Citrix NetScaler and Citrix XenDesktop 7 Deployment Guide

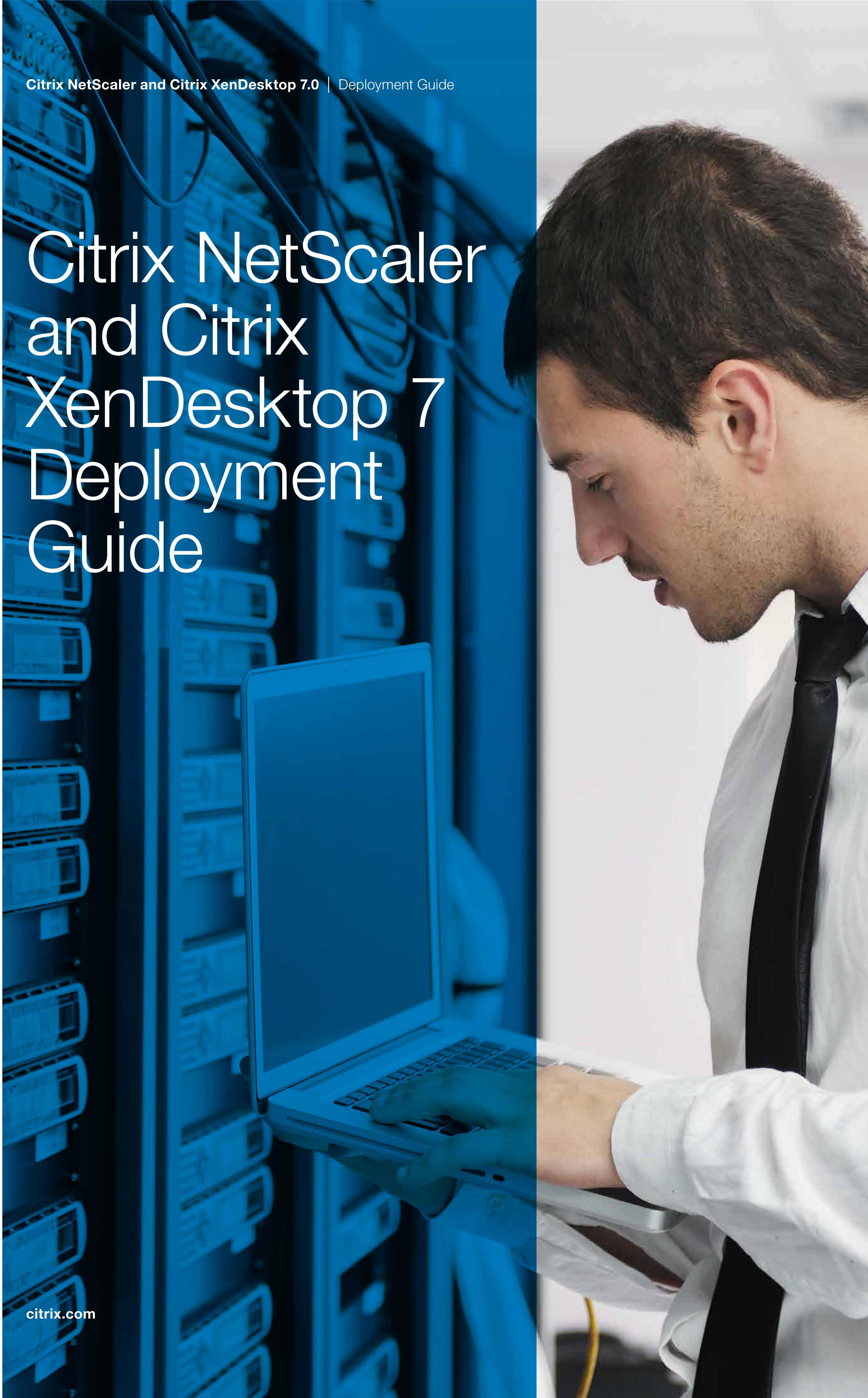


Table of contents

Click on the section names above to navigate to that portion of the book and the arrow icon to return to the table of contents from any page.

This guide demonstrates how to deploy Citrix NetScaler in conjunction with Citrix XenDesktop 7 with a focus on both simplicity in configuration and advanced features not easily delivered with other products.

Executive summary and document overview

1. Introduction

In this guide you'll learn how to provision the XenDesktop 7 infrastructure, the NetScaler appliance and NetScaler Insight Center services to extend Citrix virtual desktop infrastructure and services to remote users in small to medium-size enterprises.

1.1 Overview summary

Best end user experience: With an integrated Citrix solution for remote and portable workstyles, end users enjoy a seamless experience resulting in fewer help desk calls and reduced training needs. Citrix Receiver client software is installed on the user device (iPhone, Android phone, thin client) to allow users, by way of the NetScaler appliance delivering high availability, scale and security, to access their desktops, applications and data through Citrix StoreFront. StoreFront, which ships with XenDesktop 7, authenticates users to XenDesktop sites and Citrix XenApp farms, enumerating and aggregating available desktops and applications into stores that users can access through Citrix Receiver or Receiver for Web. The StoreFront database records details of users' application subscriptions to enable synchronization of those applications across all their devices. Benefits of the NetScaler/StoreFront solution include one-click configuration for user setup, local and remote access, automatically provisioned applications, self-service simplicity, a consistent user experience across any device and persistent access to applications and desktops.

End-to-end application visibility: New NetScaler 10.1 with HDX Insight seamlessly integrates with Desktop Director to provide a single location for management and monitoring of the XenApp and XenDesktop infrastructure. IT teams can drill down into network protocols (primarily ICA) through Desktop Director to troubleshoot individual user issues from a single console. The AppFlow capability of NetScaler allows you to export this data to third-party tools such as Splunk for in-depth correlation, analysis and reporting. The reports generated by NetScaler Insight Center, such as the applications and users consuming the most resources, can help IT determine peak usage and proactively allocate bandwidth accordingly. Response time measurements can help detect and resolve problems before a critical network or application failure occurs.

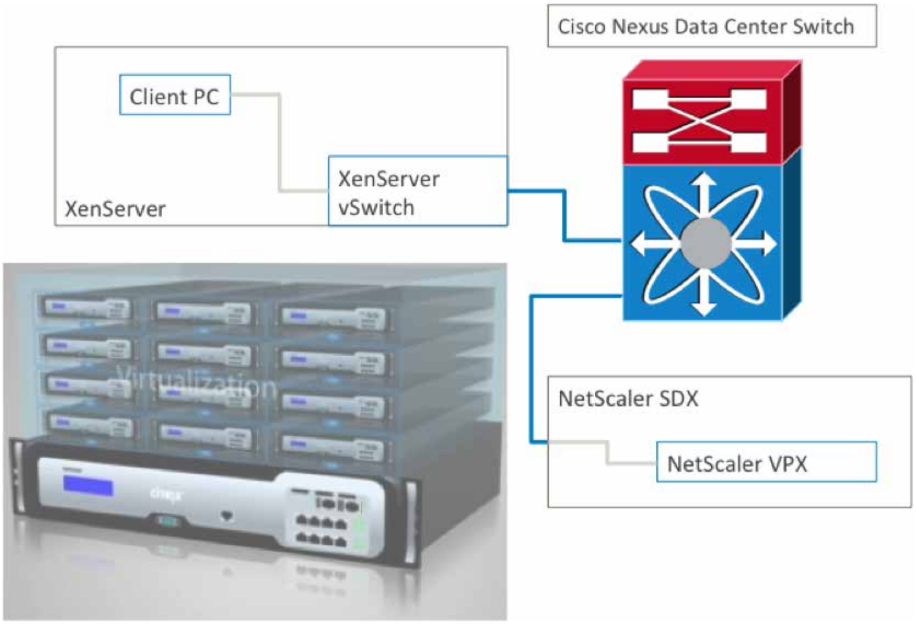
Enhanced security: By acting as a full proxy for ICA connections, NetScaler filters these connections before they hit the backend server, ensuring they are attack free. Proper integration with Secure Ticketing Authority (STA) prevents internal user and server data, including IP address information, from leaking. SmartAccess allows you to control access to published XenApp virtual applications and XenDesktop virtual desktops on a server through the use of NetScaler Access Gateway session policies. NetScaler Access Gateway is a full-featured SSL VPN that is an integral component of NetScaler. It gives administrators granular, application-level control while empowering users with remote access to their virtual desktops from anywhere.

End-to-end support from a single vendor: Integration between NetScaler and IT Desktop Director provides a single console for troubleshooting end-user issues concerning the network and desktops. It also helps lower support and training costs (TCO) in the long run and enables IT teams to stay abreast of product roadmap updates. Choosing one vendor instead of multiple providers prevents finger pointing on integration issues.

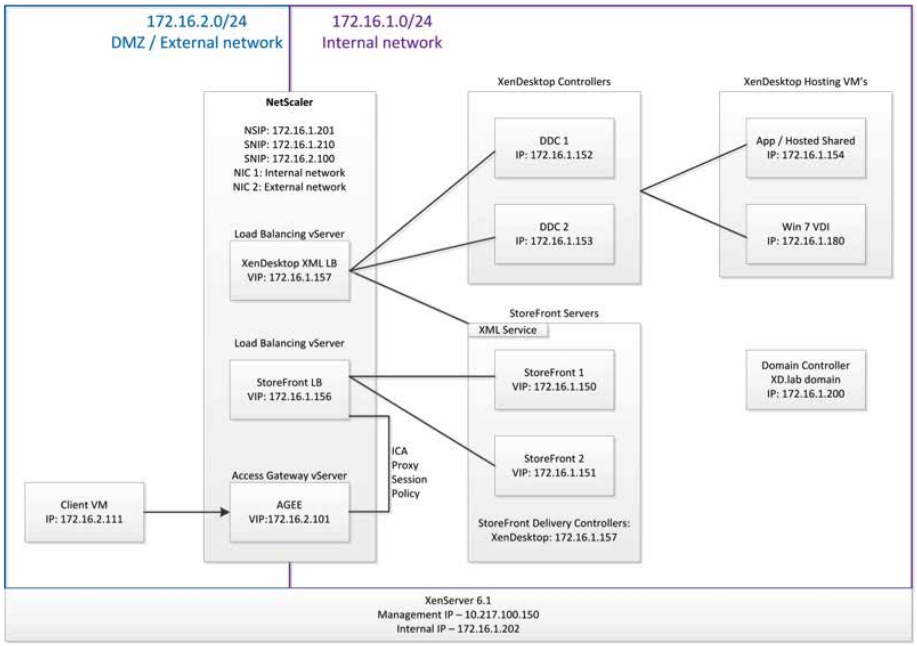
2. Architectural overview

The environment described in this guide has been deployed on a single host, with internal networks configured to simulate an internal corporate network and a DMZ. The following diagrams illustrate the machines and network configuration in this deployment.

2.1 Physical view



2.2 Logical view



2.3 Target architecture

The following components have been installed on each of the machines:

1. Domain controller (DC)
    - Active Directory domain services
    - DNS
    - DHCP
    - Citrix License Server 11.11
2. Dynamic Delivery Controller 1 (DDC1)
    - XenDesktop 7
    - SQL Server Express 2012
3. Dynamic Delivery Controller 2 (DDC2)
    - XenDesktop 7
4. App/hosted shared desktops (APP)
    - XenDesktop 7 Virtual Desktop Agent (VDA)
5. Windows 8 VDI (XDVDI)
    - XenDesktop 7 VDA
6. StoreFront 1 (SF1)
    - StoreFront 1.3
7. StoreFront 2 (SF2)
    - StoreFront 1.3
8. Client machine (client)
    - Citrix Receiver 3.4

Cloud infrastructure

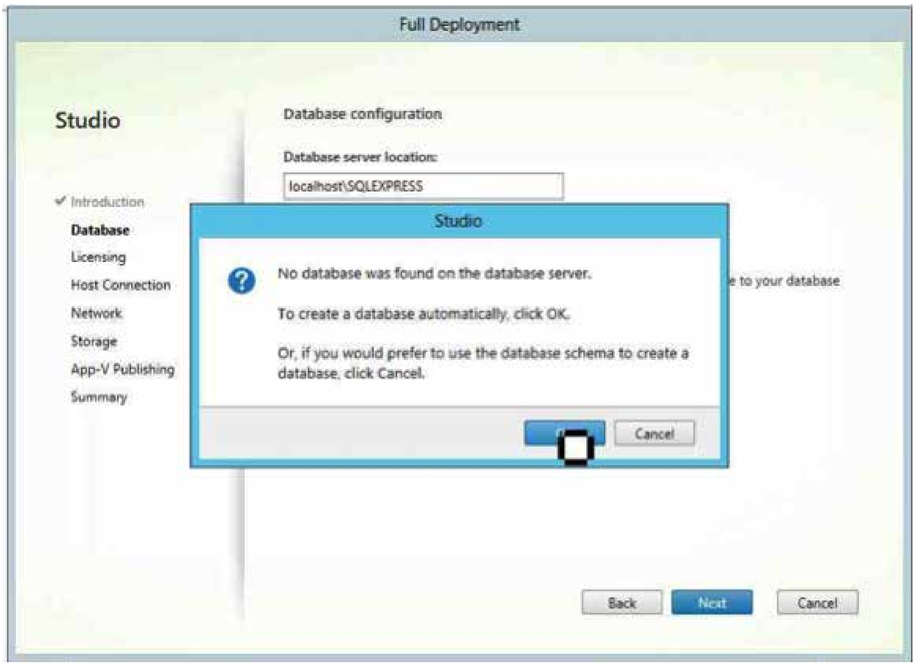
3. XenDesktop 7 management infrastructure setup

This section defines the steps required to build the complete infrastructure.

3.1 Install Citrix XenDesktop 7 and supporting components

The XenDesktop 7 install process is a simple next/next/finish install. The services installed on each machine in this deployment are described in the previous section.

Once XenDesktop is installed, a site must be created. Click on **Create a site** in the studio mmc, and click **Next** on the introduction step. On the database configuration page, enter the details to connect to the SQL server. In this case, SQL Server Express has been installed on DDC1 and no database has been configured. As long as connectivity tests to the SQL Server pass, XenDesktop will create the database automatically. Enter whatever you want the database to be called in the database name field.



Full Deployment

Studio

Database configuration

Database server location: localhost\SQLEXPRESS

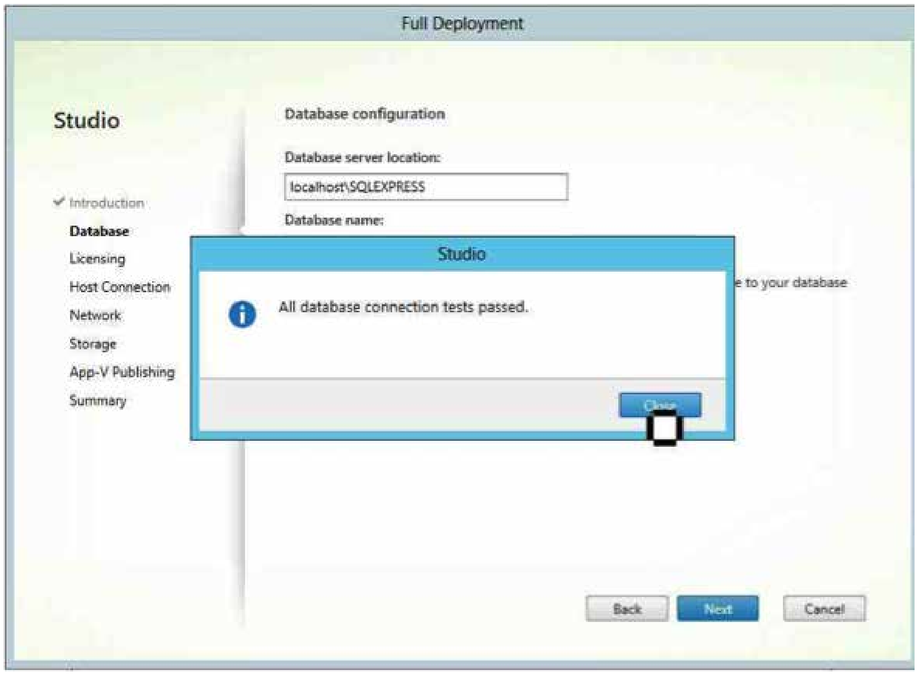
Studio

No database was found on the database server.

To create a database automatically, click OK.

Or, if you would prefer to use the database schema to create a database, click Cancel.

Click **Test** to confirm the database can be connected to.



Database configuration

Database server location: localhost\SQLEXPRESS

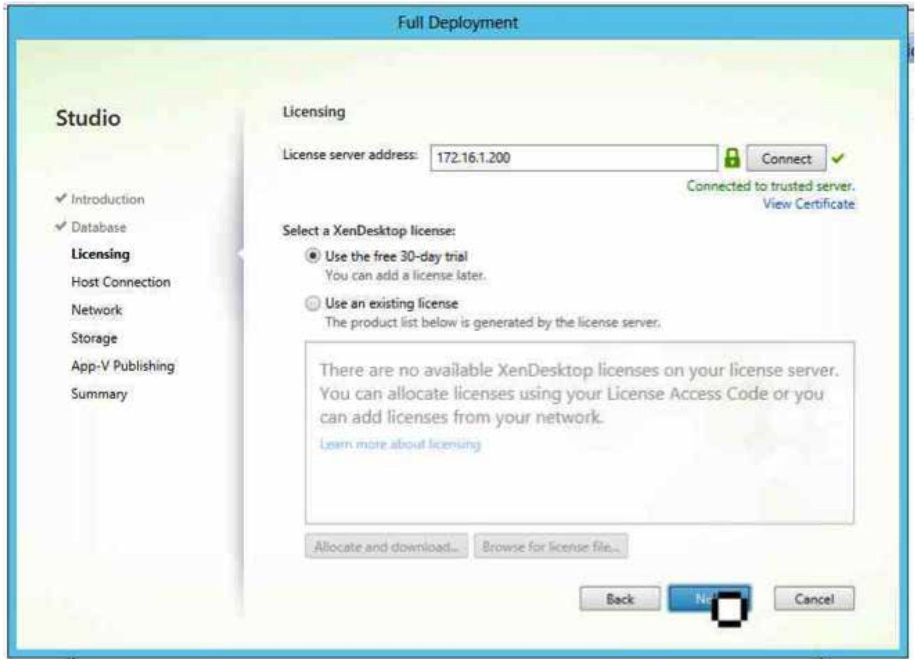
Database name:

e to your database

Studio

All database connection tests passed.

Configure the license server and license for XenDesktop. In this deployment the license server has been installed on the domain controller, and we are using a trial license.



Licensing

License server address: 172.16.1.200 ✓

Connected to trusted server.

Select a XenDesktop license:

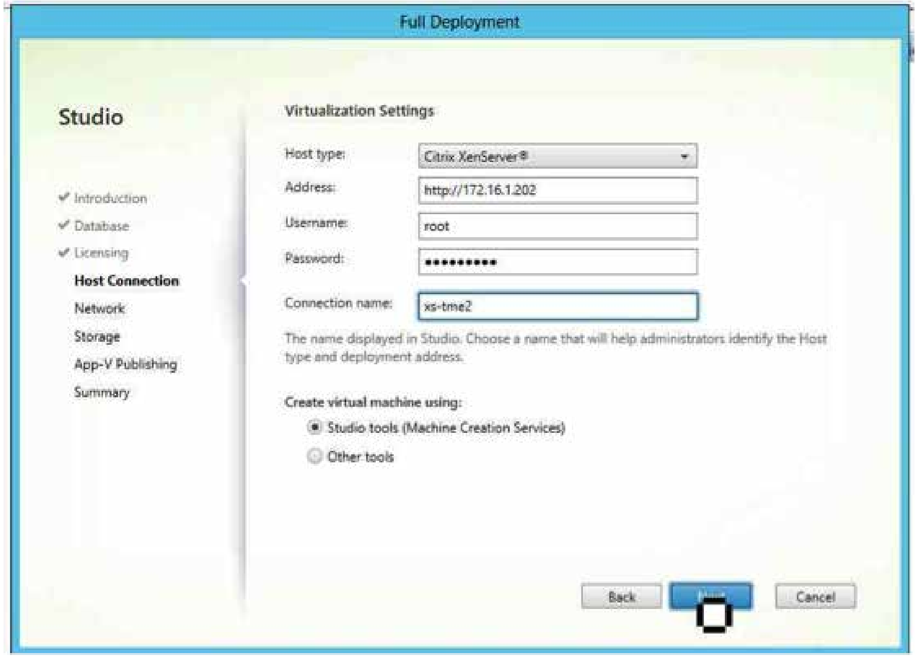
● Use the free 30-day trial
You can add a license later.

