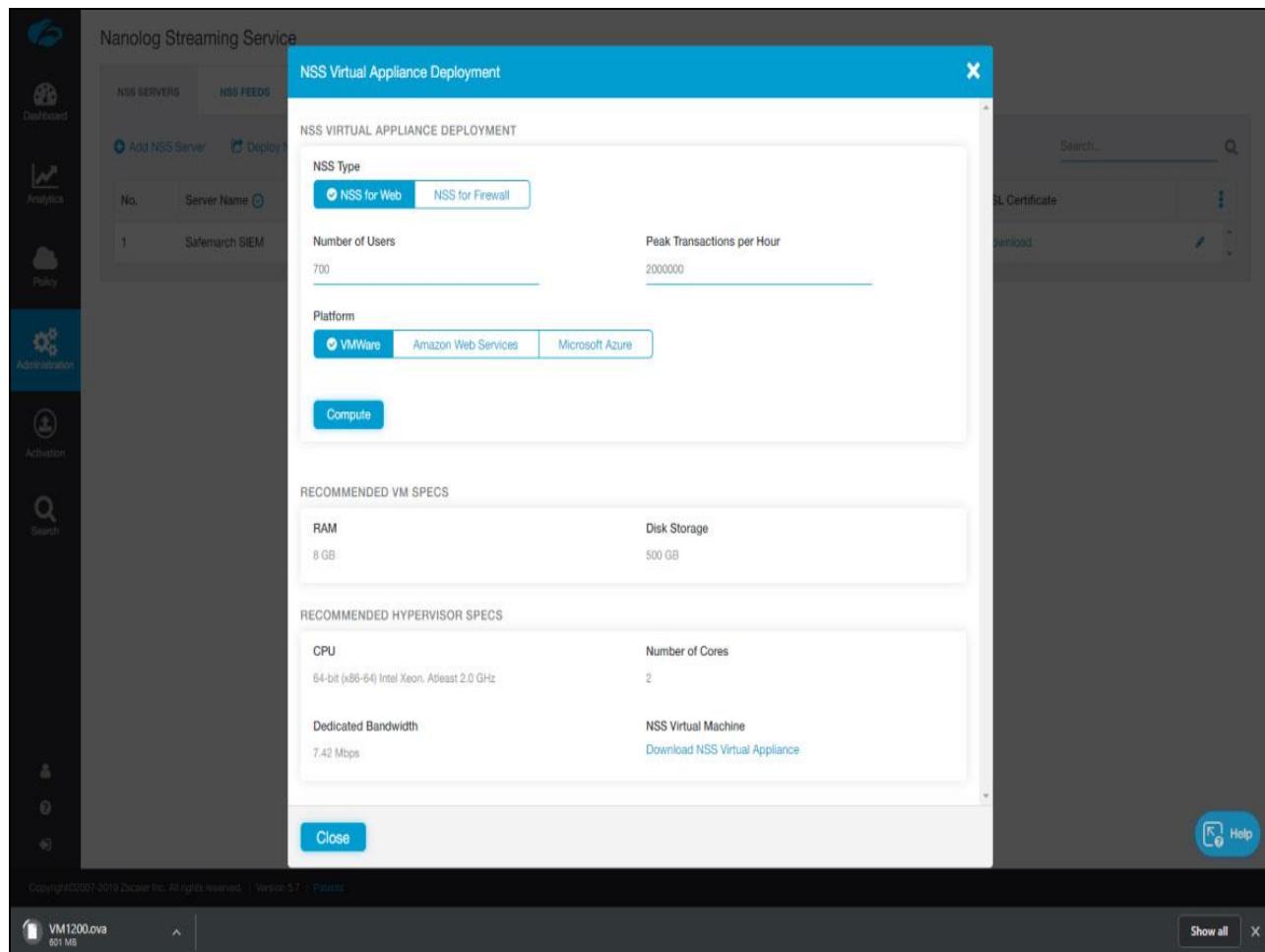
Slide notes

and click “Compute”.

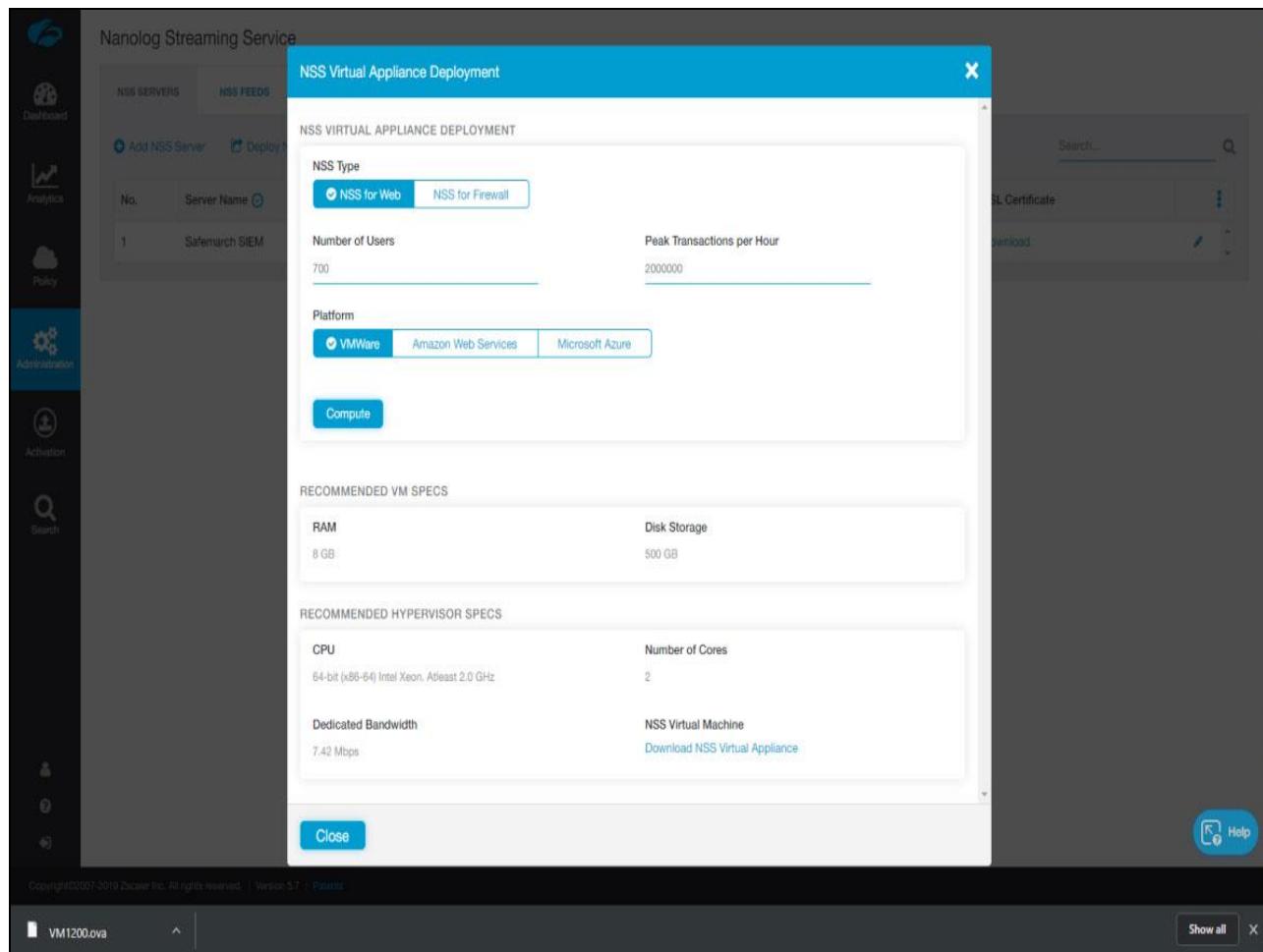


Slide notes

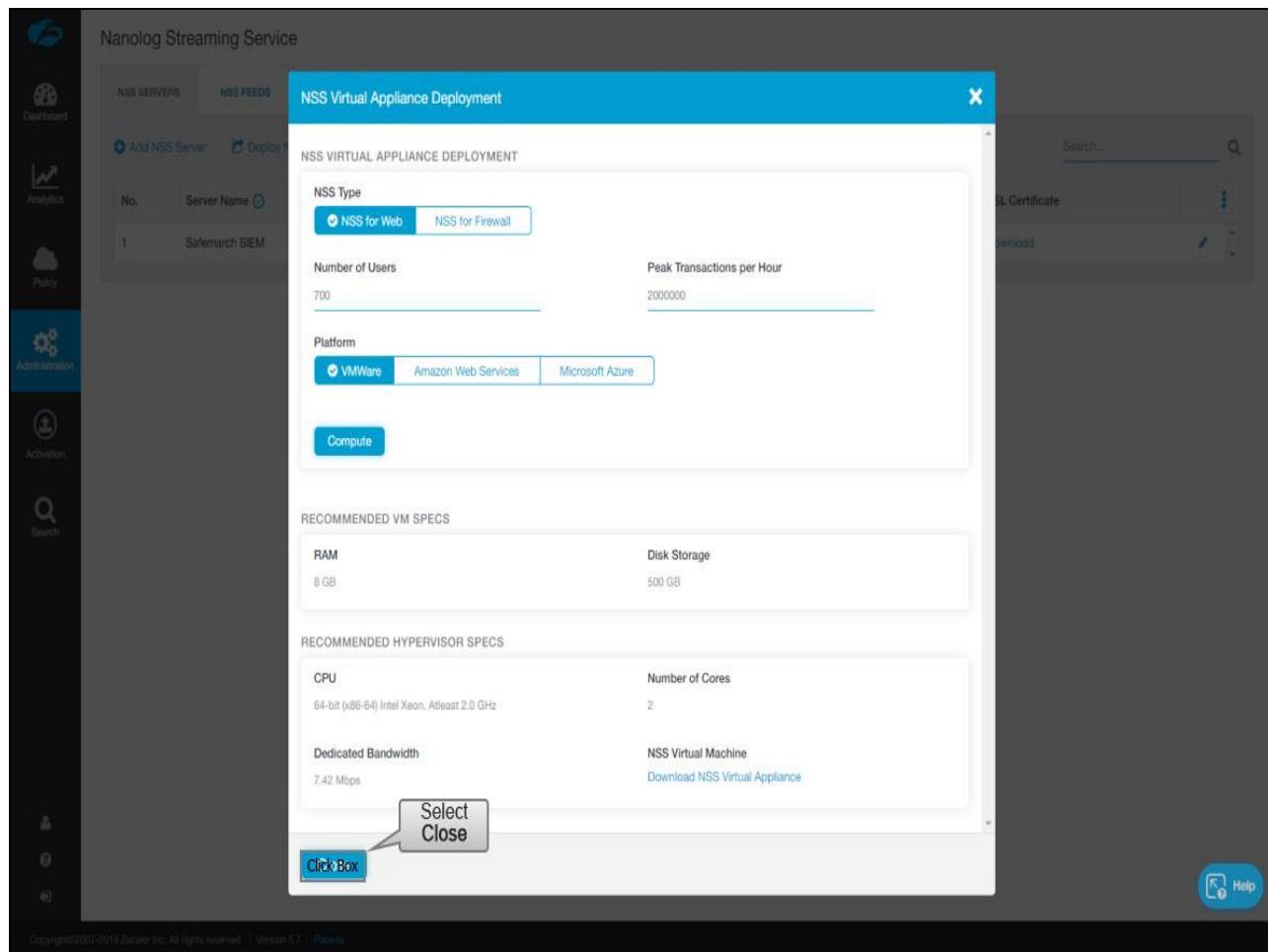
The VM specs will be listed there. Once you've made a note of the specs click "Download NSS Virtual Appliance".



Slide notes



Slide notes



Slide notes

Click “Close”.

Nanolog Streaming Service

NSS SERVERS NSS FEEDS

Add NSS Server Deploy NSS Virtual Appliance Download MIB Files Search... Q

No.	Server Name	Type	Status	State	SSL Certificate
1	Safemarch SIEM	NSS for Web	Enabled	Unhealthy	Download Click Box

Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents Help

A vertical sidebar on the left contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The Administration icon is highlighted in blue.

A callout box labeled "Select Download" points to the "Download" button in the SSL Certificate column of the table.

Slide notes

Next, Download the SSL client certificate.

The screenshot shows the Nanolog Streaming Service interface. On the left, there is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Nanolog Streaming Service" and has tabs for "NSS SERVERS" (selected) and "NSS FEEDS". Below the tabs are buttons for "Add NSS Server", "Deploy NSS Virtual Appliance", and "Download MIB Files". A search bar is also present. The main content area displays a table with one row of data:

No.	Server Name	Type	Status	State	SSL Certificate
1	Safemarch SIEM	NSS for Web	Enabled	Unhealthy	Download

At the bottom of the interface, there is a copyright notice: "Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents". A download link for "NssCertificate.zip" is shown, along with "Show all" and "Help" buttons.

Slide notes

Nanolog Streaming Service

NSS SERVERS NSS FEEDS

Add NSS Server Deploy NSS Virtual Appliance Click Box Files

No. Server Name Type Status State SSL Certificate

No.	Server Name	Type	Status	State	SSL Certificate
1	Safemarch SIEM	NSS for Web	Select Download MIB Files	Unhealthy	Download

Search... Q

Copyright 2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents

NssCertificate.zip Show all X Help

Slide notes

If you would like to monitor your NSS via SNMP, download a copy of the Zscaler NSS MIB for import into your SNMP manager. Click Download MIB Files.

The screenshot shows the Nanolog Streaming Service interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has a title 'Nanolog Streaming Service' and tabs for 'NSS SERVERS' (selected) and 'NSS FEEDS'. Below the tabs are buttons for 'Add NSS Server', 'Deploy NSS Virtual Appliance', and 'Download MIB Files'. A search bar is at the top right. A table lists one server entry:

No.	Server Name	Type	Status	State	SSL Certificate
1	Safemarch SIEM	NSS for Web	Enabled	Unhealthy	Download

At the bottom, there's a copyright notice 'Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents' and a help button.

Slide notes

Nanolog Streaming Service

NSS SERVERS NSS FEEDS

Add NSS Server Deploy Click Box at Appliance Download MIB Files

No.	Server Name	Type	Status	State	SSL Certificate
1	Safemarch SIEM	NSS	Select Deploy NSS Virtual Appliance	Unhealthy	Download

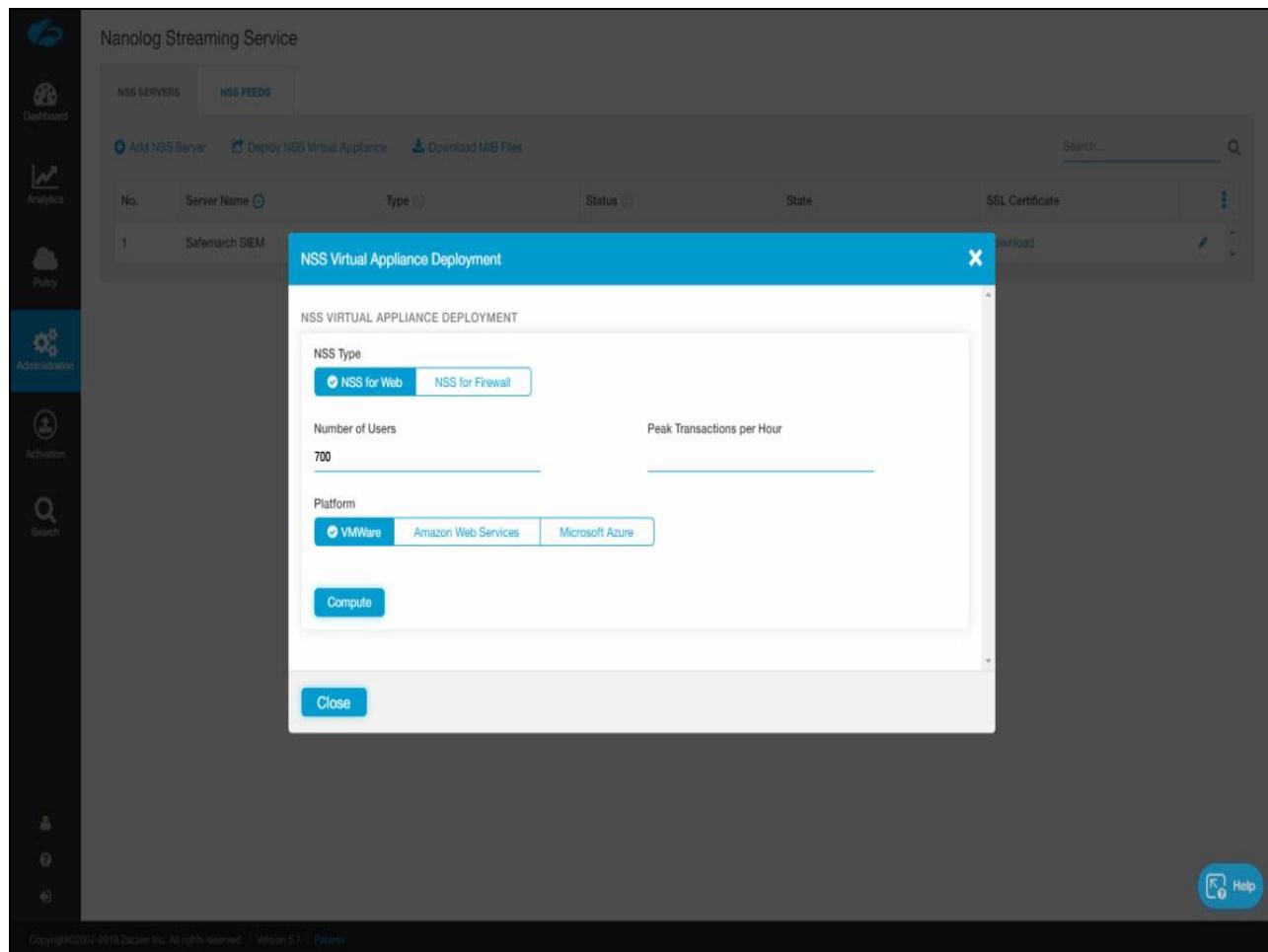
Search... Q

Dashboard Analytics Policy Administration Activation Search Help

Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents

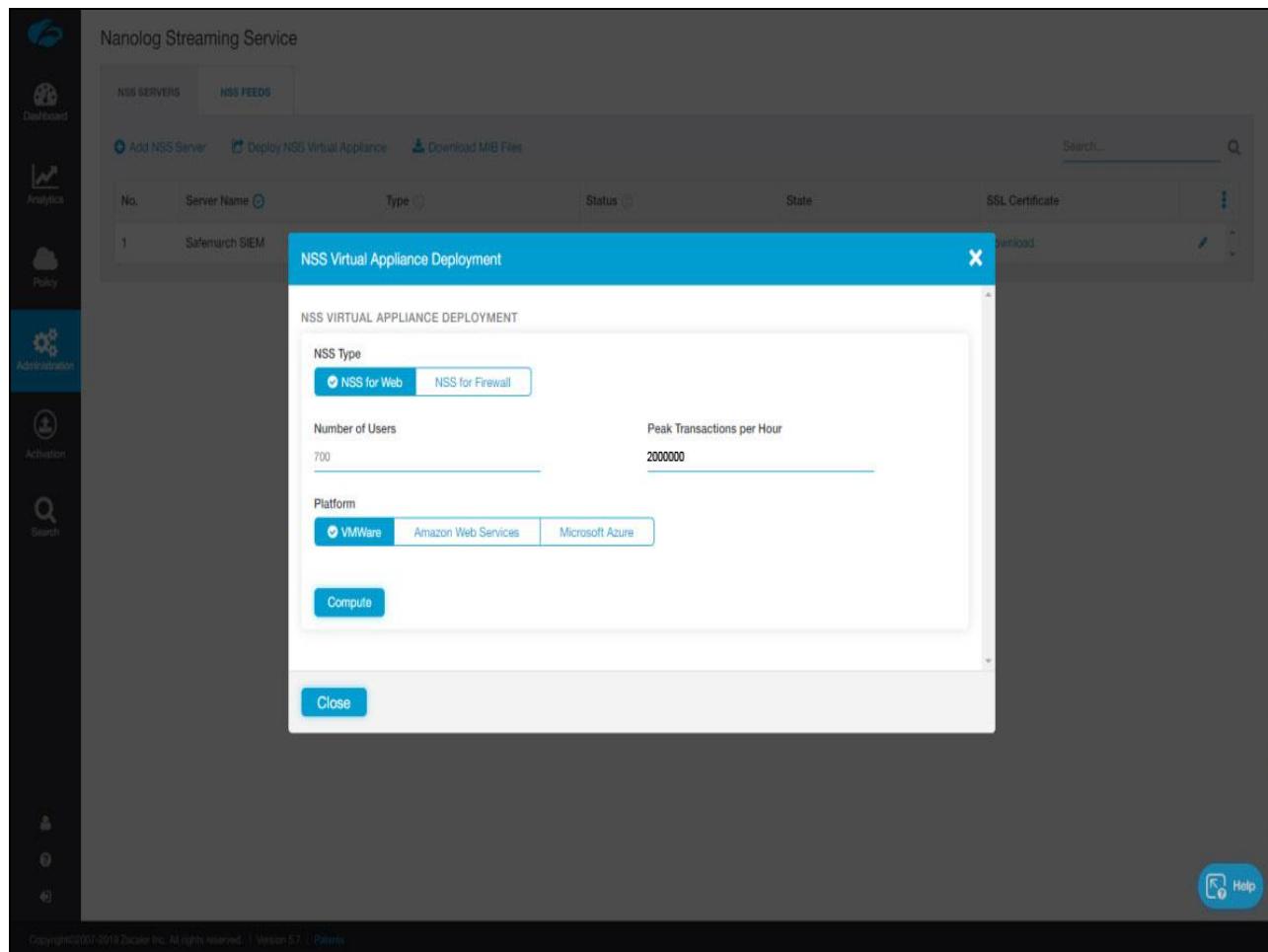
Slide notes

Let's take a look at the process of deploying an NSS instance in AWS. Click Deploy NSS Virtual Appliance.



