Citrix NetScaler Virtual Appliance

Integration Guide

gemalto
security to be free

All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any publicly accessible network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-013602-001, Rev. A

Release Date: August 2016

Contents

Preface

This document covers the necessary information to install, configure, and integrate Citrix NetScaler Virtual Appliance with SafeNet Luna Hardware Security Module.

Scope

This document provides the necessary steps to install, configure, and integrate Citrix NetScaler Virtual Appliance with SafeNet Luna Hardware Security Module. A SafeNet network HSM is designed to protect critical cryptographic keys and to accelerate sensitive cryptographic operations across a wide range of security applications.

Gemalto Rebranding

In early 2015, Gemalto completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the Luna name has been removed from the SafeNet HSM product line, with the SafeNet name being retained. As a result, the product names for SafeNet HSMs have changed as follows:

Old product name	New product name
Luna SA HSM	SafeNet Network HSM
Luna PCI-E HSM	SafeNet PCI-E HSM
Luna G5 HSM	SafeNet USB HSM
Luna Client	SafeNet HSM Client

NOTE: These branding changes apply to the documentation only. The SafeNet HSM software and utilities continue to use the old names.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION: Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

WARNING: Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following: • Command-line commands and options (Type **dir /p**.) • Button names (Click **Save As**.) • Check box and radio button names (Select the **Print Duplex** check box.) • Window titles (On the **Protect Document** window, click **Yes**.) • Field names (**User Name:** Enter the name of the user.) • Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) • User input (In the **Date** box, type **April 1**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
`Consolas`	Denotes syntax, prompts, and code examples.

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1
Introduction

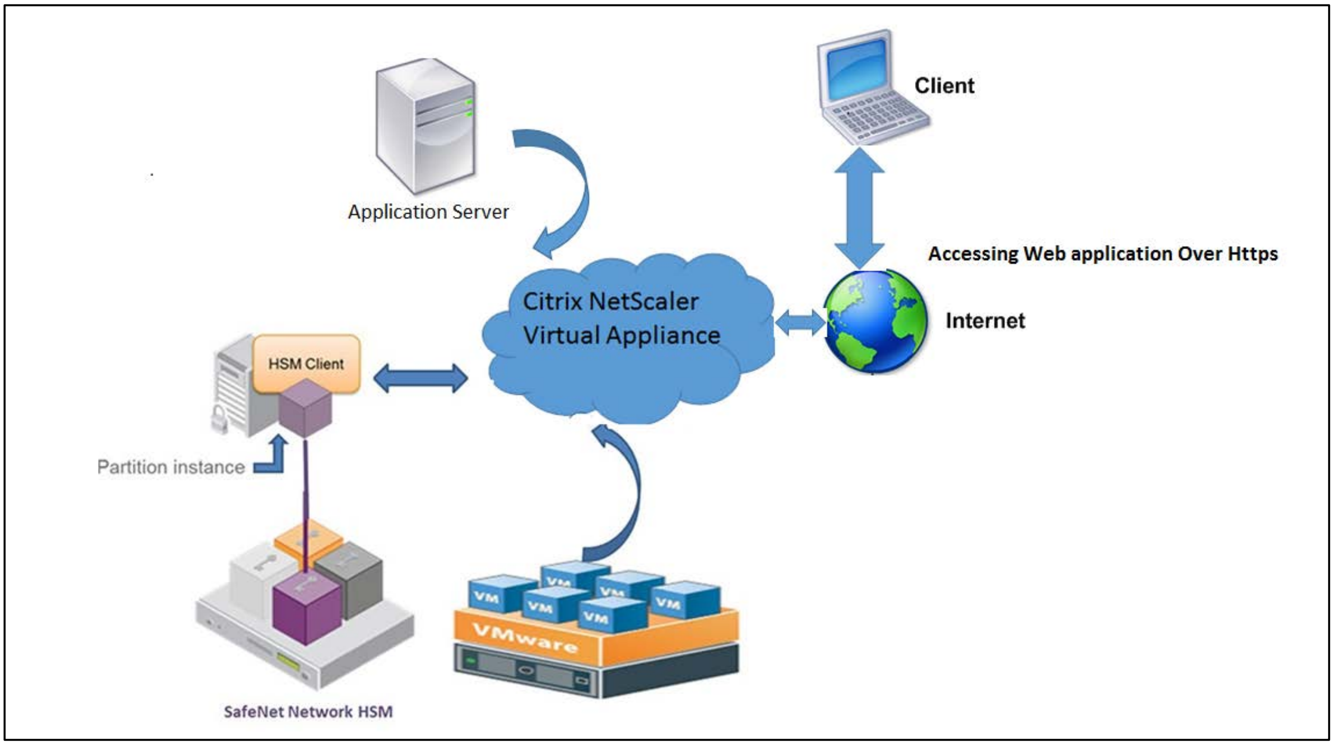
Overview

A non-FIPS NetScaler appliance stores the server's private key on the hard disk. On a FIPS appliance, the key is stored in a cryptographic module known as a hardware security module (HSM). Storing a key in the HSM protects it from physical and software attacks. In addition, the keys are encrypted with special FIPS approved ciphers.

Only the NetScaler MPX 9700/10500/12500/15500 FIPS appliances support a FIPS card. Support for FIPS is not available on other MPX appliances, or on the SDX and VPX appliances. This limitation is addressed by supporting a SafeNet network HSM on all NetScaler MPX, SDX, and VPX appliances except the MPX 9700/10500/12500/15500 FIPS appliances.

A SafeNet Network HSM is designed to protect critical cryptographic keys and to accelerate sensitive cryptographic operations across a wide range of security applications.

This Integration guide outlines the integration steps for Citrix VPX appliances, but the same integration steps are supported on the MPX and SDX appliances noted previously.



3rd party Application Details

- Citrix NetScaler Virtual Appliance

NOTE: You require a VPX Citrix License for Load Balancing feature.

Supported Platforms

Third Party Details	SafeNet Appliance version	Firmware Version
Citrix NetScaler Virtual Appliance(11.1-47.14_nc)	Appliance Version-5.4.7-1	6.10.9

NOTE: SafeNet Luna Client 6.0.0 provided with Citrix build does not work in HA mode with Citrix Virtual Appliance.

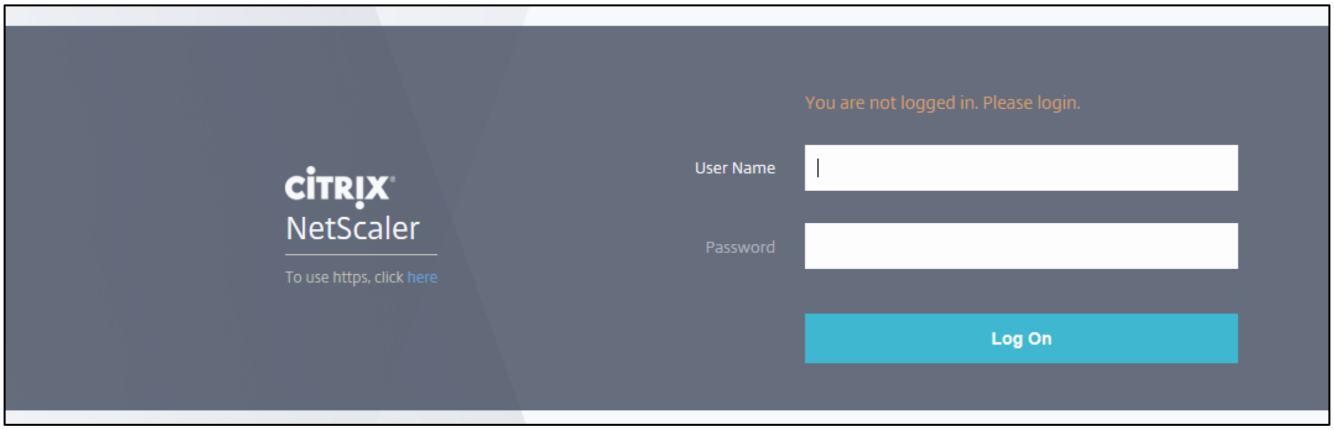
NOTE: This integration has been also tested using two Citrix NetScaler Virtual appliances in HA mode with SafeNet Luna HSM.

Citrix NetScaler Virtual Appliance Setup

Use the appropriate virtual image file to deploy the virtual appliance on the VMware.