○ Use an existing license
The product list below is generated by the license server.

There are no available XenDesktop licenses on your license server. You can allocate licenses using your License Access Code or you can add licenses from your network.

You may receive a certificate warning during this step if you do not have a computer certificate on the domain controller.

Enter the hypervisor information. XenDesktop must be able to create machines on the hypervisor, so root permission is required. Use the root account for Citrix XenServer.



Virtualization Settings

Host type: Citrix XenServer®

Address: http://172.16.1.202

Username: root

Password: ••••••••••

Connection name: xs-tme2

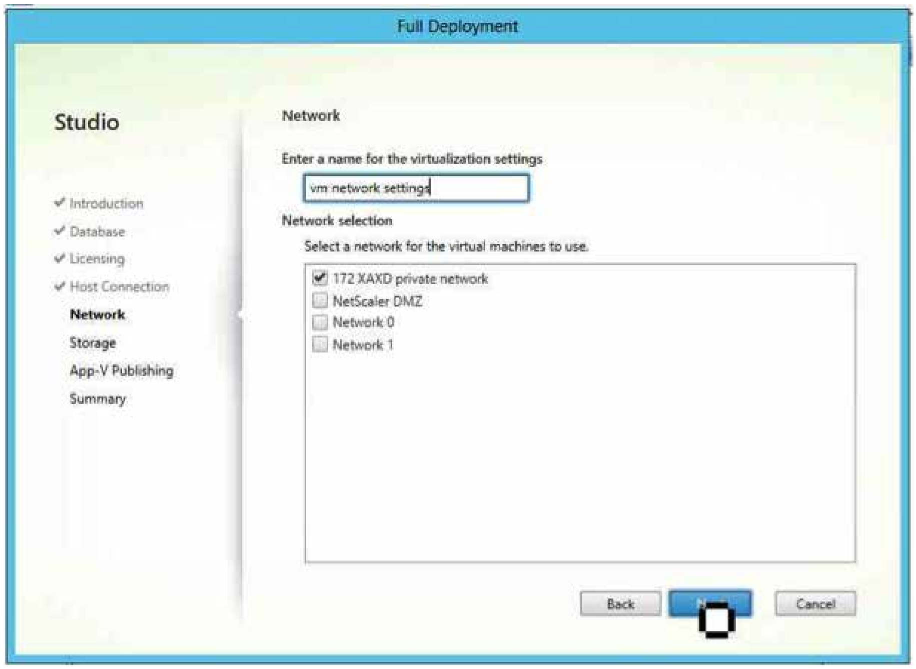
The name displayed in Studio. Choose a name that will help administrators identify the Host type and deployment address.

Create virtual machine using:

● Studio tools (Machine Creation Services)

○ Other tools

Select the network on which you would like new machines to be created.



Network

Enter a name for the virtualization settings

vm network settings

Network selection

Select a network for the virtual machines to use.

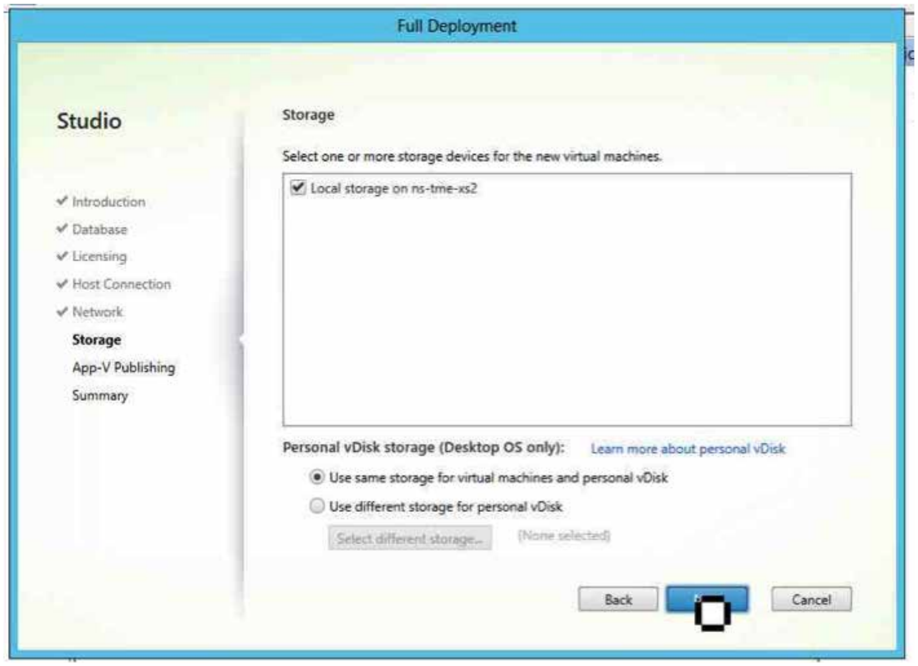
☑ 172 XAXD private network

□ NetScaler DMZ

□ Network 0

□ Network 1

Select the storage location where the new devices will be placed.



Storage

Select one or more storage devices for the new virtual machines.

☑ Local storage on ns-tme-xs2

Personal vDisk storage (Desktop OS only): Learn more about personal vDisk

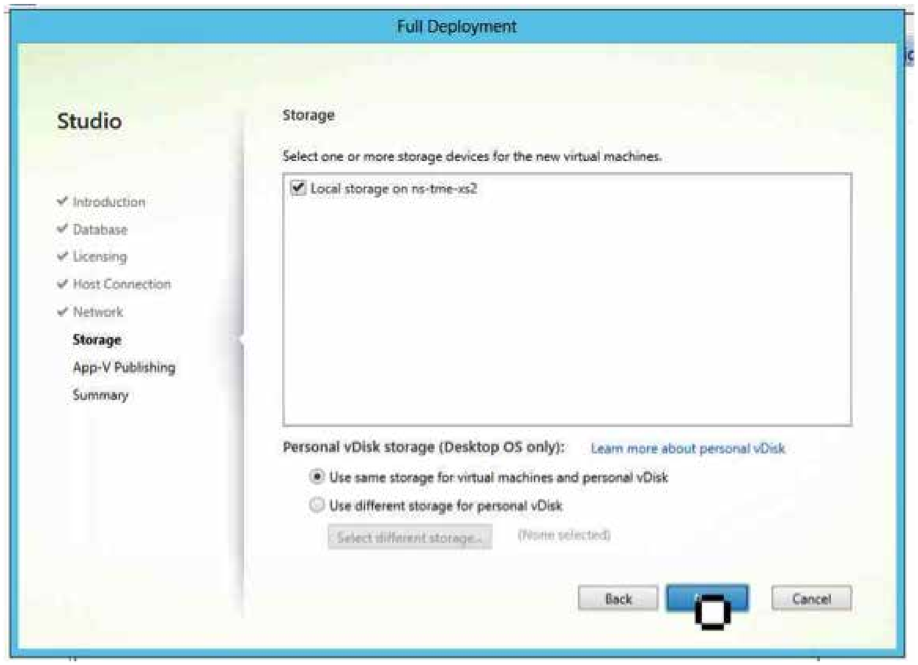
● Use same storage for virtual machines and personal vDisk

○ Use different storage for personal vDisk

Select different storage... (None selected)

Add App-V if necessary, as it was not configured as part of this deployment.

Review the settings and click **Finish**. A new site will be **created**.



Storage

Select one or more storage devices for the new virtual machines.

☑ Local storage on ns-tme-xs2

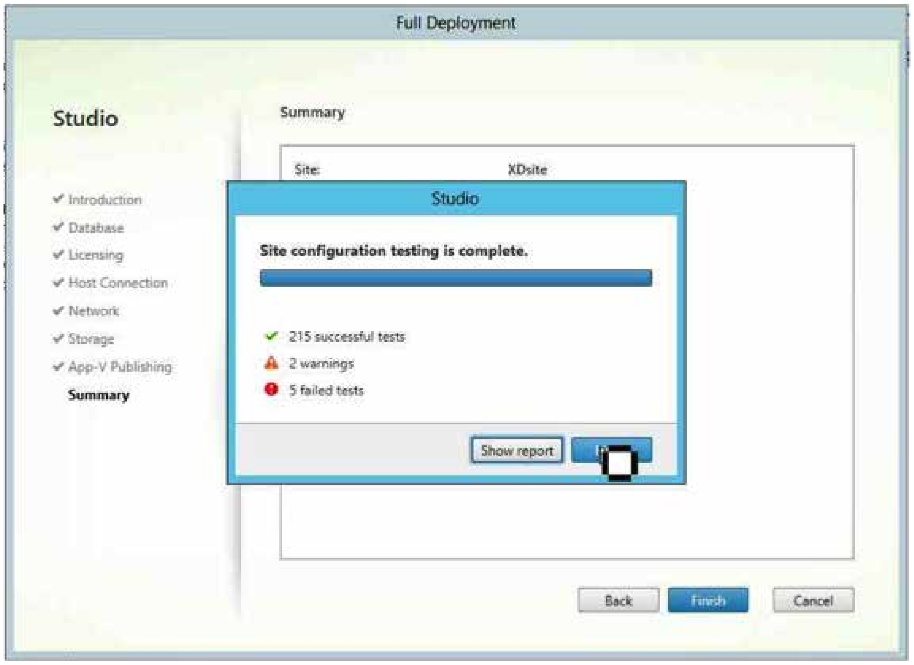
Personal vDisk storage (Desktop OS only): Learn more about personal vDisk

● Use same storage for virtual machines and personal vDisk

○ Use different storage for personal vDisk

Select different storage... (None selected)

Some of the site configuration tests may fail. In this case the failed tests were SQL Server reference schema tests, which have no impact on the XenDesktop deployment.



Site: XDsite

Site configuration testing is complete.

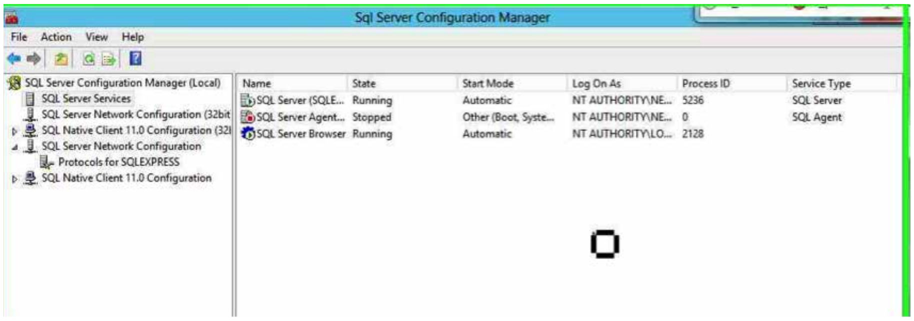
✓ 215 successful tests

⚠ 2 warnings

● 5 failed tests

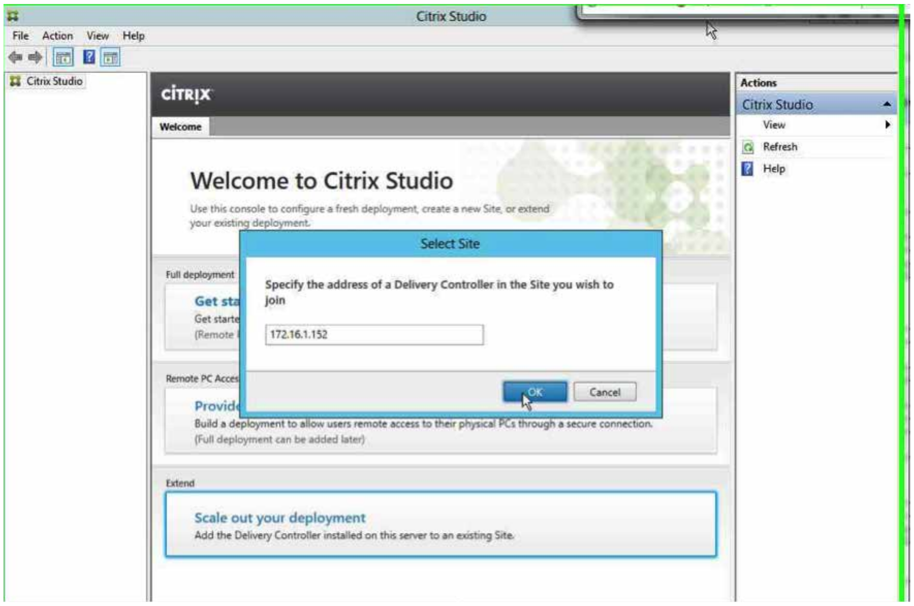
3.2 Add DDCs to XenDesktop

If you are using SQL Server Express, you will have to start the browser on the SQL Server before you can add DDCs to the site, as without the browser remote machines cannot access the database.


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 11.0 Configuration (32l
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 11.0 Configuration

Name	State	Start Mode	Log On As	Process ID	Service Type
SQL Server (SQLE...	Running	Automatic	NT AUTHORITY\NE...	5236	SQL Server
SQL Server Agent...	Stopped	Other (Boot, Syste...	NT AUTHORITY\NE...	0	SQL Agent
SQL Server Browser	Running	Automatic	NT AUTHORITY\LO...	2128	

From the studio MMC, click **Scale out your deployment** and input the address of the existing DDC in the deployment.



Welcome to Citrix Studio

Use this console to configure a fresh deployment, create a new Site, or extend your existing deployment.

Select Site

Specify the address of a Delivery Controller in the Site you wish to join

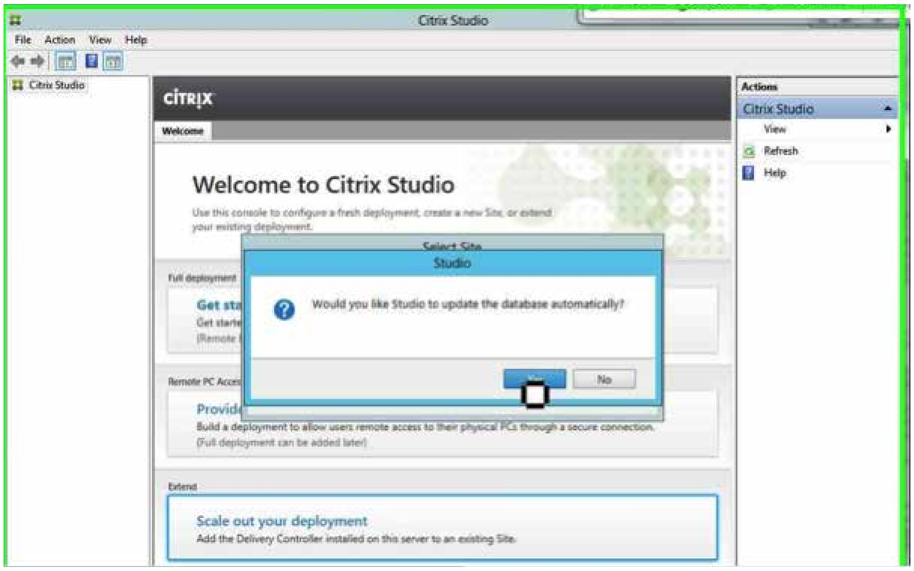
172.16.1.152

Build a deployment to allow users remote access to their physical PCs through a secure connection. (Full deployment can be added later)

Scale out your deployment

Add the Delivery Controller installed on this server to an existing Site.

Click **Yes** to update the Citrix Studio database automatically.



Welcome to Citrix Studio

Use this console to configure a fresh deployment, create a new Site, or extend your existing deployment.

Would you like Studio to update the database automatically?

Build a deployment to allow users remote access to their physical PCs through a secure connection. (Full deployment can be added later)

Scale out your deployment

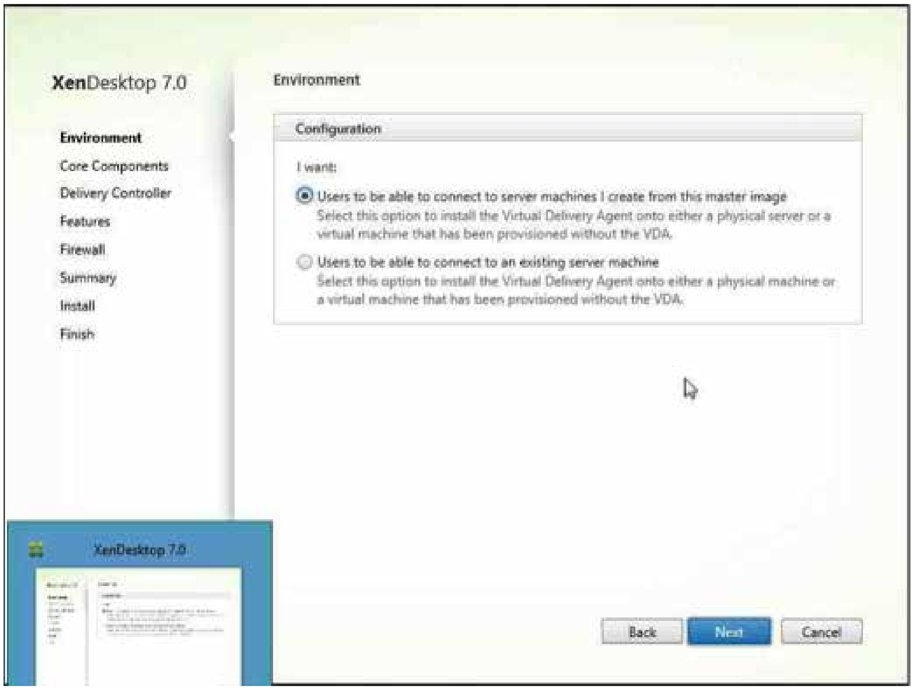
Add the Delivery Controller installed on this server to an existing Site.

Verify by navigating to **Desktop Studio, Configuration, Controllers** in the left panel. You should see both servers listed.

3.3 Install the Virtual Delivery Agent

The VDA must be installed on all machines that will deliver desktops or apps. Load the XenDesktop install media onto the target machines to launch the VDA installation.

Since we will be creating machines from this image with Machine Creation Services (MCS), we select the first option.



XenDesktop 7.0

Environment

Core Components

Delivery Controller

Features

Firewall

Summary

Install

Finish

Environment

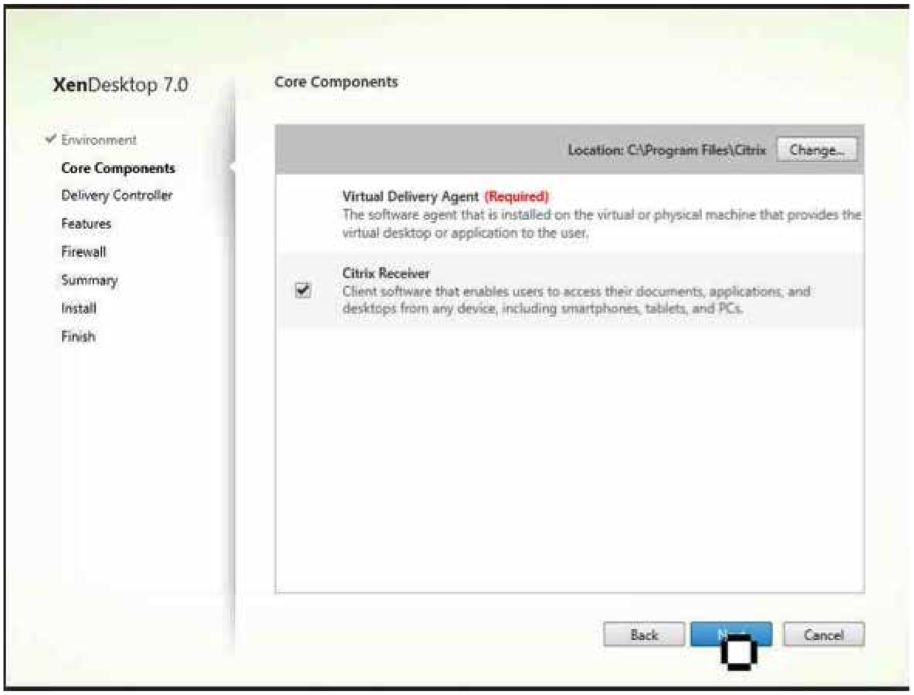
Configuration

I want:

● Users to be able to connect to server machines I create from this master image
Select this option to install the Virtual Delivery Agent onto either a physical server or a virtual machine that has been provisioned without the VDA.

