THALES

Citrix ADC: Integration Guide

THALES LUNA HSM

Document Information

Document Part Number	007-013602-001
Revision	D
Release Date	22 September 2021

Trademarks, Copyrights, and Third-Party Software

CONTENTS

Overview

Citrix ADC is an application delivery controller and load balancing solution. Thales Luna HSM is used to generate and store the private keys that Citrix ADC uses for SSL communication. The benefits of integrating Citrix ADC with Luna HSM include:

- Full life cycle management of keys.
- Access to the HSM audit trail.
- Significant performance improvements by off-loading cryptographic operations from servers.

Certified Platforms

The following platforms are certified for integrating CitrixADC with Luna HSM:

Third Party Details	Luna HSM Version	Luna Firmware Version
Citrix ADC Virtual Appliance (13.0-47.24_nc)	Appliance Version- 7.3.0-165	7.3.3
Citrix ADC Virtual Appliance (13.0-41.20_nc)	Appliance Version- 7.3.0-165	7.3.0
Citrix ADC Virtual Appliance (12.1-51.19_nc)	Appliance Version- 6.3.0-1048	6.27.0
Citrix NetScaler Virtual Appliance(11.1-47.14_nc)	Appliance Version-5.4.7-1	6.10.9

Luna HSM: Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. Luna HSM on premise offerings include the Luna Network HSM, Luna PCIe HSM, and Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

Prerequisites

Before you proceed with the integration, complete the following processes:

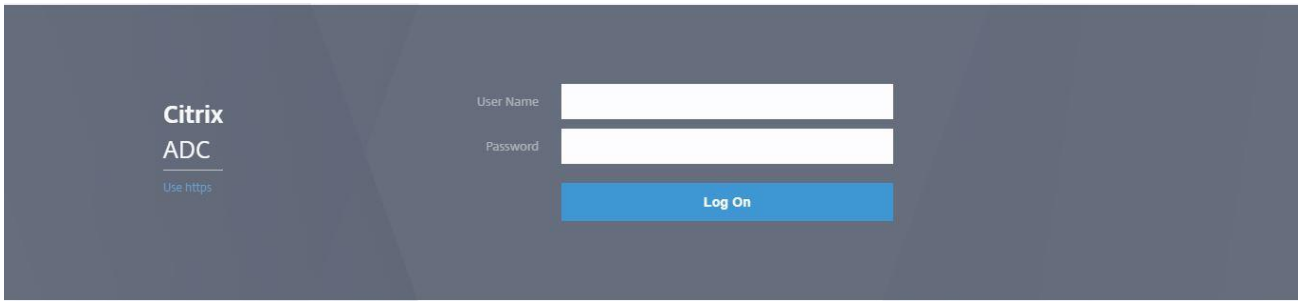
Set up Citrix ADC virtual appliance

Configure Luna HSM

Set up Citrix ADC virtual appliance

Use the appropriate virtual image file to deploy the virtual appliance on the VMware. Refer to the Citrix Product Portal and Citrix Product Documentation for further information. When your virtual appliance is available on a VMware, access the Citrix ADC Web console through the IP address that was configured during deployment. For example: `<http:/CitrixADCWebIP-Address>.`

NOTE: You require a VPX Citrix License to access the Load Balancing feature.



Configure Luna HSM

Before you get started, ensure that the HSM is configured and has an initialized partition.

NOTE: The integration guide details creating a Network Trust Link (NTL) between the Citrix ADC host environment and the Luna HSM appliance.

Integrating Citrix ADC with a Luna HSM

For integrating Citrix ADC with the Luna HSM to generate and store the Citrix ADC SSL communication private keys, complete the following steps:

> Create the NTL

> Generate a key pair and certificate on Luna HSM

> Add the key pair and certificate to Citrix ADC

> Create a test load balancing virtual server

Create the NTL

Create the Network Trust Link (NTL) between the Luna HSM and the Citrix ADC server and configure the Citrix ADC server to access the Luna HSM. To create the NTL:

NOTE: For Citrix ADC 13.x.x skip step 1 and 2 given below.