When your virtual appliance is on a VMware, perform the following steps:

- Access the Citrix NetScaler WebGUI through the IP address that was configured during deployment. For example: <http://IP-Address>



You are not logged in. Please login.

Prerequisites

Refer to the SafeNet Network HSM documentation for installation steps and details regarding configuring and setting up the box. Before you get started, ensure the following:

- SafeNet Network HSM appliance and a secure admin password.
- SafeNet Network HSM, and a hostname, suitable for your network.
- SafeNet Network HSM parameters are set to work with your network.
- Initialize the SafeNet Network HSM appliance.
- Copy the corresponding NetScaler build (build-11.1-47.14_nc.tgz) on the NetScaler Virtual Appliance.
- Untar the build and execute the installns script (./installns)

  This build installs the SafeNet client setup and directory structure. (`/var/safenet/safenet/lunaclient/bin/`)
- When you load the NetScaler build by using the installns script, the safenet_dirs.tar file is copied into the /var/ directory. If no“/var/safenet/” directory is present, the installns script creates a “safenet” directory in the /var/ directory.
- Configure the NTLS between SafeNet Luna HSM client and HSM.After the “/var/safenet/” directory is created, perform the following tasks:

  a. Change directory to /var/safenet/config/ and run the “safenet_config” script. At the shell prompt, type:

     ```
     cd /var/safenet/config
     sh safenet_config
     ```

     This script copies the “Chrystoki.conf” file into the /etc/ directory. It also generates a symbolic link “libCryptoki2_64.so” in the “/usr/lib/” directory.
- Create and transfer a certificate and key between the SafeNet Luna HSM Client and the SafeNet HSM. In order to communicate securely, the Client and the HSM must exchange certificates. Create a certificate and key on the SafeNet HSM Client and then transfer it to the HSM. Copy the HSM certificate to the Client.

  a. Change directory to /var/safenet/safenet/lunaclient/bin.

     ```
     ./vtl createCert –n <ip address of NetScaler>
     ```

b. Copy the certificate to the HSM. At the shell prompt, type:

```
scp /var/safenet/safenet/lunaclient/cert/client/<ip address of NS>.pem <SafeNet_HSM
account>@<IP address of SafeNet HSM>
```

c. Copy the certificate and key from the HSM to the NetScaler

```
scp <HSM account>@<HSM IP>:server.pem /var/safenet/safenet/lunaclient/server_<HSM ip>.pem
```

d. Register the NetScaler ADC on the SafeNet HSM.

```
client register –client <client name> -ip <netscaler ip>
```

e. Assign the client a partition from the partition list.

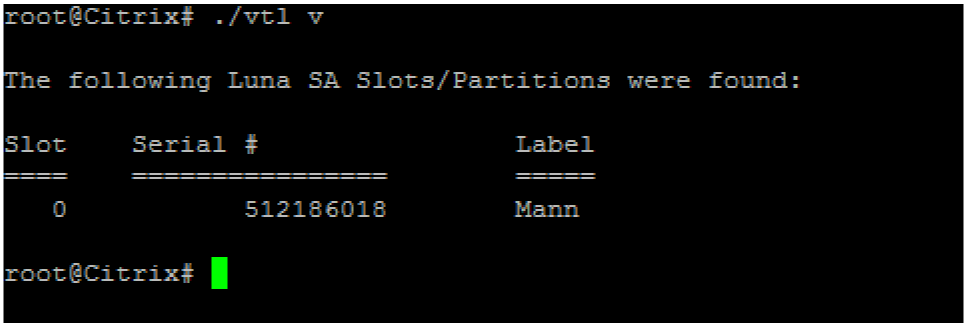
```
client assignPartition –client <Client Name> -par <Partition Name>
```

f. Register the HSM with its certificate on the SafeNet Luna Client.

```
./vtl addserver –n <IP addr of HSM> -c /var/safenet/safenet/lunaclient/server_<HSM_IP>.pem
```

g. Verify the network trust links (NTLS) connectivity between the Client and HSM. At the shell prompt, type:

```
./vtl verify
```



```
root@Citrix# ./vtl v

The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
   0           512186018        Mann

root@Citrix#
```

- Save the configuration.

  ```
  cp /etc/Chrystoki.conf /var/safenet/config/
  ```

  The above steps update the “/etc/Chrystoki.conf” configuration file. This file is deleted when the ADC is started. Copy the configuration to the default configuration file, which is used when an ADC is restarted.

- Configure automatic start of the gateway daemon at boot time.

  ```
  touch /var/safenet/safenet_is_enrolled
  ```

2 Integrating Citrix NetScaler Virtual Appliance with SafeNet Network HSM

Configure SafeNet Network HSM with Citrix NetScaler

Perform the following steps to integrate SafeNet Network HSM with Citrix NetScaler:

- Generate a key pair using third party.
- Add Key and Certificate on Citrix NetScaler.
- Create a Load Balancing Virtual Server and Service.

Generate Key on SafeNet Network HSM

Before creating a key on HSM, ensure you have already established the NTLS connection with SafeNet Network HSM.

Traverse to the Luna Client installation directory Path (`/var/safenet/safenet/lunaclient/bin/`) and execute the following command using Certificate Management utility:

1. Generate the key pair using the below commands.

   ```
   ./cmu gen -modulusBits=2048 -publicExponent=65537 -sign=T -verify=T -encrypt=1 -decrypt=1 –wrap=1 –unwrap=1 –label=Citrix_Keys
   ```

2. Cmu list to list the generated key pair.

   ```
   ./cmu list

   Please enter password for token in slot 0 : ********

   handle=31       label=Citrix_Keys

   handle=28       label=Citrix_Keys
   ```

3. Generate a certificate request.

   ```
   ./cmu requestcertificate
   ```

   Enter the handle id for which request needs to be generated and certificate request details.

   Certificate Request file is by default saved in `/var/safenet/safenet/lunaclient/bin/`. Get the Signed certificate from the trusted CA and copy the certificate in this directory /var/safenet/safenet/lunaclient/bin/

4. Import the certificate.

   ```
   ./cmu import
   ```

   Enter the Certificate input file name.

5. Export the Certificate in .pem format using CMU.

   ```
   ./cmu export
   ```

   Enter the output file name (For Example Citrix.pem)

6. Copy the certificate to the /nsconfig/ssl/ directory on the ADC

   ```
   cp <cert.pem> /nsconfig/ssl/
   ```

Add Key and Certificate on Citrix NetScaler

1. Add an HSM key on the ADC. At the command prompt, type:

   ```
   add ssl hsmkey <KeyName> -hsmType SAFENET –serialNum <serial number of partition> -password
   <Partition_password>
   ```

2. Add a certificate-key pair on the ADC

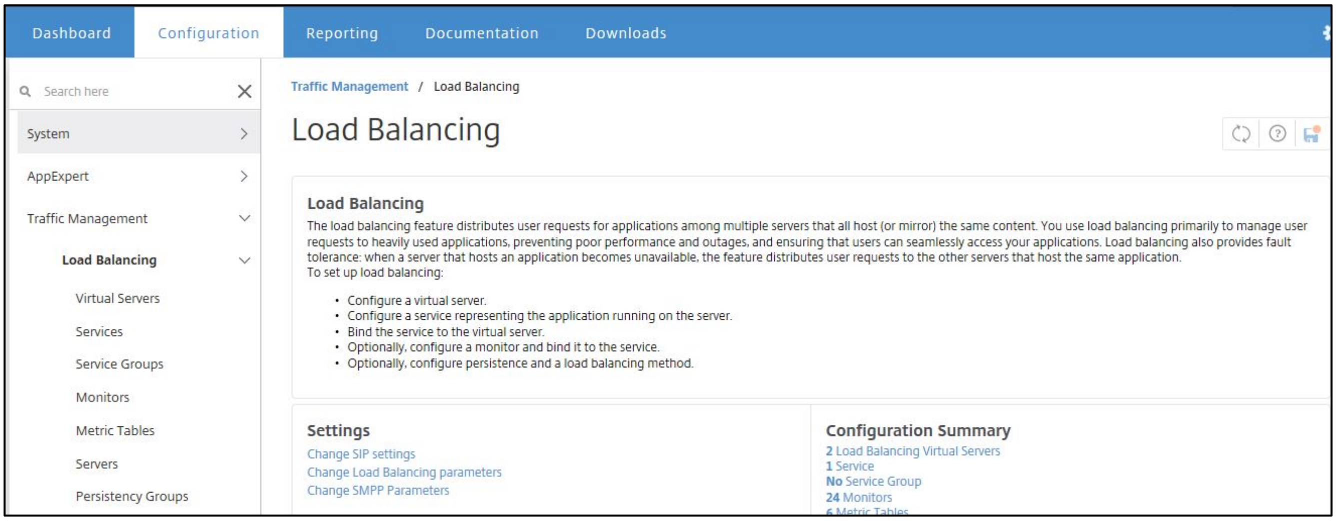
   ```
   add ssl certkey <CertkeyName> -cert <cert name> -hsmkey <KeyName>
   ```

Load Balancing Virtual Server and Service on NetScaler

We have deployed IBM WebSphere and used the snoop application to test the integration.