○ Users to be able to connect to an existing server machine
Select this option to install the Virtual Delivery Agent onto either a physical machine or a virtual machine that has been provisioned without the VDA.

Add Citrix Receiver to the installation so that users can access applications from within hosted desktops.



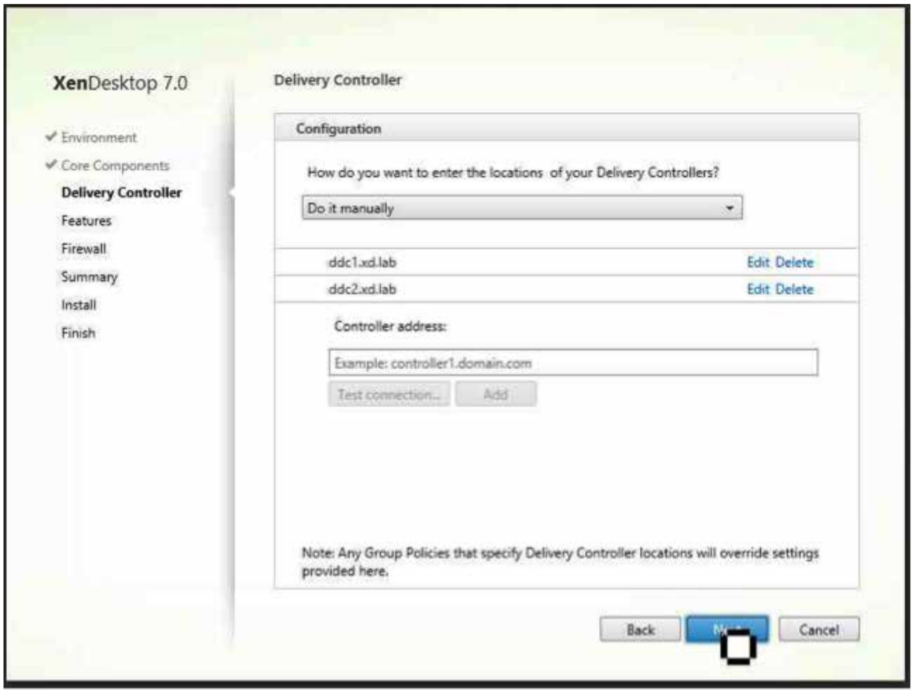
Core Components

Location: C:\Program Files\Citrix

Virtual Delivery Agent (Required)
The software agent that is installed on the virtual or physical machine that provides the virtual desktop or application to the user.

☑ Citrix Receiver
Client software that enables users to access their documents, applications, and desktops from any device, including smartphones, tablets, and PCs.

Add both delivery controllers to the configuration. These must be FQDNs, so make sure that the machine is configured to use your DNS server and verify that the DNS entries are correct.



Delivery Controller

Configuration

How do you want to enter the locations of your Delivery Controllers?

Do it manually

ddc1.xd.lab

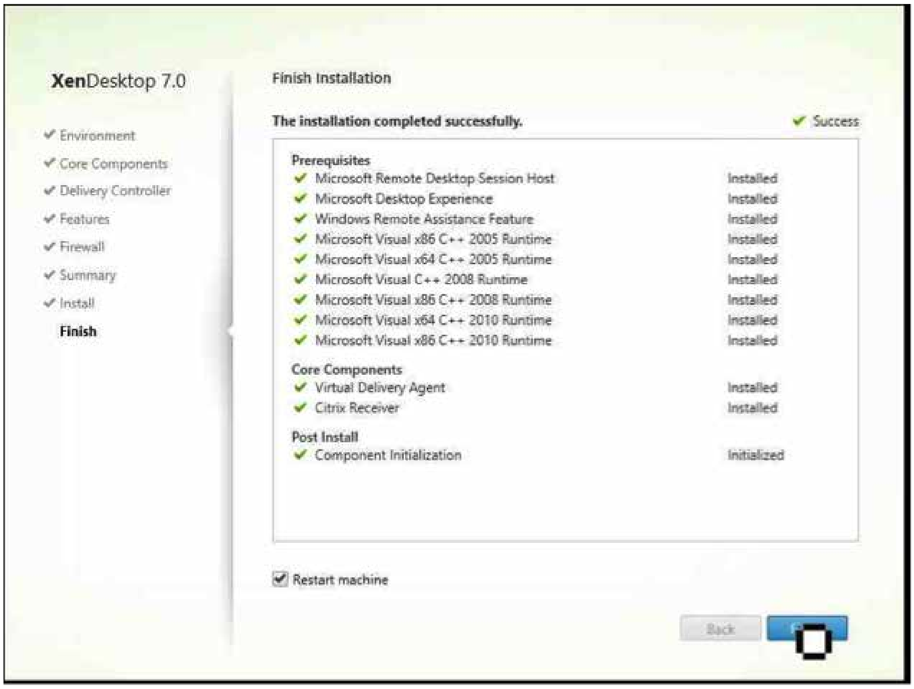
ddc2.xd.lab

Controller address:

Example: controller1.domain.com

Note: Any Group Policies that specify Delivery Controller locations will override settings provided here.

Leave the default features and firewall configuration unchanged and click **Install**. The machine will restart during installation. Verify that installation has completed successfully.



XenDesktop 7.0

- ✓ Environment
- ✓ Core Components
- ✓ Delivery Controller
- ✓ Features
- ✓ Firewall
- ✓ Summary
- ✓ Install
- Finish

Finish Installation

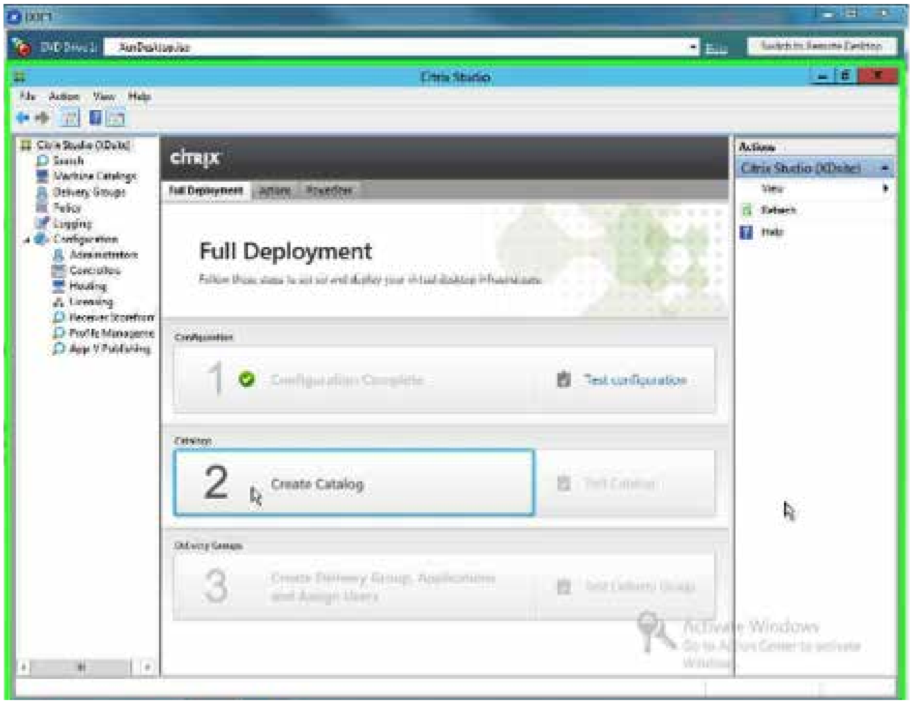
The installation completed successfully. ✓ Success

Prerequisites	
✓ Microsoft Remote Desktop Session Host	Installed
✓ Microsoft Desktop Experience	Installed
✓ Windows Remote Assistance Feature	Installed
✓ Microsoft Visual x86 C++ 2005 Runtime	Installed
✓ Microsoft Visual x64 C++ 2005 Runtime	Installed
✓ Microsoft Visual C++ 2008 Runtime	Installed
✓ Microsoft Visual x86 C++ 2008 Runtime	Installed
✓ Microsoft Visual x64 C++ 2010 Runtime	Installed
✓ Microsoft Visual x86 C++ 2010 Runtime	Installed
Core Components	
✓ Virtual Delivery Agent	Installed
✓ Citrix Receiver	Installed
Post Install	
✓ Component Initialization	Initialized

☑ Restart machine

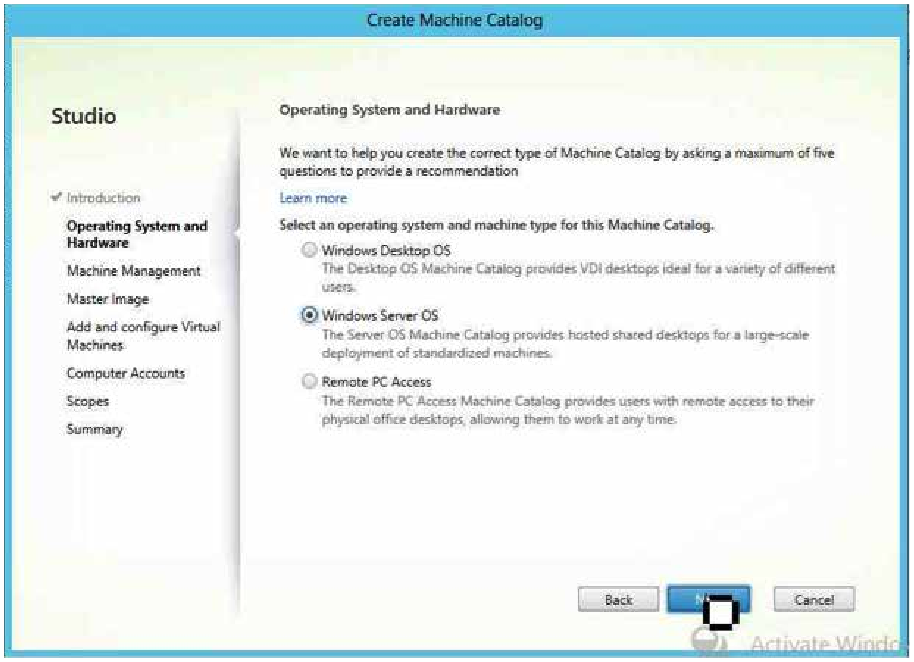
3.4 Create machine catalogs

From the studio MMC, click **Create Catalog**.



Click **Next** on the welcome screen.

Select the type of deployment. This will be a Windows Server OS catalog for hosting applications on RDS and hosted shared desktops.



Create Machine Catalog

Studio

- ✓ Introduction
- **Operating System and Hardware**
- Machine Management
- Master Image
- Add and configure Virtual Machines
- Computer Accounts
- Scopes
- Summary

Operating System and Hardware

We want to help you create the correct type of Machine Catalog by asking a maximum of five questions to provide a recommendation

Learn more

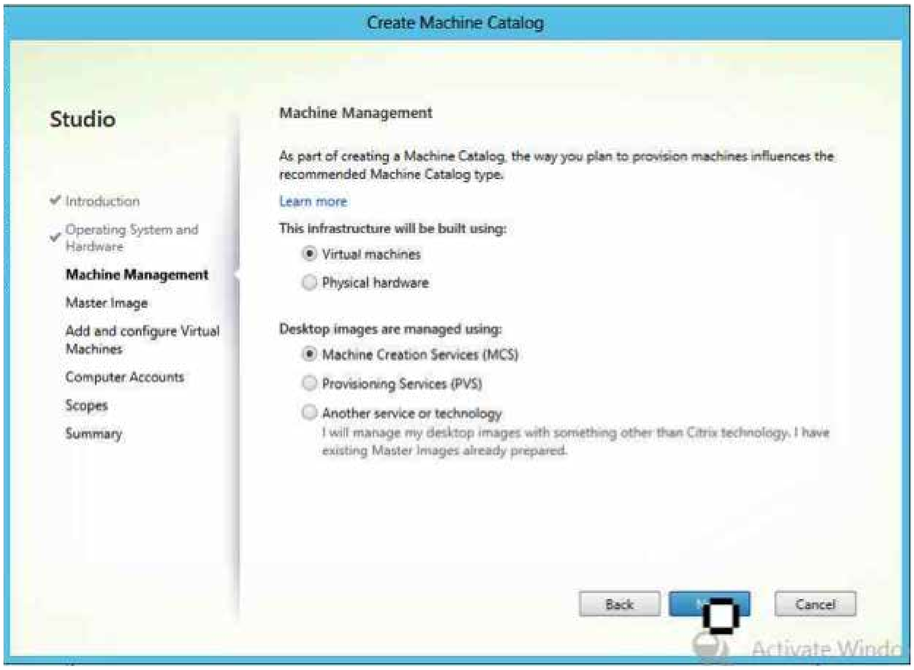
Select an operating system and machine type for this Machine Catalog.

○ Windows Desktop OS
The Desktop OS Machine Catalog provides VDI desktops ideal for a variety of different users.

● Windows Server OS
The Server OS Machine Catalog provides hosted shared desktops for a large-scale deployment of standardized machines.

○ Remote PC Access
The Remote PC Access Machine Catalog provides users with remote access to their physical office desktops, allowing them to work at any time.

Select **virtual machines** (VMs) or **physical hardware** and the image management you want to use. In this case we are managing virtual machines with MCS.



Create Machine Catalog

Studio

- ✓ Introduction
- ✓ Operating System and Hardware
- **Machine Management**
- Master Image
- Add and configure Virtual Machines
- Computer Accounts
- Scopes
- Summary

Machine Management

As part of creating a Machine Catalog, the way you plan to provision machines influences the recommended Machine Catalog type.

Learn more

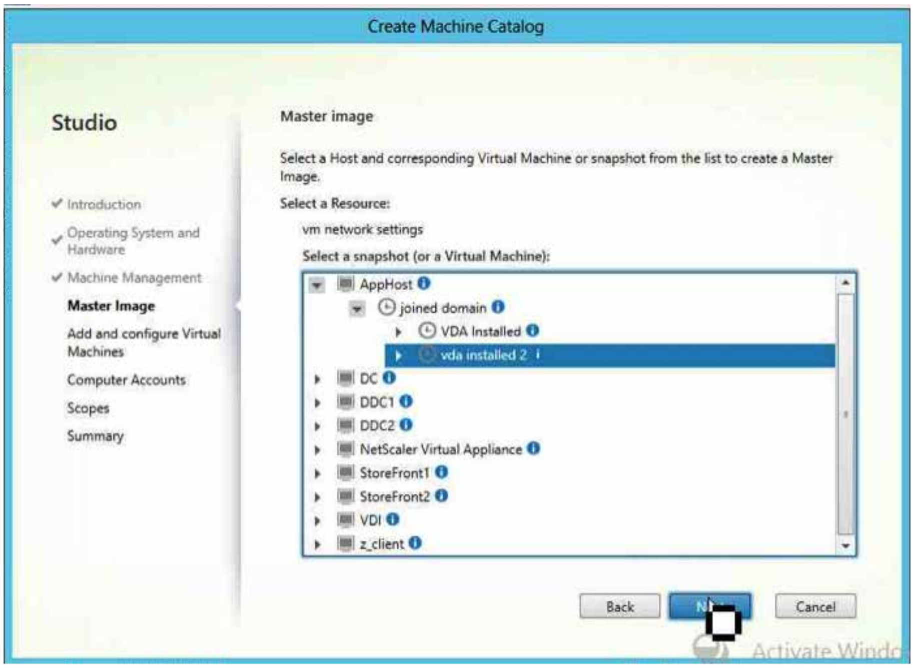
This infrastructure will be built using:

● Virtual machines
○ Physical hardware

Desktop images are managed using:

● Machine Creation Services (MCS)
○ Provisioning Services (PVS)
○ Another service or technology
I will manage my desktop images with something other than Citrix technology. I have existing Master Images already prepared.

Select the snapshot of the master image to be used for image creation.



Master image

Select a Host and corresponding Virtual Machine or snapshot from the list to create a Master Image.

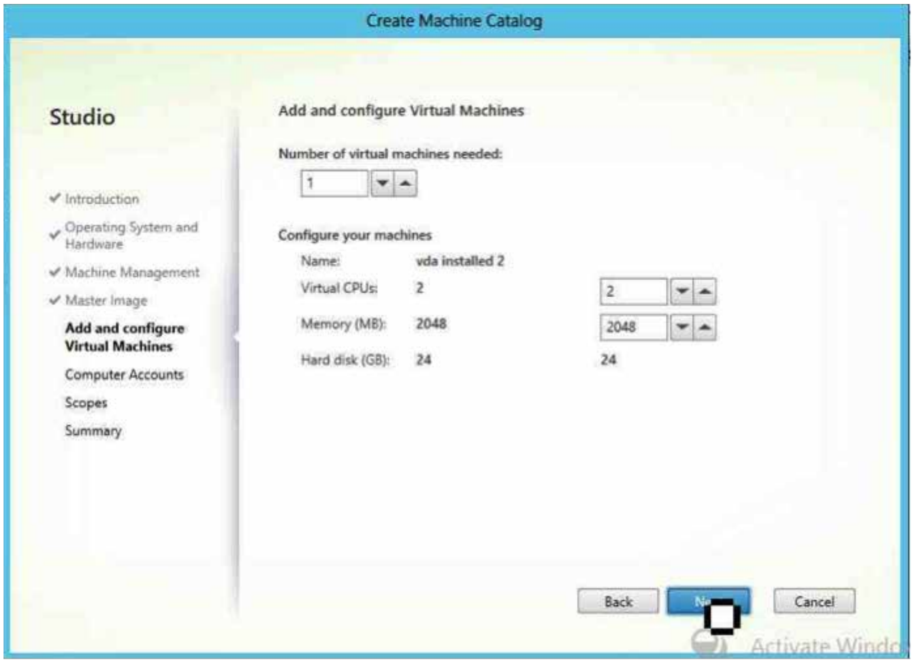
Select a Resource:

vm network settings

Select a snapshot (or a Virtual Machine):

- AppHost
  - joined domain
    - VDA Installed
    - vda installed 2
- DC
- DDC1
- DDC2
- NetScaler Virtual Appliance
- StoreFront1
- StoreFront2
- VDI
- z_client

Select machine parameters for created VMs.



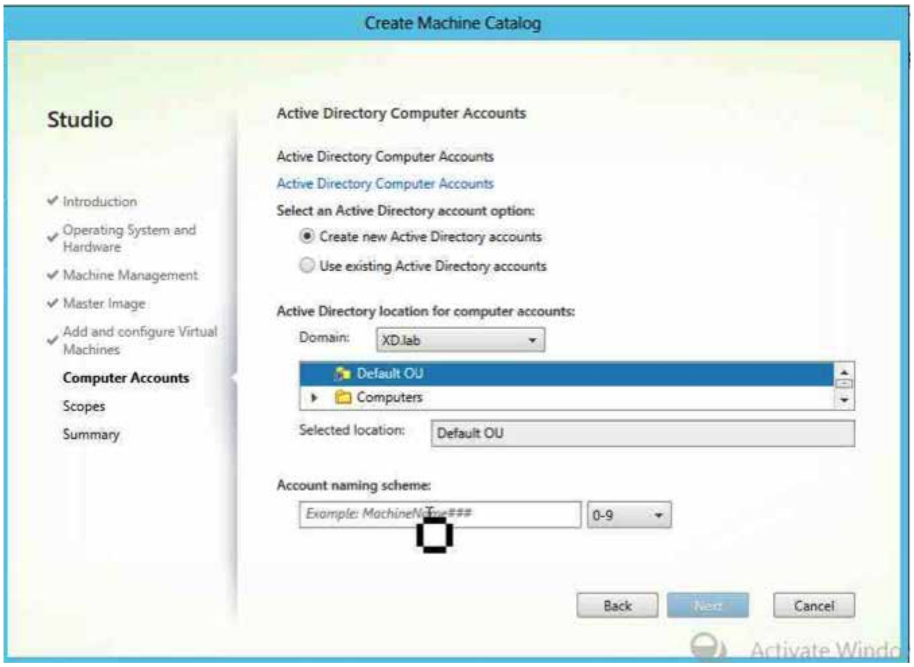
Add and configure Virtual Machines

Number of virtual machines needed: 1

Configure your machines

Name:	vda installed 2	
Virtual CPUs:	2	2
Memory (MB):	2048	2048
Hard disk (GB):	24	24

Specify the naming scheme and organizational unit (OU) for Active Directory accounts.