1. Copy the required Citrix ADC build containing Luna libraries (for example, build-12.1-51.19_nc_64.tgz) to the **/var** directory on the Citrix ADC Virtual Appliance.
2. Untar the build in the var directory and run the **installns** script.

   ```
   # ./installns
   ```

3. Navigate to the **/var/safenet** directory and execute the installation script.

   ```
   # ./install_client.sh -v 722
   ```

NOTE: Where 722 is the Luna client version for v7.2.2. Update the label according to your Luna client version. The Luna Client 6.0.0 provided with the Citrix build does not work in HA mode with Citrix Virtual Appliance.

4. Go to **/var/safenet/config** and run the **safenet_config** file. 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.

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

5. Create an NTL between Citrix ADC and the HSM in order to communicate securely.

   a. Change directory to **/var/safenet/safenet/lunaclient/bin** and create a certificate for Citrix ADC.

```
# ./vtl createCert -n <IP address of Citrix ADC>
```

   b. Copy the certificate to the HSM.

```
# scp /var/safenet/safenet/lunaclient/cert/client/<IP address of Citrix ADC
>.pem <HSM account>@<HSM IP>
```

   c. Copy the certificate from the HSM to the ADC.

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

   d. Register the ADC on Luna HSM.

```
# client register –client <client name> -ip <Citrix ADC IP>
```

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

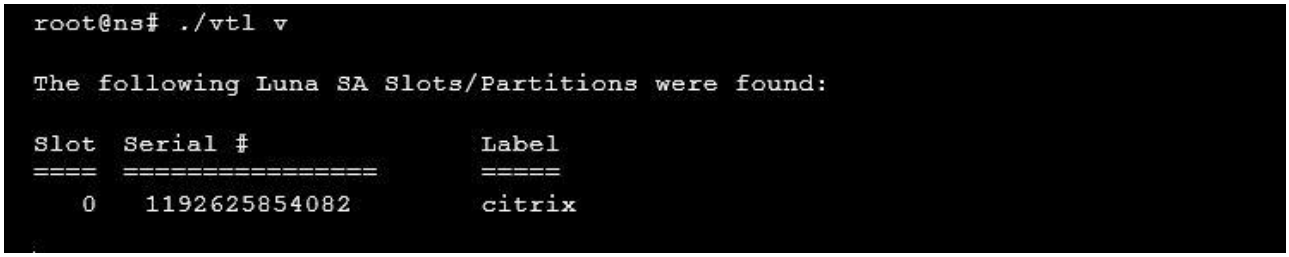
```
# client assignPartition –client <Client Name> -par <Partition Name>
```

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

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

   g. Verify the NTL connectivity between the Client and HSM. At the shell prompt, type:

```
# ./vtl verify
```



   h. Exit and log back into ADC CLI and save the configuration.

```
# save ns config
```

   i. Go back to BSD shell and copy the **/etc/Chrystoki.conf** file into the **/var/safenet/config** directory to allow the ADC to start the SafeNet Client processes automatically on reboot:

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

   j. Start the SafeNet Gateway client process:

```
# sh /var/safenet/gateway/start_safenet_gw
```

   k. Create the **/var/safenet/safenet_is_enrolled** file to signal the ADC to automatically start the SafeNet client processes after reboot:

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

l. Reboot the ADC to verify that the processes are started automatically at boot time.

```
# reboot
```

m. After reboot, verify the SafeNet Gateway client process is running:

```
# ps –aux | grep safenet_gw
```

```
root@ns# ps -aux | grep safenet_gw
root       2226  0.0  0.1 10068  1152  ??  Ss    6:45AM  0:00.00 var/safenet/gateway/safenet_gw
```

Generate a key pair and certificate on Luna HSM

Generate a key pair on the Luna HSM using the cmu utility and then create a certificate request using the keys generated. To generate a key pair and certificate:

1. Go to /var/safenet/safenet/lunaclient/bin and generate a key pair.

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

Provide partition password when prompted.