Add the details of the Server machine in NetScaler on which IBM WebSphere application server is running and sample application is deployed

1. Traverse to **Traffic Management**->**Load Balancing**->**Servers**



Load Balancing

Load Balancing

The load balancing feature distributes user requests for applications among multiple servers that all host (or mirror) the same content. You use load balancing primarily to manage user requests to heavily used applications, preventing poor performance and outages, and ensuring that users can seamlessly access your applications. Load balancing also provides fault tolerance: when a server that hosts an application becomes unavailable, the feature distributes user requests to the other servers that host the same application.
To set up load balancing:

- Configure a virtual server.
- Configure a service representing the application running on the server.
- Bind the service to the virtual server.
- Optionally, configure a monitor and bind it to the service.
- Optionally, configure persistence and a load balancing method.

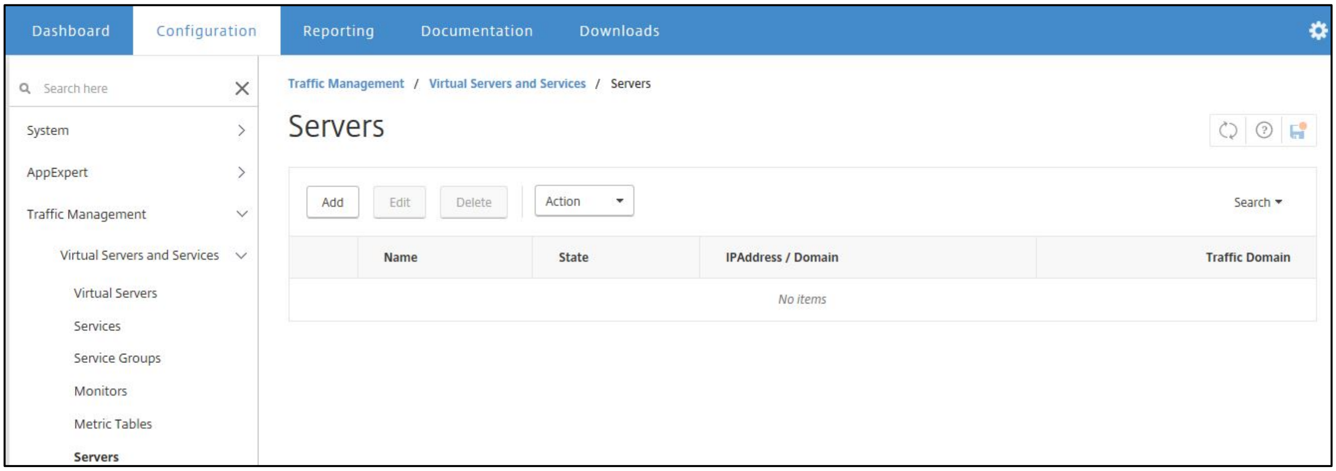
Settings

Change SIP settings
Change Load Balancing parameters
Change SMPP Parameters

Configuration Summary

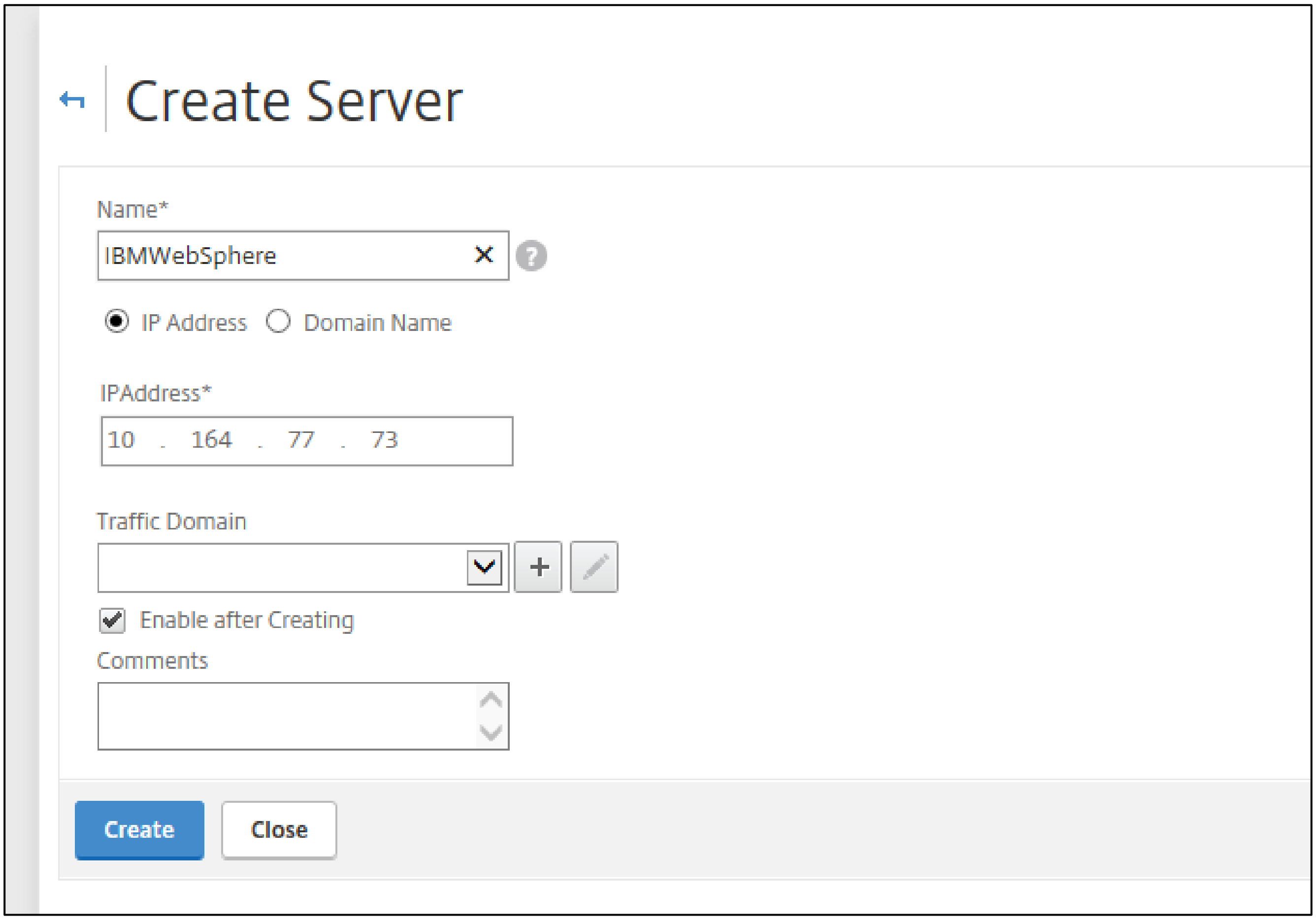
2 Load Balancing Virtual Servers
1 Service
No Service Group
24 Monitors
6 Metric Tables