Active Directory Computer Accounts

Active Directory Computer Accounts

Active Directory Computer Accounts

Select an Active Directory account option:

● Create new Active Directory accounts

○ Use existing Active Directory accounts

Active Directory location for computer accounts:

Domain: XD.lab

Default OU

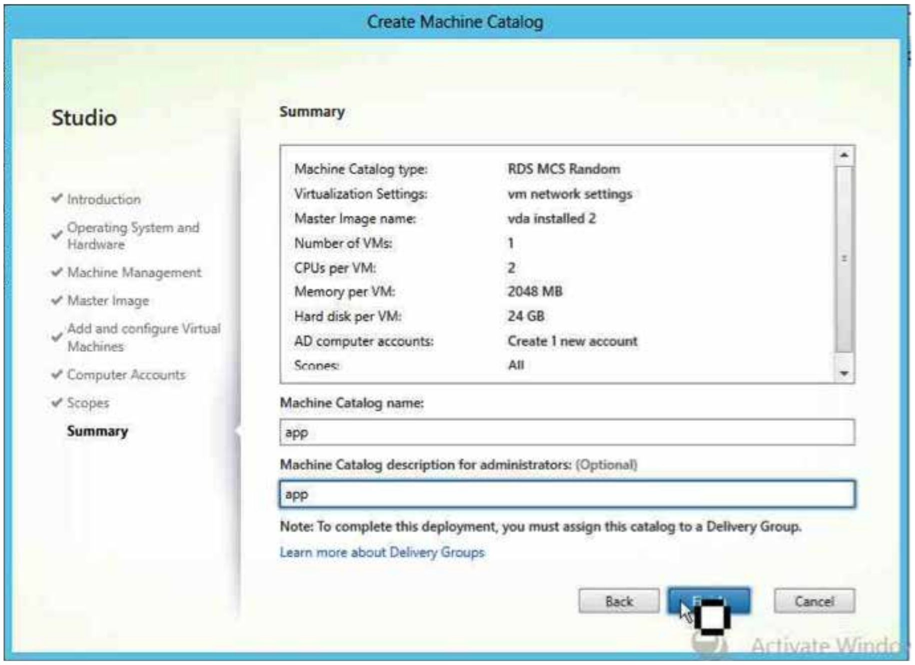
Computers

Selected location: Default OU

Account naming scheme:

Example: MachineName### 0-9

Add a scope if necessary. No scope was defined for machine catalogs in this deployment. Name the catalog and review the settings.



Summary

Machine Catalog type:	RDS MCS Random
Virtualization Settings:	vm network settings
Master Image name:	vda installed 2
Number of VMs:	1
CPUs per VM:	2
Memory per VM:	2048 MB
Hard disk per VM:	24 GB
AD computer accounts:	Create 1 new account
Scopes:	All

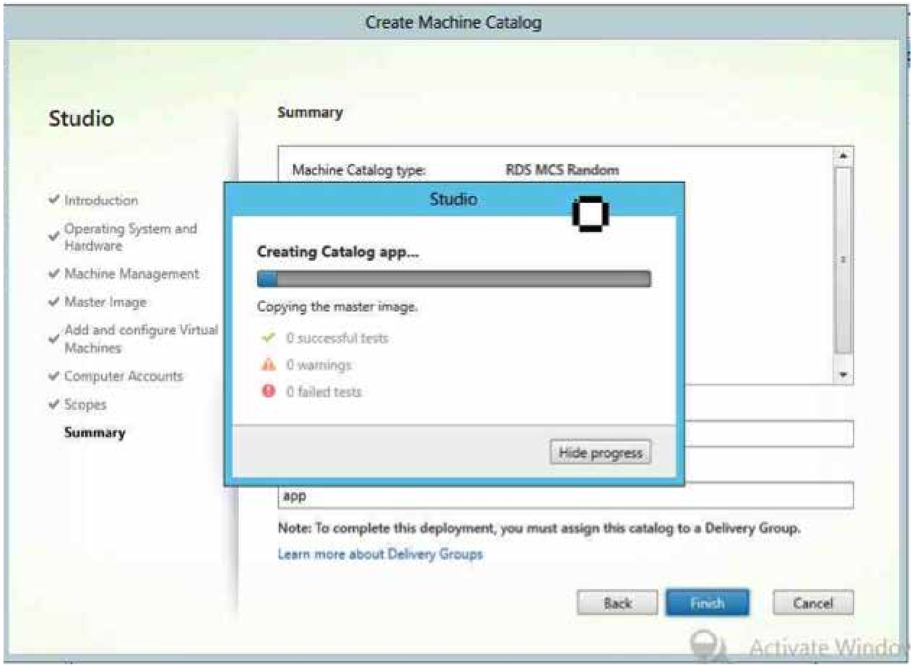
Machine Catalog name: app

Machine Catalog description for administrators: (Optional) app

Note: To complete this deployment, you must assign this catalog to a Delivery Group.

Learn more about Delivery Groups

Studio will begin creating the machine catalog, and this will take a while.



Create Machine Catalog

Studio

✓ Introduction
✓ Operating System and Hardware
✓ Machine Management
✓ Master Image
✓ Add and configure Virtual Machines
✓ Computer Accounts
✓ Scopes
Summary

Summary

Machine Catalog type: RDS MCS Random

Studio

Creating Catalog app...

Copying the master image.

✓ 0 successful tests
⚠ 0 warnings
❗ 0 failed tests

Hide progress

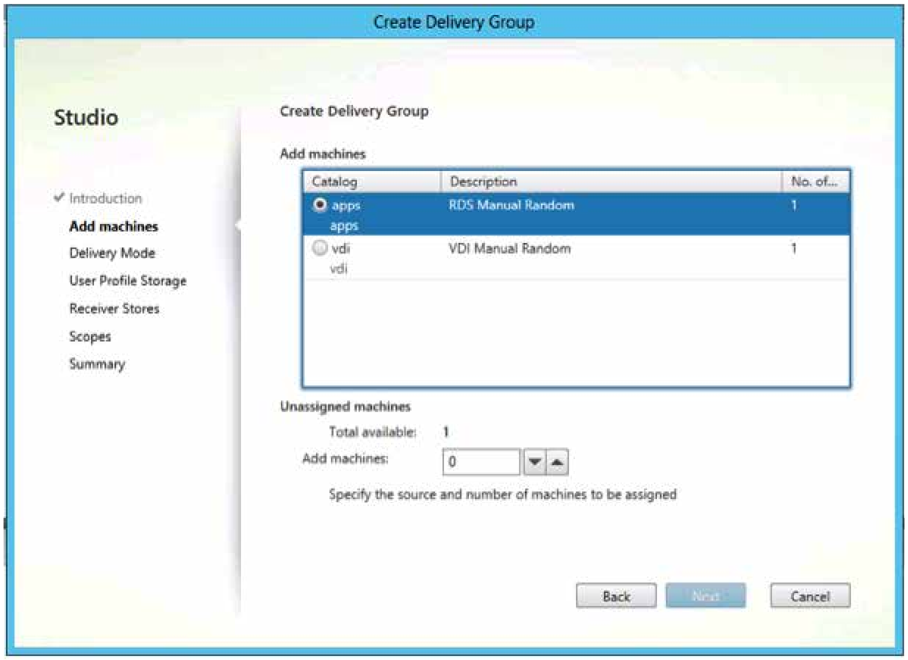
app

Note: To complete this deployment, you must assign this catalog to a Delivery Group.

Learn more about Delivery Groups

Back | Finish | Cancel

3.5 Create XenDesktop delivery groups



Create Delivery Group

Studio

✓ Introduction
Add machines
Delivery Mode
User Profile Storage
Receiver Stores
Scopes
Summary

Create Delivery Group

Add machines

Catalog	Description	No. of...
● apps apps	RDS Manual Random	1
○ vdi vdi	VDI Manual Random	1

Unassigned machines

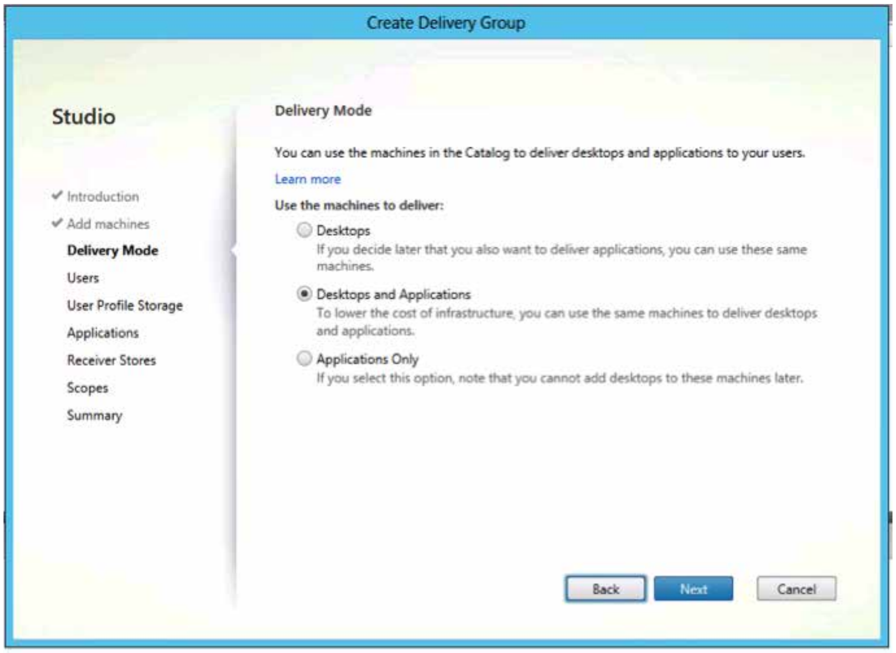
Total available: 1

Add machines: 0

Specify the source and number of machines to be assigned

Back | Next | Cancel

Add some machines and click **Next**.



Create Delivery Group

Studio

- ✓ Introduction
- ✓ Add machines
- **Delivery Mode**
- Users
- User Profile Storage
- Applications
- Receiver Stores
- Scopes
- Summary

Delivery Mode

You can use the machines in the Catalog to deliver desktops and applications to your users.

Learn more

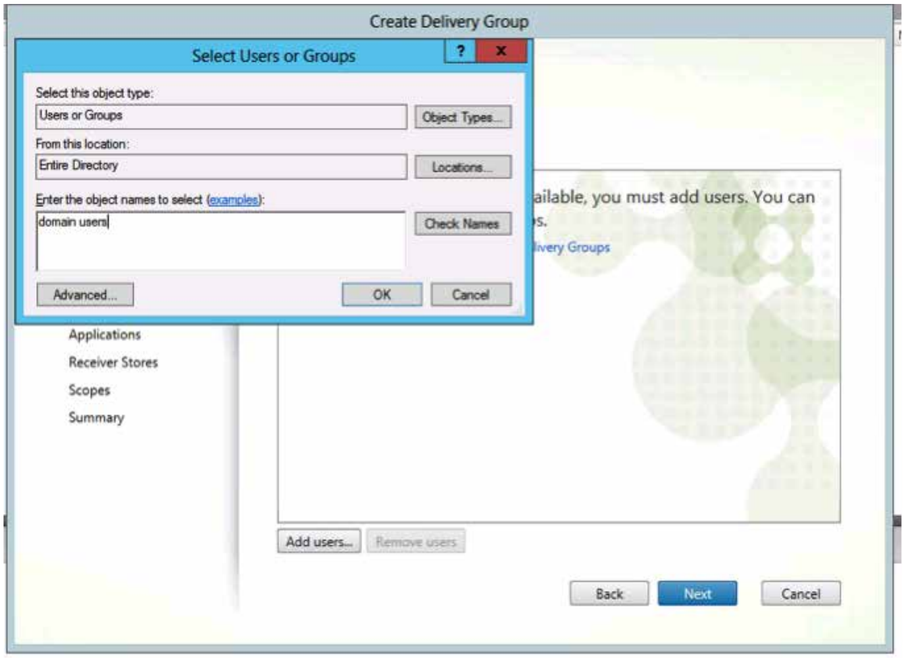
Use the machines to deliver:

○ Desktops
If you decide later that you also want to deliver applications, you can use these same machines.

● Desktops and Applications
To lower the cost of infrastructure, you can use the same machines to deliver desktops and applications.

○ Applications Only
If you select this option, note that you cannot add desktops to these machines later.

Add users.



Create Delivery Group

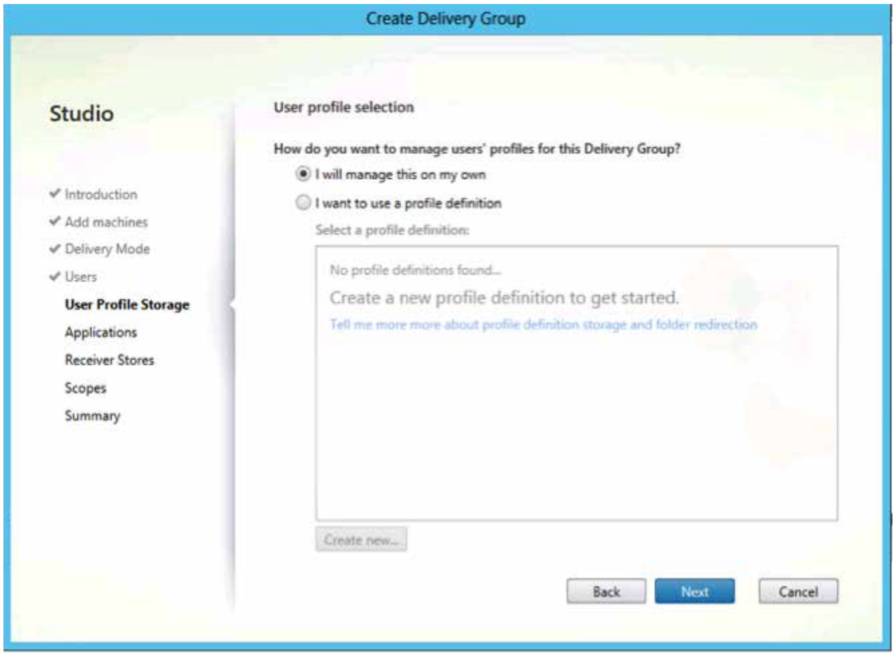
Select Users or Groups

Select this object type:
Users or Groups

From this location:
Entire Directory

Enter the object names to select (examples):
domain users

Create profile definitions.



Create Delivery Group

Studio

- ✓ Introduction
- ✓ Add machines
- ✓ Delivery Mode
- ✓ Users
- **User Profile Storage**
- Applications
- Receiver Stores
- Scopes
- Summary

User profile selection

How do you want to manage users' profiles for this Delivery Group?

● I will manage this on my own

○ I want to use a profile definition

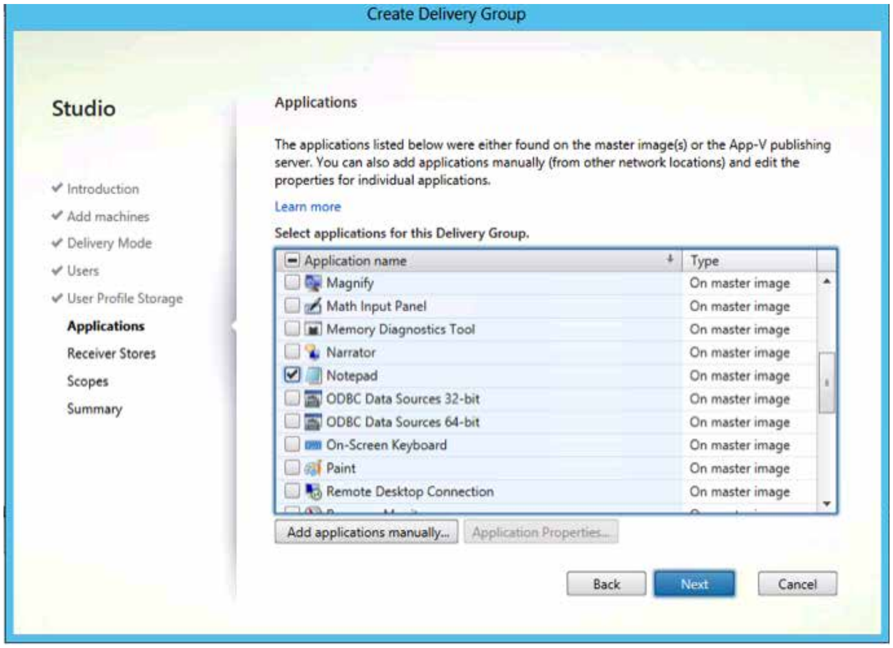
Select a profile definition:

No profile definitions found...

Create a new profile definition to get started.

Tell me more more about profile definition storage and folder redirection

Add applications.



Create Delivery Group

Studio

- ✓ Introduction
- ✓ Add machines
- ✓ Delivery Mode
- ✓ Users
- ✓ User Profile Storage
- **Applications**
- Receiver Stores
- Scopes
- Summary

Applications

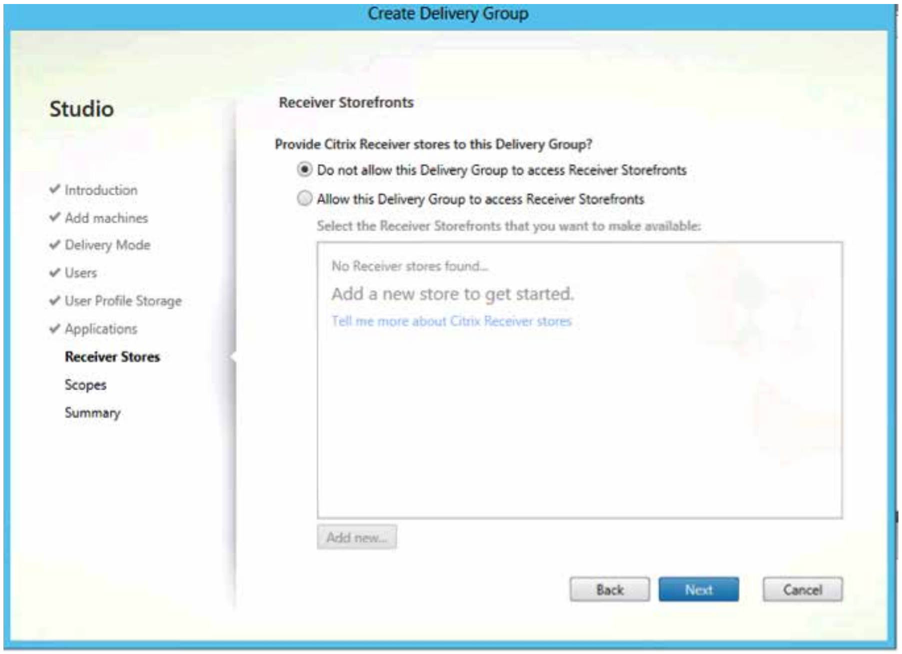
The applications listed below were either found on the master image(s) or the App-V publishing server. You can also add applications manually (from other network locations) and edit the properties for individual applications.

Learn more

Select applications for this Delivery Group.

☐ Application name	Type
☐ Magnify	On master image
☐ Math Input Panel	On master image
☐ Memory Diagnostics Tool	On master image
☐ Narrator	On master image
☑ Notepad	On master image
☐ ODBC Data Sources 32-bit	On master image
☐ ODBC Data Sources 64-bit	On master image
☐ On-Screen Keyboard	On master image
☐ Paint	On master image
☐ Remote Desktop Connection	On master image

Add StoreFront access for application access within hosted shared desktops.