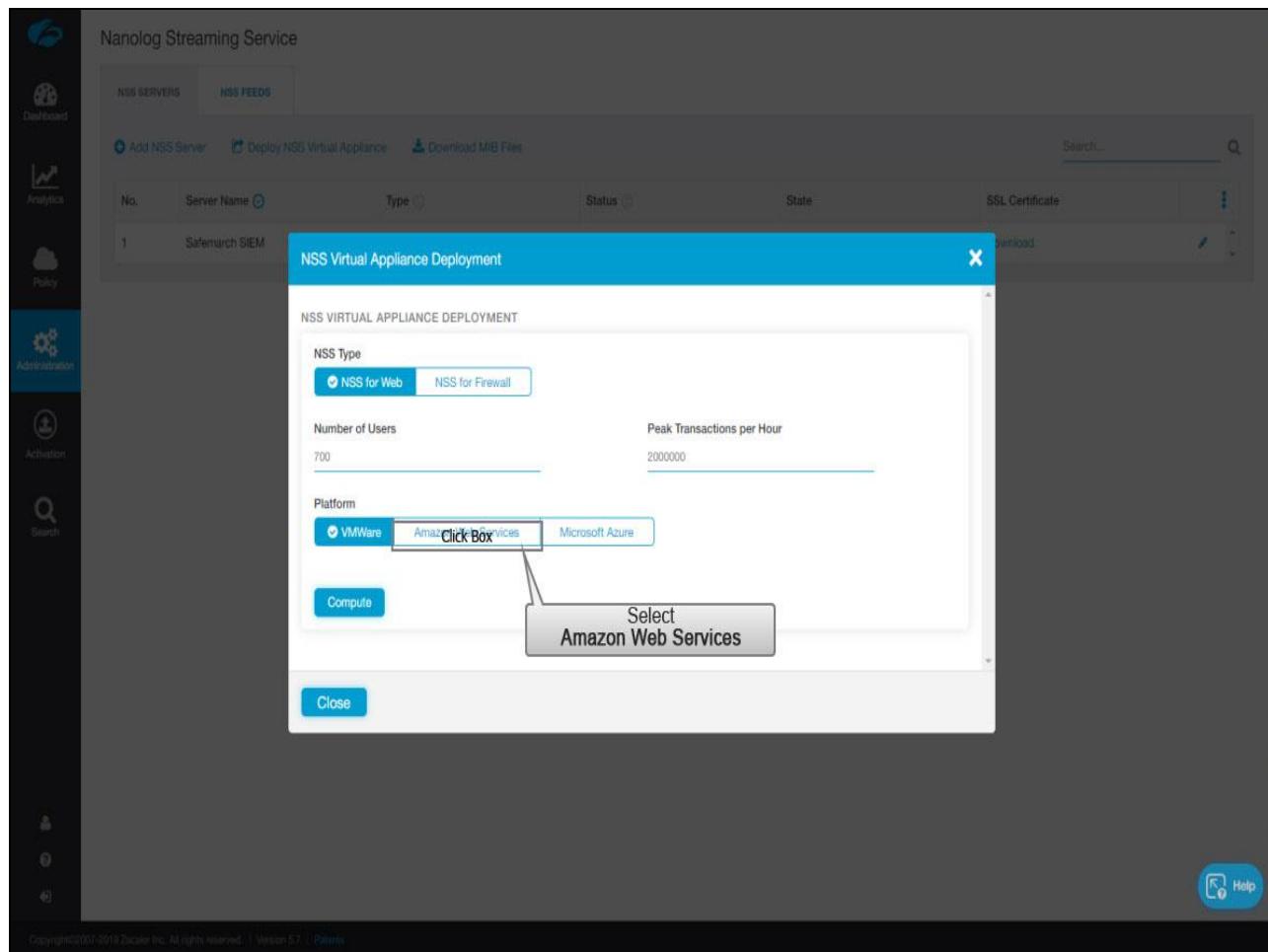
Slide notes

Enter 700 users



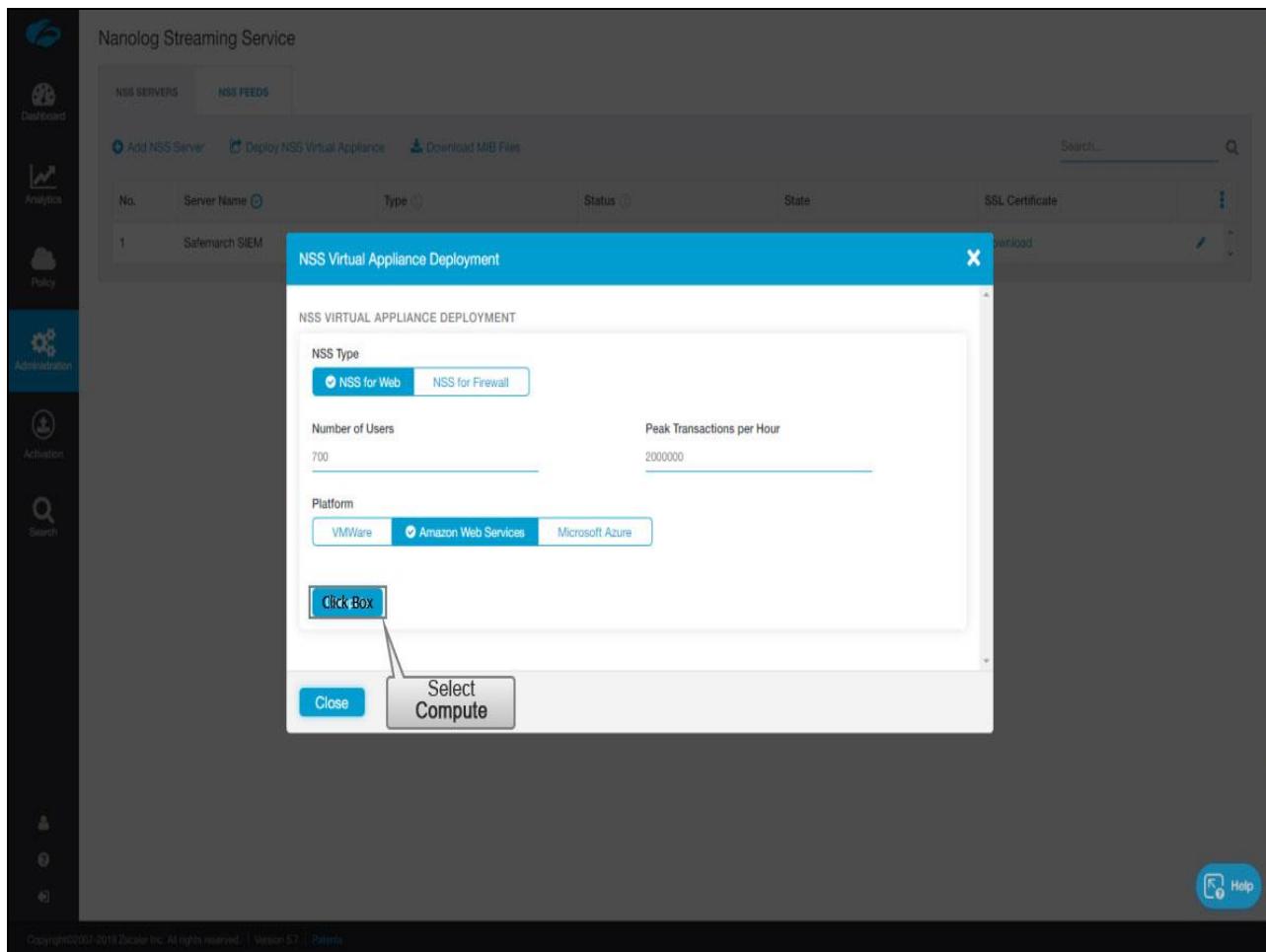
Slide notes

and 2,000,000 transactions.



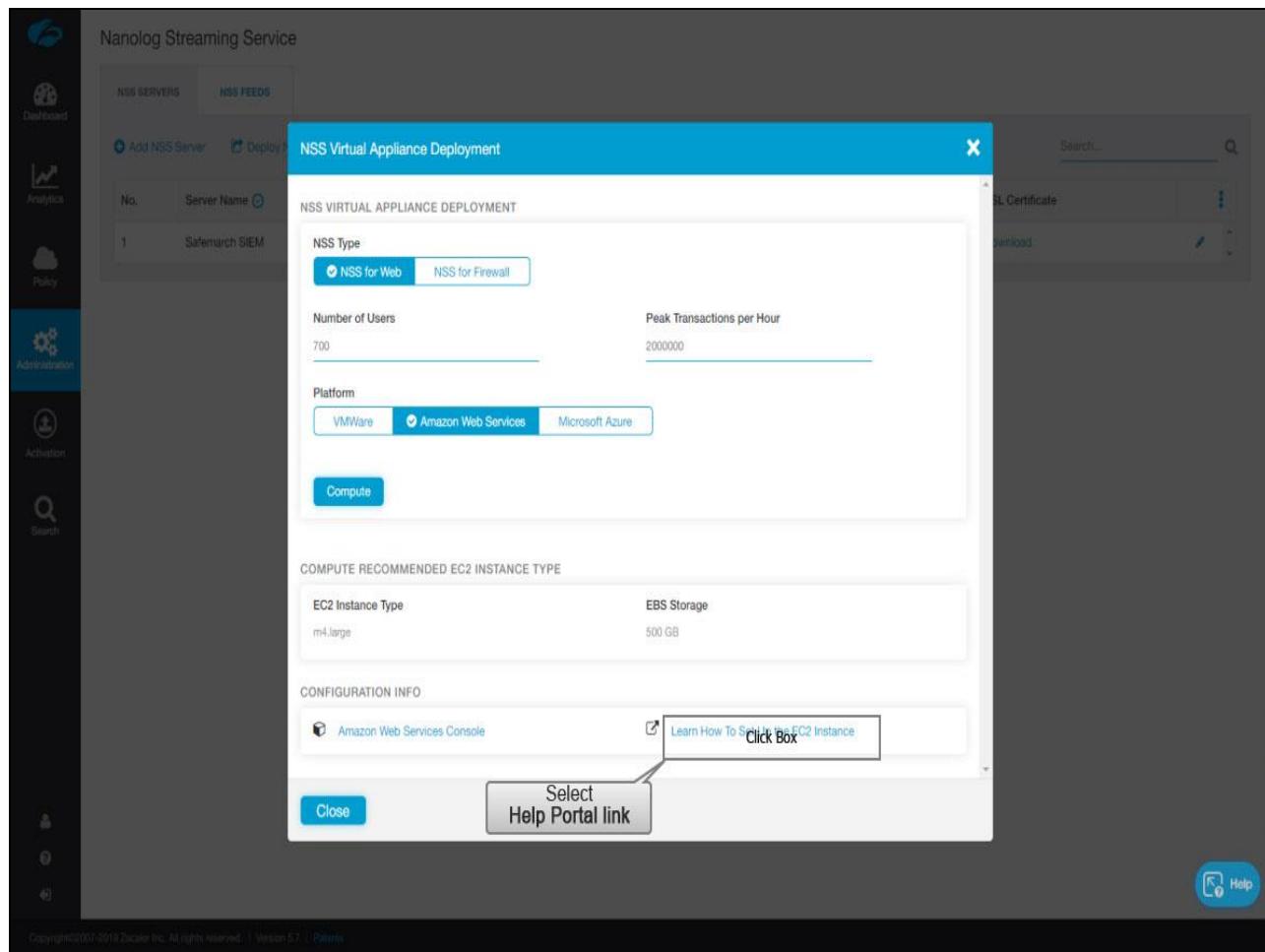
Slide notes

In the previous example you downloaded the .ova file to deploy the NSS instance on-premise. In this example, click on Amazon Web Services to deploy the NSS in AWS.



Slide notes

and click “Compute”.



Slide notes

To see the details on how to deploy your NSS instance in AWS click the Help Portal article link. Be sure to record your recommendations for your EC2 instance before closing this page

The screenshot shows a web browser window with the Zscaler logo at the top left. A search bar at the top right contains the text "Search ZIA & Z App" with a magnifying glass icon. Below the header, a breadcrumb navigation path is visible: ZIA Help > Analytics > NSS > NSS Deployment Guides > NSS Deployment Guide for Amazon Web Services. The main content area has a title "NSS Deployment Guide for Amazon Web Services" with a "ZIA" icon to its left. A callout box contains the text: "Contact Zscaler Support to request a share of the NSS AMI. Provide your AWS account ID and AWS region in which you want the AMI. After deployment, the NSS VM receives automatic software updates from the Zscaler cloud." Below this, a list of steps is provided:

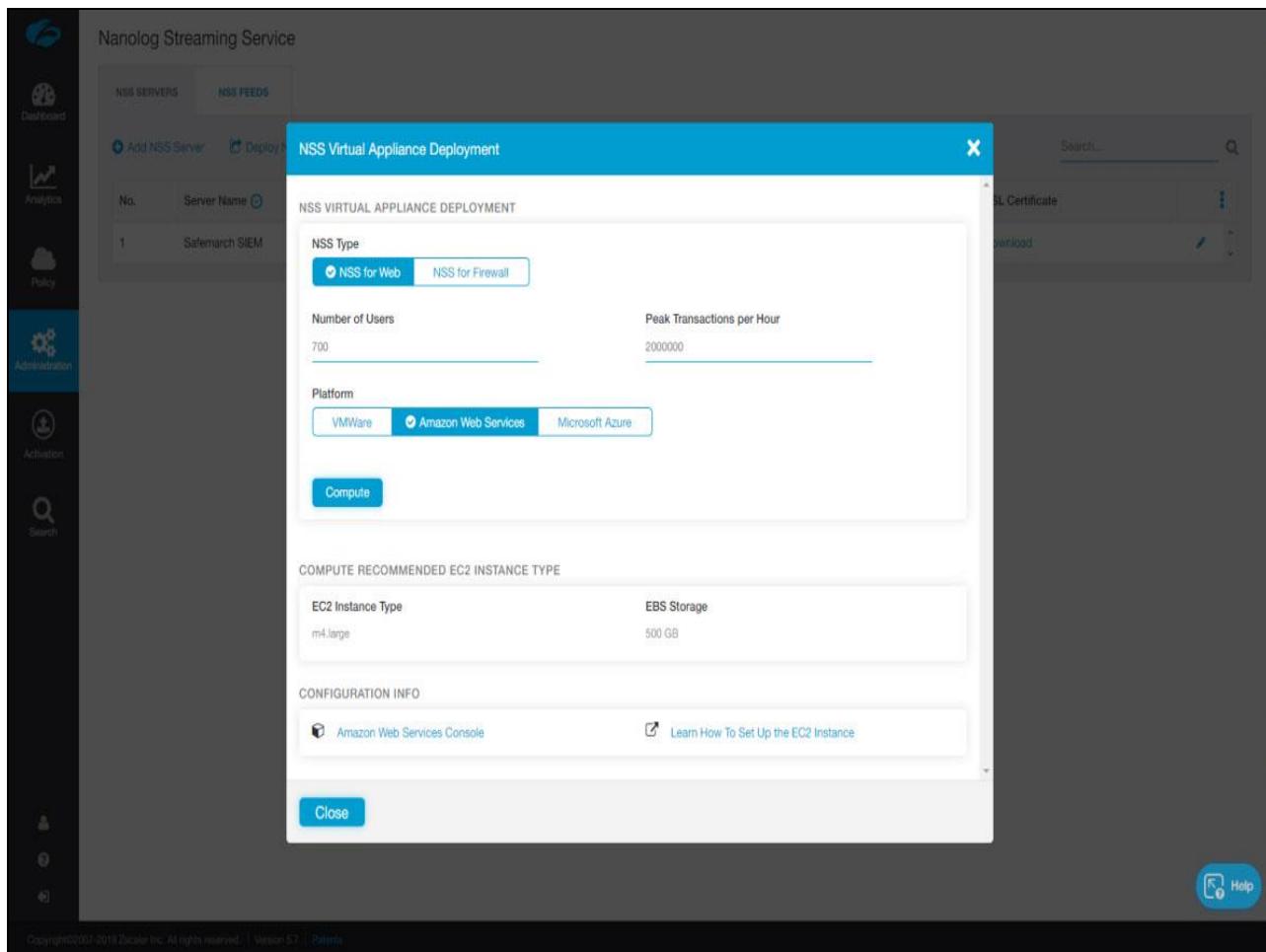
- Step 1: Make sure that you have met all of the NSS Deployment prerequisites
- Step 2: In the Zscaler Admin Portal, add an NSS server and download the SSL certificate
- Step 3: In the Zscaler Admin Portal, get the recommended VM instance specifications
- Step 4: Use the AWS Console to provision and configure an EC2 instance
- Step 5: Configure and start NSS on the VM instance.
- Step 6: Add NSS Feeds for each NSS