2. Click **Add** to add the Details of the application server.



	Name	State	IPAddress / Domain	Traffic Domain
		No items		

3. Click **Create** to add the server. The added server displays in the list.



Create Server

Name*: IBMWebSphere

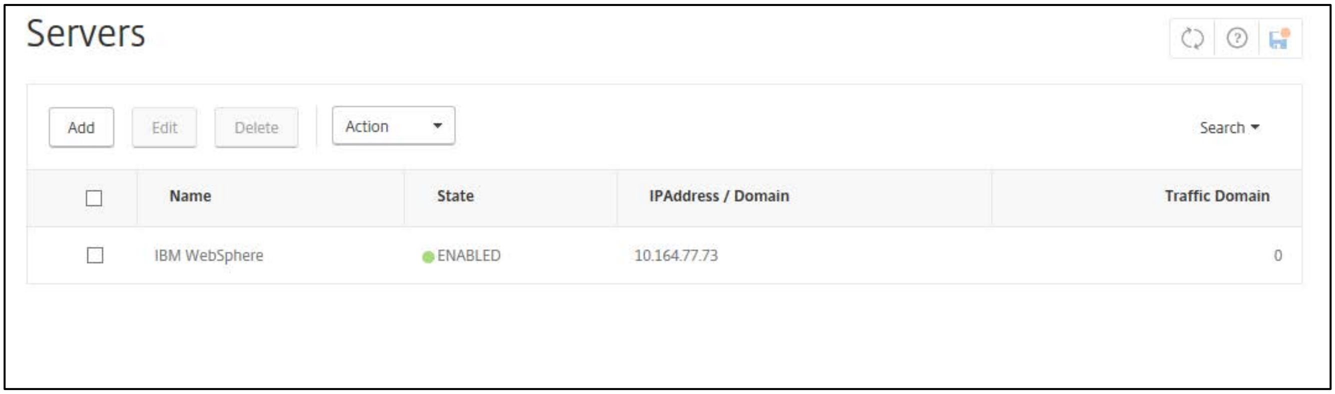
● IP Address ○ Domain Name

IPAddress*: 10 . 164 . 77 . 73

Traffic Domain:

☑ Enable after Creating

Comments:



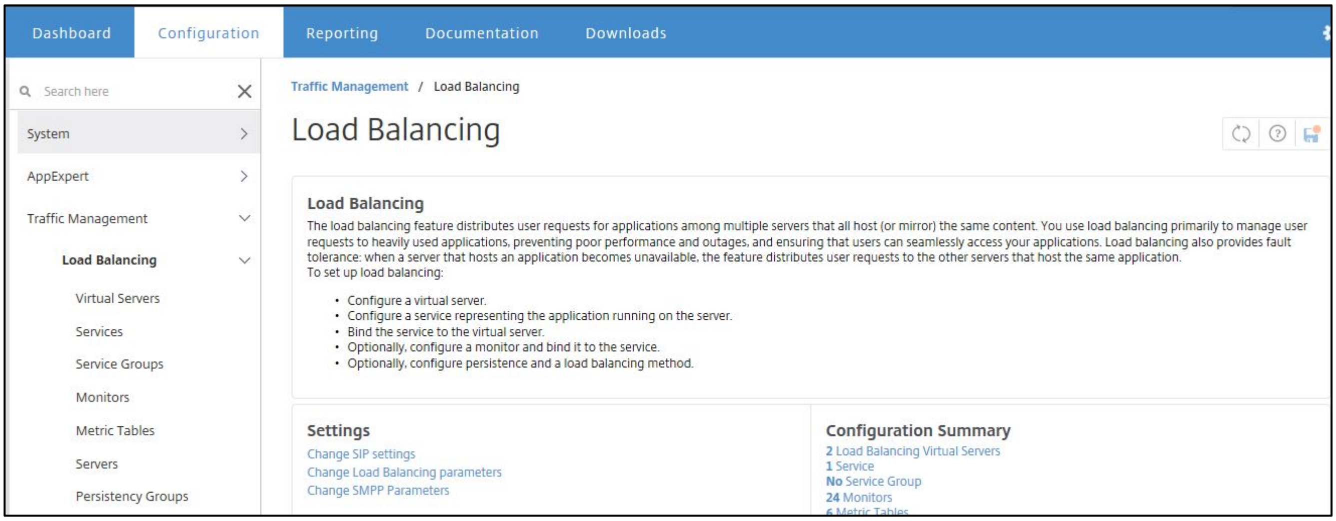
Servers

□	Name	State	IPAddress / Domain	Traffic Domain
□	IBM WebSphere	● ENABLED	10.164.77.73	0

Add Service

Open the NetScaler GUI using the IP Address For example < http://10.164.74.121>

1. Traverse to **Traffic Management**->**Load Balancing**->**Services**



Load Balancing

Load Balancing

The load balancing feature distributes user requests for applications among multiple servers that all host (or mirror) the same content. You use load balancing primarily to manage user requests to heavily used applications, preventing poor performance and outages, and ensuring that users can seamlessly access your applications. Load balancing also provides fault tolerance: when a server that hosts an application becomes unavailable, the feature distributes user requests to the other servers that host the same application.
To set up load balancing:

- Configure a virtual server.
- Configure a service representing the application running on the server.
- Bind the service to the virtual server.
- Optionally, configure a monitor and bind it to the service.
- Optionally, configure persistence and a load balancing method.

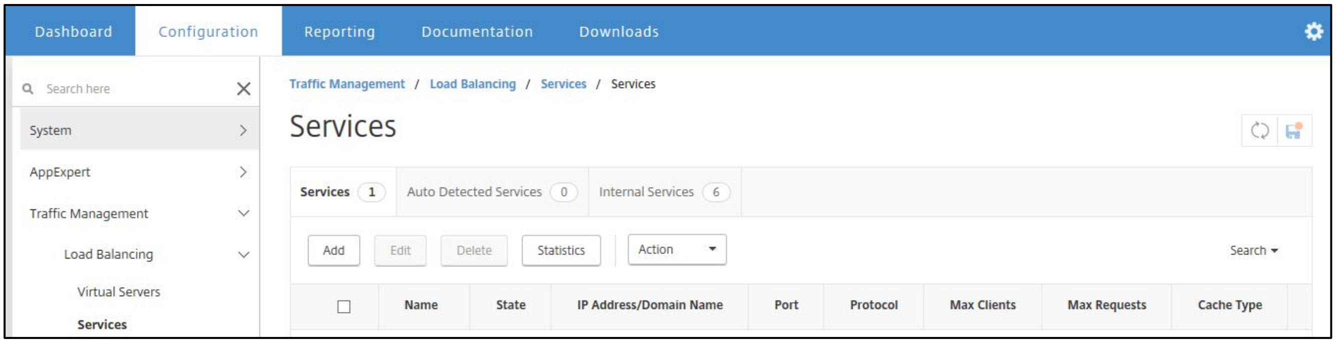
Settings

Change SIP settings
Change Load Balancing parameters
Change SMPP Parameters

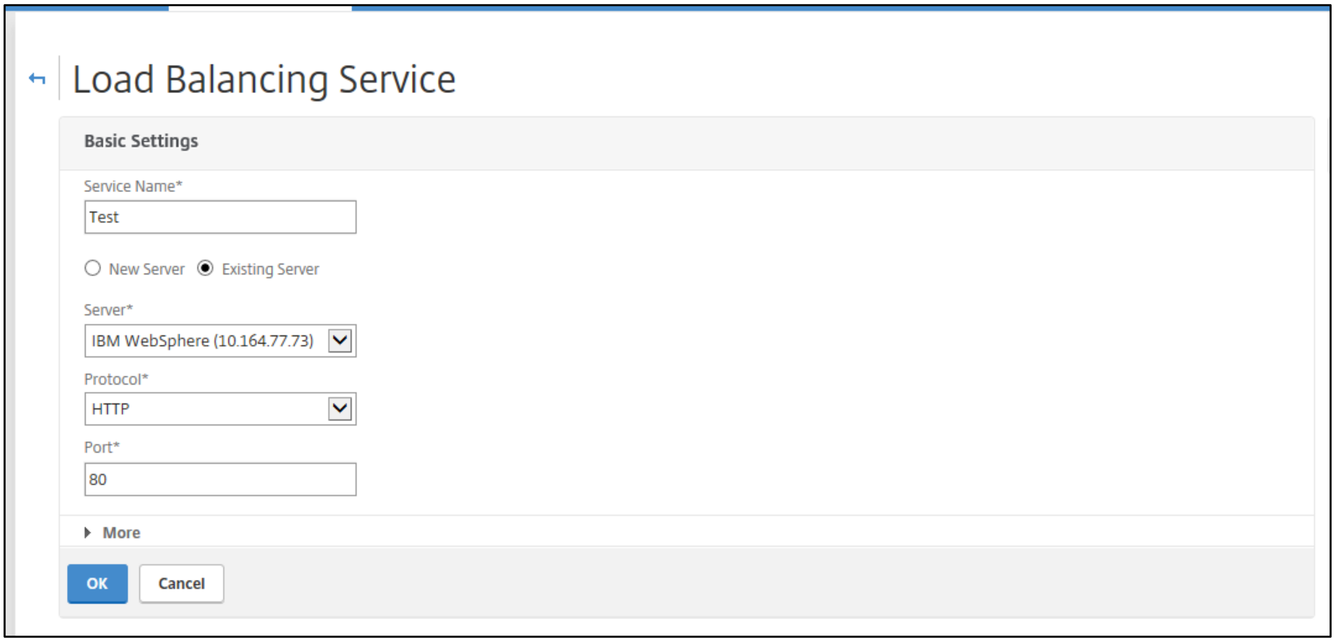
Configuration Summary

2 Load Balancing Virtual Servers
1 Service
No Service Group
24 Monitors
6 Metric Tables

2. Click **Add** to add the services.



3. Click **OK** to add the service.



Load Balancing Service

Basic Settings

Service Name*: Test

○ New Server ● Existing Server

Server*: IBM WebSphere (10.164.77.73)