2. Run cmu list to list the generated key pair.

```
# ./cmu list
```

Provide partition password when prompted

```
root@ns# ./cmu list
Please enter password for token in slot 0 : ********
handle=188label=Citrix_Keys
handle=182label=Citrix_Keys
```

3. Generate a certificate request.

```
# ./cmu requestcertificate
```

Provide partition password when prompted

```
root@ns# ./cmu requestcertificate
Please enter password for token in slot 0 : ********
Enter Subject 2-letter Country Code (C) : In N
Enter Subject State or Province Name (S) : UP
Enter Subject Locality Name (L) : Noida
Enter Subject Organization Name (O) : Thales
Enter Subject Organization Unit Name (OU) : HSM
Enter Subject Common Name (CN) : thalesgroup.com
Enter EMAIL Address (E) : abc@def.com
Enter output filename : Citrixcert
```

The certificate request file is by default saved in /var/safenet/safenet/lunaclient/bin directory.

4. Get the signed certificate from the trusted CA and copy the certificate to the /var/safenet/safenet/lunaclient/bin directory.

5. Import the certificate.

```
# ./cmu import
```

Provide partition password when prompted.

Enter the Certificate input file name.

```
root@ns# ./cmu import
Please enter password for token in slot 0 : ********
Enter input filename : certnew.cer
```

6. Export the certificate in .pem format using cmu.

   ```
   # ./cmu export
   ```

   Provide partition password when prompted

   Enter the output file name.

```
root@ns# ./cmu export
Please enter password for token in slot 0 : ********
Enter output filename : Citrixcert.pem
```

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

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

Add the key pair and certificate to Citrix ADC

Add the newly generated keys and certificates to Citrix ADC. To add the key and certificate on Citrix ADC:

1. Add the HSM key on the Citrix ADC CLI.

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

   Ignore the error `Internal error while adding HSM key.` The key will be still added to Citrix.

2. Verify the HSM key was added successfully.

   ```
   # show run | grep –i hsm
   ```

3. Add the HSM certificate-key pair on the Citrix ADC.

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

4. Verify the certificate key-pair were added successfully.

   ```
   # show run | grep –i hsm
   ```

```
> show run | grep -i hsm
add ssl hsmKey Citrix_Keys -hsmKeyBootTime 100 -hsmType SAFENET -
serialNum 1192625854082 -password
bace4ef2487dc50ba317a95e3b71a91d9c91c20f36e4afb3042a8c713f04e774 -
encrypted -encryptmethod ENCMTHD_3
add ssl certKey Citrixcert -cert "/nsconfig/ssl/Citrixcert.pem" -hsmKey
Citrix_Keys
>
```

Creating a test load balancing virtual server

Once the keys and certificate are added to the Citrix ADC, verify it is working correctly by creating a test load balancing virtual server. For the purpose of demonstration, Microsoft IIS has been used as the backend server.

To create a load balancing virtual server, log on to `<http:/CitrixADCWebIP-Address>` and complete the following steps:

> Add servers

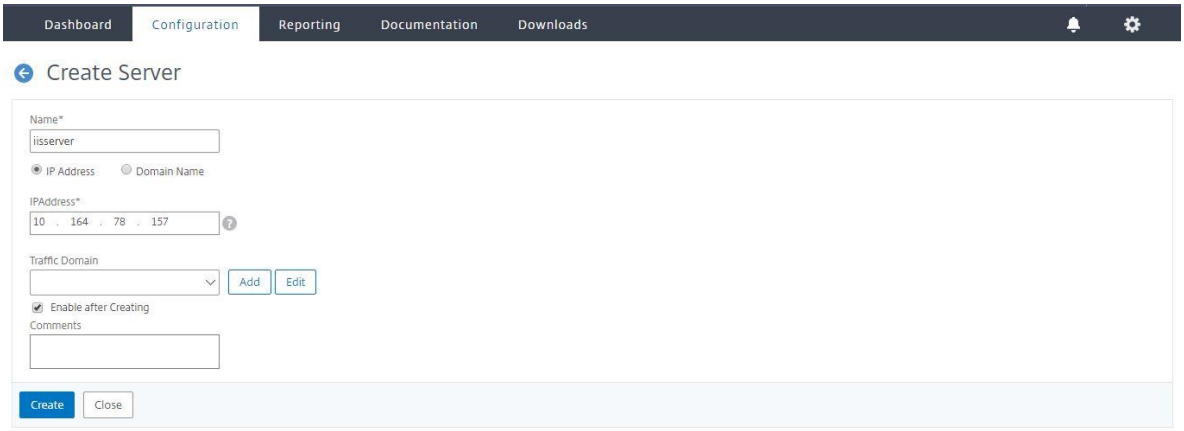
> Add services

> Add virtual servers

Add servers

Add a server to configure virtual load balancing. To add servers:

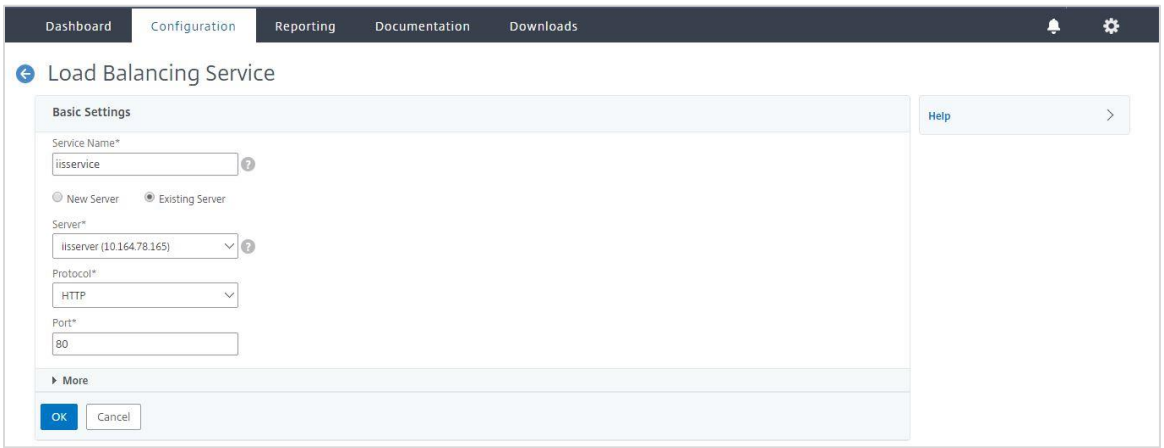
1. Navigate to **Traffic Management**->**Load Balancing**->**Servers**.
2. Click **Add** to add the details of the application server.
3. Click **Create** to add the server. The added server appears in the list.