Below the steps, a note states: "Once you have verified your deployment, you can perform additional tasks:" followed by a bulleted list:

- Deploying Multiple NSS Virtual Machines
- How to configure an additional management interface, service interface, and local NTP server. See [NSS Advanced Deployment](#).
- Troubleshooting NSS

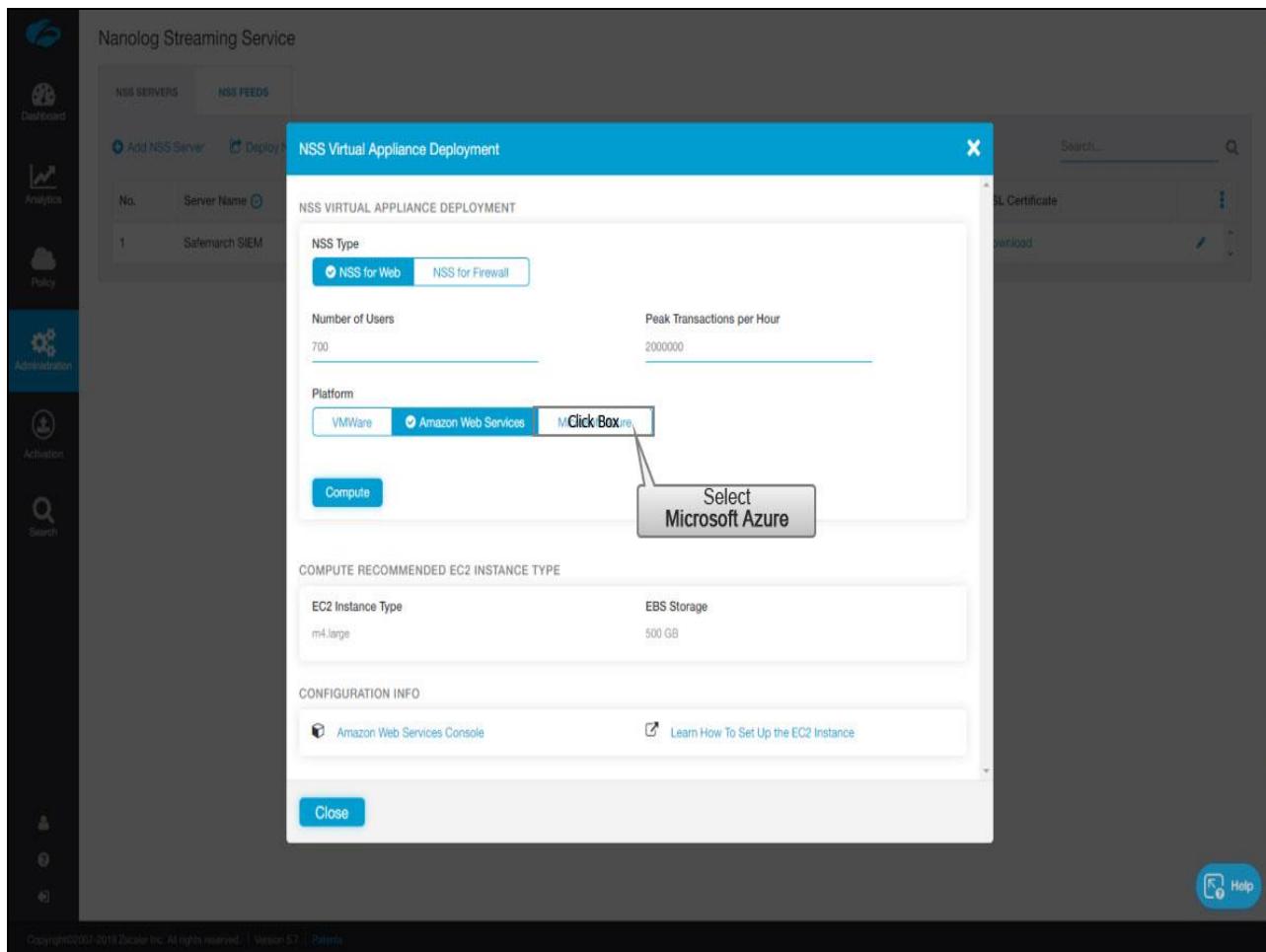
Slide notes

Full details for deploying NSS in AWS are available on this page. Expand the steps in the article to see all the steps involved.



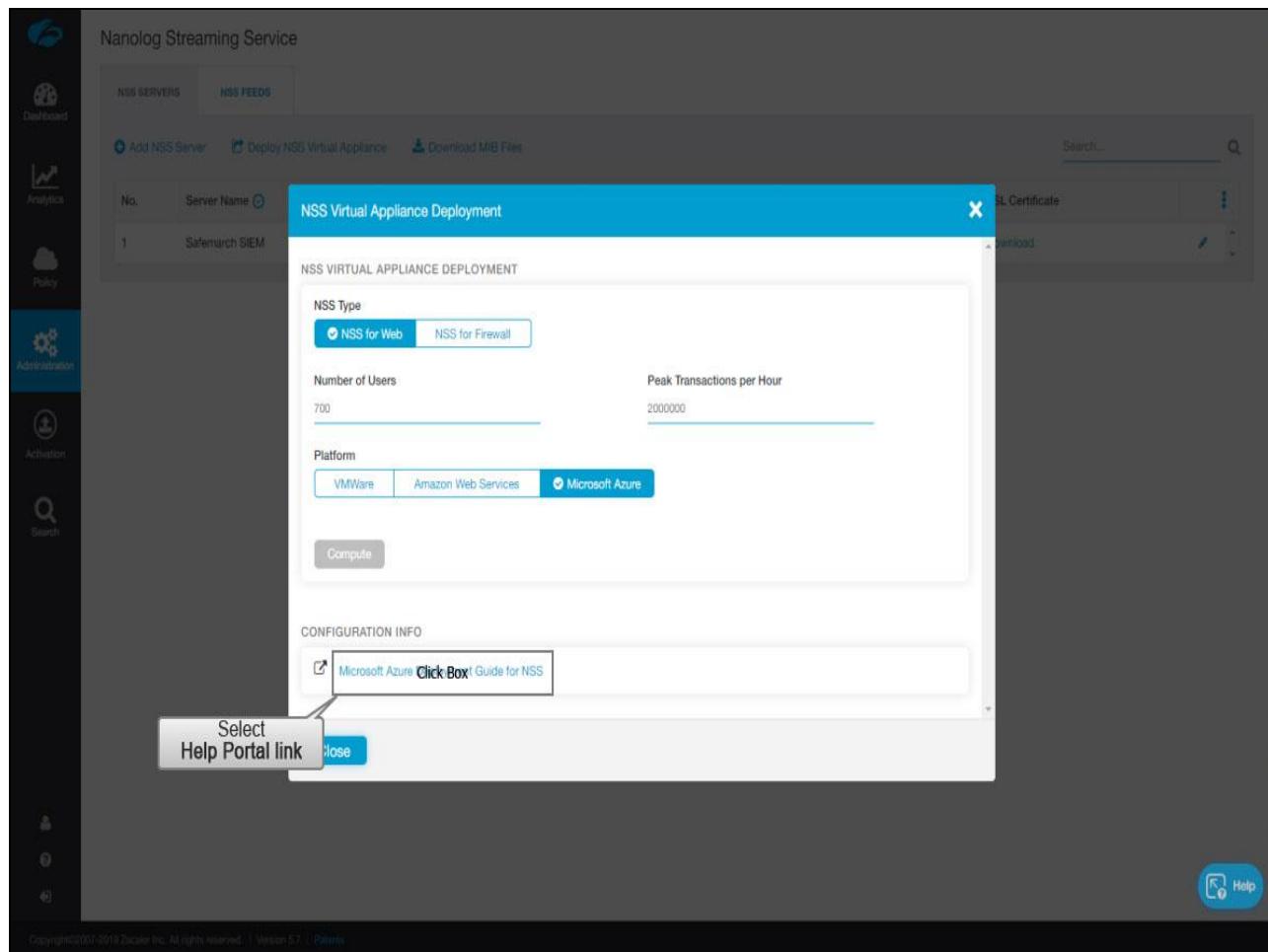
Slide notes

Similarly, to see the steps involved in deploying NSS in Microsoft Azure, click Microsoft Azure.



Slide notes

Similarly, to see the steps involved in deploying NSS in Microsoft Azure, click Microsoft Azure.



Slide notes

Then click the Help Portal link.

The screenshot shows a web browser window with the Zscaler logo at the top left. A search bar at the top right contains the text "Search ZIA & Z App". Below the header, a breadcrumb navigation path is visible: ZIA Help > Analytics > NSS > NSS Deployment Guides > NSS Deployment Guide for Microsoft Azure. The main content area has a title "NSS Deployment Guide for Microsoft Azure" with a globe icon to its left. A callout bubble labeled "ZIA" is positioned above the title. To the right of the title is a blue downward arrow icon. On the far right edge of the content area, there are three small blue icons: a left arrow, a grid, and a right arrow. The main content includes a paragraph about deployment tasks, a warning message about AzureRM deprecation, and a list of six steps for deployment. At the bottom, there's a note about additional tasks and a bullet point for "Deploying Multiple NSS Virtual Machines".

ZIA Help > Analytics > NSS > NSS Deployment Guides > NSS Deployment Guide for Microsoft Azure

NSS Deployment Guide for Microsoft Azure

This guide describes the tasks required to deploy a Nanolog Streaming Service (NSS) to stream either web logs or firewall logs to a SIEM.

⚠️ Before you begin deployment, contact Support to obtain the NSS VHD SAS token and the Azure VM instance type recommendations.

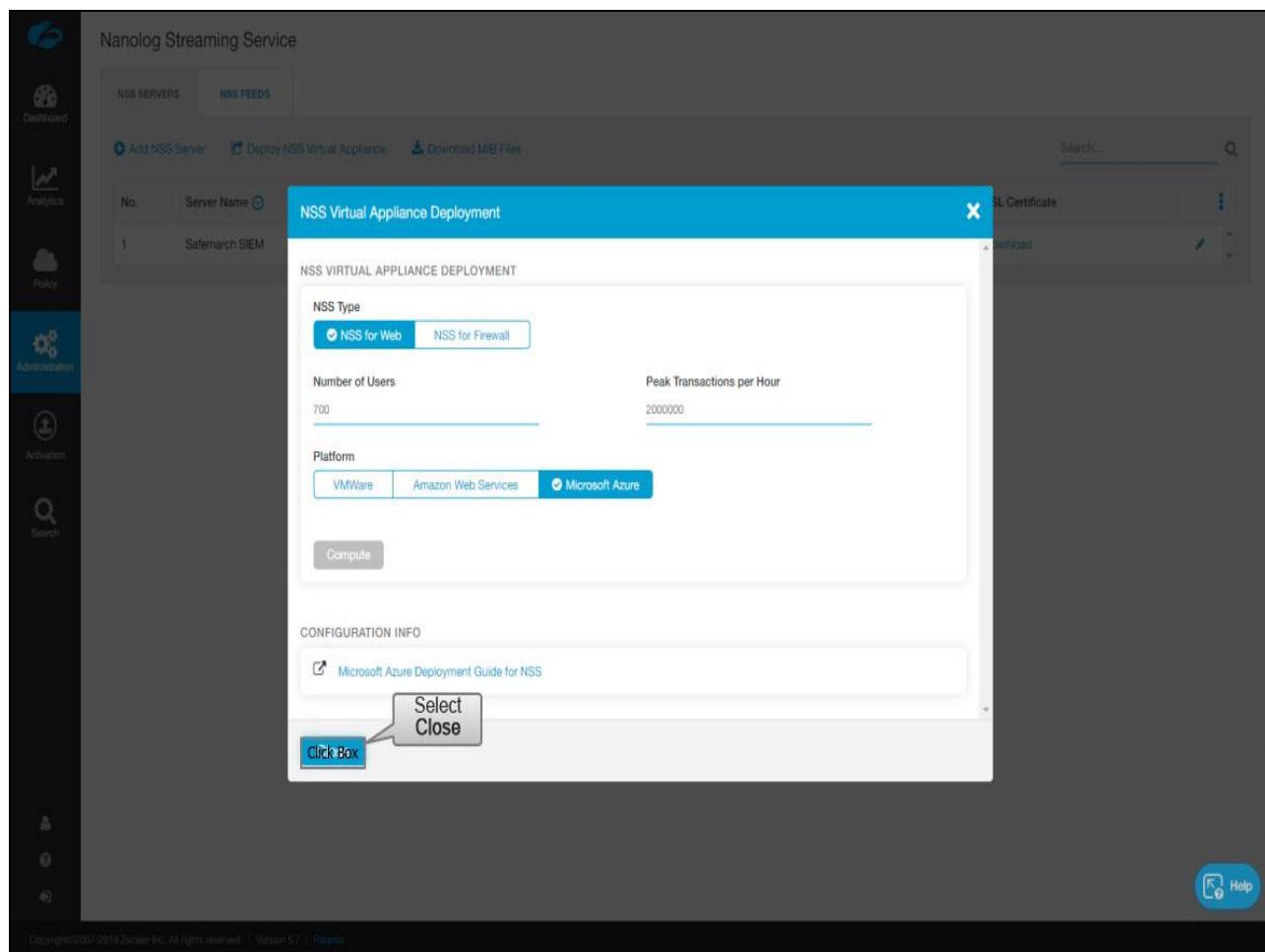
📝 Microsoft recently deprecated the AzureRM module. Zscaler is currently adjusting the PowerShell-based deployment scripts for the new Az module. Zscaler recommends that you use the Azure Portal deployment process only. To learn more, see the Microsoft article [Migrate Azure PowerShell from AzureRM to Az](#).

- Step 1: Make sure that you have met all of the NSS Deployment prerequisites
- Step 2: In the Zscaler Admin Portal, add an NSS server and download the SSL certificate
- Step 3: Use Azure Storage Explorer or PowerShell to copy the OS disk and data disk VHD files to your Azure Storage Account
- Step 4: Use Azure Portal or PowerShell to create the VM instance and validate the configuration
- Step 5: Configure and start NSS on the VM instance
- Step 6: Add NSS Feeds for each NSS

Once you have verified your deployment, you can perform additional tasks:

- [Deploying Multiple NSS Virtual Machines](#)

Slide notes



Slide notes

The screenshot shows the Nanolog Streaming Service interface. On the left, there is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Nanolog Streaming Service" and has tabs for "NSS SERVERS" (which is selected) and "NSS FEEDS". Below the tabs are buttons for "Add NSS Server", "Deploy NSS Virtual Appliance", and "Download MIB Files". A search bar with a magnifying glass icon is also present. The main content area displays a table with one row of data:

No.	Server Name	Type	Status	State	SSL Certificate
1	Safemarch SIEM	NSS for Web	Enabled	Unhealthy	Download

At the bottom of the interface, there is a copyright notice: "Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents". On the far right, there is a "Help" button with a question mark icon.

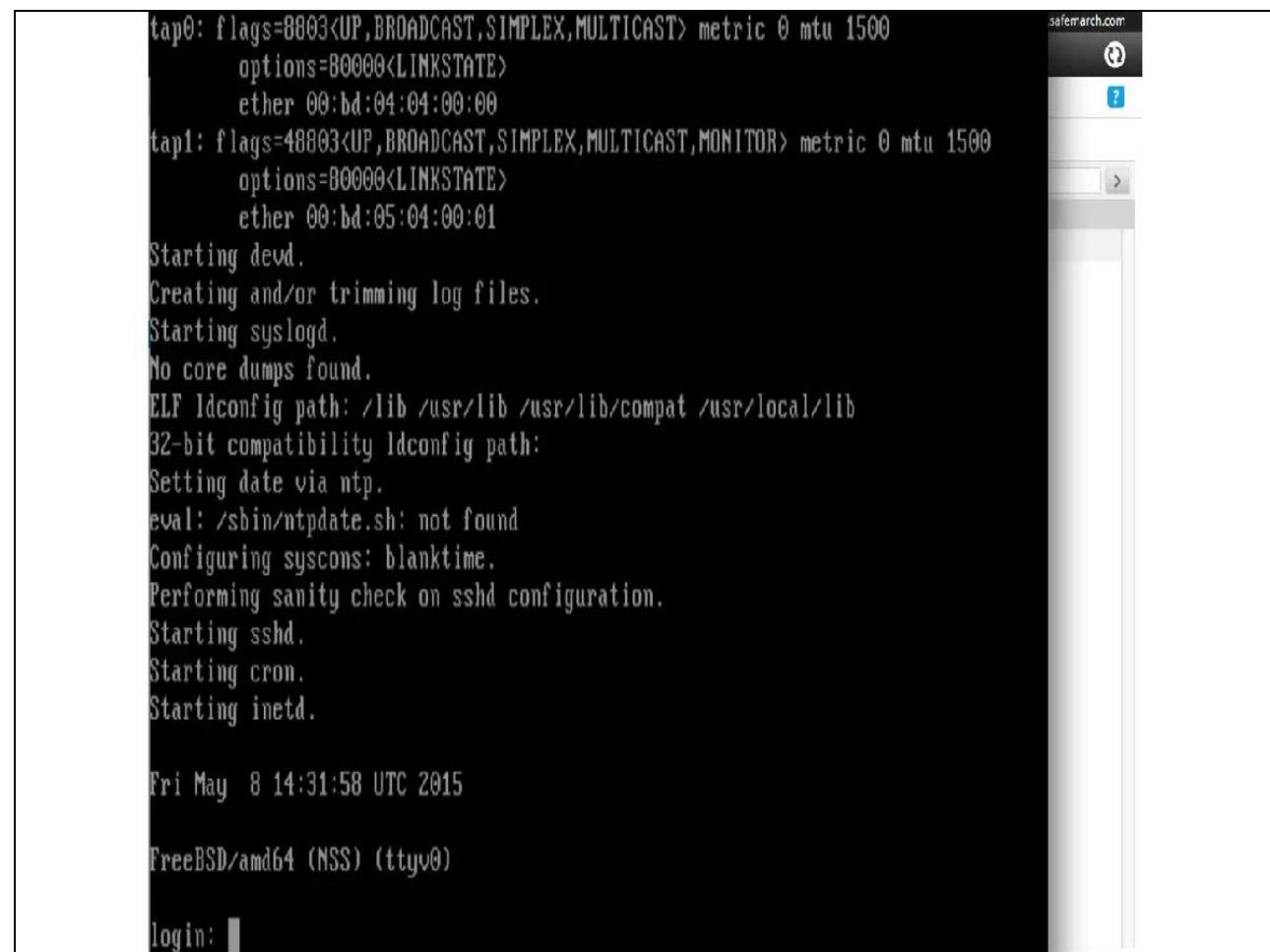
Slide notes



Configuring the NSS VM

Slide notes

We will now turn our attention away from the Admin UI and look at the configuration process for the NSS instance via the NSS console.