Create Delivery Group

Receiver Storefronts

Provide Citrix Receiver stores to this Delivery Group?

● Do not allow this Delivery Group to access Receiver Storefronts

○ Allow this Delivery Group to access Receiver Storefronts

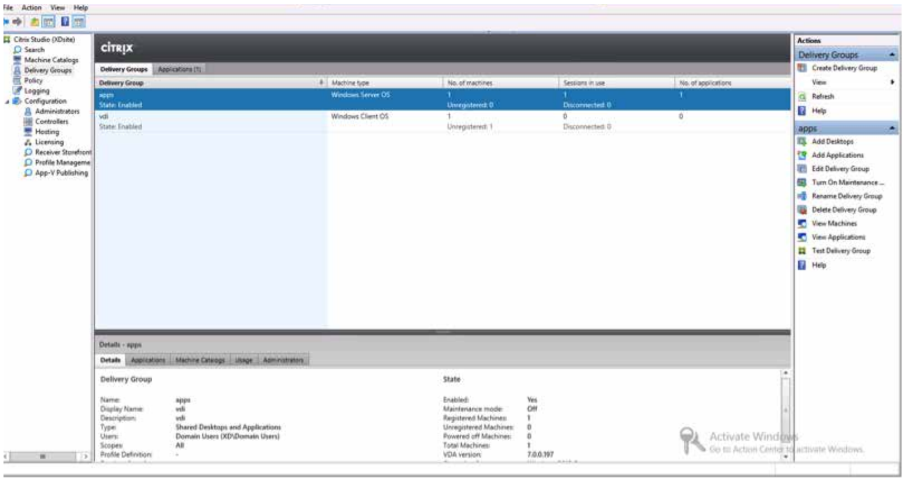
Select the Receiver Storefronts that you want to make available:

No Receiver stores found...

Add a new store to get started.

Tell me more about Citrix Receiver stores

Repeat as necessary for all delivery groups.



Delivery Group	Machine type	No. of machines	Sessions in use	No. of applications
apps State: Enabled	Windows Server OS	1 Unregistered: 0	1 Disconnected: 0	1
vdi State: Enabled	Windows Client OS	1 Unregistered: 1	0 Disconnected: 0	0

Details - apps

Delivery Group

Name: apps
Display Name: vdi
Description: vdi
Type: Shared Desktops and Applications
Users: Domain Users (XD\Domain Users)
Scopes: All
Profile Definition: -

State

Enabled: Yes
Maintenance mode: Off
Registered Machines: 1
Unregistered Machines: 0
Powered off Machines: 0
Total Machines: 1
VDA version: 7.0.0.197

At this point, XenDesktop and apps and desktops are configured. In the next section you'll install StoreFront to test the configuration.

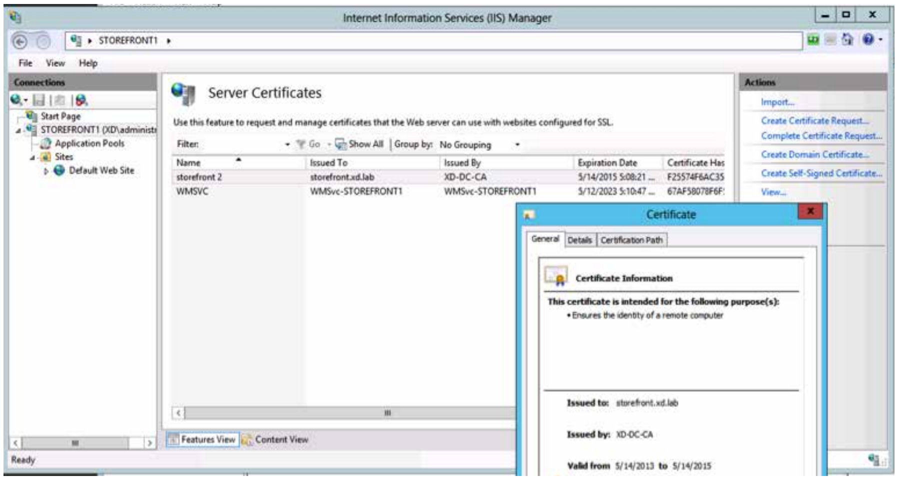
3.6 StoreFront configuration

Once StoreFront in installed, you must switch IIS to HTTPS before configuring StoreFront.

Go to IIS -> server certificates.

We will be using a domain certificate from the domain CA.

Import or create a web certificate for the URL that the clients will be using to access the environment. This certificate can be for the machine name. The URL that users will enter to access the environment will point to the load balancing server, so that server requires a matching certificate.



Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued By	Expiration Date	Certificate Has
storefront 2	storefront.xd.lab	XD-DC-CA	5/14/2015 5:08:21 ...	F25574F6AC35
WMSVC	WMSvc-STOREFRONT1	WMSvc-STOREFRONT1	5/12/2023 5:10:47 ...	67AF58078F6F:

This certificate is intended for the following purpose(s):

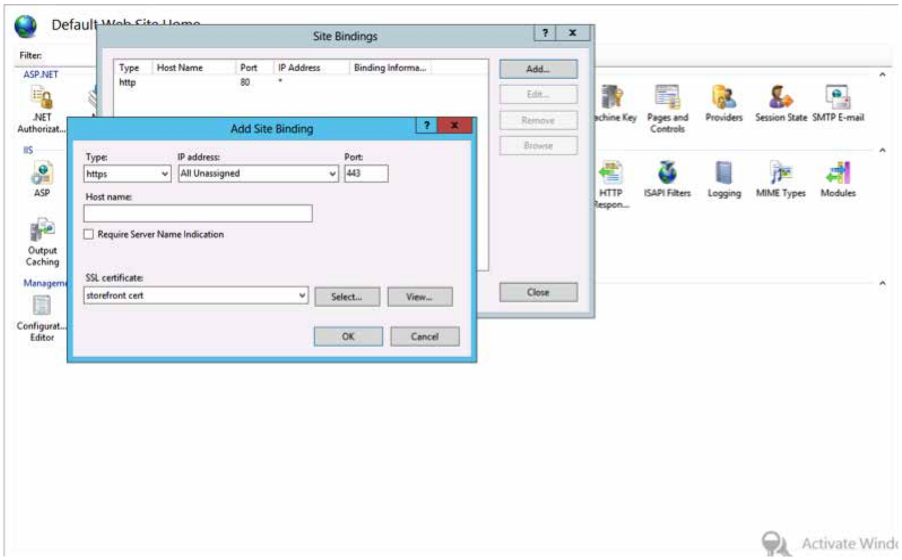
- Ensures the identity of a remote computer

Issued to: storefront.xd.lab

Issued by: XD-DC-CA

Valid from 5/14/2013 to 5/14/2015

Edit the site bindings and add an HTTPS binding using the certificate just added to IIS.



Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	

Type: https

IP address: All Unassigned

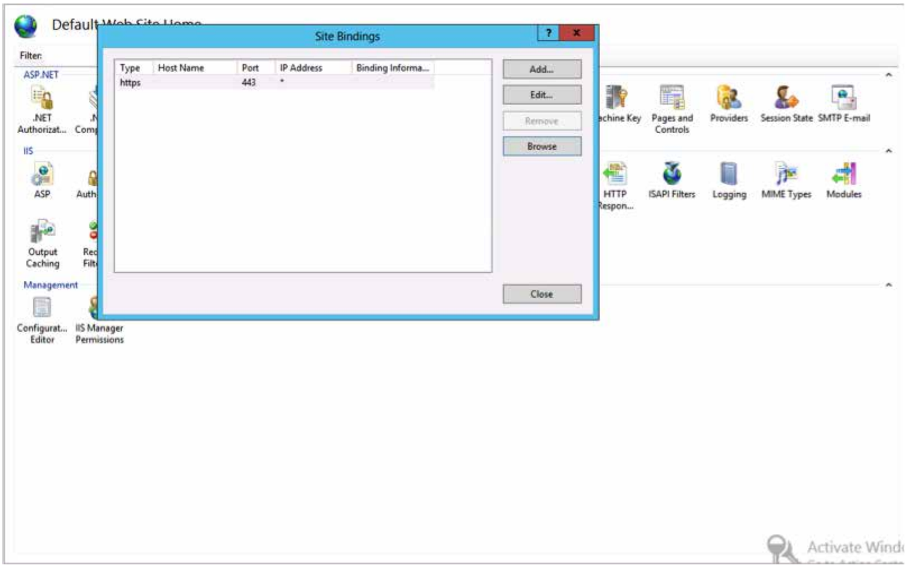
Port: 443

Host name:

□ Require Server Name Indication

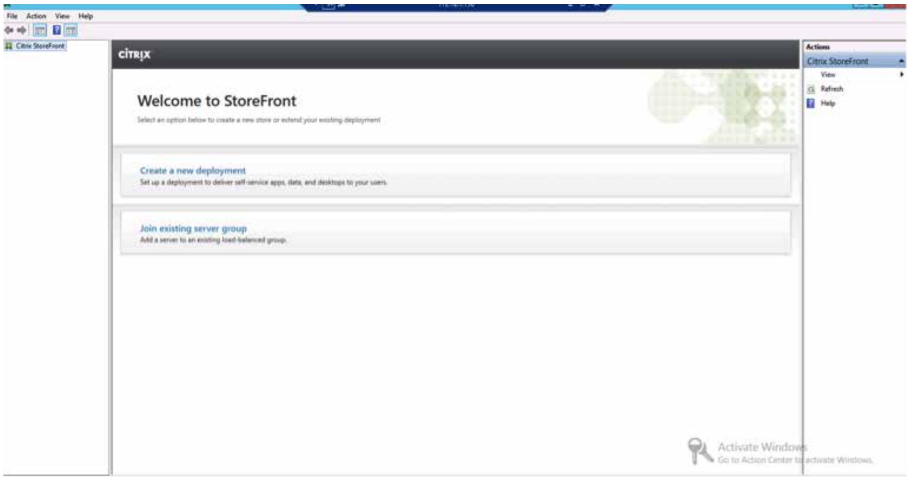
SSL certificate: storefront cert

Remove the HTTPS binding.



Type	Host Name	Port	IP Address	Binding Informa...
https		443	*	

Launch StoreFront MMC.



Welcome to StoreFront

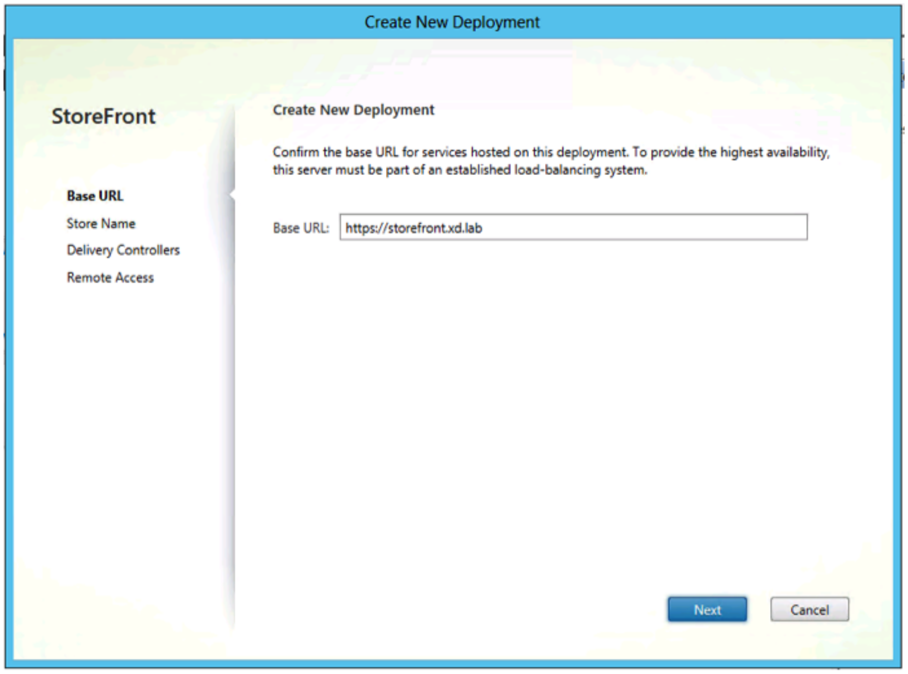
Select an option below to create a new store or extend your existing deployment

Create a new deployment
Set up a deployment to deliver self-service apps, data, and desktops to your users.

Join existing server group
Add a server to an existing load-balanced group.

Select **Create New Deployment.**

The Create New Deployment wizard will launch with HTTPS and the common name of the certificate as the base URL. This is the URL that users will enter to access the environment, and will eventually resolve to the Access Gateway IP address.



Create New Deployment

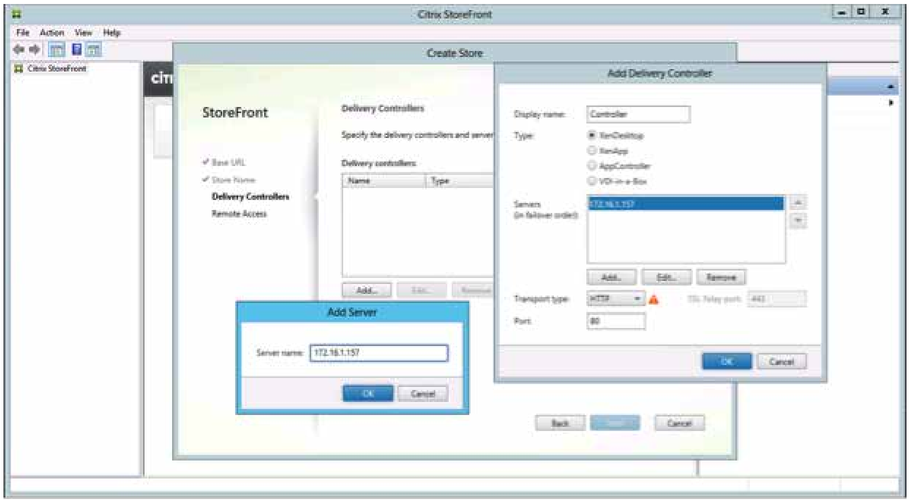
StoreFront

Create New Deployment

Confirm the base URL for services hosted on this deployment. To provide the highest availability, this server must be part of an established load-balancing system.

Base URL: https://storefront.xd.lab

Name the store and click **Next**. Enter the delivery controllers. In this case, we want to load balance the delivery controllers with NetScaler, so each delivery controller entered here will be the load balancing vServer VIP, not the actual DDCs. Even if you have not configured load balancing yet, as we don't, put in the IP of whatever the load balancing VIP will be when it is set up.



Citrix StoreFront

Create Store

StoreFront

Delivery Controllers

Specify the delivery controllers and server

Delivery controllers:

Name	Type

Add Delivery Controller

Display name: Controller

Type: ● XenDesktop ○ XenApp ○ AppController ○ VDI-in-a-Box

Servers (in failover order): 172.16.1.157

Transport type: HTTP

SSL Relay port: 443

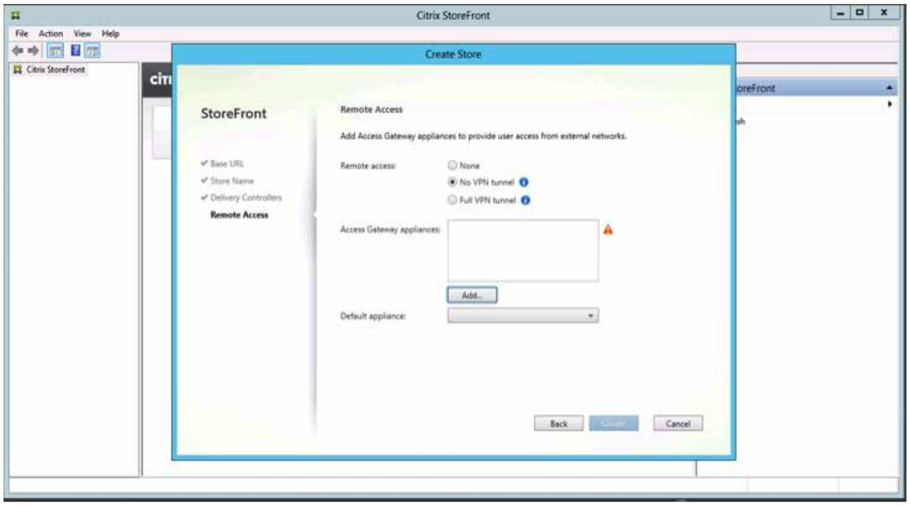
Port: 80

Add Server

Server name: 172.16.1.157

Access to the store typically does not need to be on SSL because it is completely internal traffic; however, SSL can be used if the DDCs and the load balancing vServer have certificates.

On the Remote Access page, select **No VPN tunnel** to specify the use of Access Gateway in ICA proxy mode. Click **Add**.



Remote Access

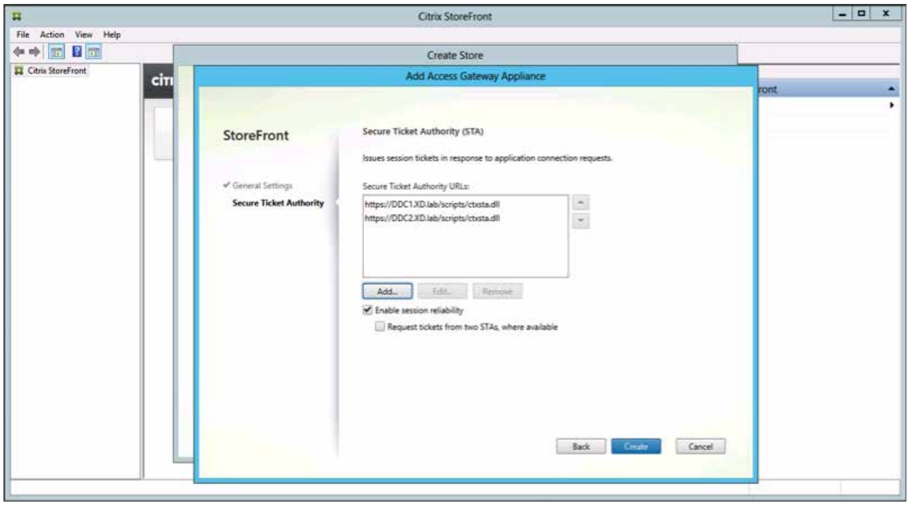
Add Access Gateway appliances to provide user access from external networks.

Remote access: ○ None ● No VPN tunnel ○ Full VPN tunnel

Access Gateway appliances:

Default appliance:

Add the two DDCs as Secure Ticket Authorities (STAs).



Secure Ticket Authority (STA)

Issues session tickets in response to application connection requests.

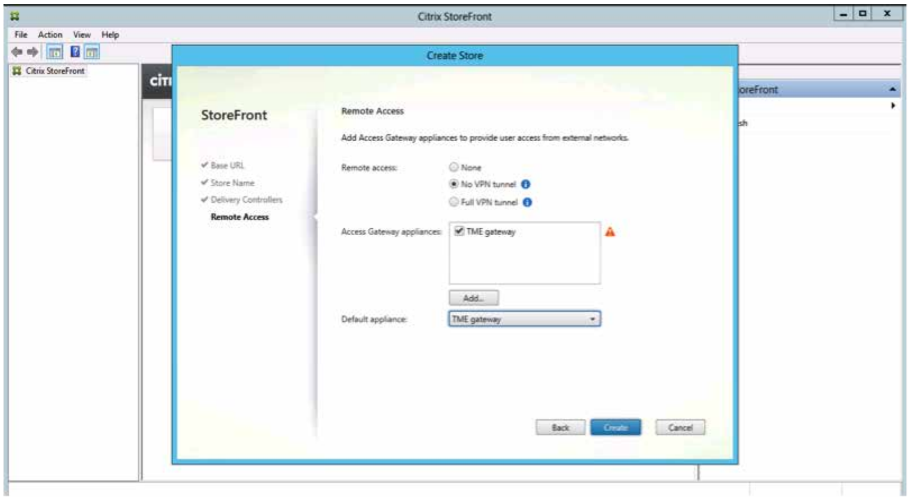
Secure Ticket Authority URLs:

https://DDC1.XD.lab/scripts/ctxsta.dll
https://DDC2.XD.lab/scripts/ctxsta.dll

☑ Enable session reliability

☐ Request tickets from two STAs, where available

Click **Create** and Access Gateway will appear in the list of appliances.