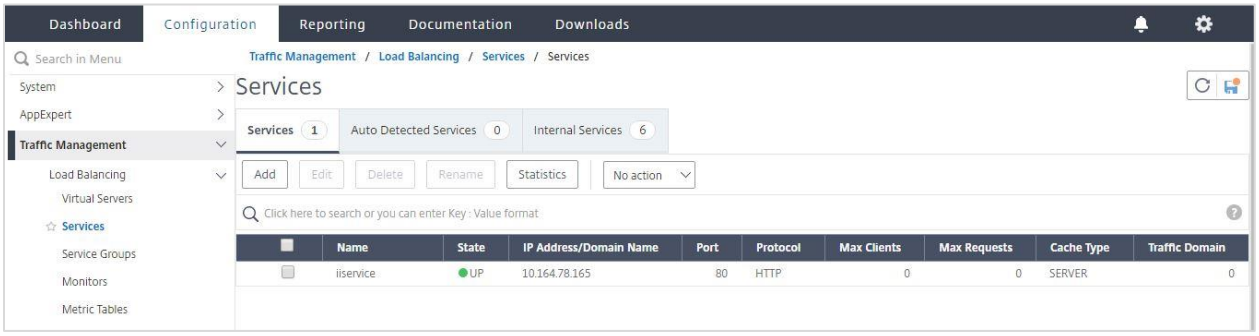
Add services

Create a service on the server to complete the load balancing operation on failure. To add services:

1. Navigate to **Traffic Management**->**Load Balancing**->**Services**.
2. Click **Add** to add the services.
3. In the server field, add the IP of the machine where your application is already running. Select the protocol and port, as shown in the following image.



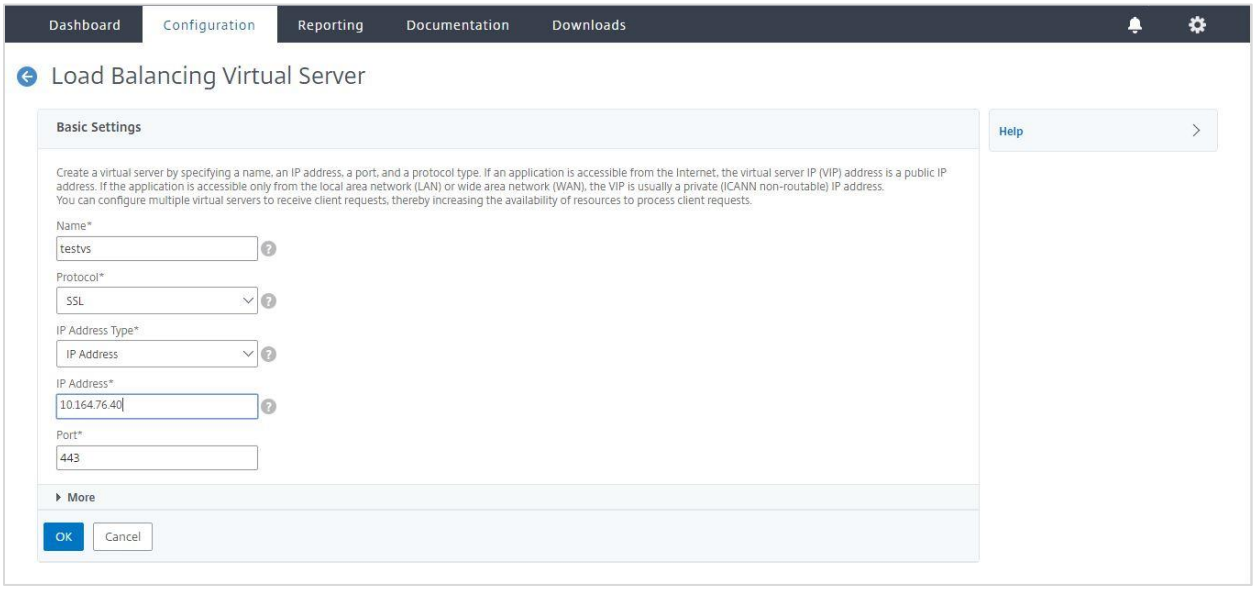
4. Click **OK** to add the service. This will bring up the Services page.
5. Verify that the **State** column of the Services Table displays state **UP**.