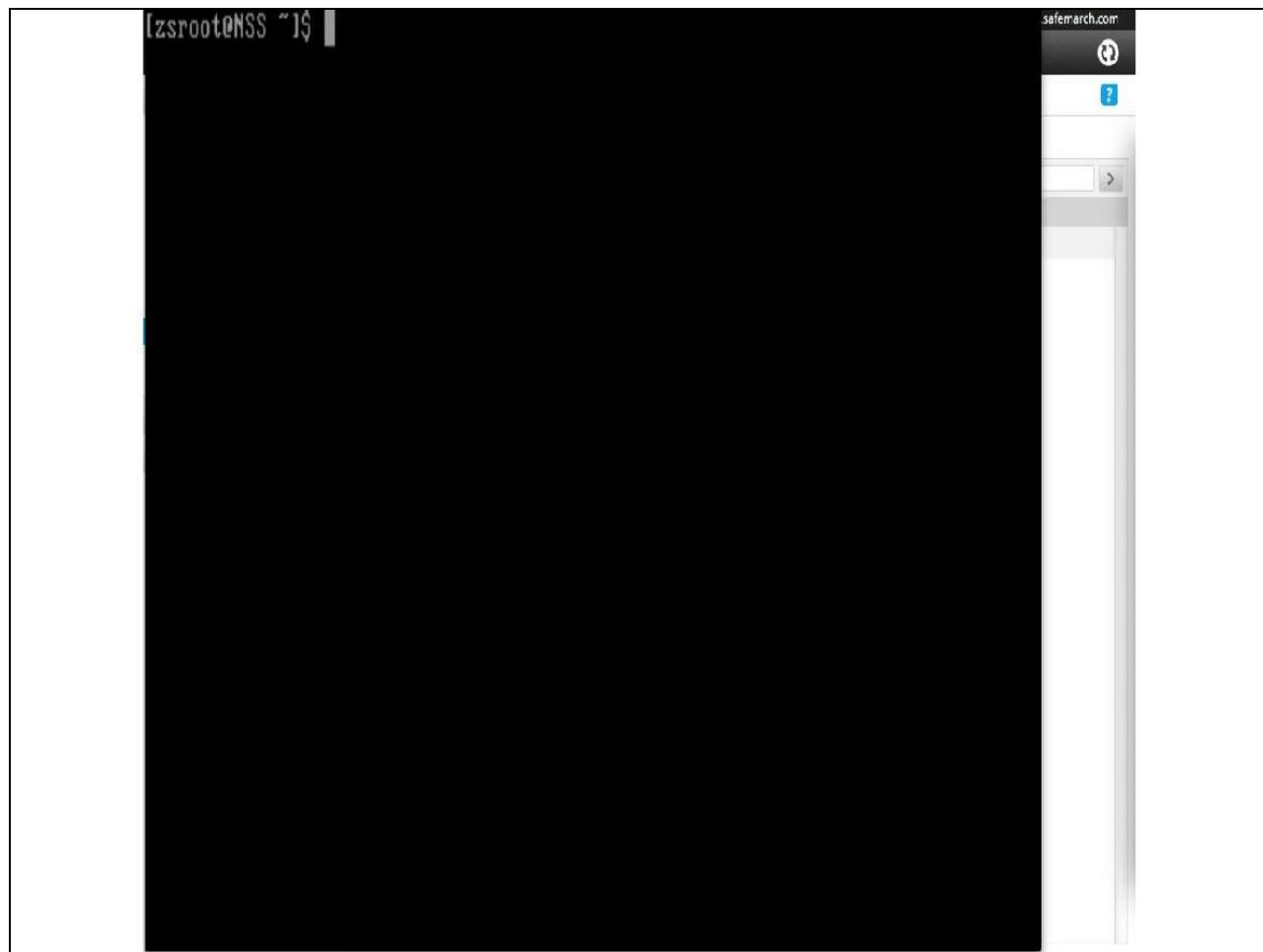
The screenshot shows a terminal window with a black background and white text. It displays the FreeBSD boot process, starting with network interface configuration (tap0 and tap1), followed by the start of devd, log file trimming, syslogd, and core dump handling. It then shows the ldconfig path, date setting via ntp, and various service starts (ntpd, sshd, cron, inetc). The log concludes with the current date and time (Fri May 8 14:31:58 UTC 2015), the system identifier (FreeBSD/amd64 (NSS) (ttyv0)), and a login prompt (login: [REDACTED]). A vertical scrollbar is visible on the right side of the terminal window.

```
tap0: flags=8003<UP,BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
      options=80000<LINKSTATE>
      ether 00:bd:04:04:00:00
tap1: flags=48803<UP,BROADCAST,SIMPLEX,MULTICAST,MONITOR> metric 0 mtu 1500
      options=80000<LINKSTATE>
      ether 00:bd:05:04:00:01
Starting devd.
Creating and/or trimming log files.
Starting syslogd.
No core dumps found.
ELF ldconfig path: /lib /usr/lib /usr/lib/compat /usr/local/lib
32-bit compatibility ldconfig path:
Setting date via ntp.
eval: /sbin/ntpdate.sh: not found
Configuring syscons: blanktime.
Performing sanity check on sshd configuration.
Starting sshd.
Starting cron.
Starting inetc.
Fri May 8 14:31:58 UTC 2015
FreeBSD/amd64 (NSS) (ttyv0)
login: [REDACTED]
```

Slide notes

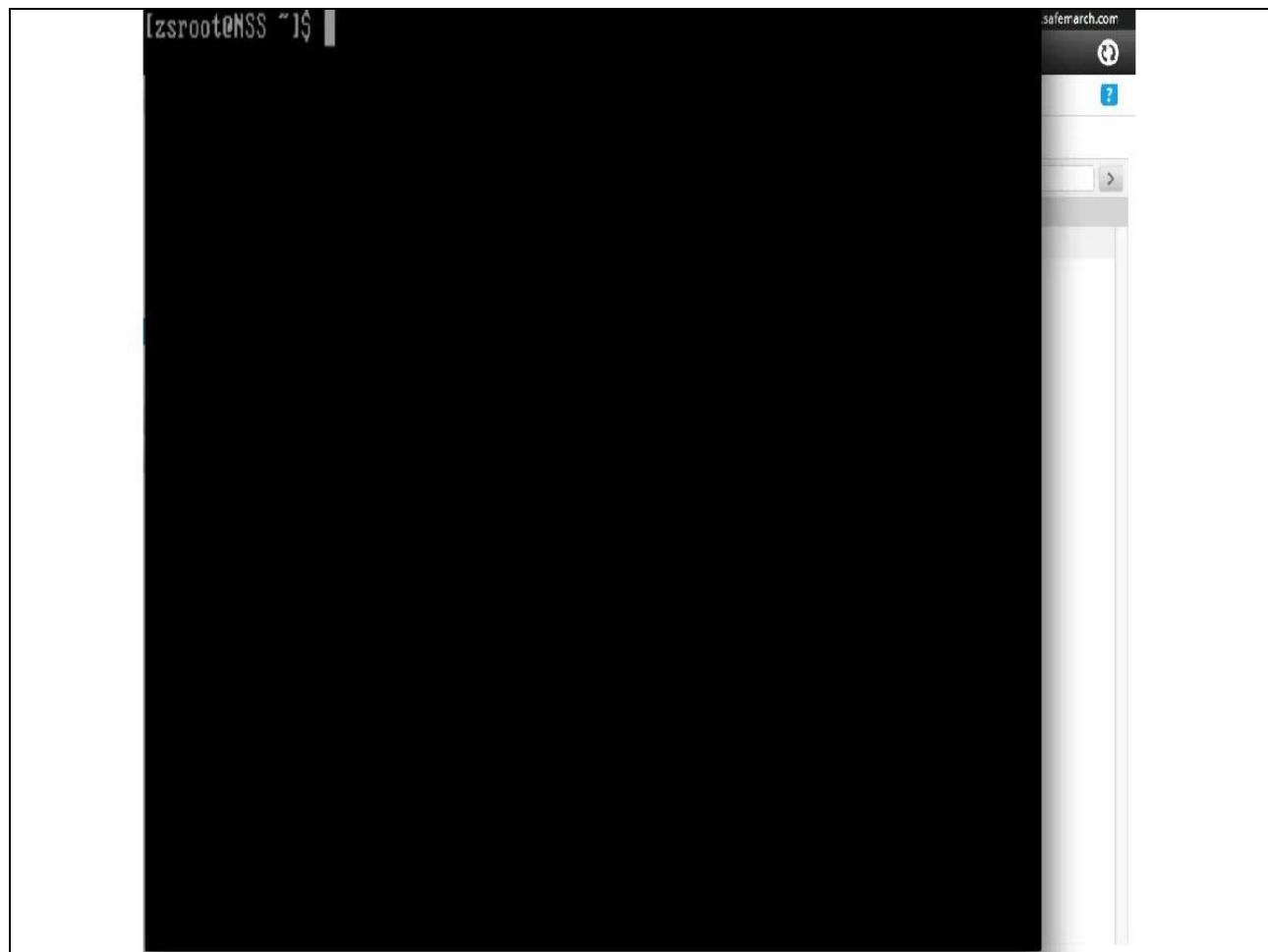
Once the VM is running, connect to the console. Log in as user zsroot and password zsroot. Your first task is to run the passwd command to change the default password. Now we will configure the network interfaces. Run the command, sudo nss configure. Enter the DNS server IP, management interface IP and gateway, and service IP address IP and gateway.

Note that the management and service IPs can be on different subnets as long as the DNS server is reachable from both interfaces. Now we need to upload the client certificate. You can use FTP, SCP, or SFTP to upload the certificate file.



Slide notes

We'll use SCP in this demonstration. To install the certificate run the command sudo nss install-cert.



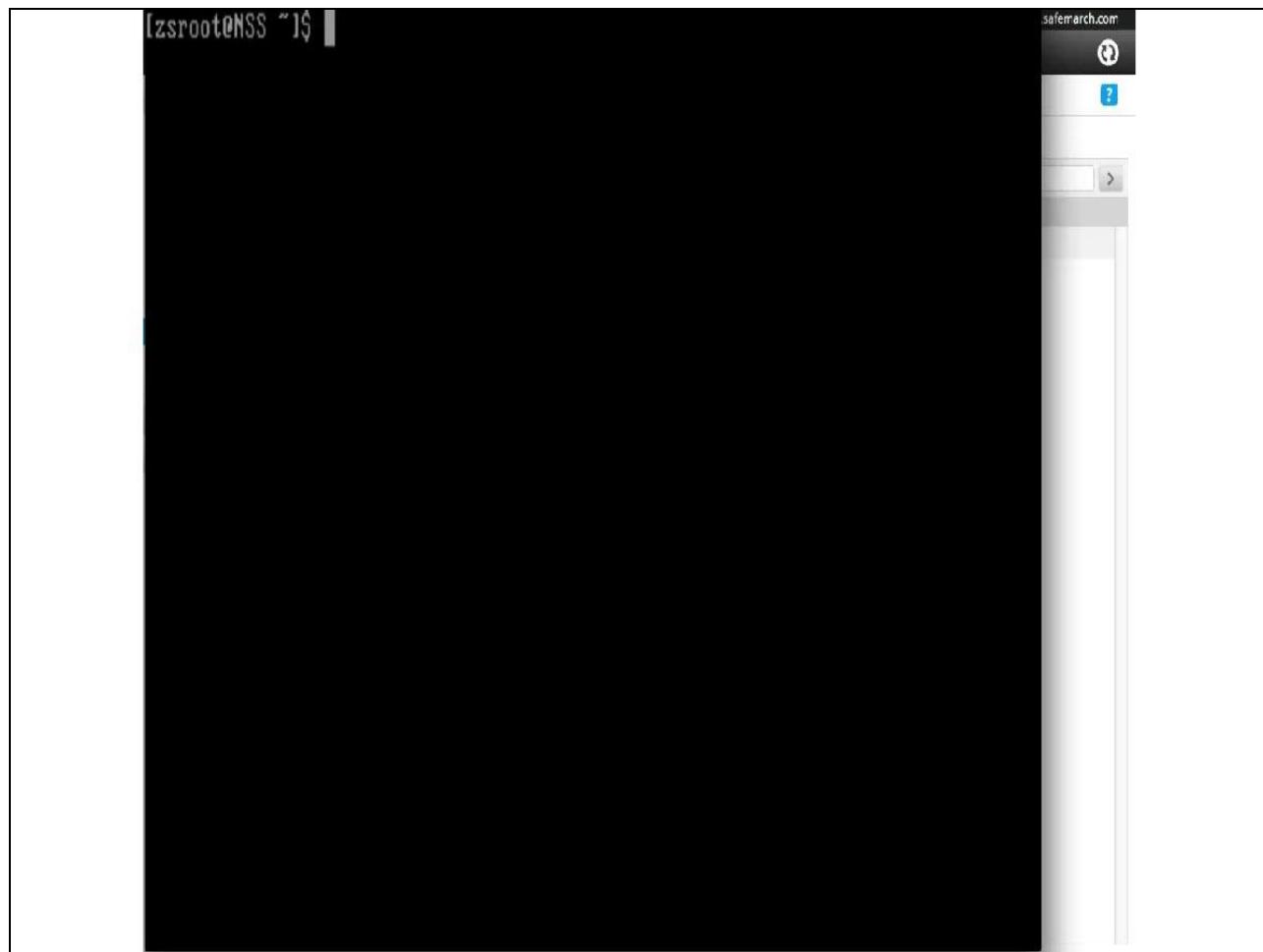
Slide notes

You can verify the cert was loaded by running the command sudo nss dump config.

```
[zsroot@NSS ~]$ sudo nss dump-config
Configured Values:
CloudName:zscalertwo.net
nameserver:192.168.1.34
Mgmt IP:192.168.1.150/24
Default gateway for Mgmt IP:192.168.1.1
Service IP:192.168.1.151/24
Default gateway for Service IP:192.168.1.1
[zsroot@NSS ~]$
```

Slide notes

Next we will download the latest NSS binaries. Once NSS is running the system will automatically update whenever new versions are available. Run the command sudo nss update-now. Next, start NSS by running the command sudo nss start and make sure nss starts automatically by running the command sudo nss enable-autostart.



Slide notes

You can verify that nss is running by entering sudo nss troubleshoot netstat | grep tcp and look for a connection to Zscaler on port 9422



Configuring NSS Feeds/Alerts

Slide notes



Configuring NSS Feeds/Alerts

1. • Create at least 2 feeds
 - Logs
 - NSS Alerts
2. • Enter SIEM IP address and TCP port
3. • Define Feed Output Type/Format (Splunk, QRadar, Custom)
4. • Define filters – see NSS Guide on Help Portal
5. • Save and verify
 - `nss troubleshoot netstat | grep tcp`

Slide notes

Now that the NSS virtual machine is running, we need to specify where and how to send the logs. Zscaler recommends creating 2 feeds. One for user logs and one for alerts about the status of NSS itself. After that we'll enter our SIEM address and TCP port, define the Feed Output Type, Define Filter, and then Save and Verify.

The screenshot shows the Nanolog Streaming Service interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Nanolog Streaming Service" and contains a sub-header "NSS SERVERS". A "Click Box" highlights the "NSS SERVERS" tab. Below it are buttons for "Add NSS Server", "Deploy NSS Virtual Appliance", and "Download MIB Files". A search bar with placeholder "Search..." is also present. A table lists one server entry:

No.	Server Name	Status	State	SSL Certificate
1	Safemarch SIEM	Enabled	Unhealthy	Download

A callout box points to the "NSS Feeds" tab in the top navigation bar, which is currently highlighted. At the bottom of the screen, there is a copyright notice: "Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents".

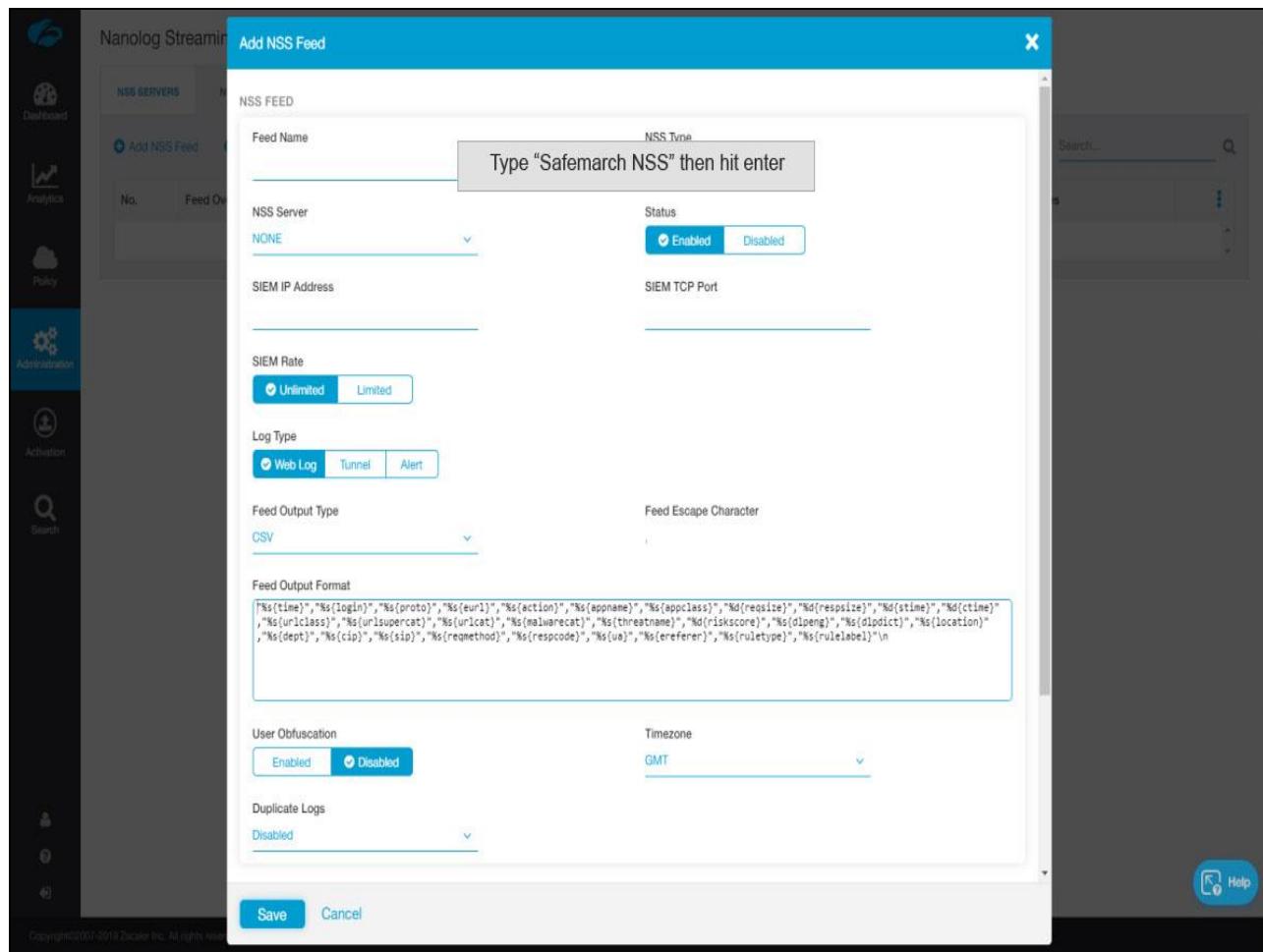
Slide notes

We'll start with the Alerts feed. Click the "NSS Feeds" tab.

The screenshot shows the Nanolog Streaming Service interface. On the left, there is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Nanolog Streaming Service" and has tabs for "NSS SERVERS" and "NSS FEEDS". The "NSS FEEDS" tab is active. It contains a search bar, a "Click Box feed" section, and a "Add MCAS NSS Feed" button. Below these are sections for "Feed Overview", "Log Filter", "Feed Output Format", and "Feed Attributes". A callout box points to the "Add NSS Feeds" button. At the bottom of the main area, it says "No matching items found". The footer of the page includes copyright information: "Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents" and a "Help" button.