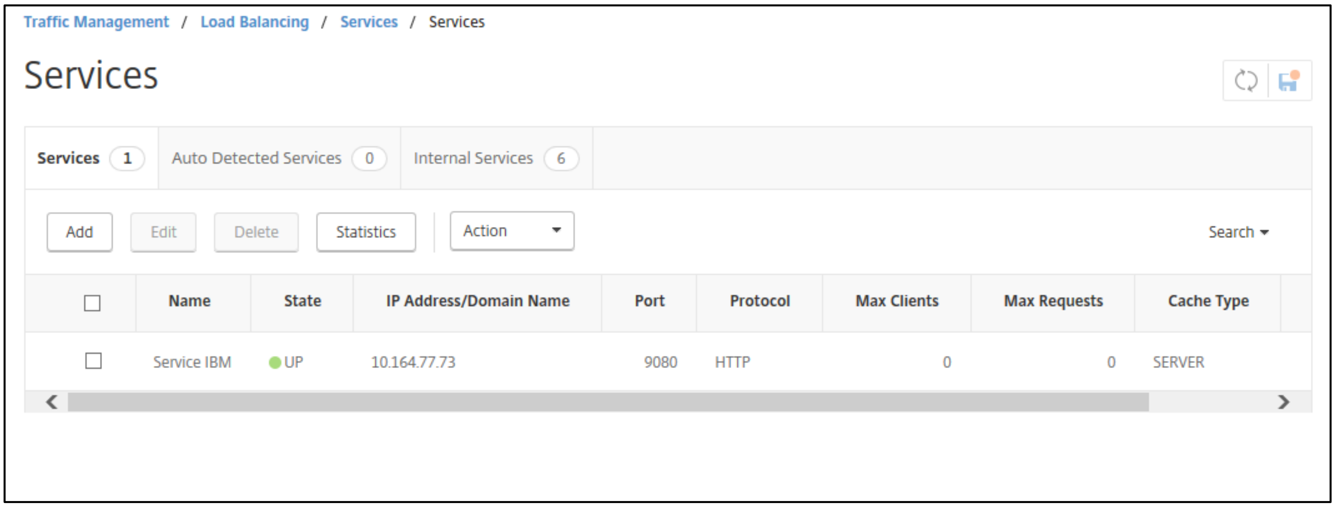
Protocol*: HTTP

Port*: 80

We have deployed IBM WebSphere and used the snoop application to test the integration.

In the server field add the IP of the machine where your application is already running. Select the Protocol and port as shown in Screen shot.

4. The Services page displays. The State of the Service should be **UP**.



Traffic Management / Load Balancing / Services / Services

Services

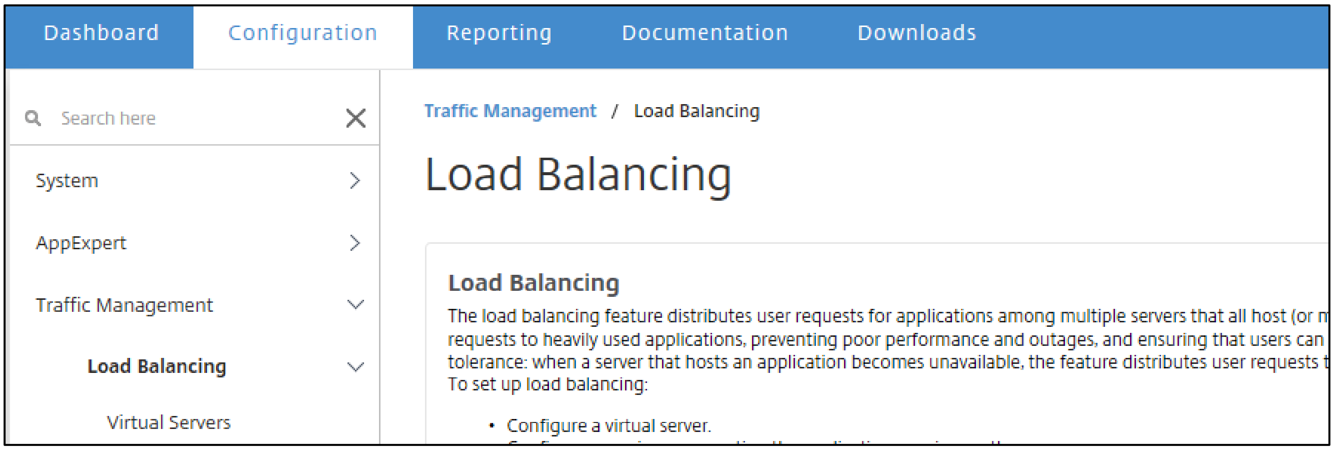
Services 1 | Auto Detected Services 0 | Internal Services 6

□	Name	State	IP Address/Domain Name	Port	Protocol	Max Clients	Max Requests	Cache Type
□	Service IBM	● UP	10.164.77.73	9080	HTTP	0	0	SERVER