Add virtual servers

Create and configure a virtual server to act as the load-balancer for the backend server and connect the virtual server to the shared service. To add virtual servers:

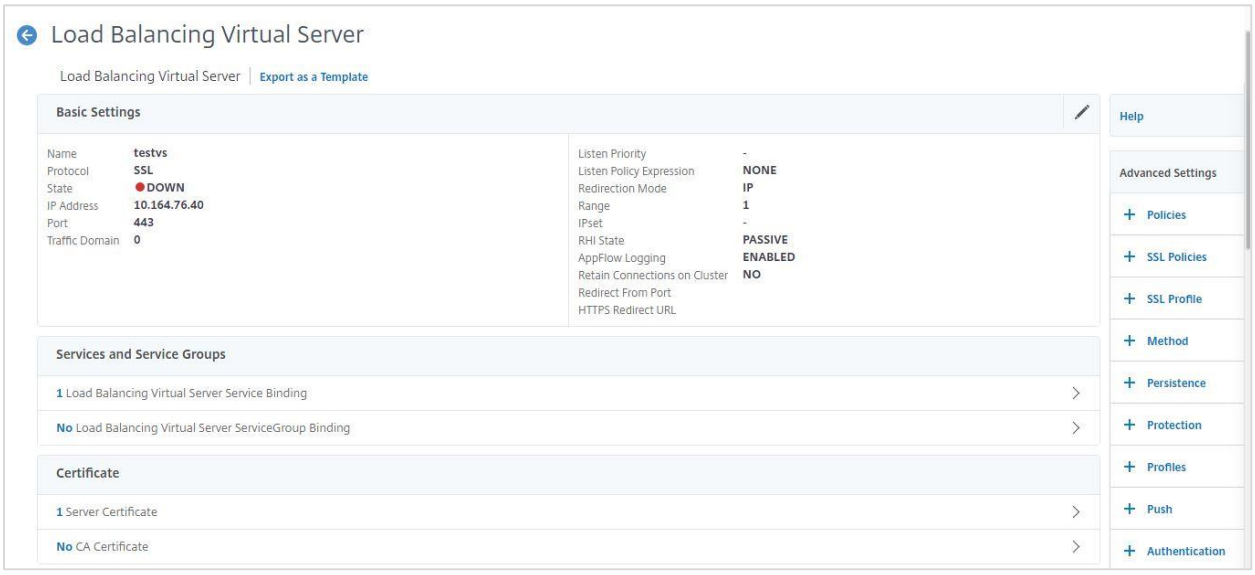
1. Navigate to **Traffic Management**->**Load Balancing**->**Virtual Servers**
2. Click **Add**.
3. Enter the details of the Virtual Server. Select the **Protocol** as SSL and then click **OK**.



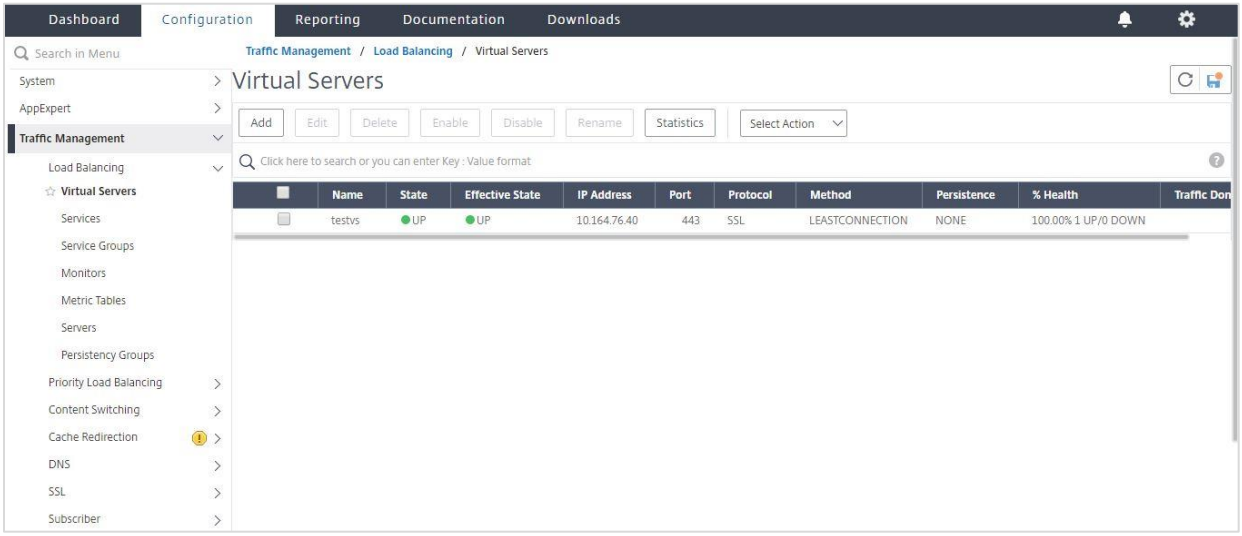
The **State** column in the **Basic Settings** should display **Down**.