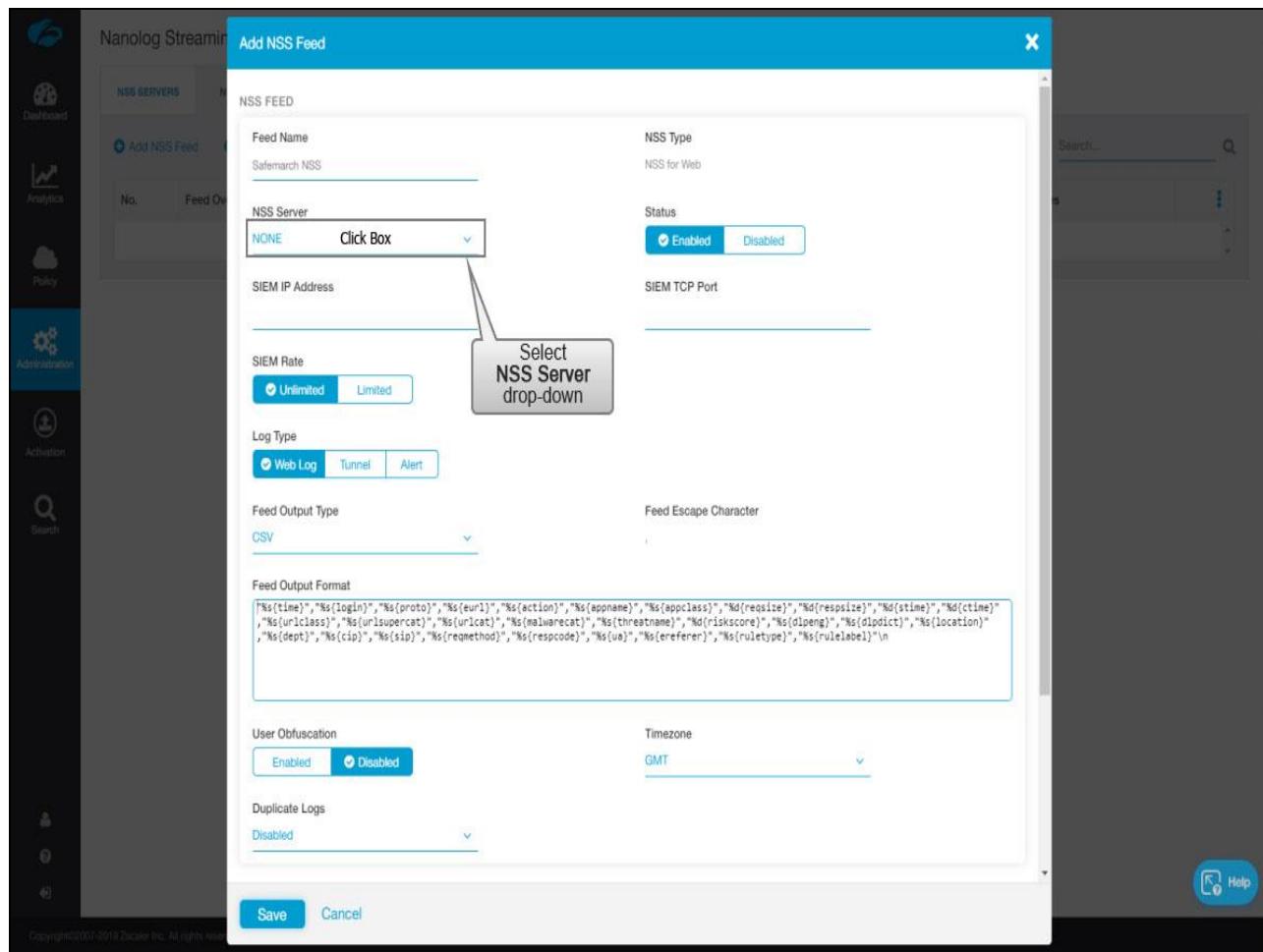
Slide notes

Click “Add NSS Feeds”.



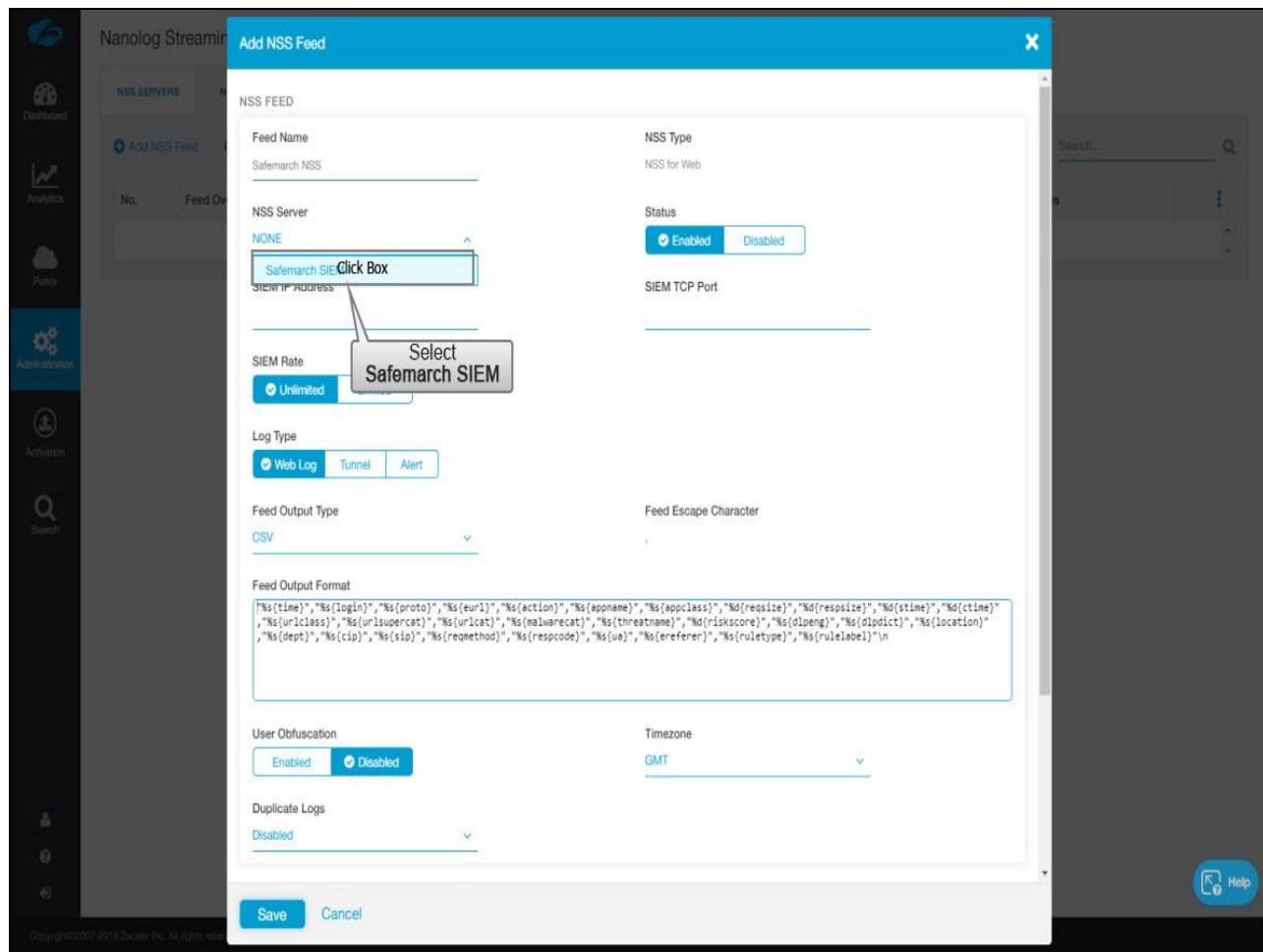
Slide notes

Enter a name for the Feed.

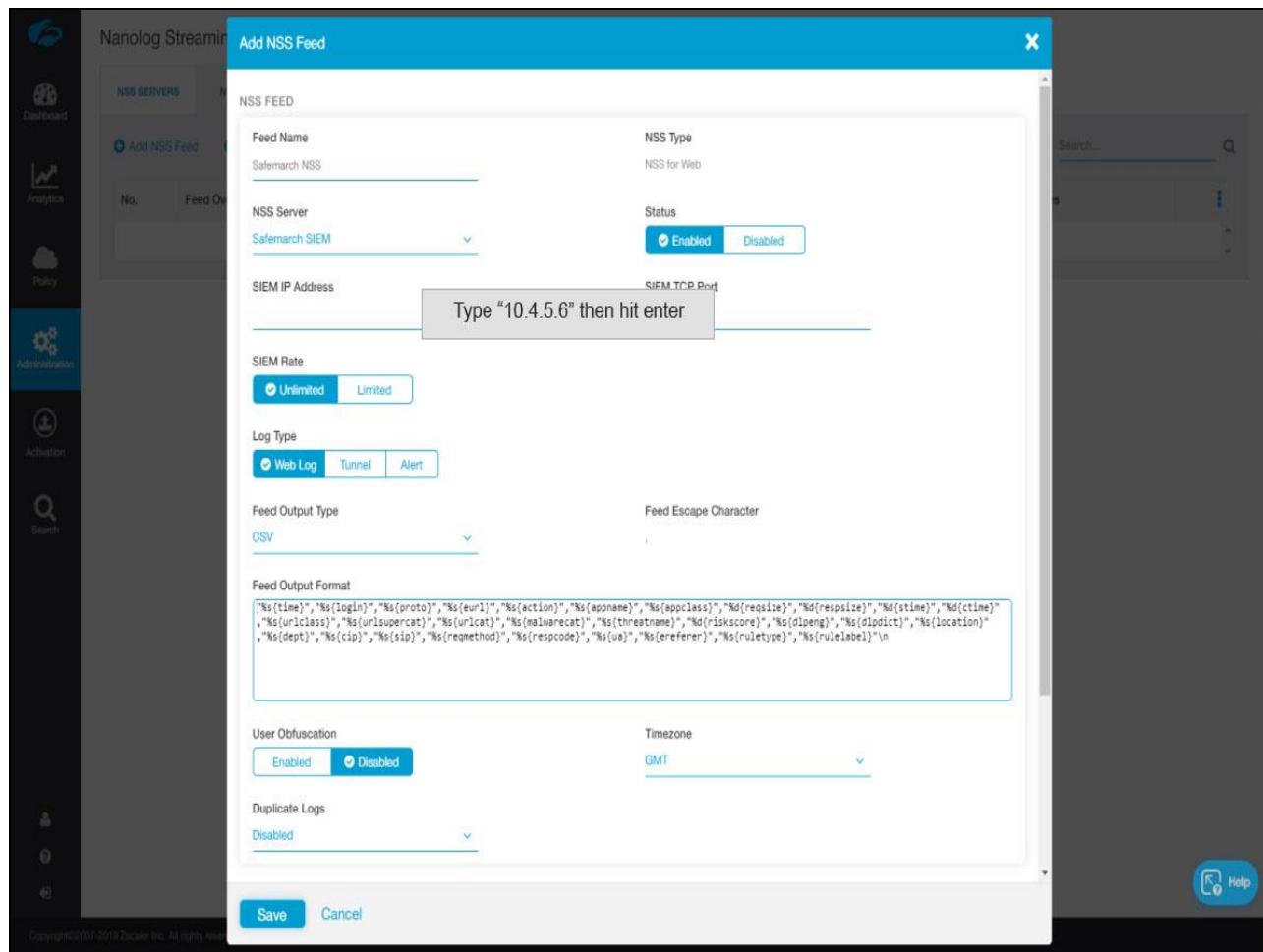


Slide notes

Then select the NSS server.

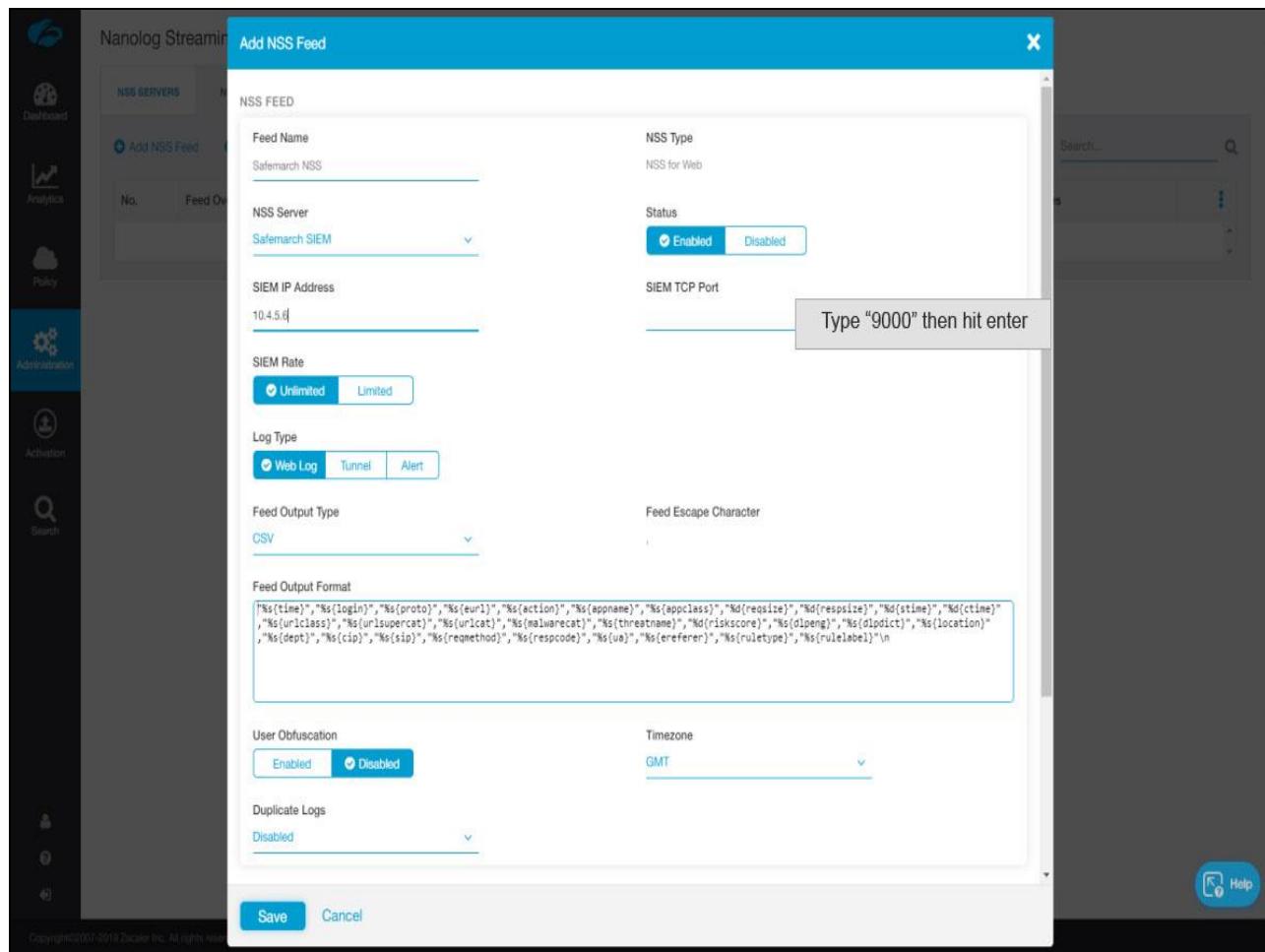


Slide notes

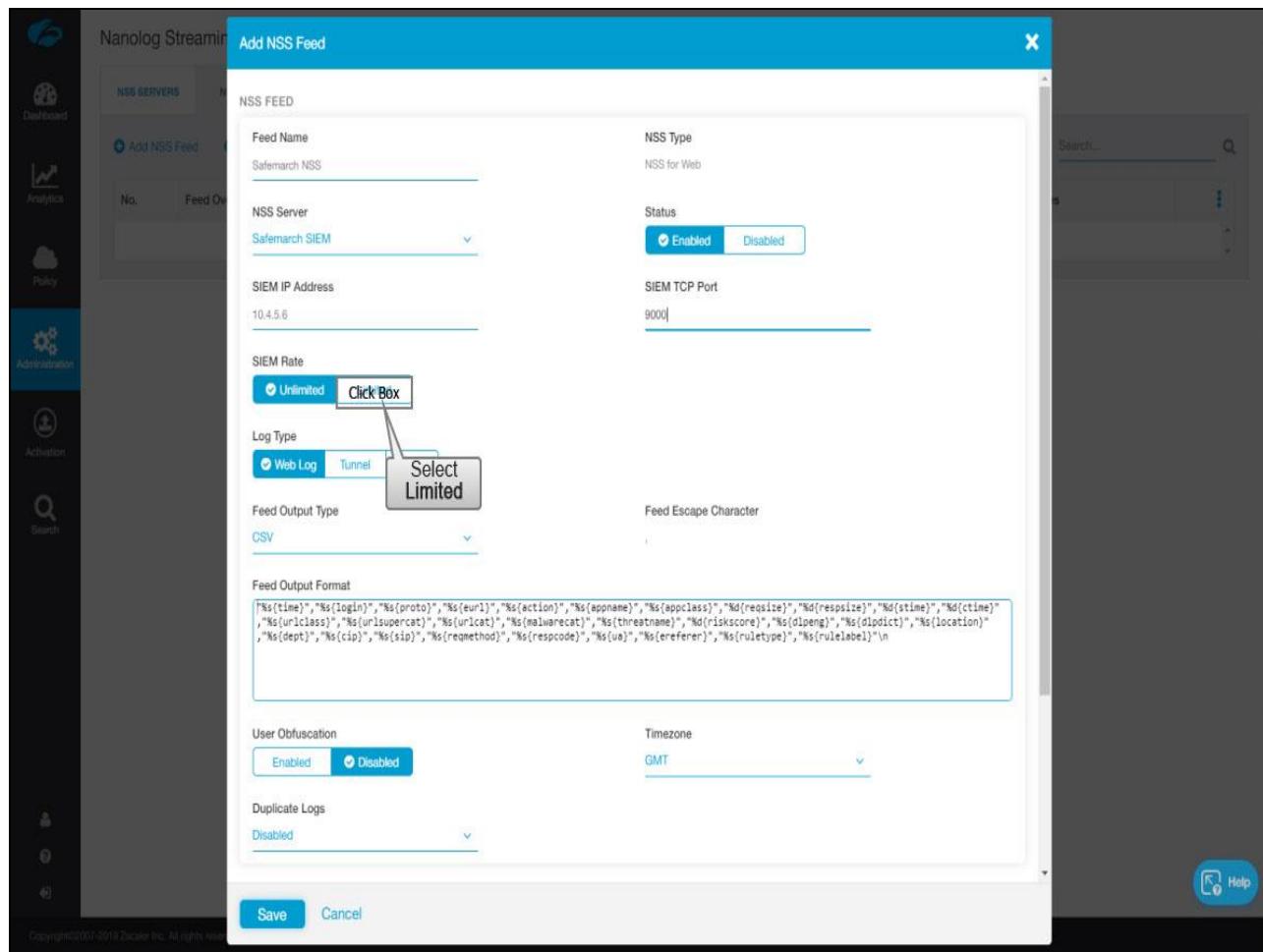


Slide notes

Enter the IP address and TCP port of your SIEM.