Virtual Server

Open the NetScaler GUI using the IP Address < http://10.164.74.121>

1. Traverse to **Traffic Management**->**Load Balancing**->**Virtual Servers**

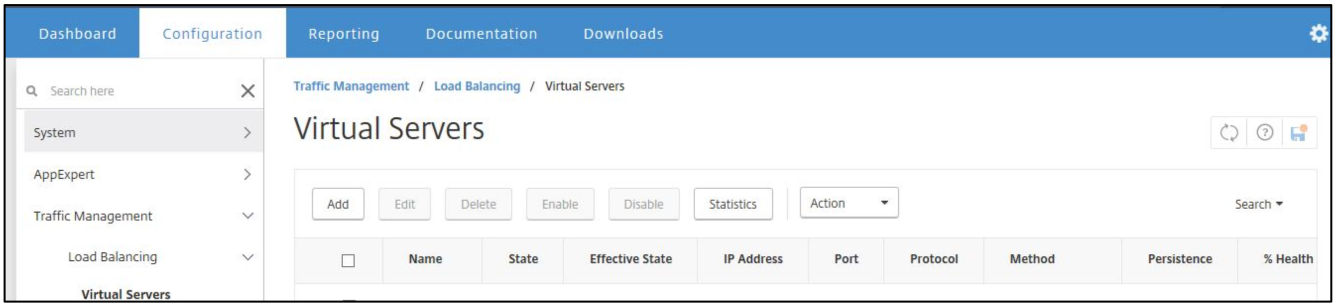


Load Balancing

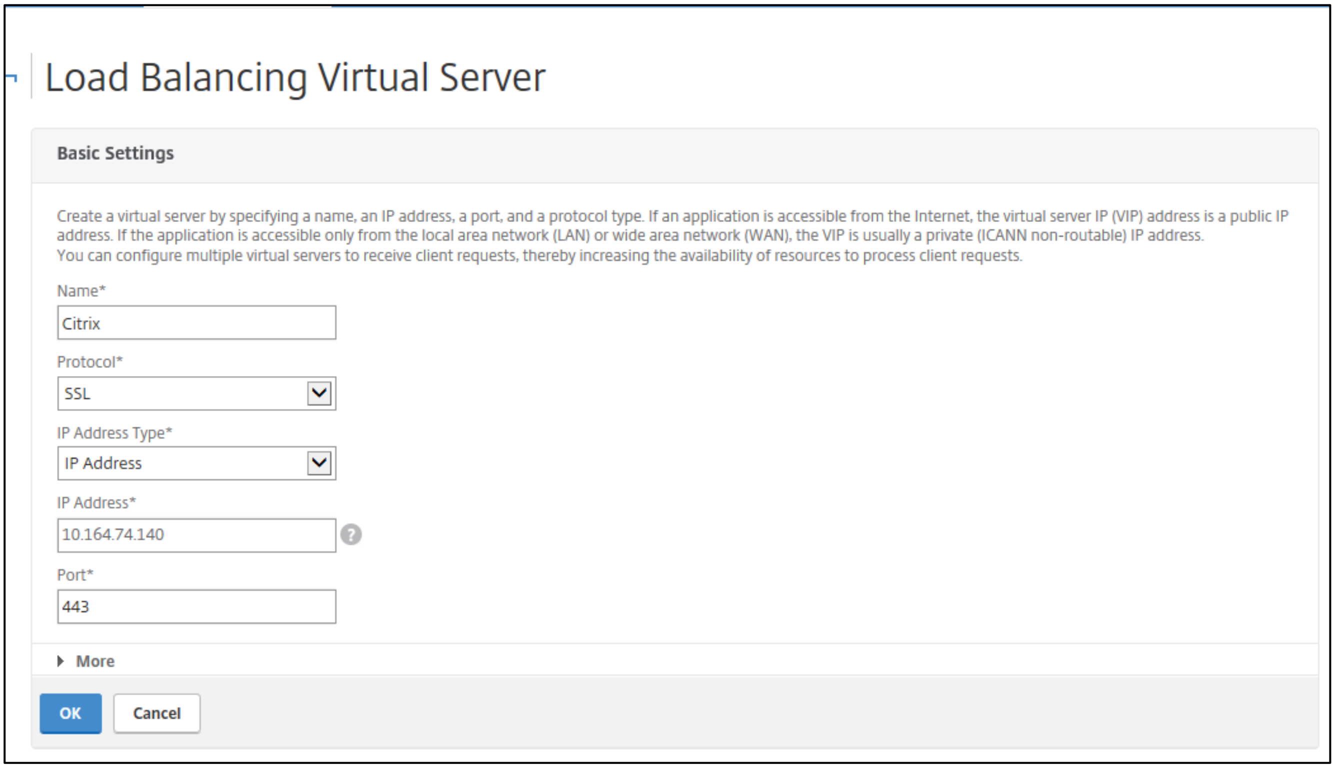
The load balancing feature distributes user requests for applications among multiple servers that all host (or m
requests to heavily used applications, preventing poor performance and outages, and ensuring that users can
tolerance: when a server that hosts an application becomes unavailable, the feature distributes user requests t
To set up load balancing:

- Configure a virtual server.

2. Click **Add**.



3. Enter the details of the Virtual Server. Select the Protocol as SSL and then click **OK**.



Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address.
You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name* Citrix

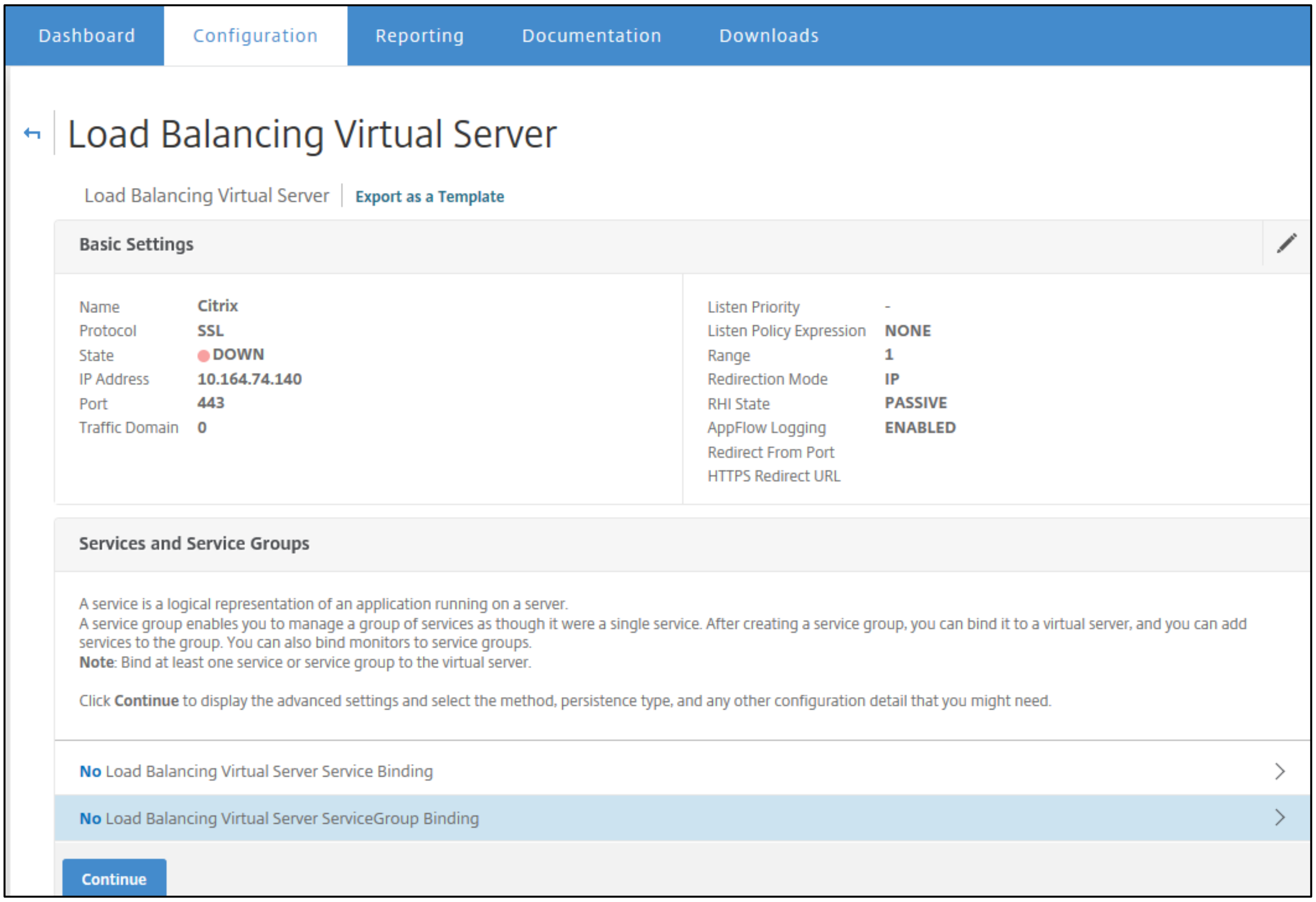
Protocol* SSL

IP Address Type* IP Address

IP Address* 10.164.74.140

Port* 443

4. The Virtual Server should be created in list with State as Down. Click **No Load Balancing Virtual Service Binding**.



Load Balancing Virtual Server

Load Balancing Virtual Server | Export as a Template

Basic Settings

Name	Citrix	Listen Priority	-
Protocol	SSL	Listen Policy Expression	NONE
State	● DOWN	Range	1
IP Address	10.164.74.140	Redirection Mode	IP
Port	443	RHI State	PASSIVE
Traffic Domain	0	AppFlow Logging	ENABLED
		Redirect From Port	
		HTTPS Redirect URL	

Services and Service Groups

A service is a logical representation of an application running on a server.
A service group enables you to manage a group of services as though it were a single service. After creating a service group, you can bind it to a virtual server, and you can add services to the group. You can also bind monitors to service groups.
Note: Bind at least one service or service group to the virtual server.