Remote Access

Add Access Gateway appliances to provide user access from external networks.

Remote access: ○ None ● No VPN tunnel ○ Full VPN tunnel

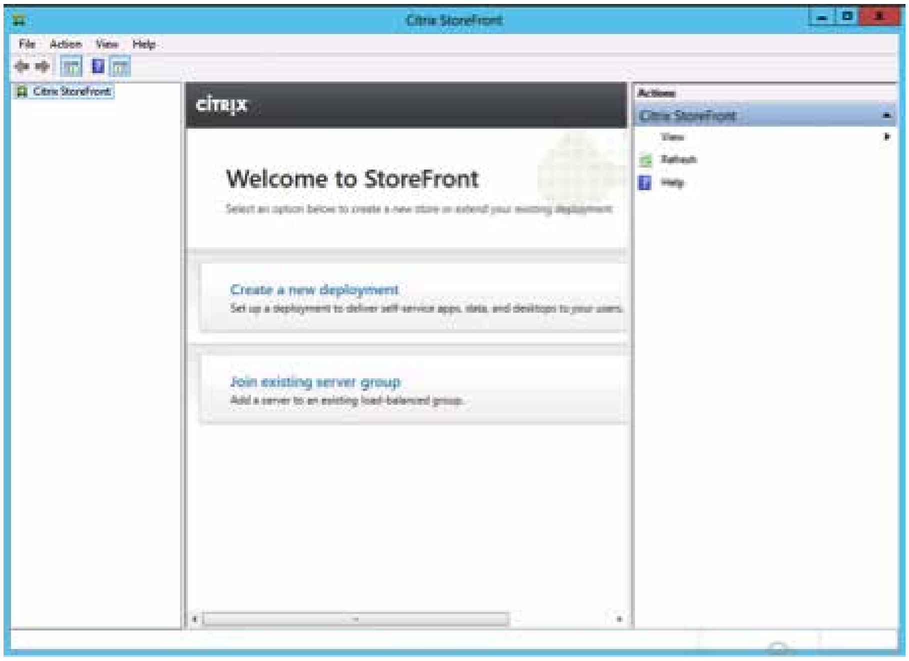
Access Gateway appliances: ☑ TME gateway

Default appliance: TME gateway

Click **Create** and the store will be configured. The authentication, stores, Receiver for Web and Access Gateway should all be configured and visible from the StoreFront MMC.

3.7 Adding StoreFront servers to the deployment

To add servers to the existing StoreFront deployment, open the StoreFront MMC on the machine you wish to add and click **Join existing server group**.



Welcome to StoreFront

Select an option below to create a new store or extend your existing deployment

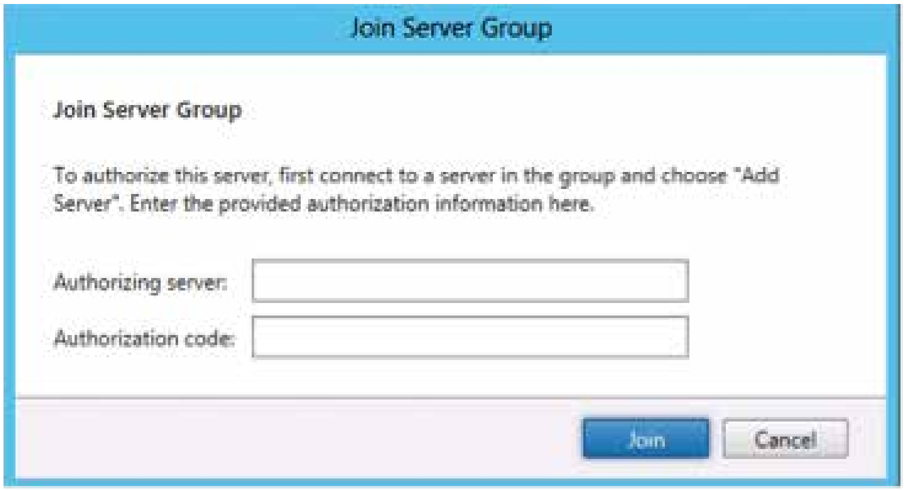
Create a new deployment

Set up a deployment to deliver self-service apps, data, and desktops to your users.

Join existing server group

Add a server to an existing load-balanced group.

The server will ask for the name and code of an authorizing server.



Join Server Group

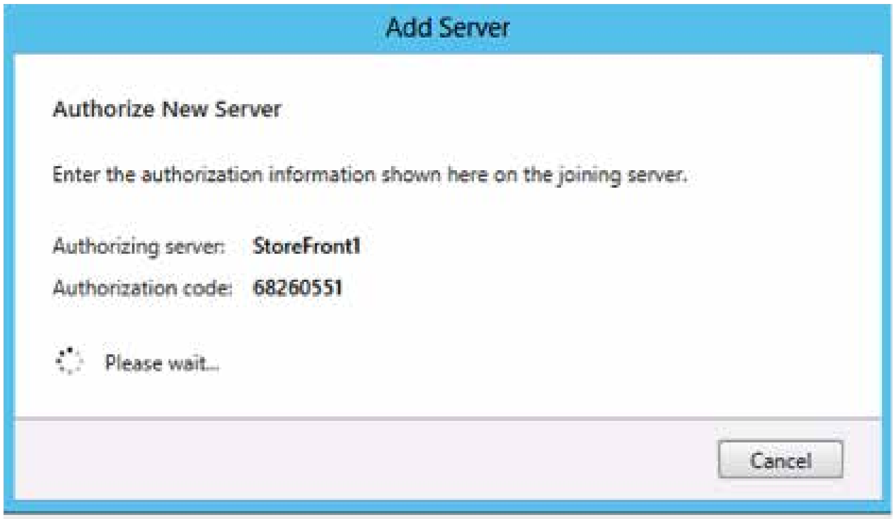
Join Server Group

To authorize this server, first connect to a server in the group and choose "Add Server". Enter the provided authorization information here.

Authorizing server:

Authorization code:

A code for authorizing a new server will be generated. Enter this code on the server you want to join the deployment.



Add Server

Authorize New Server

Enter the authorization information shown here on the joining server.

Authorizing server: StoreFront1

Authorization code: 68260551

Please wait...

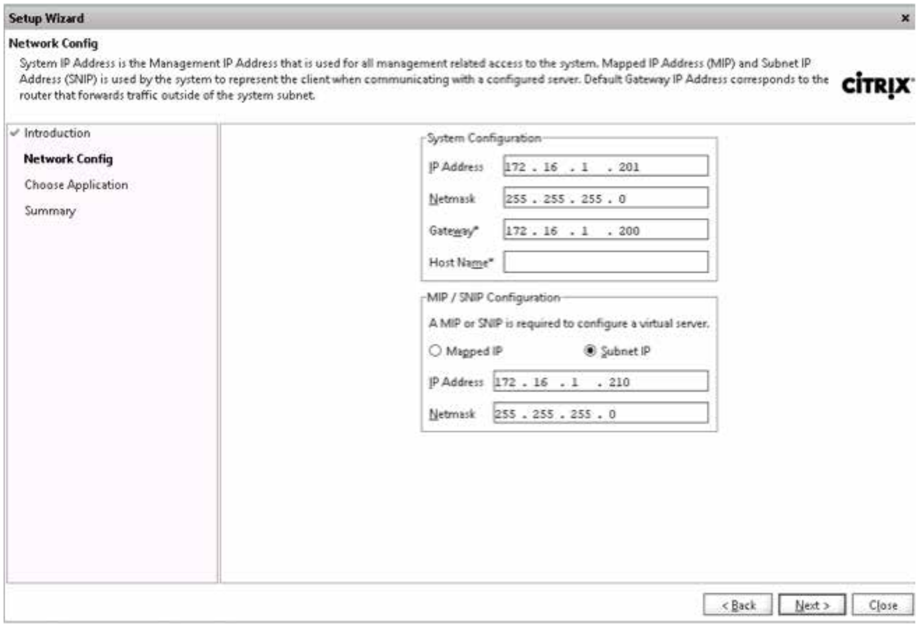
The server will join the deployment. Click **OK**.

Citrix NetScaler

4. NetScaler configuration

4.1 Initial configuration

Once NetScaler is licensed, run the setup wizard to configure the IP address that will be used for communication with internal servers.



Setup Wizard

Network Config

System IP Address is the Management IP Address that is used for all management related access to the system. Mapped IP Address (MIP) and Subnet IP Address (SNIP) is used by the system to represent the client when communicating with a configured server. Default Gateway IP Address corresponds to the router that forwards traffic outside of the system subnet.

System Configuration

IP Address: 172 . 16 . 1 . 201

Netmask: 255 . 255 . 255 . 0

Gateway*: 172 . 16 . 1 . 200

Host Name*:

MIP / SNIP Configuration

A MIP or SNIP is required to configure a virtual server.

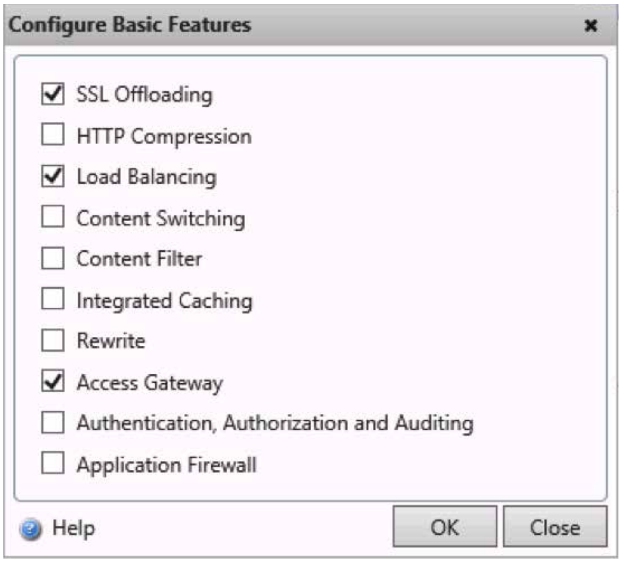
○ Mapped IP ● Subnet IP

IP Address: 172 . 16 . 1 . 210

Netmask: 255 . 255 . 255 . 0

In this deployment we've chosen to skip the configuration wizard for load balancing XenApp and XenDesktop and perform these configurations manually instead. Once the initial setup wizard is complete, go to Network/IPs and confirm that the SNIP is set correctly.

Go to system/settings and configure basic features.

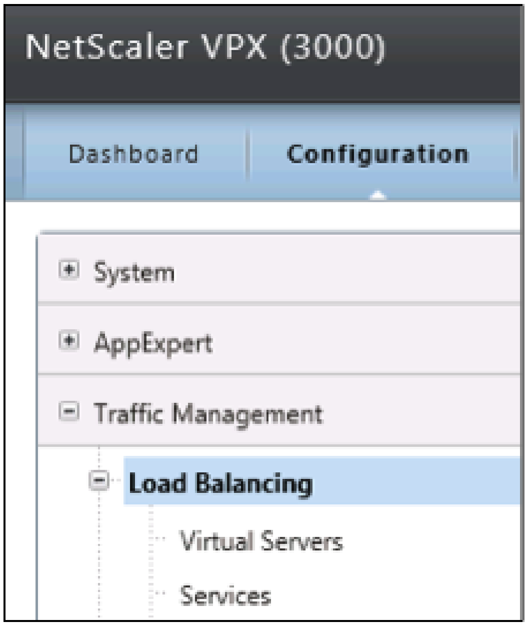


Configure Basic Features

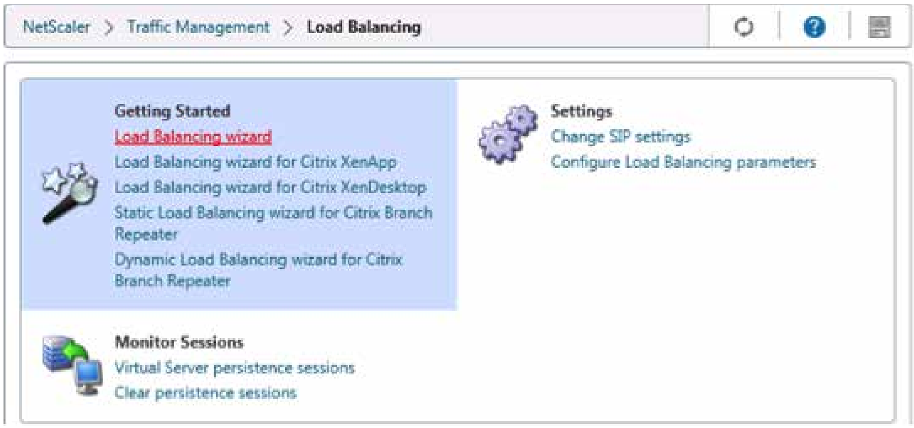
☑ SSL Offloading
☐ HTTP Compression
☑ Load Balancing
☐ Content Switching
☐ Content Filter
☐ Integrated Caching
☐ Rewrite
☑ Access Gateway
☐ Authentication, Authorization and Auditing
☐ Application Firewall

4.2 Load balancing StoreFront—wizard

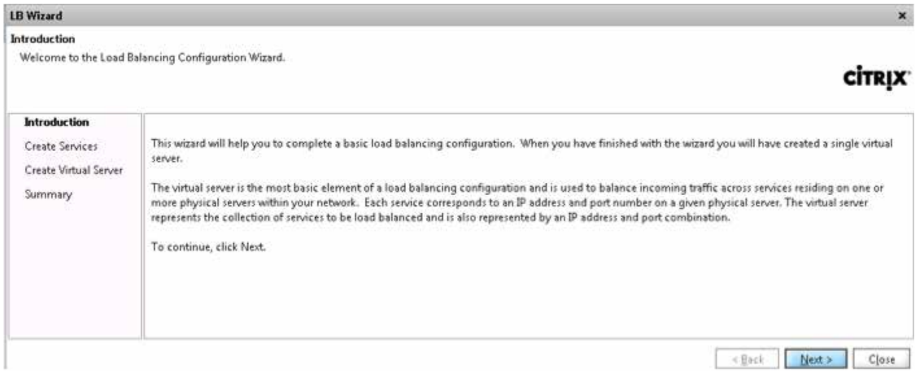
From the navigation tree on the left, select **Traffic Management** and click on **Load Balancing**.



Click **Load Balancing wizard**.


NetScaler > Traffic Management > Load Balancing
Getting Started
Load Balancing wizard
Load Balancing wizard for Citrix XenApp
Load Balancing wizard for Citrix XenDesktop
Static Load Balancing wizard for Citrix Branch Repeater
Dynamic Load Balancing wizard for Citrix Branch Repeater
Settings
Change SIP settings
Configure Load Balancing parameters
Monitor Sessions
Virtual Server persistence sessions
Clear persistence sessions

Click **Next** on the **Introduction** screen.



LB Wizard

Introduction

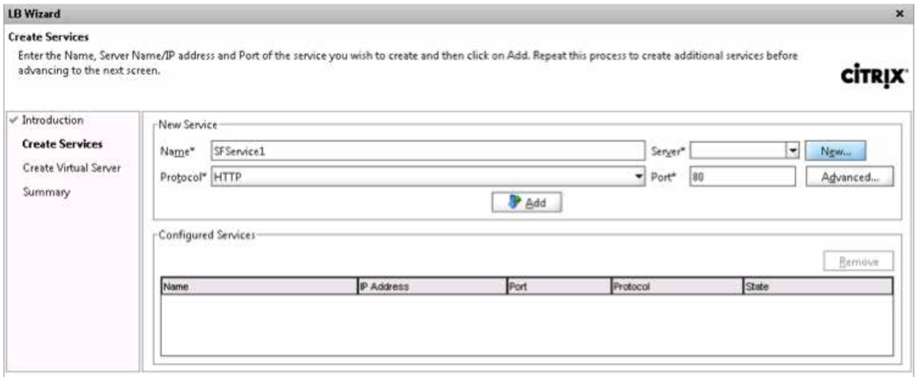
Welcome to the Load Balancing Configuration Wizard.

This wizard will help you to complete a basic load balancing configuration. When you have finished with the wizard you will have created a single virtual server.

The virtual server is the most basic element of a load balancing configuration and is used to balance incoming traffic across services residing on one or more physical servers within your network. Each service corresponds to an IP address and port number on a given physical server. The virtual server represents the collection of services to be load balanced and is also represented by an IP address and port combination.

To continue, click Next.

Enter **SFService1** for the **Name** and click the **New** button.



LB Wizard

Create Services

Enter the Name, Server Name/IP address and Port of the service you wish to create and then click on Add. Repeat this process to create additional services before advancing to the next screen.

New Service

Name* SFService1

Server*

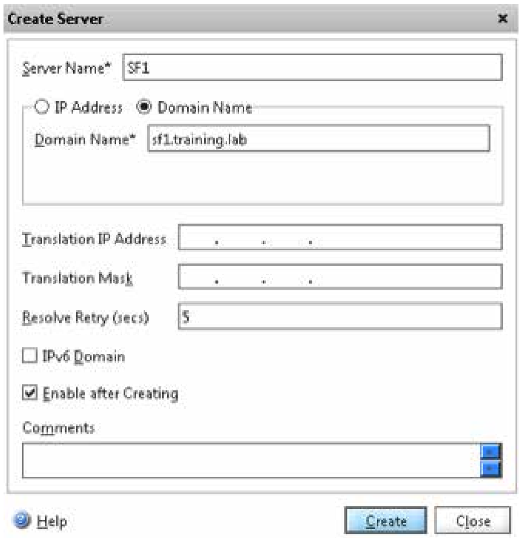
Protocol* HTTP

Port* 80

Configured Services

Name	IP Address	Port	Protocol	State

Enter **SF1** for the server name, click **Domain Name** and enter **storefront1.xd.lab**. Then click **Create**.



Create Server

Server Name* SF1

○ IP Address ● Domain Name

Domain Name* sf1.training.lab

Translation IP Address . . .

Translation Mask . . .

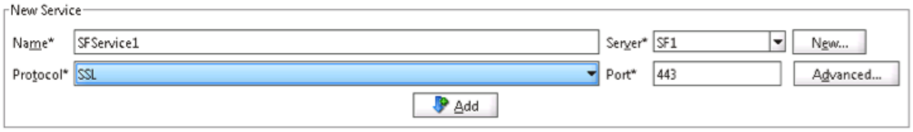
Resolve Retry (secs) 5

☐ IPv6 Domain

☑ Enable after Creating

Comments

Select **SSL** for the protocol.



New Service

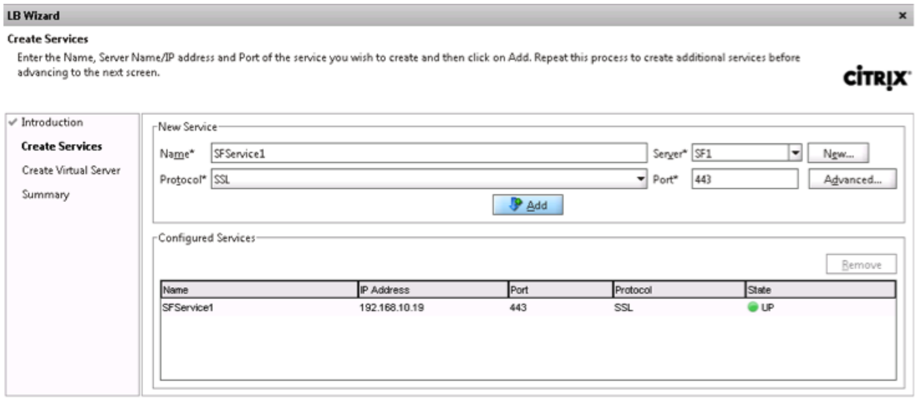
Name* SFService1

Server* SF1

Protocol* SSL

Port* 443

Click the **Add** button to add in the first service.



LB Wizard

Create Services

Enter the Name, Server Name/IP address and Port of the service you wish to create and then click on Add. Repeat this process to create additional services before advancing to the next screen.