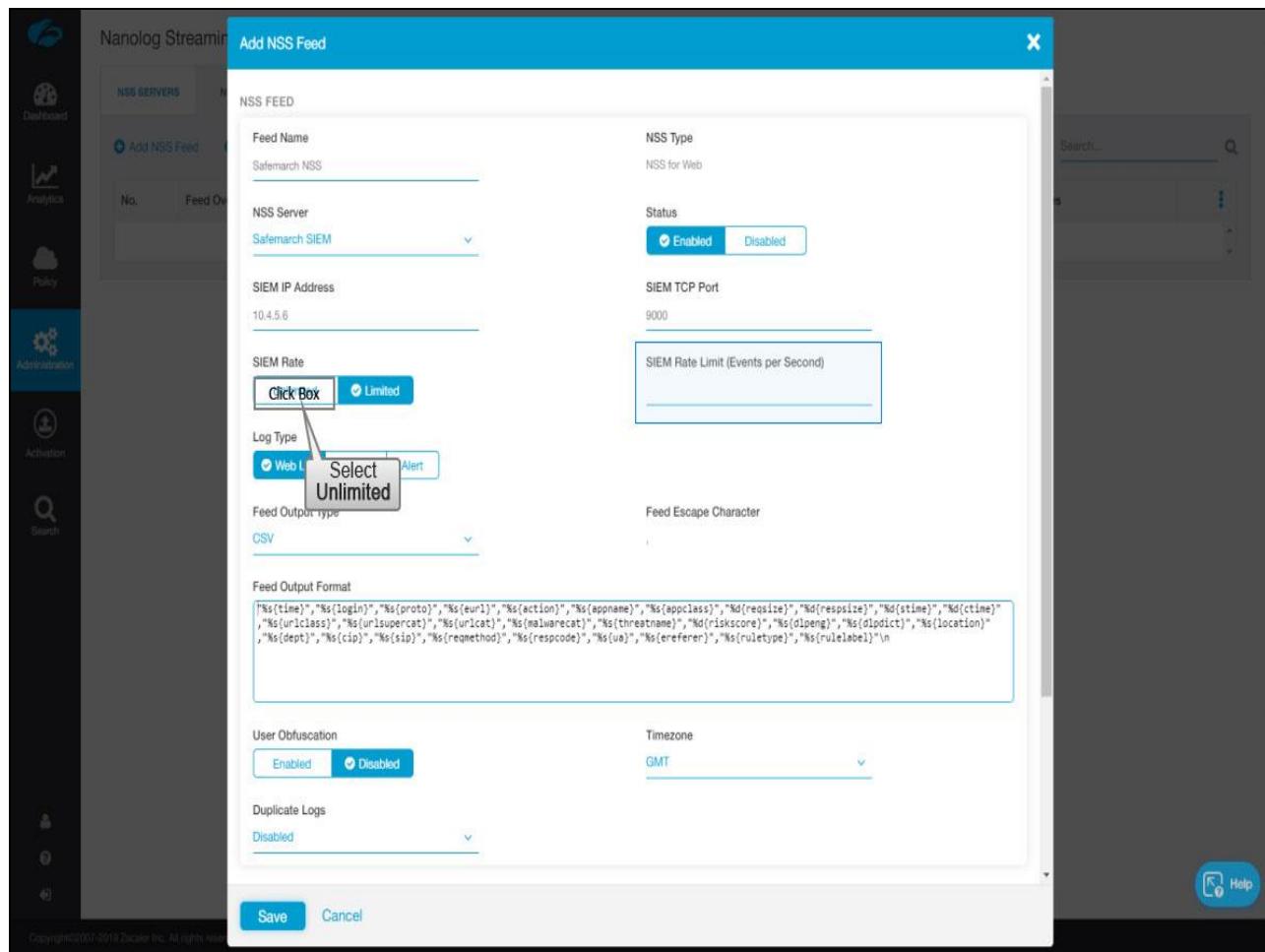


Slide notes

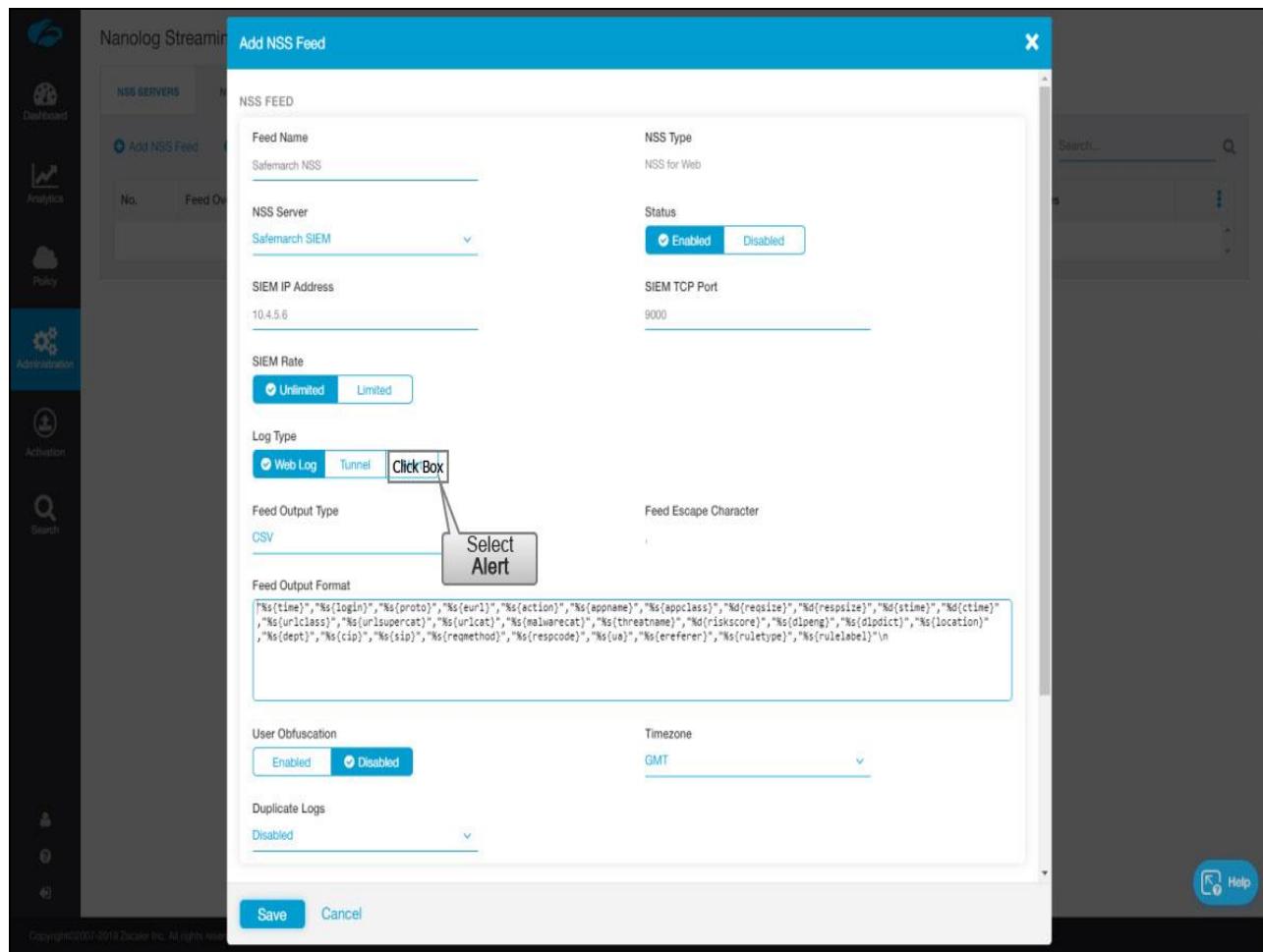


Slide notes

You can throttle the number of events per second that are streamed to your SIEM. Click Limited.

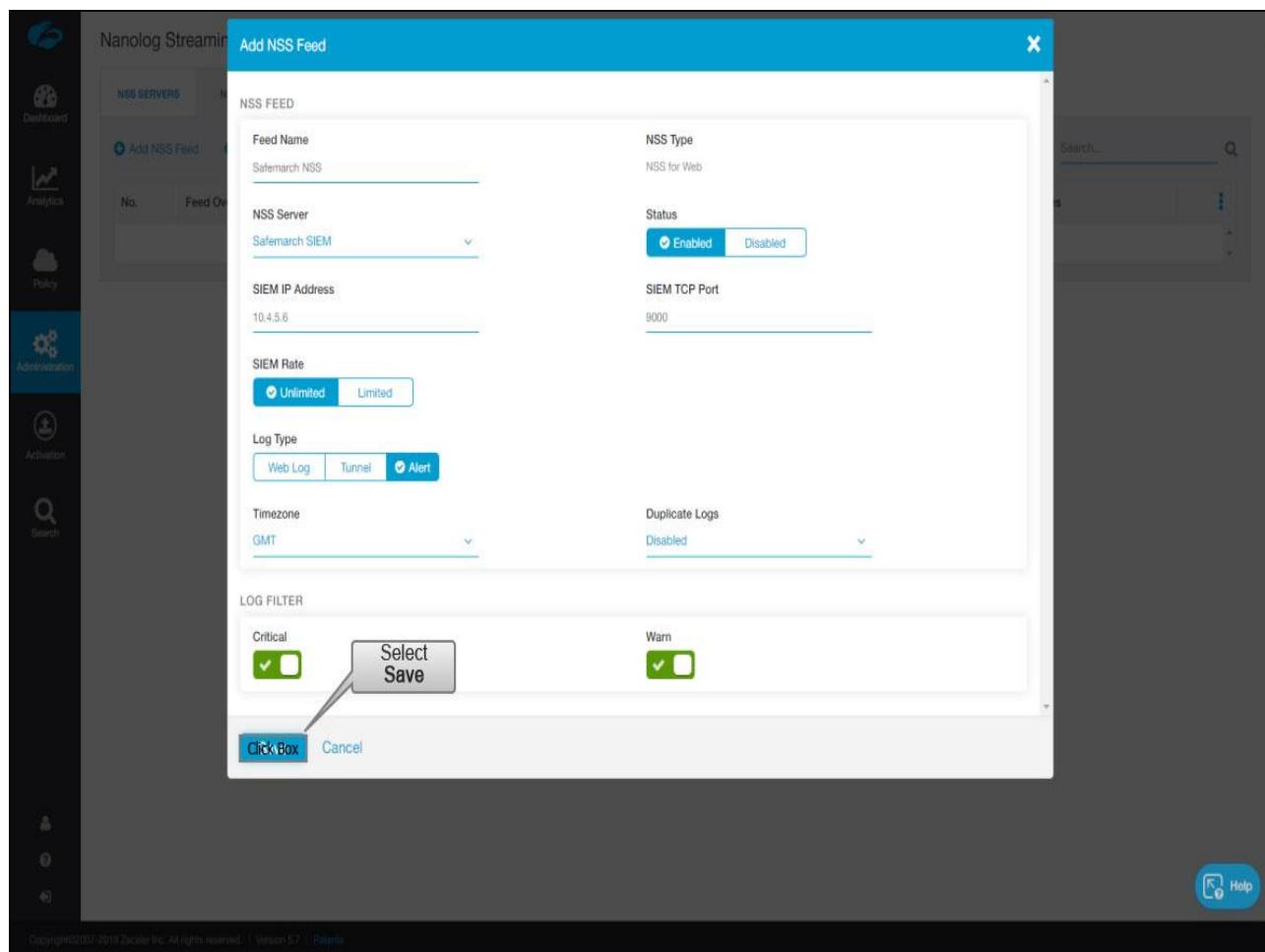


Slide notes



Slide notes

For log type click “Alert”.



Slide notes

Click “Save”.

The screenshot shows the Nanolog Streaming Service interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Nanolog Streaming Service" and has tabs for "NSS SERVERS" and "NSS FEEDS". Below the tabs are buttons for "Add NSS Feed" and "Add MCAS NSS Feed". A search bar is at the top right. The main content area displays a table for "Feed Overview". The table has columns for "No.", "Feed Overview", "Log Filter", "Feed Output Format", and "Feed Attributes". There is one row in the table:

No.	Feed Overview	Log Filter	Feed Output Format	Feed Attributes
1	<p>Feed Name: Safemarch NSS NSS Server: Safemarch SIEM Status: Enabled Output Destination: 10.4.5.6:9000 Log Type: Alert Feed Type: Syslog More...</p>	<p>Alerts: Critical, Warn</p>	---	<p>Duplicate Logs: Disabled Timezone: GMT SIEM Rate: Unlimited</p>

At the bottom left of the main area, there is a copyright notice: "Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents". At the bottom right is a "Help" button.

Slide notes

Then **Activate** your changes.

The screenshot shows the ZCCP-IA NSS Student Guide 5.7 interface. On the left, there is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The Activation icon is highlighted with a blue background. The main content area is titled "MY ACTIVATION STATUS" and shows "CURRENTLY EDITING (1)" activation for "admin@zccp-ia.com". The "Activation" section includes a "Log Filter" dropdown set to "Alerts Critical, Warn", a "Feed Output Format" dropdown set to "...", and a "Feed Attributes" table with rows for "Duplicate Logs" (Disabled), "Timezone" (GMT), and "SIEM Rate" (Unlimited). A large blue "Activate" button is visible. At the bottom of the interface, there is a copyright notice: "Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents".

Slide notes

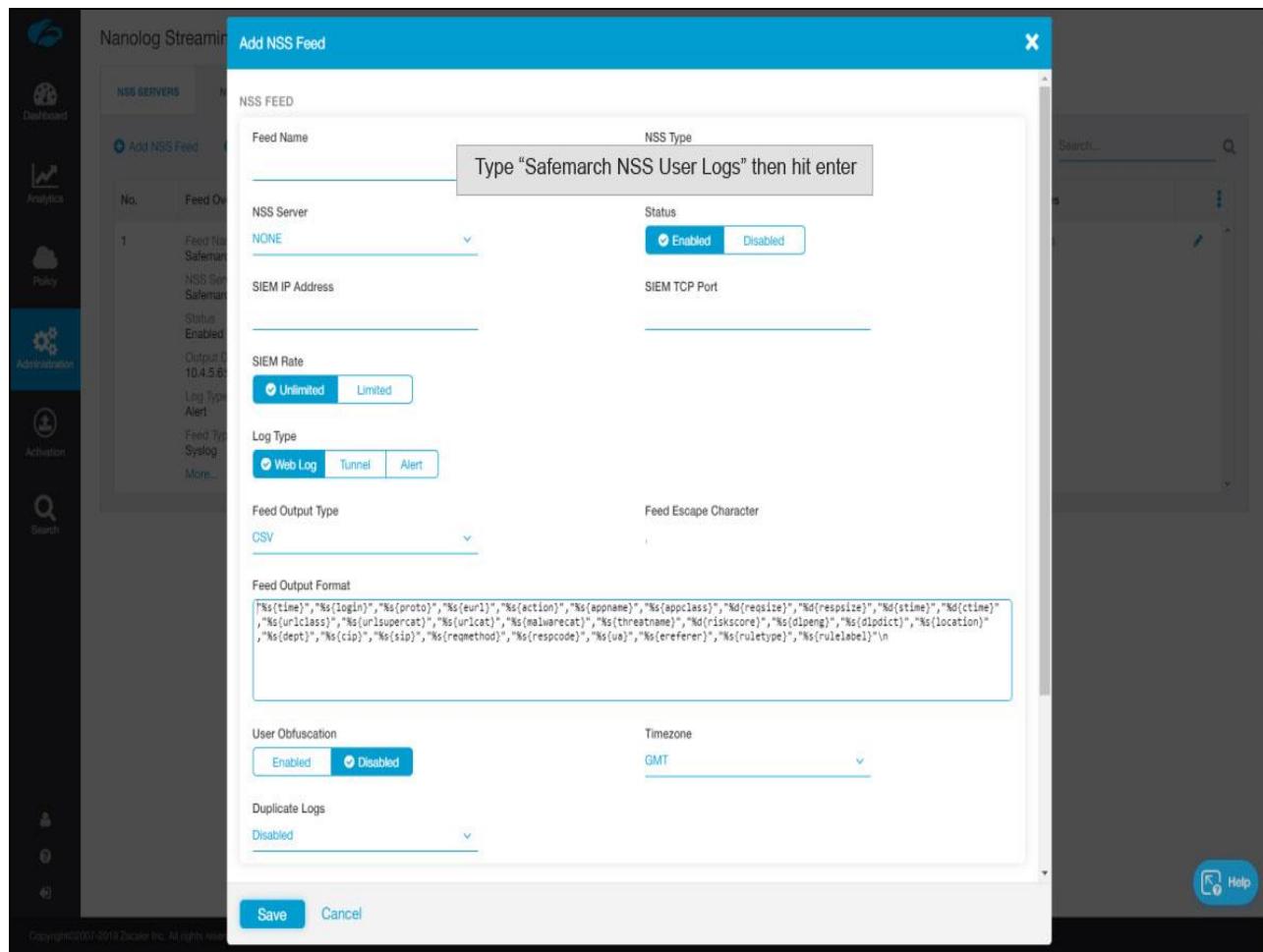
The screenshot shows the Nanolog Streaming Service interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Nanolog Streaming Service" and has tabs for "NSS SERVERS" and "NSS FEEDS". The "NSS FEEDS" tab is active, showing a table with one row. A tooltip "Select Add NSS Feeds" points to the "Add MCAS NSS Feed" button. The table columns include No., Feed Overview, Log Filter, Feed Output Format, and Feed Attributes. The first row shows the following details:

No.	Feed Overview	Log Filter	Feed Output Format	Feed Attributes
1	Feed Safe NSS Server SafeMarch SIEM Status Enabled Output Destination 10.4.5.6:9000 Log Type Alert Feed Type Syslog More...	Alerts Critical, Warn	...	Duplicate Logs: Disabled Timezone: GMT SIEM Rate: Unlimited

At the bottom left, it says "Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents". At the bottom right is a "Help" button.