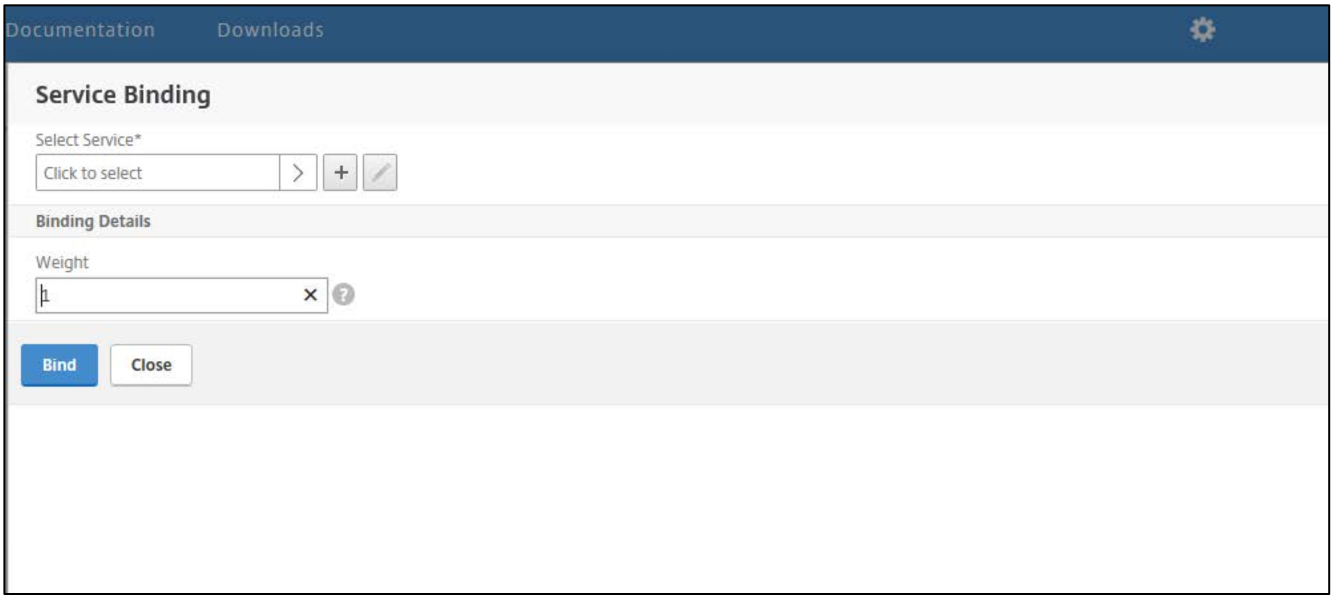
Click **Continue** to display the advanced settings and select the method, persistence type, and any other configuration detail that you might need.

No Load Balancing Virtual Server Service Binding

No Load Balancing Virtual Server ServiceGroup Binding

5. The Service Binding page displays.

   Click **select service** and select the service created above. Click the **Bind** button.



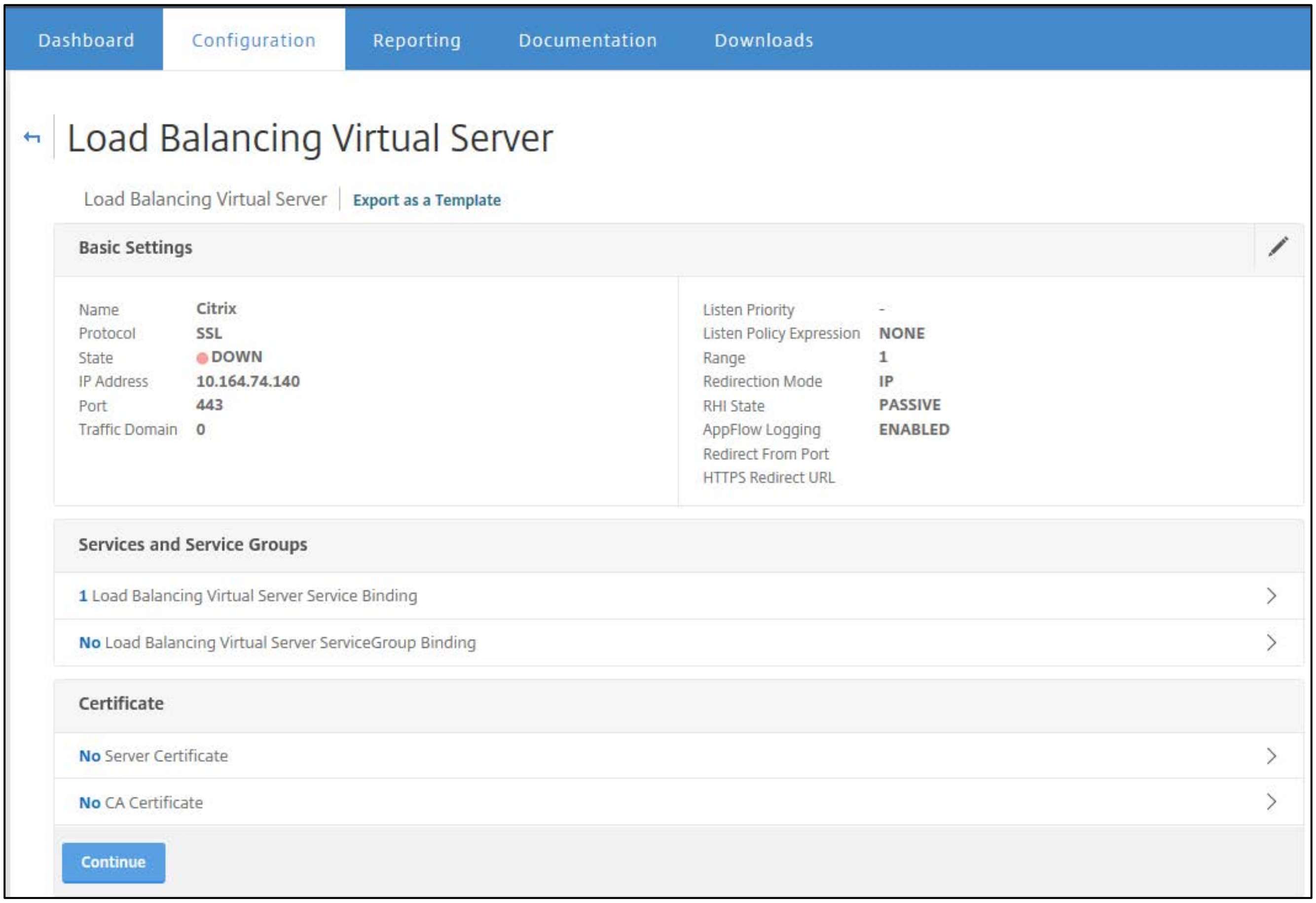
Service Binding

Select Service*: Click to select

Binding Details

Weight: 1

6. After service binding, click **Continue**.
7. Click **No Server Certificate**.



Load Balancing Virtual Server

Load Balancing Virtual Server | Export as a Template

Basic Settings

Name	Citrix	Listen Priority	-
Protocol	SSL	Listen Policy Expression	NONE
State	● DOWN	Range	1
IP Address	10.164.74.140	Redirection Mode	IP
Port	443	RHI State	PASSIVE
Traffic Domain	0	AppFlow Logging	ENABLED
		Redirect From Port	
		HTTPS Redirect URL	

Services and Service Groups

1 Load Balancing Virtual Server Service Binding

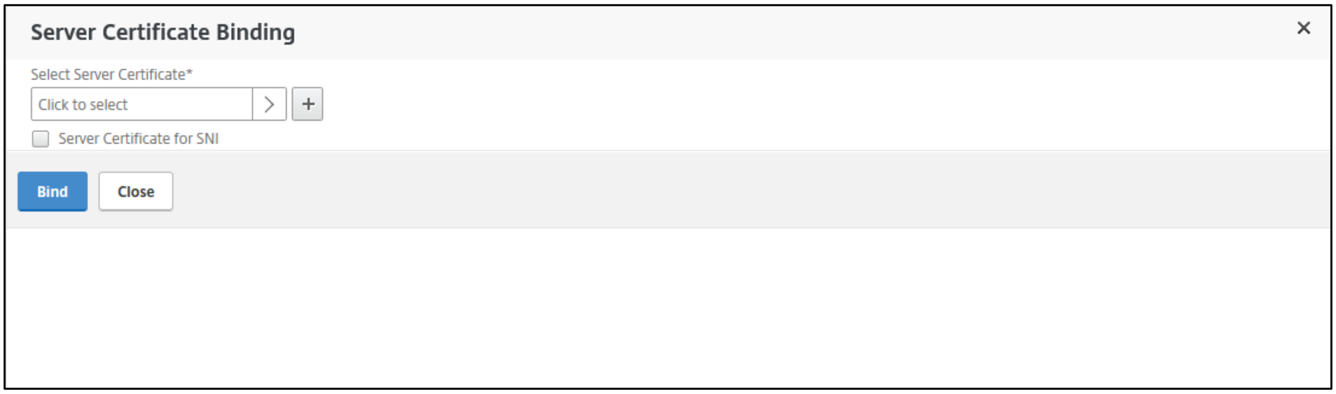
No Load Balancing Virtual Server ServiceGroup Binding