- ✓ Introduction
- **Create Services**
- Create Virtual Server
- Summary

New Service

Name* SFService1

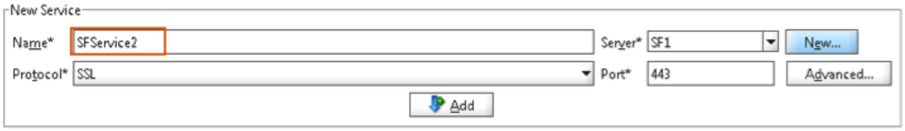
Server* SF1

Protocol* SSL

Port* 443

Name	IP Address	Port	Protocol	State
SFService1	192.168.10.19	443	SSL	● UP

Enter **SFService2** for the name and click the **New** button.



New Service

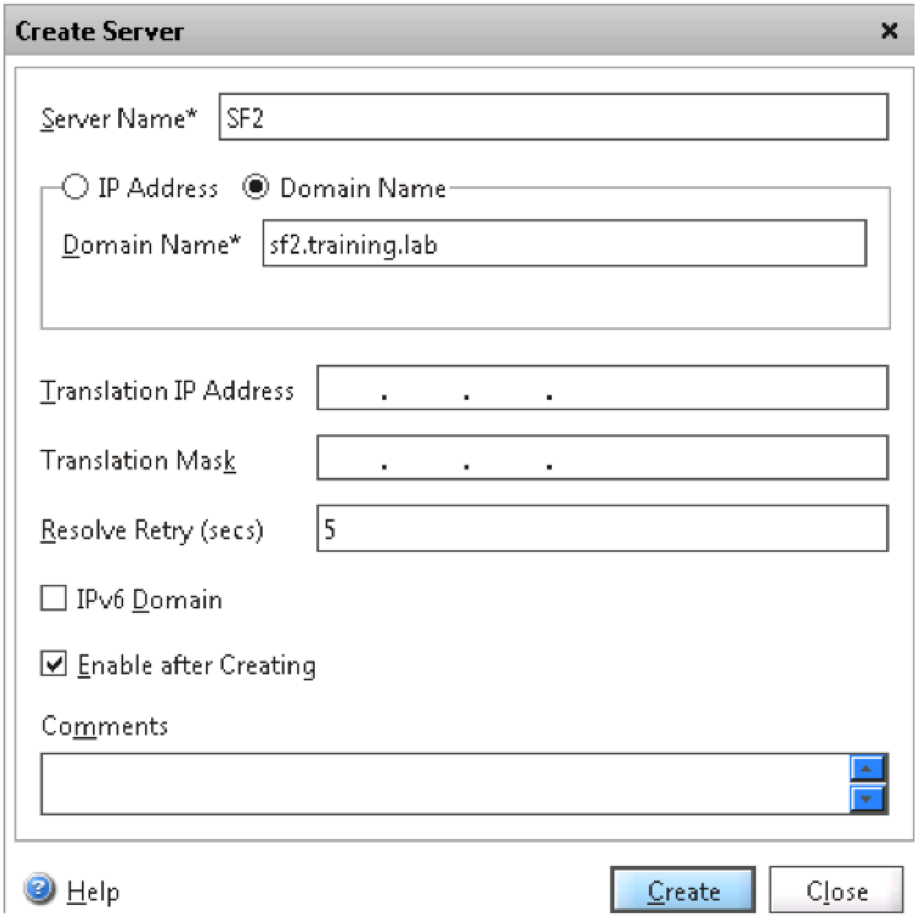
Name* SFService2

Server* SF1

Protocol* SSL

Port* 443

Enter **SF2** for the server name, click **Domain Name** and enter **storefront2.xd.lab**. Then click **Create**.



Create Server

Server Name* SF2

○ IP Address ● Domain Name

Domain Name* sf2.training.lab

Translation IP Address . . .

Translation Mask . . .

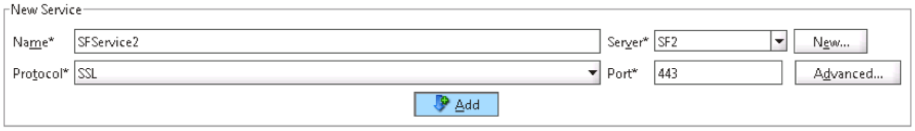
Resolve Retry (secs) 5

□ IPv6 Domain

☑ Enable after Creating

Comments

Click the **Add** button to add in the second service.



New Service

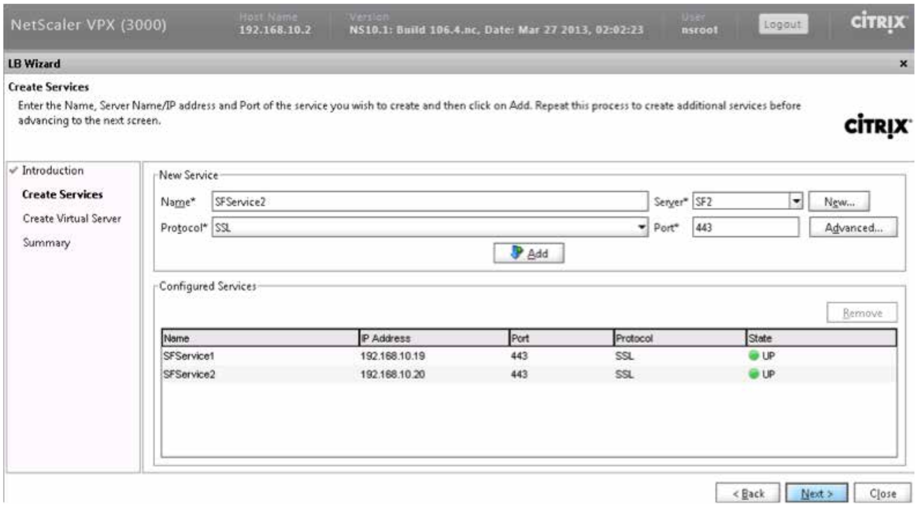
Name* SFService2

Server* SF2

Protocol* SSL

Port* 443

Click **Next**.



Create Services

Enter the Name, Server Name/IP address and Port of the service you wish to create and then click on Add. Repeat this process to create additional services before advancing to the next screen.

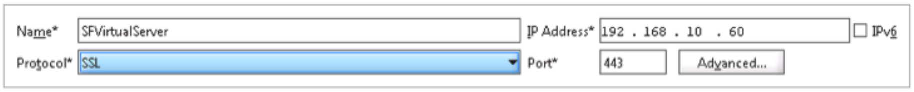
New Service

Name* SFService2
Server* SF2
Protocol* SSL
Port* 443

Configured Services

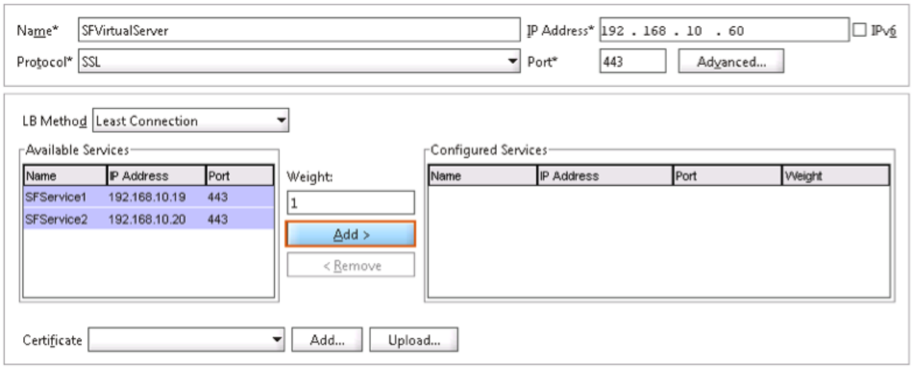
Name	IP Address	Port	Protocol	State
SFService1	192.168.10.19	443	SSL	● UP
SFService2	192.168.10.20	443	SSL	● UP

Enter **StoreFrontLB** for the name and **172.16.1.156** for the IP address. Select **SSL** for the protocol.



Name* SFVirtualServer
IP Address* 192 . 168 . 10 . 60
□ IPv6
Protocol* SSL
Port* 443

Select both services and click **Add**.



Name* SFVirtualServer
IP Address* 192 . 168 . 10 . 60
□ IPv6
Protocol* SSL
Port* 443

LB Method Least Connection

Available Services

Name	IP Address	Port
SFService1	192.168.10.19	443
SFService2	192.168.10.20	443

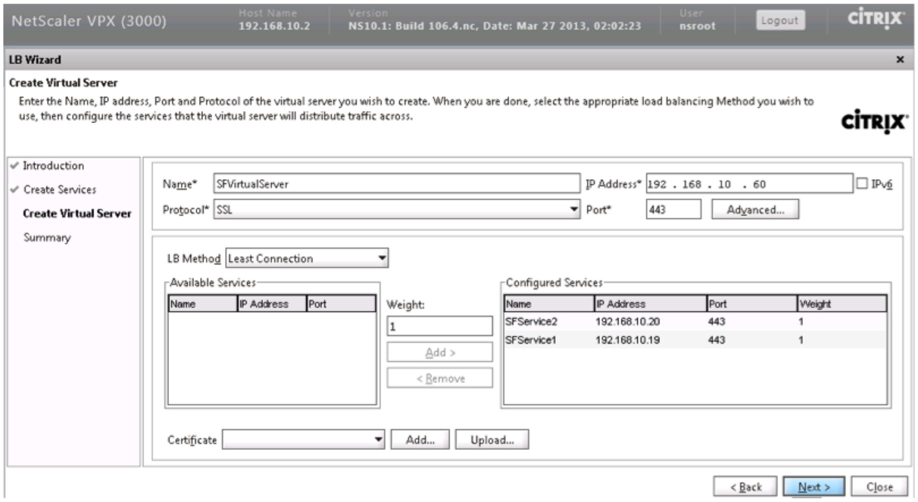
Weight: 1

Configured Services

Name	IP Address	Port	Weight

Certificate

Click **Next**.



Host Name 192.168.10.2
Version NS10.1: Build 106.4.nc, Date: Mar 27 2013, 02:02:23
User nsroot

LB Wizard

Create Virtual Server

Enter the Name, IP address, Port and Protocol of the virtual server you wish to create. When you are done, select the appropriate load balancing Method you wish to use, then configure the services that the virtual server will distribute traffic across.

Name* SFVirtualServer
IP Address* 192 . 168 . 10 . 60
□ IPv6
Protocol* SSL
Port* 443
LB Method Least Connection
Weight: 1
Certificate

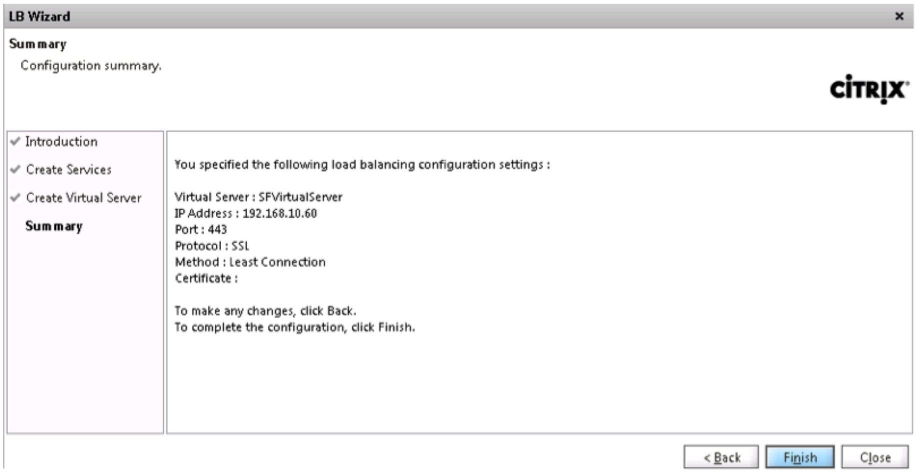
Available Services

Name	IP Address	Port

Configured Services

Name	IP Address	Port	Weight
SFService2	192.168.10.20	443	1
SFService1	192.168.10.19	443	1

Click **Finish** to complete the wizard. Then click **Exit**.



LB Wizard

Summary

Configuration summary.

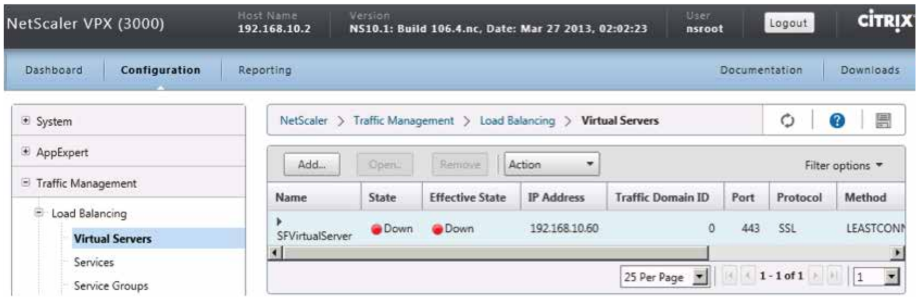
You specified the following load balancing configuration settings :

Virtual Server : SFVirtualServer
IP Address : 192.168.10.60
Port : 443
Protocol : SSL
Method : Least Connection
Certificate :

To make any changes, click Back.
To complete the configuration, click Finish.

It is normal for the StoreFront virtual server to be in a down state at this point. We have created an SSL server but not added a certificate, causing the server to be in a down state. A certificate will be added next.

Under Load Balancing > Virtual Servers, double-click the new entry of **SFVirtualServer** that was created.



NetScaler VPX (3000)

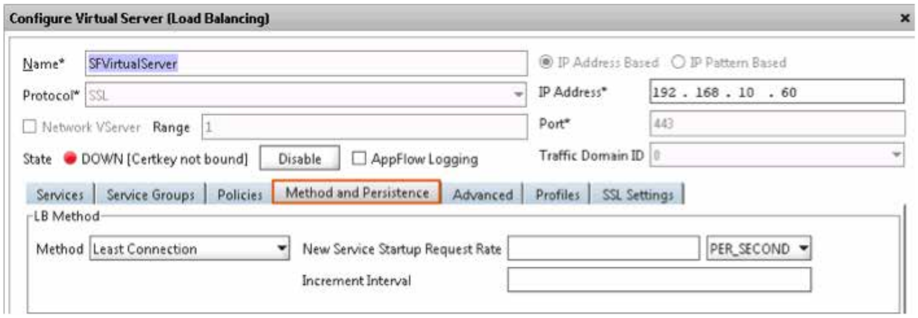
Host Name 192.168.10.2

Version NS10.1: Build 106.4.nc, Date: Mar 27 2013, 02:02:23

User nsroot

Name	State	Effective State	IP Address	Traffic Domain ID	Port	Protocol	Method
SFVirtualServer	● Down	● Down	192.168.10.60	0	443	SSL	LEASTCONN

Click the **Method and Persistence** tab.



Name* SFVirtualServer

◉ IP Address Based ○ IP Pattern Based

Protocol* SSL

IP Address* 192 . 168 . 10 . 60

□ Network VServer Range 1

Port* 443

State ● DOWN [Certkey not bound]

□ AppFlow Logging

Traffic Domain ID 0

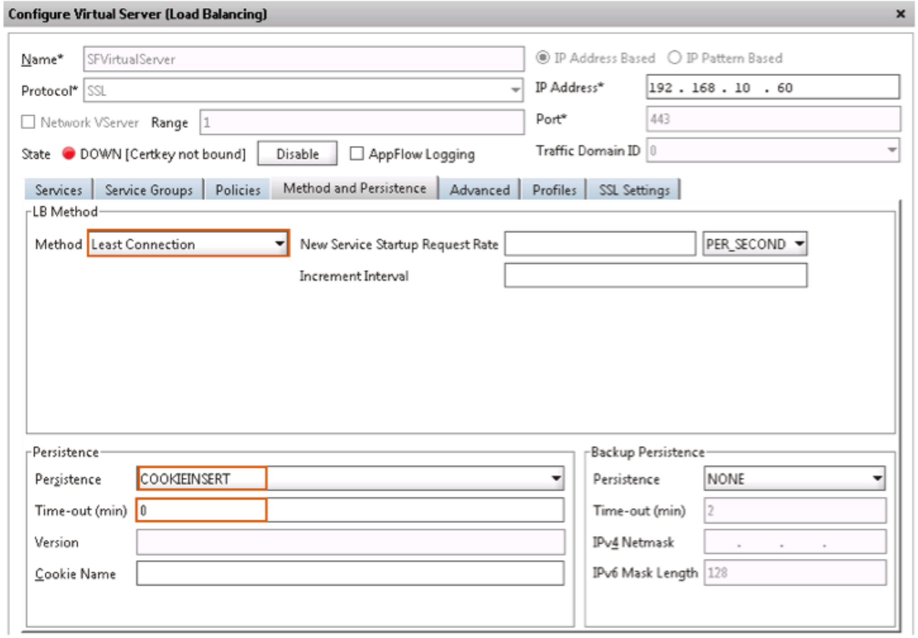
LB Method

Method Least Connection

New Service Startup Request Rate PER_SECOND

Increment Interval

Ensure the method is set to **Least Connection**, persistence is set to **COOKIEINSERT** and time-out value is set to 0.



Name* SFVirtualServer

◉ IP Address Based ○ IP Pattern Based

Protocol* SSL

IP Address* 192 . 168 . 10 . 60

□ Network VServer Range 1

Port* 443

State ● DOWN [Certkey not bound]

□ AppFlow Logging

Traffic Domain ID 0

LB Method

Method Least Connection

New Service Startup Request Rate PER_SECOND

Increment Interval

Persistence

Persistence COOKIEINSERT

Time-out (min) 0

Version

Cookie Name

Backup Persistence

Persistence NONE

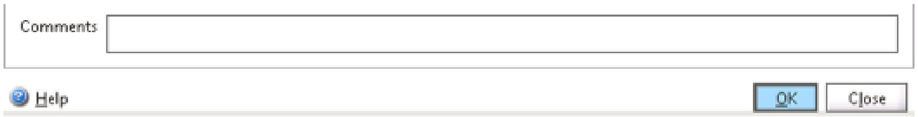
Time-out (min) 2

IPv4 Netmask . . .

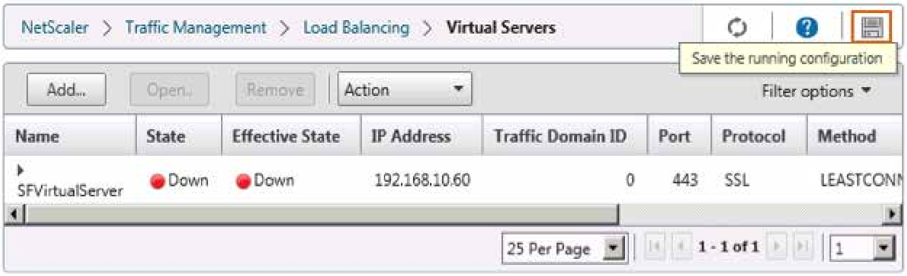
IPv6 Mask Length 128

NOTE: This will result in fair-share load balancing between the two servers and ensure that open connections between clients persist to the same backend server. A time-out of 0 means that the session will only remain valid as long as the browser is open.

Click **OK**.

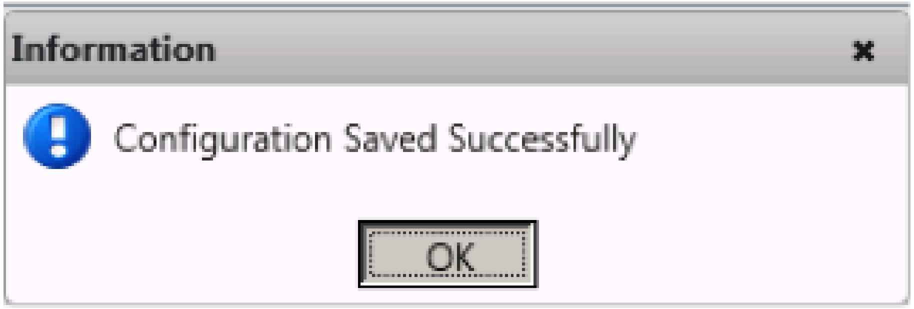


Click the **disk icon** towards the top right and then **Yes** to save the running state to disk.