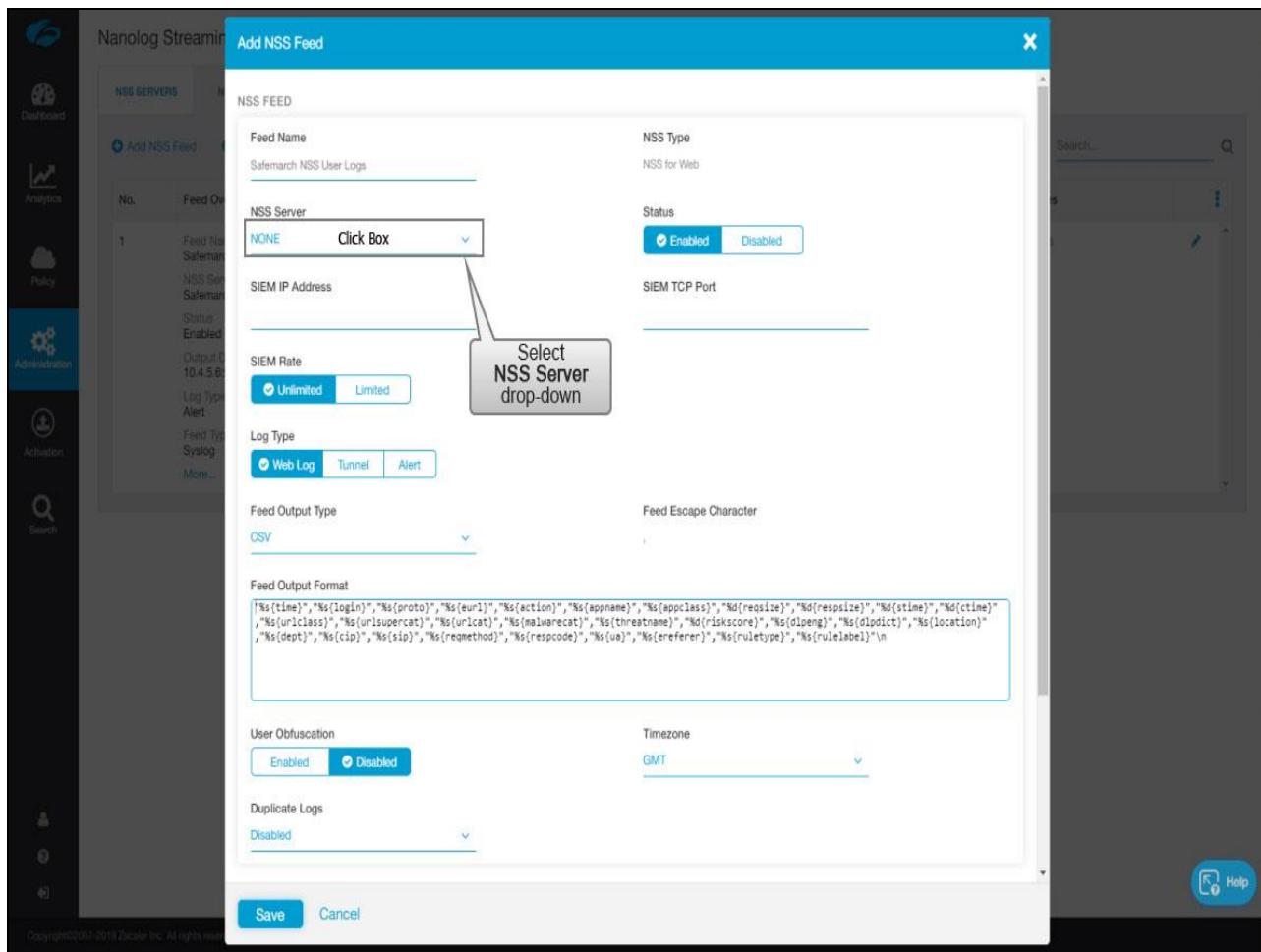
Slide notes

Now we'll configure the log feed. Click "Add NSS Feed".



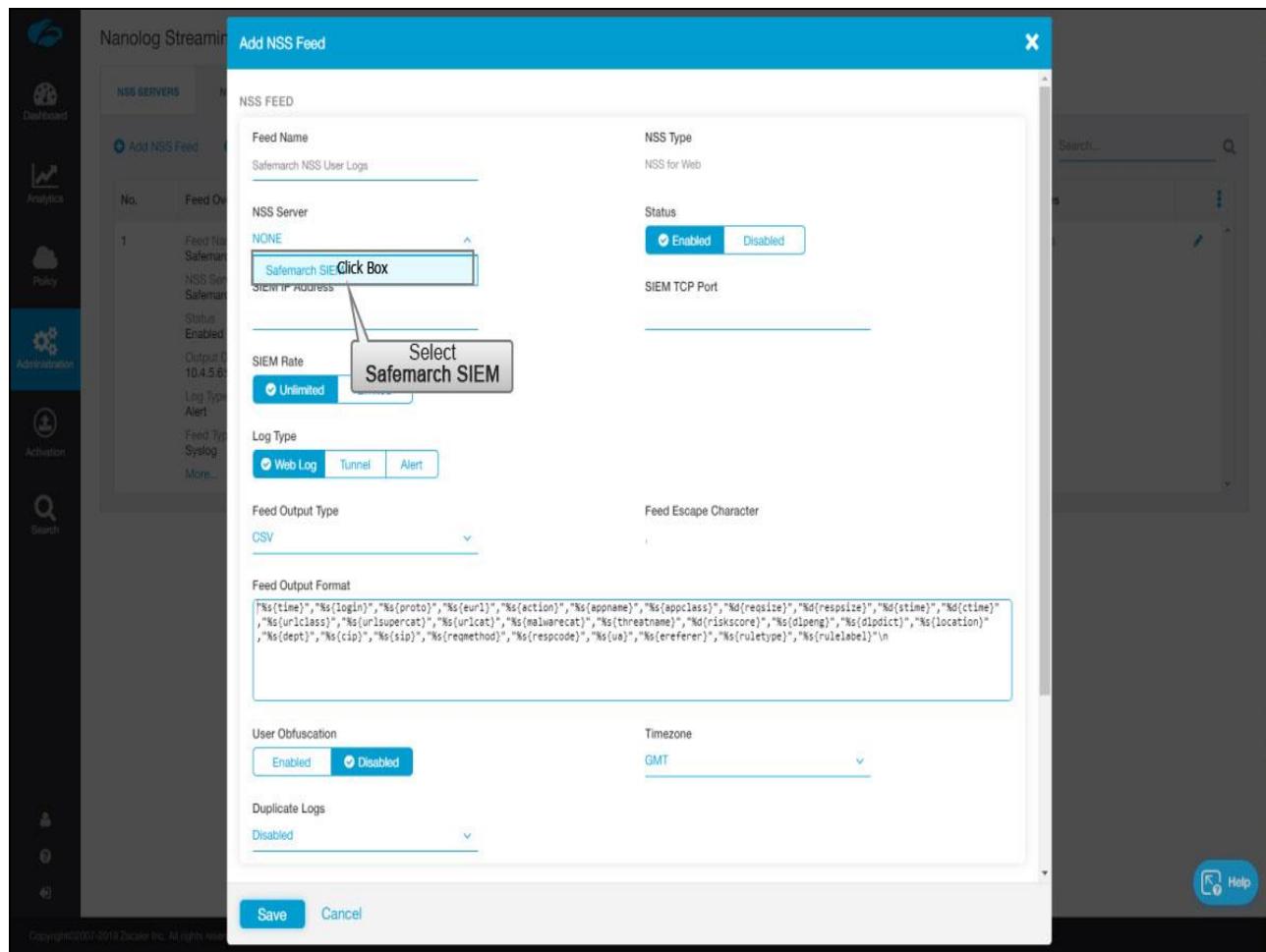
Slide notes

Enter a name for the feed

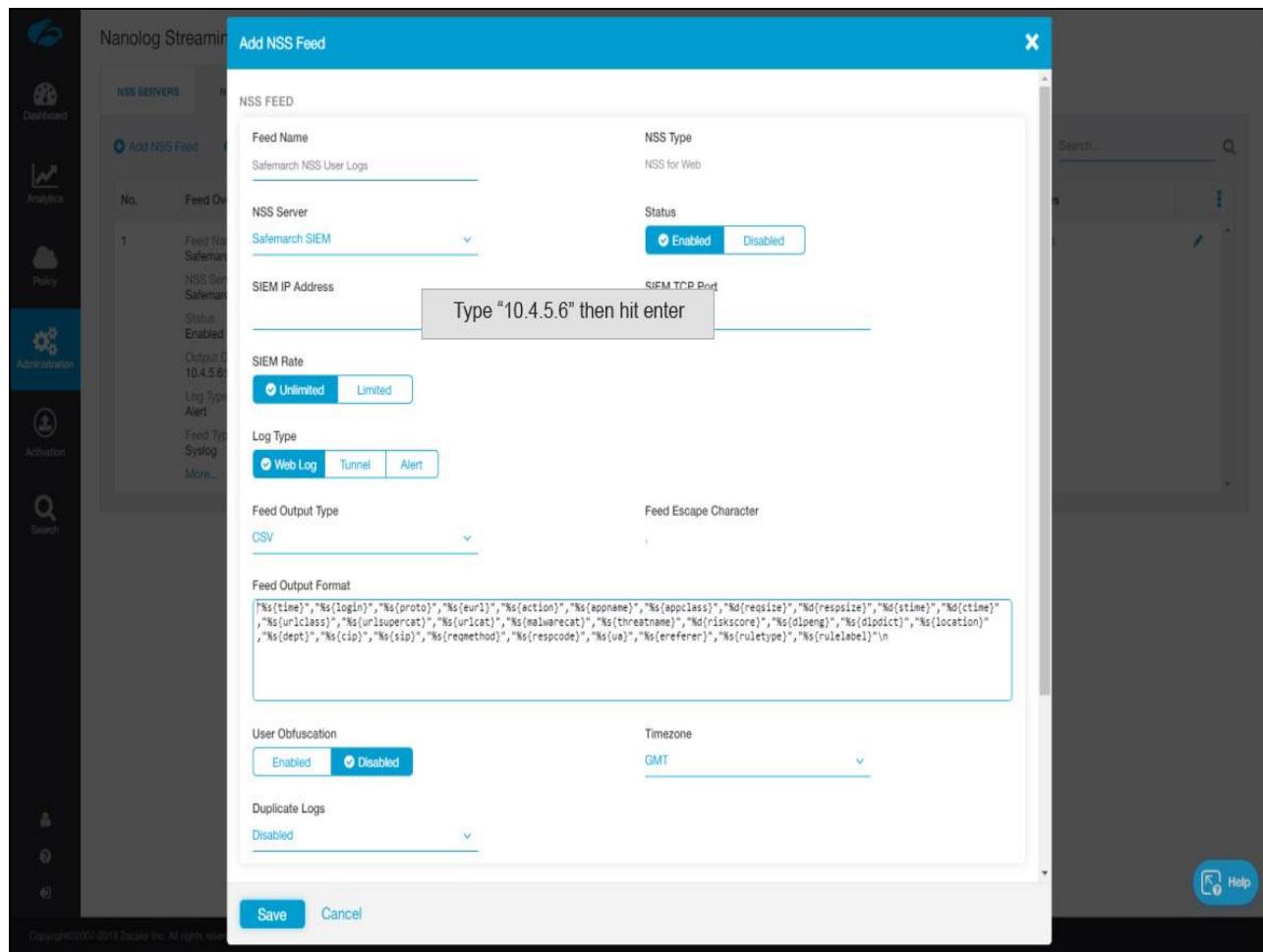


Slide notes

and select the NSS server.

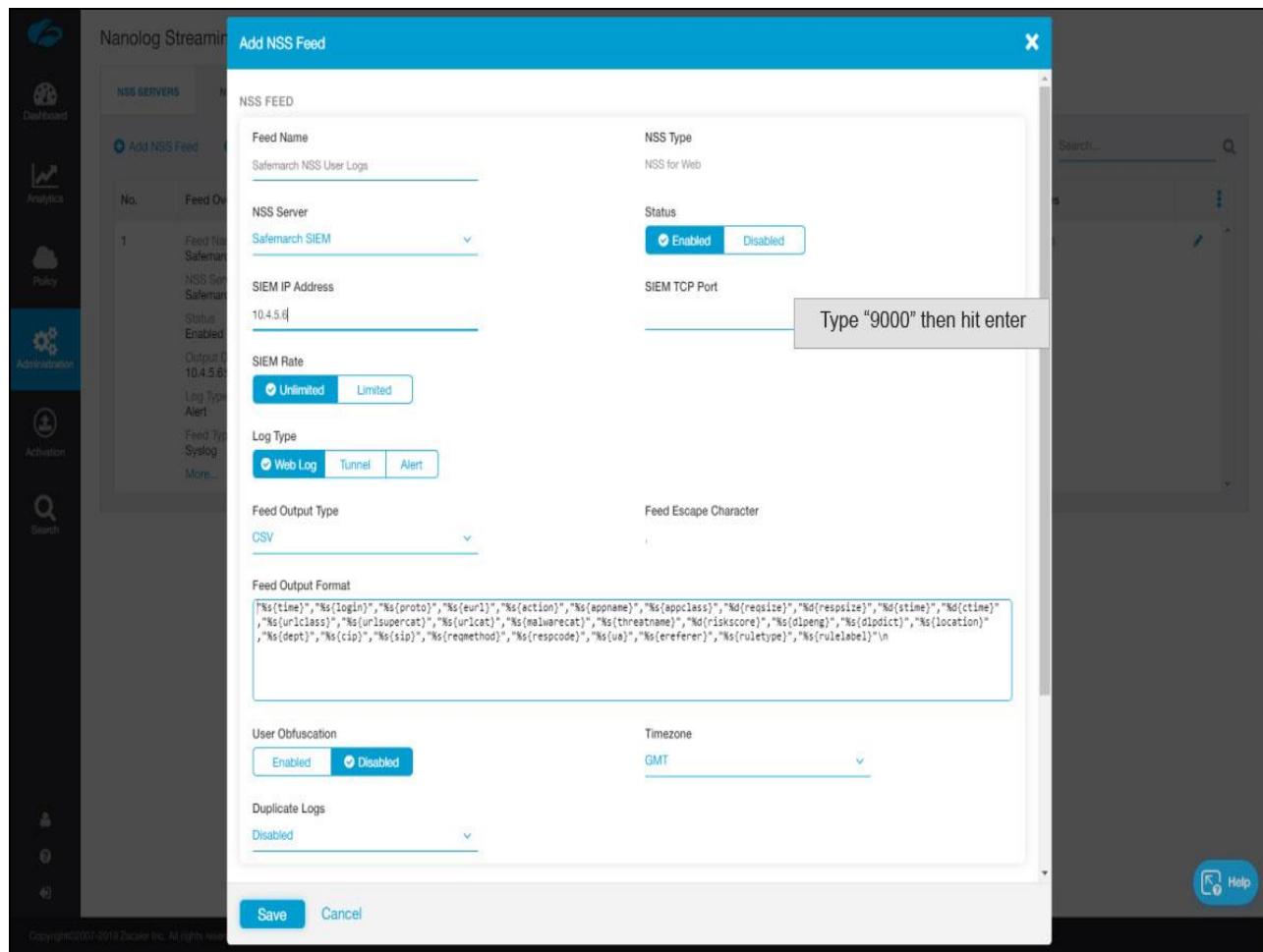


Slide notes

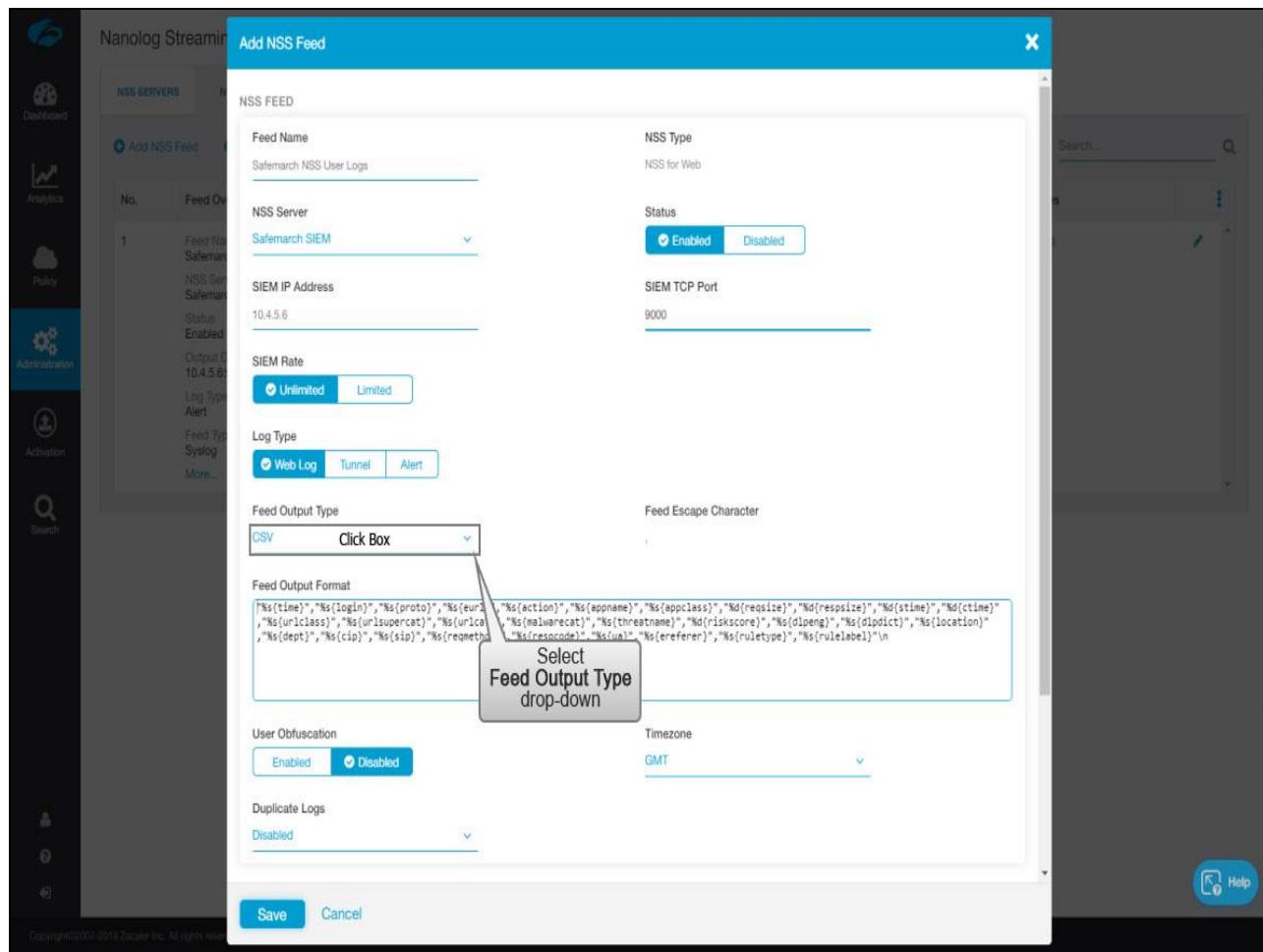


Slide notes

Enter the IP address and TCP port of your SIEM.