4. Click **No Load Balancing Virtual Server Service Binding**. This brings the Service Binding page on to the screen.
5. Click **select service** and select the service created above. Click the **Bind** button.
6. After service binding, click **Continue**.
7. Click **No Server Certificate**.

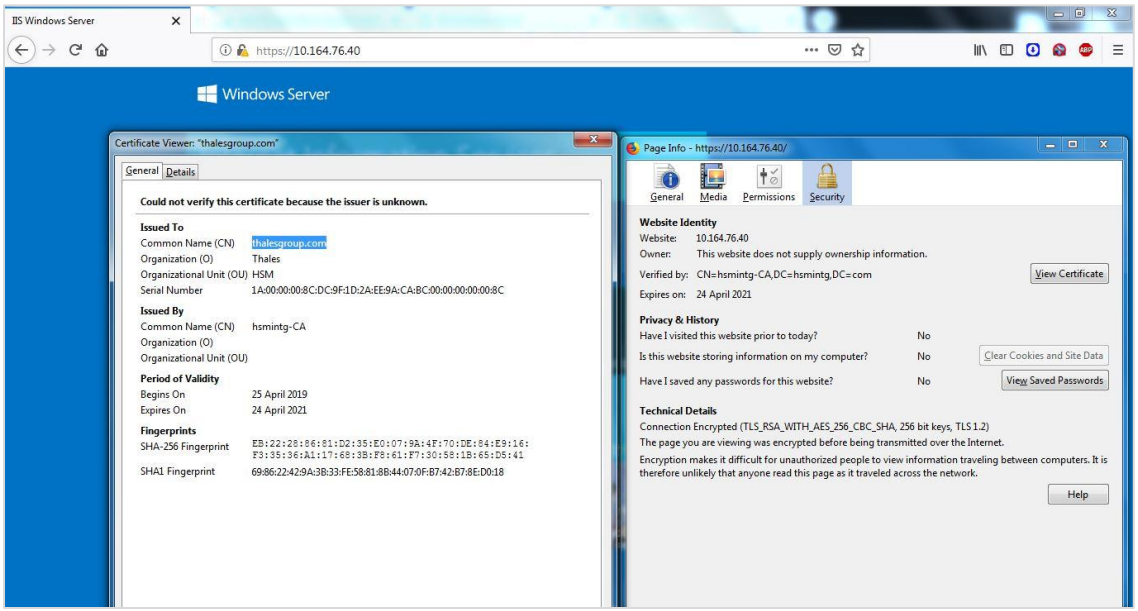
8. Select the recently generated server certificate and click **Bind**. Click **Continue** and then **Done**.



9. After successful binding of certificate and service, the **State and Effective State** column of the Services Table should display state **UP**.



10. Access the application over HTTPS using the IP of the virtual server on port 443. Verify the certificate.



This completes the integration of Citrix ADC with Luna HSM.

Contacting Customer Support

If you encounter a problem during this integration, contact your supplier or Thales Customer Support. Thales 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 Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.