Certificate

No Server Certificate

No CA Certificate

8. Select Server Certificate and click **Bind**.

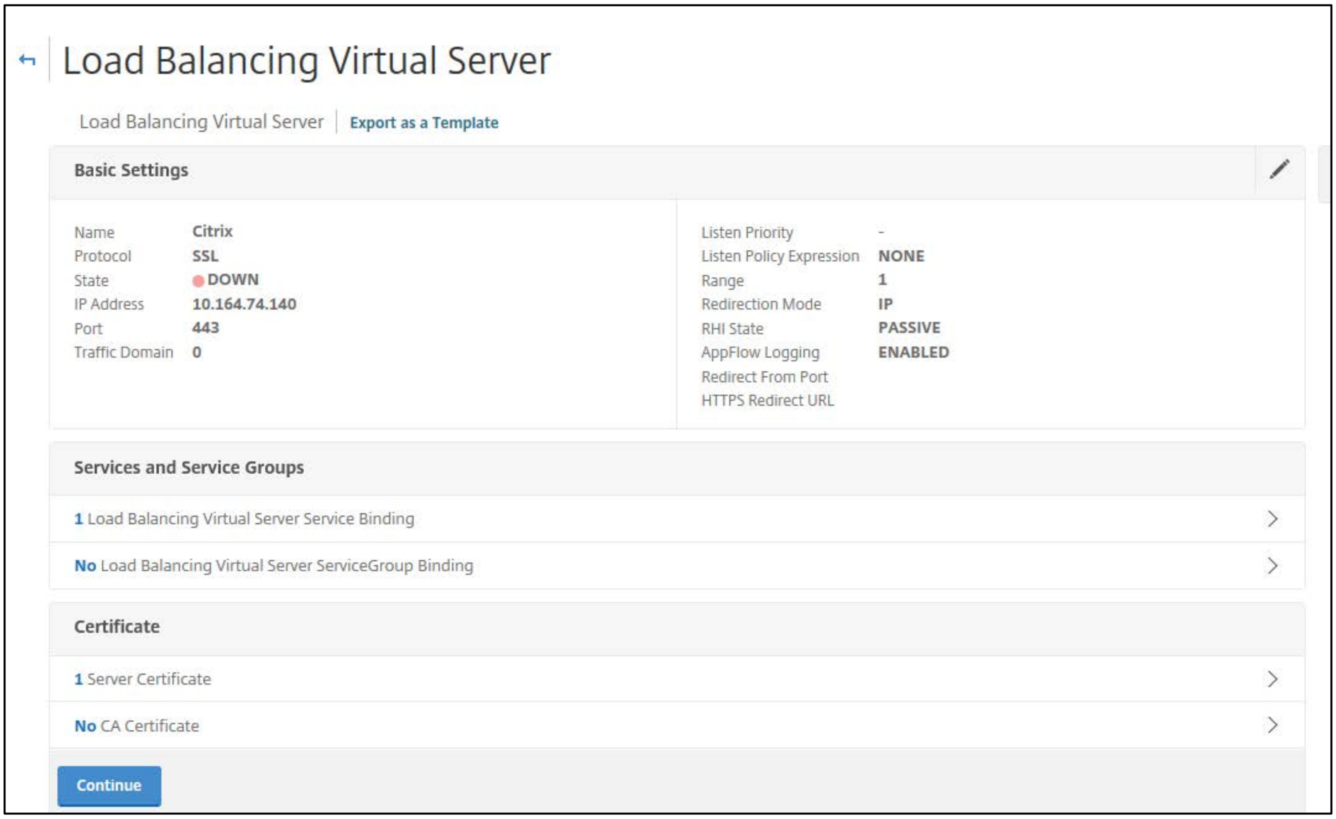


Server Certificate Binding

Select Server Certificate*

Click to select

□ Server Certificate for SNI



Load Balancing Virtual Server

Load Balancing Virtual Server | Export as a Template

Basic Settings

Name	Citrix	Listen Priority	-
Protocol	SSL	Listen Policy Expression	NONE
State	● DOWN	Range	1
IP Address	10.164.74.140	Redirection Mode	IP
Port	443	RHI State	PASSIVE
Traffic Domain	0	AppFlow Logging	ENABLED
		Redirect From Port	
		HTTPS Redirect URL	

Services and Service Groups

1 Load Balancing Virtual Server Service Binding

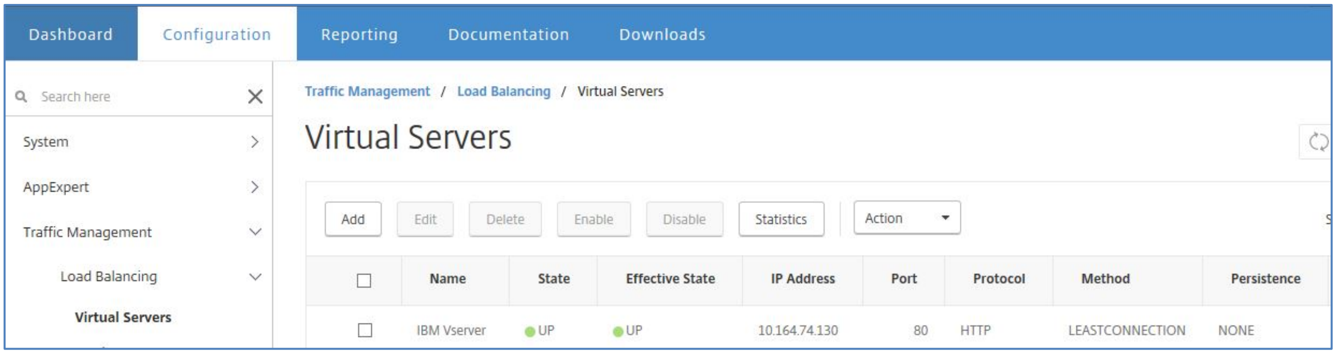
No Load Balancing Virtual Server ServiceGroup Binding

Certificate

1 Server Certificate

No CA Certificate

After Successful Binding of Certificate and service the state of Virtual Server Should be **UP**.



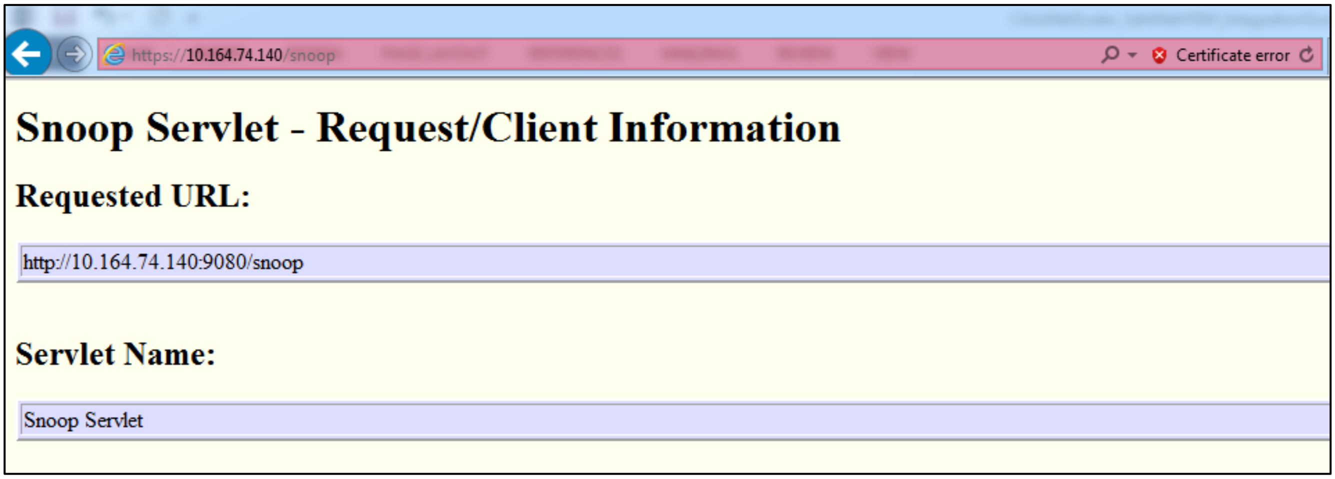
Traffic Management / Load Balancing / Virtual Servers

Virtual Servers

□	Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence
□	IBM Vserver	● UP	● UP	10.164.74.130	80	HTTP	LEASTCONNECTION	NONE

Now access the application over https using the IP of the virtual server on port 443.

For Example: https://10.164.74.140/snoop



Snoop Servlet - Request/Client Information

Requested URL:

http://10.164.74.140:9080/snoop

Servlet Name:

Snoop Servlet