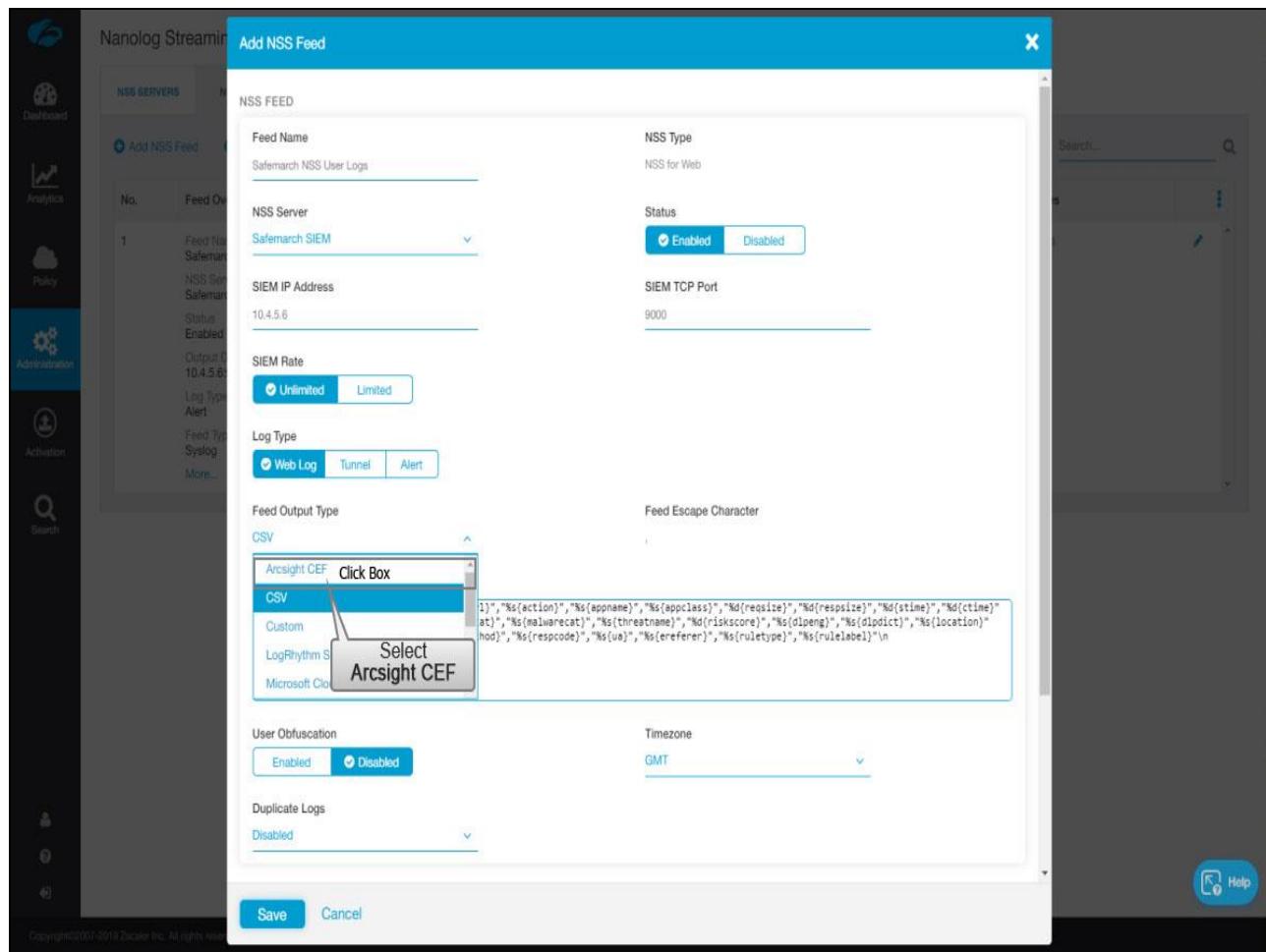


Slide notes



Slide notes

For Feed output type, choose your SIEM.



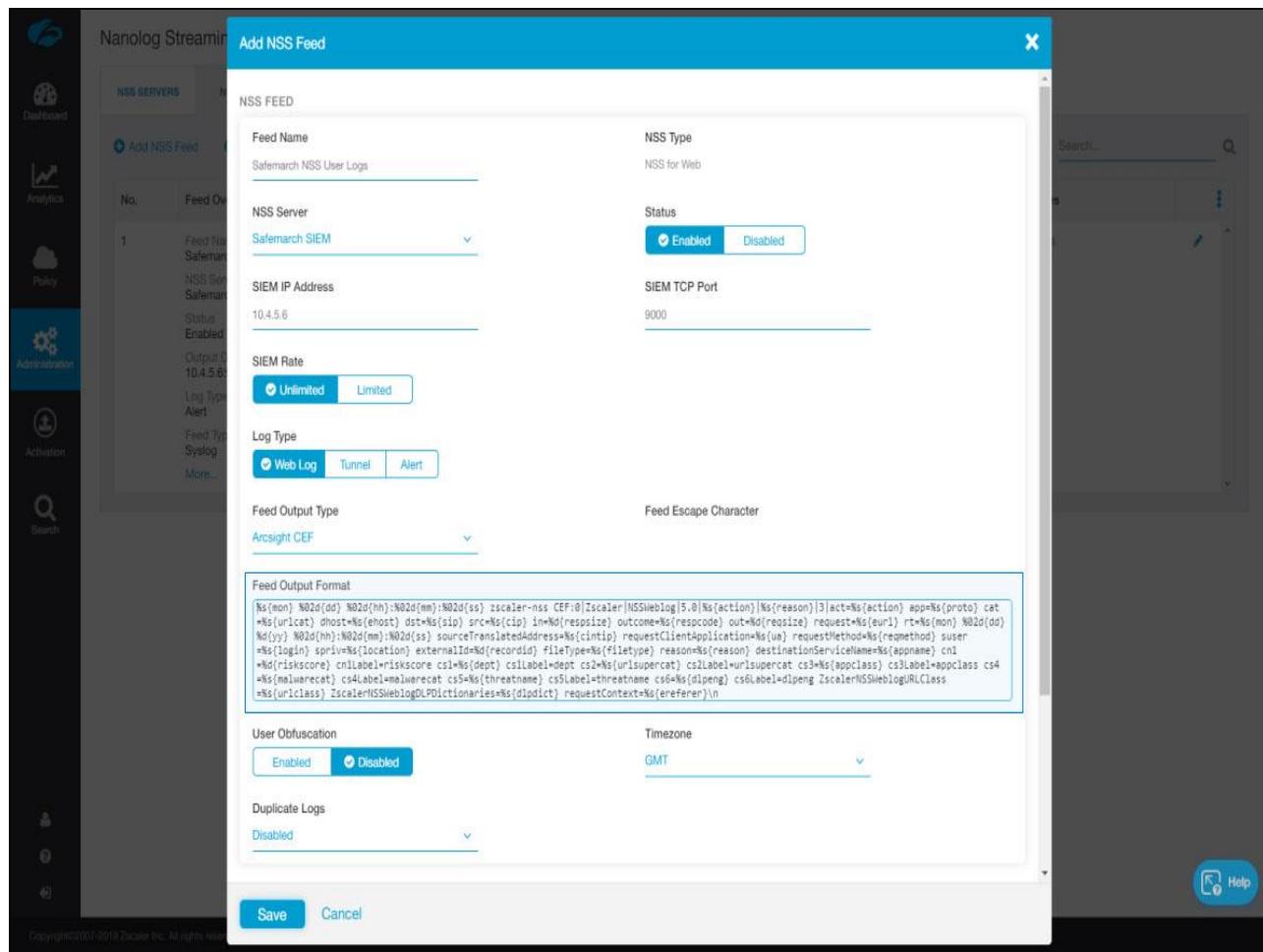
Slide notes

The screenshot shows the Zscaler Nanolog Stream interface with the 'Add NSS Feed' dialog box open. The dialog box contains the following fields:

- NSS FEED**
- Feed Name:** Safemarch NSS User Logs
- NSS Type:** NSS for Web
- NSS Server:** Safemarch SIEM
- Status:** Enabled (radio button selected)
- NSS IP Address:** 10.4.5.6
- SIEM TCP Port:** 9000
- SIEM Rate:** Unlimited (radio button selected)
- Log Type:** Web Log (radio button selected)
- Feed Output Type:** CSV (selected)
- Feed Escape Character:** A large text area containing a sample log entry in JSON format.
- User Obfuscation:** Disabled (radio button selected)
- Timezone:** GMT
- Duplicate Logs:** Disabled

At the bottom of the dialog box are 'Save' and 'Cancel' buttons, and a 'Help' link in the bottom right corner.

Slide notes



Slide notes

This will auto populate the Feed Output format. You can edit that field if you wish. If you click the tooltip it will open a page with details on all of the available fields.

Feed Output Type
These are the fields that will be displayed in the output. You can edit the default list and if you chose Custom as the Field Output Type, change the delimiter as well. See [NSS Feed Output Format](#) for information about the available fields and their syntax.

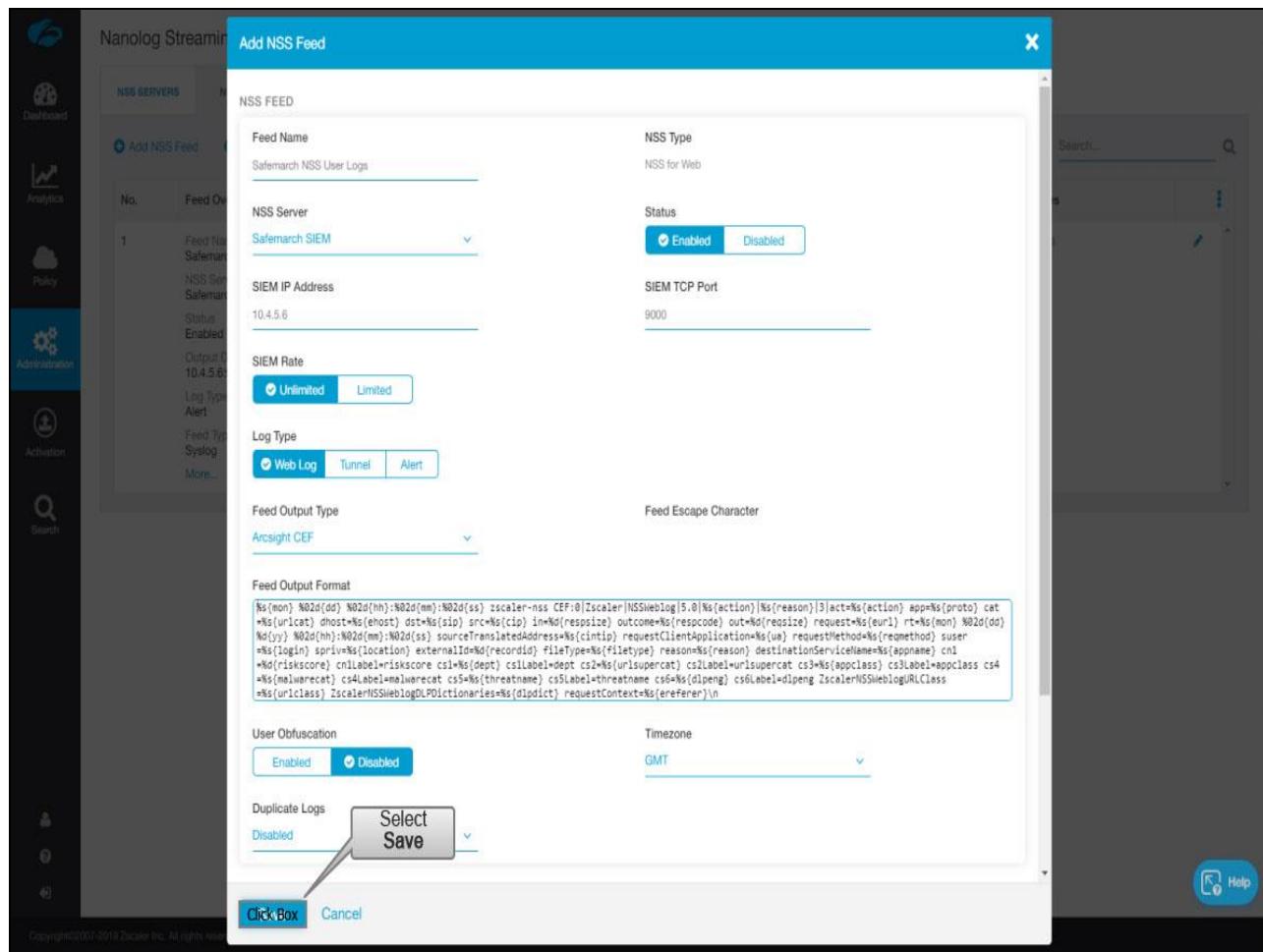
```

${(mon)} ${02d}{dd} ${02d}{mm}: ${02d}{ss} zscaler-nss CEF:0|zscaler|NSSWeblog|5.0|${action}|${reason}|${act}=${proto} cat
${uricat} dhost=${host} dst=${sip} src=${cip} in=${respcode} outcome=${respcode} out=${resize} request=${eurl} rt=${mon} ${02d}{dd}
${y} ${02d}{hh}: ${02d}{mm}: ${02d}{ss}) sourceTranslatedAddress=${cintip} requestClientApplication=${ua} requestMethod=${method} user
=${login} spriv=${location} externalId=${recordid} fileType=${filetype} reason=${reason} destinationServiceName=${appname} c1
#${riskscore} cnlabel=riskscore cs1=${dept} cs1label=dept cs2=${urlsupercat} cs2label=urlsupercat cs3=${apiclass} cs3label=apiclass cs4
=${onewrect} cs4label=onewrect cs5=${threatname} cs5label=threatname cs6=${dipeng} cs6label=dipeng zscalerNSSWeblogURLClass
${uriclass} zscalerNSSWeblogDLPictionaries=${dipdict} requestContext=${refer}|\n

```

Slide notes

Time zone defaults to whatever is specified in the Company Profile. The Duplicate Logs setting specifies how far back in time NSS should resend logs after a connectivity loss between the NSS and SIEM.



Slide notes

The last section allows you to apply filters to limit which logs are sent. In this example you will send everything so we will leave the defaults. You should check out the NSS Guide on the Help Portal for detailed information about the various filters available. Click “Save”.

Nanolog Streaming Service

All changes have been saved.

NSS SERVERS

NSS FEEDS

Add NSS Feed **Add MCAS NSS Feed**

Search...

No.	Feed Overview	Log Filter	Feed Output Format	Feed Attributes
1	Feed Name: SafeMarch NSS NSS Server: SafeMarch SIEM Status: Enabled Output Destination: 10.4.5.6:9000 Log Type: Alert Feed Type: Syslog More...	Alerts Critical, Warn	...	Duplicate Logs: Disabled Timezone: GMT SIEM Rate: Unlimited
2	Feed Name: SafeMarch NSS User Logs NSS Server: SafeMarch SIEM Status: Enabled Output Destination: 10.4.5.6:9000 Log Type: Web Log Feed Type: Arcsight CEF More...		<pre>%s(mon) %02d(dd) %02d(hh);%02d(mm);%02d(ss) zscaler-nss CEF-0;zscaler NSSWeblog 5.0 %{action} %{reason} %{act}-%{action} app=%{proto} cat=%{urlcat} dhost=%{host} ost=%{dst}-%{sp} src=%{cip} ln=%{drespcat} outcome=%{res} (rescode) out=%{id}(%{res}) request=%{eurl} rt=%{mon} %02d(dd) %02d(hh);%02d(mm);%02d(ss) sourceTranslatedAddress=%{cintp} requestClientApplication=%{ua} requestMethod=%{method} user=%{login} sprv=%{location} externalId=%{recordid} fileType=%{filetype} reason=%{reason} destinationServiceName=%{appname} cn=%{d(riskscore)} c1Label=riskscore c1=%{dept} c1Label=dept c2=%{urlsupercat} c2Label=urlsupercat c3=%{appCategory} c3Label=appCategory c4=%{malwarecat} c4Label=malwarecat c5=%{threatname} c5Label=threatname c6=%{d(peng)} c6Label=d(peng) ZscalerNSSWeblogURLClass=%{urlclass} ZscalerNSSWeblogDLPDictionary=%{d(dic)} requestContext=%{refer}ln</pre>	Duplicate Logs: Disabled User Obfuscation: Disabled Timezone: GMT SIEM Rate: Unlimited

Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | [Patents](#)

Help

Slide notes

Then Activate your changes.

Slide 118 - Slide 118

The screenshot shows the Zscaler Activation interface with the following details:

- Left Sidebar:** Includes icons for Dashboard, Analytics, Policy, Administration, Activation (selected), and Search.
- Top Bar:** Shows "MY ACTIVATION STATUS" and "CURRENTLY EDITING (1)" with the URL "admin/training@zsclearn.com". A message box says "All changes have been saved."
- Central Area:**
 - NSS Feed:** Contains sections for "Log Filter" (set to "Alerts Critical, Warn"), "Feed Output Format" (set to "..."), and "Feed Attributes" (set to "Duplicate Logs: Disabled, Timezone: GMT, SIEM Rate: Unlimited").
 - Logs:** Displays a log entry with a long JSON-like payload. The payload includes fields like `mon`, `dd`, `hh`, `mm`, `ss`, `action`, `proto`, `cat`, `dhost`, `respcode`, `out`, `reqsize`, `request`, `url`, `r`, `mon`, `dd`, `ly`, `dh`, `jm`, `sourceTranlatedAddress`, `cmtip`, `requestClientApplication`, `ua`, `requestMethod`, `user`, `login`, `spiv`, `location`, `externalId`, `recordid`, `fileType`, `reason`, `reasonCode`, `appname`, `cn1Label`, `riskScore`, `cs1Label`, `dept`, `cs2Label`, `urlSuperCat`, `cs3Label`, `apClass`, `malwareCat`, `treatName`, `dipeng`, `dipen`, `ZscalerNSSWeblogURLClass`, `uriclass`, `ZscalerNSSWeblogDLPDictionary`, and `requestContext`.
- Bottom:** Copyright information: "Copyright©2007-2019 Zscaler Inc. All rights reserved. | Version 5.7 | Patents". A "Help" button is also present.

Slide notes

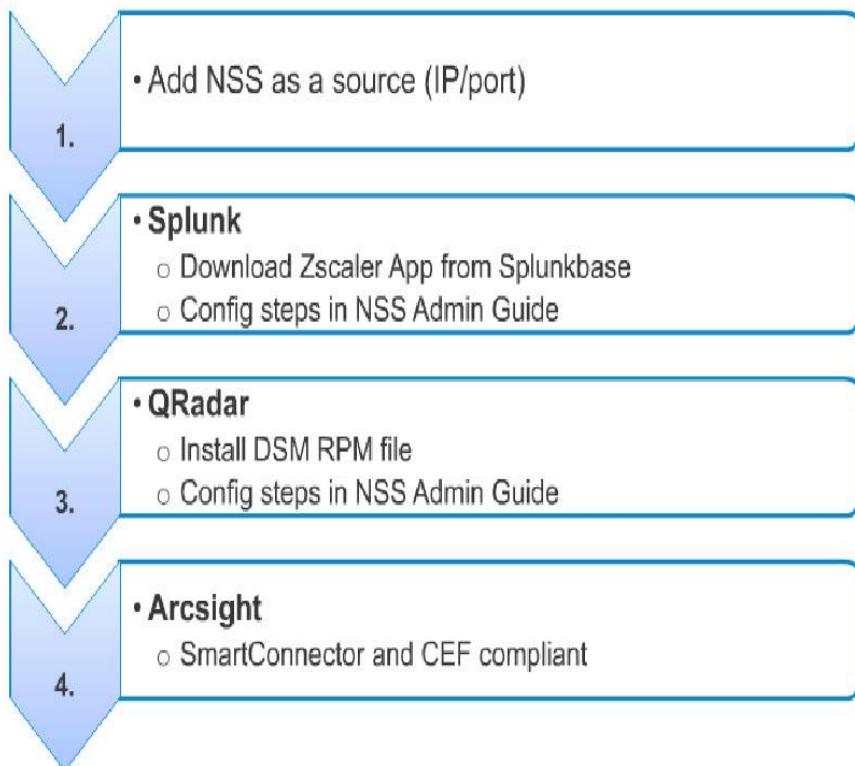


Configuring Your SIEM

Slide notes



Configuring Your SIEM



Slide notes

The last step is to configure your SIEM to accept logs from the NSS VM. There are config steps for a few SIEMs here and in the NSS Guide. If you're using a different SIEM you should follow your SIEM's documentation.



Thank You and Quiz

Slide notes

This completes the Zscaler Nanolog Streaming Service module. We hope this module has been useful to you and thank you for your time. What will follow is a short quiz to test your knowledge of the material presented in this module. You may retake the quiz as many times as necessary to pass.