NetScaler > Traffic Management > Load Balancing > Virtual Servers
Save the running configuration
Add...
Open...
Remove
Action
Filter options
25 Per Page
1 - 1 of 1
1

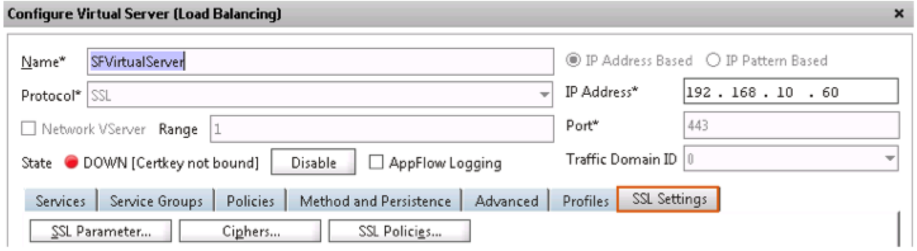
Name	State	Effective State	IP Address	Traffic Domain ID	Port	Protocol	Method
SFVirtualServer	● Down	● Down	192.168.10.60	0	443	SSL	LEASTCONN

Click **OK** on the confirmation.



Configuration Saved Successfully

Click the **SSL Settings** tab.



Name* SFVirtualServer

Protocol* SSL

□ Network VServer Range 1

State ● DOWN [Certkey not bound]

□ AppFlow Logging

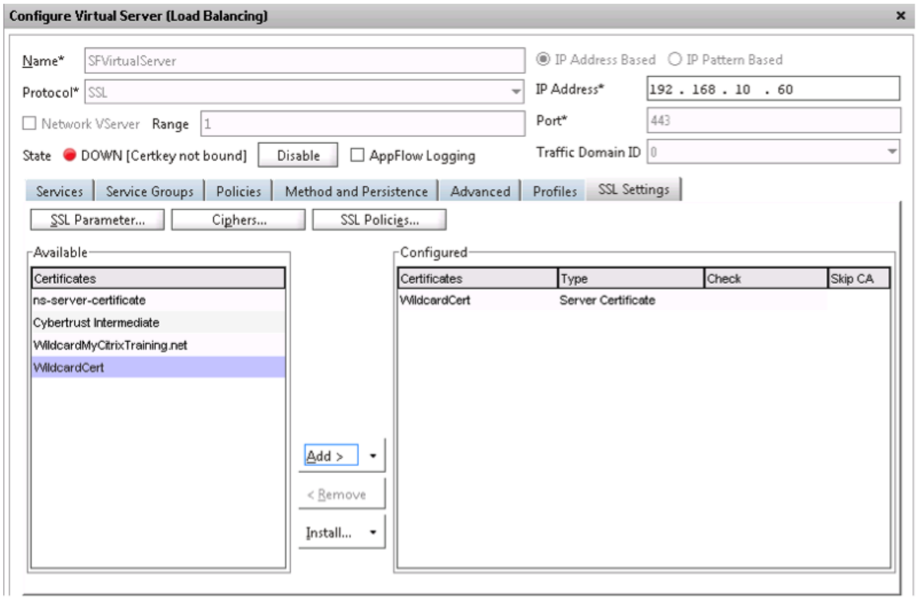
● IP Address Based ○ IP Pattern Based

IP Address* 192 . 168 . 10 . 60

Port* 443

Traffic Domain ID 0

Click **WildcardCert** and click **Add**.



Configure Virtual Server (Load Balancing)

Name* SFVirtualServer

● IP Address Based ○ IP Pattern Based

Protocol* SSL

IP Address* 192 . 168 . 10 . 60

□ Network VServer Range 1

Port* 443

State ● DOWN [Certkey not bound]

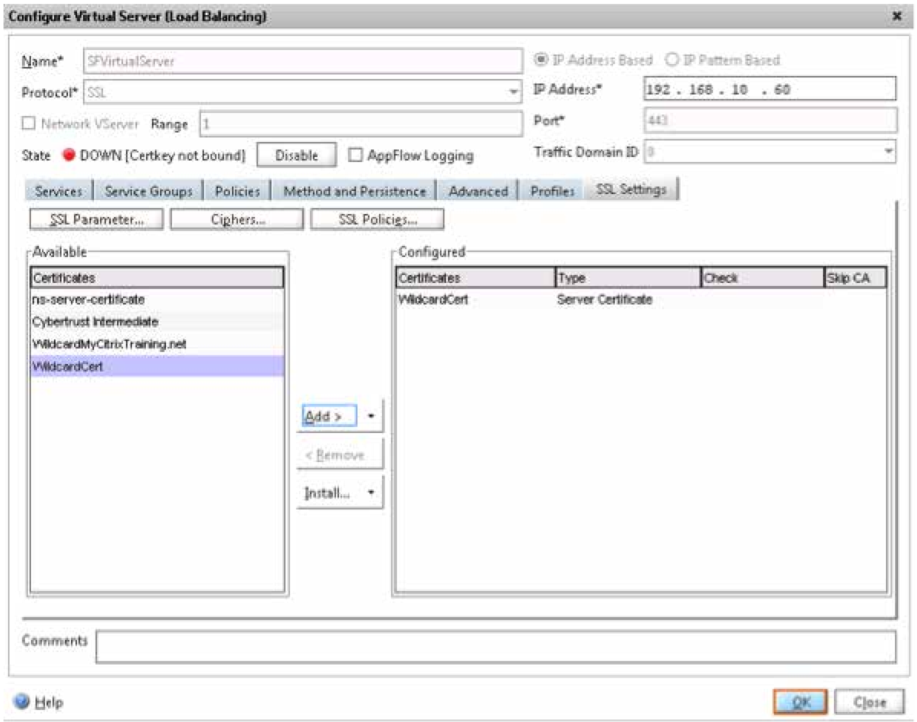
□ AppFlow Logging

Traffic Domain ID 0

Certificates
ns-server-certificate
Cybertrust Intermediate
WildcardMyCitrixTraining.net
WildcardCert

Certificates	Type	Check	Skip CA
WildcardCert	Server Certificate		

Click **OK**.



Configure Virtual Server (Load Balancing)

Name* SFVirtualServer

● IP Address Based ○ IP Pattern Based

Protocol* SSL

IP Address* 192 . 168 . 10 . 60

□ Network VServer Range 1

Port* 443

State ● DOWN [Certkey not bound]

□ AppFlow Logging

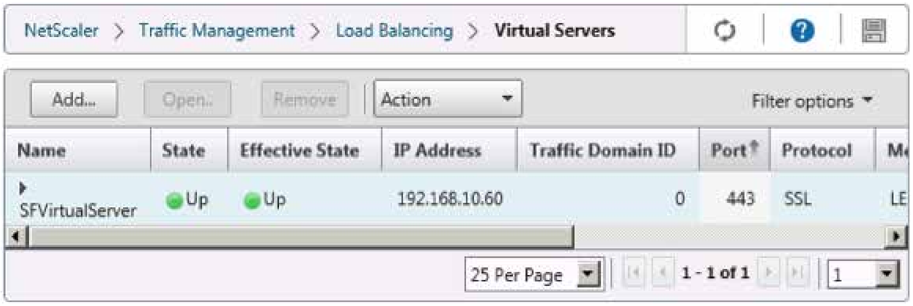
Traffic Domain ID 0

Certificates
ns-server-certificate
Cybertrust Intermediate
WildcardMyCitrixTraining.net
WildcardCert

Certificates	Type	Check	Skip CA
WildcardCert	Server Certificate		

Comments

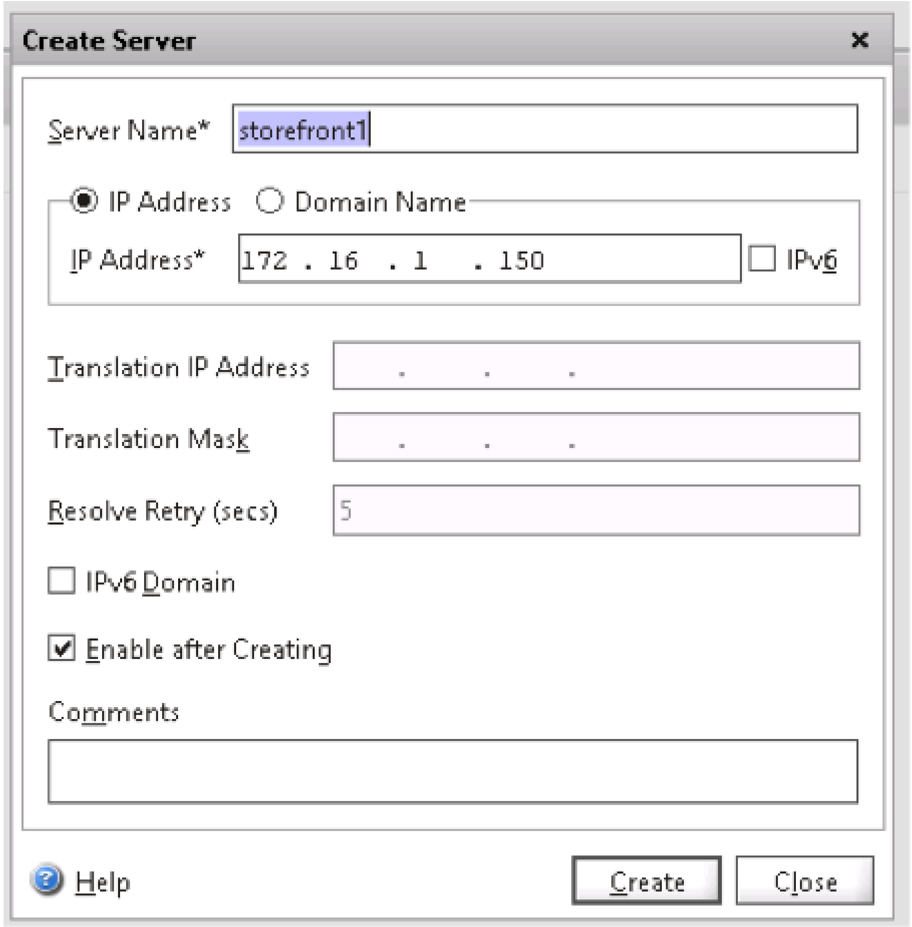
The **SFVirtualServer** should now show as Up.


NetScaler > Traffic Management > Load Balancing > Virtual Servers
Add...
Open...
Remove
Action
Filter options
25 Per Page
1 - 1 of 1
1

Name	State	Effective State	IP Address	Traffic Domain ID	Port	Protocol	Me
SFVirtualServer	● Up	● Up	192.168.10.60	0	443	SSL	LE

4.3 Load balancing StoreFront—manual setup

In this section we configure load balancing for the StoreFront servers. Go to load balancing/servers and click **Add** to add the two StoreFront servers.



Server Name* storefront1

● IP Address ○ Domain Name

IP Address* 172 . 16 . 1 . 150 □ IPv6

Translation IP Address . . .

Translation Mask . . .

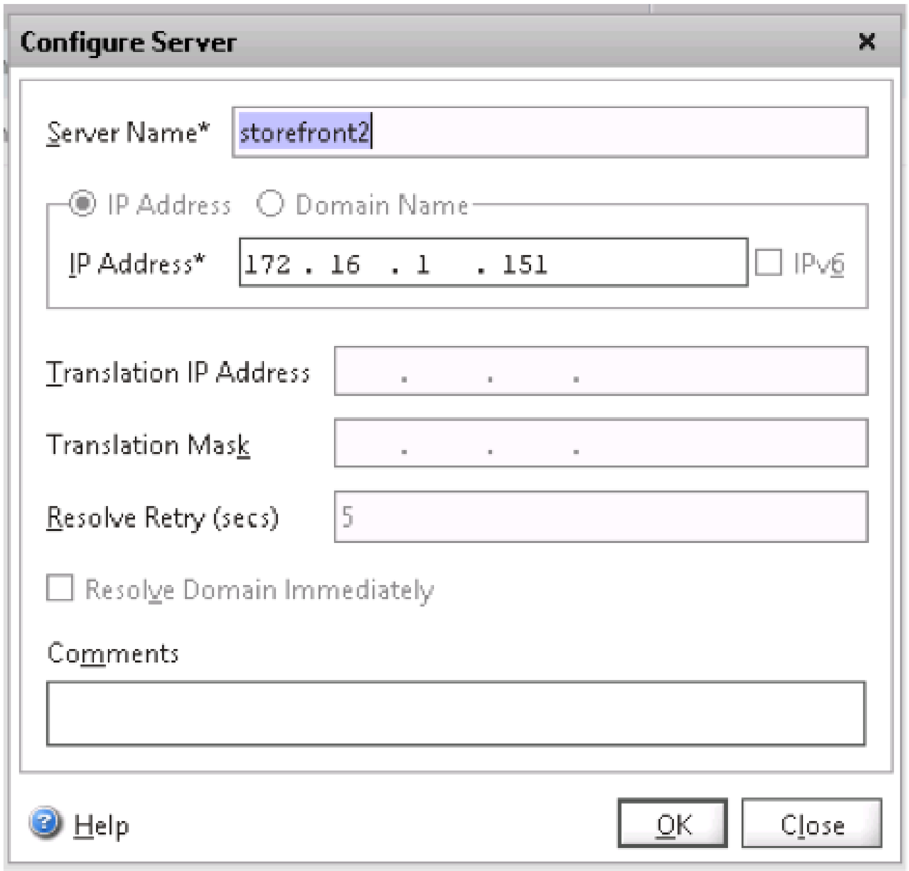
Resolve Retry (secs) 5

□ IPv6 Domain

☑ Enable after Creating

Comments

Repeat for SF2.



Server Name* storefront2

● IP Address ○ Domain Name

IP Address* 172 . 16 . 1 . 151 □ IPv6

Translation IP Address . . .

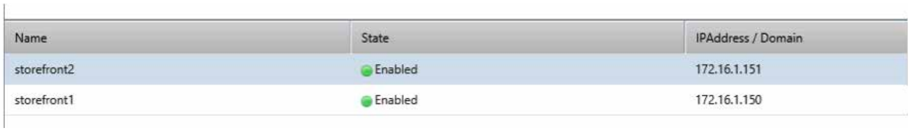
Translation Mask . . .

Resolve Retry (secs) 5

□ Resolve Domain Immediately

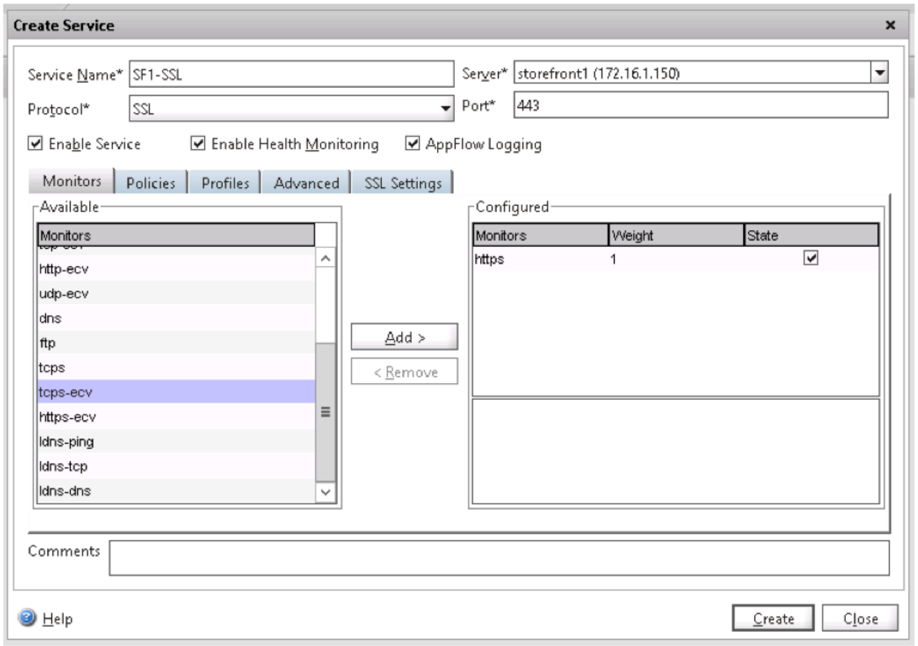
Comments

Both servers should be enabled in the list of servers.



Name	State	IPAddress / Domain
storefront2	● Enabled	172.16.1.151
storefront1	● Enabled	172.16.1.150

Next create the SSL service on these servers. This will be the web traffic going to the StoreFront servers.



Create Service

Service Name* SF1-SSL

Server* storefront1 (172.16.1.150)

Protocol* SSL

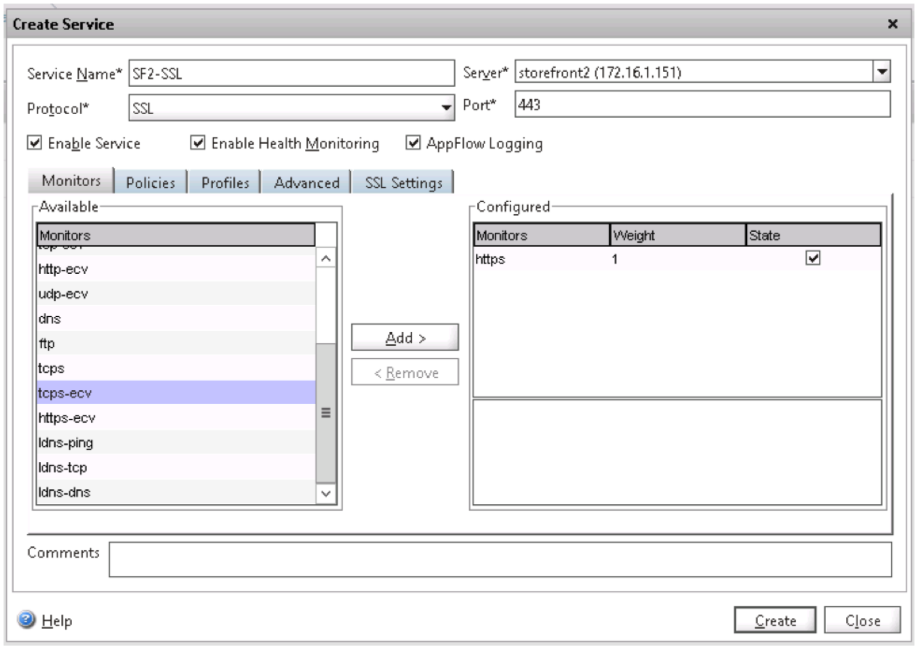
Port* 443

☑ Enable Service ☑ Enable Health Monitoring ☑ AppFlow Logging

Monitors	Weight	State
https	1	☑

Comments

Repeat for SF2.



Create Service

Service Name* SF2-SSL

Server* storefront2 (172.16.1.151)

Protocol* SSL

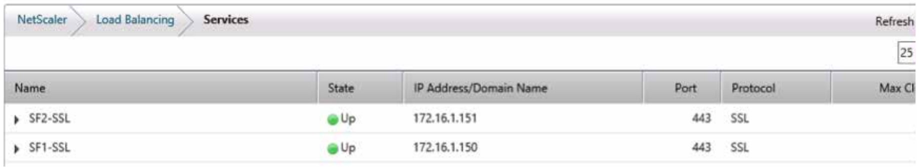
Port* 443

☑ Enable Service ☑ Enable Health Monitoring ☑ AppFlow Logging

Monitors	Weight	State
https	1	☑

Comments

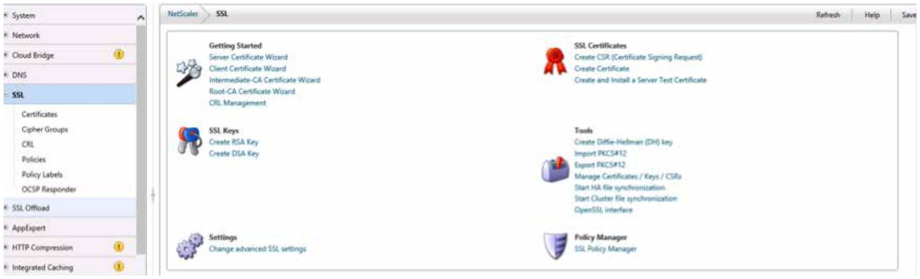
Verify that both services are up.



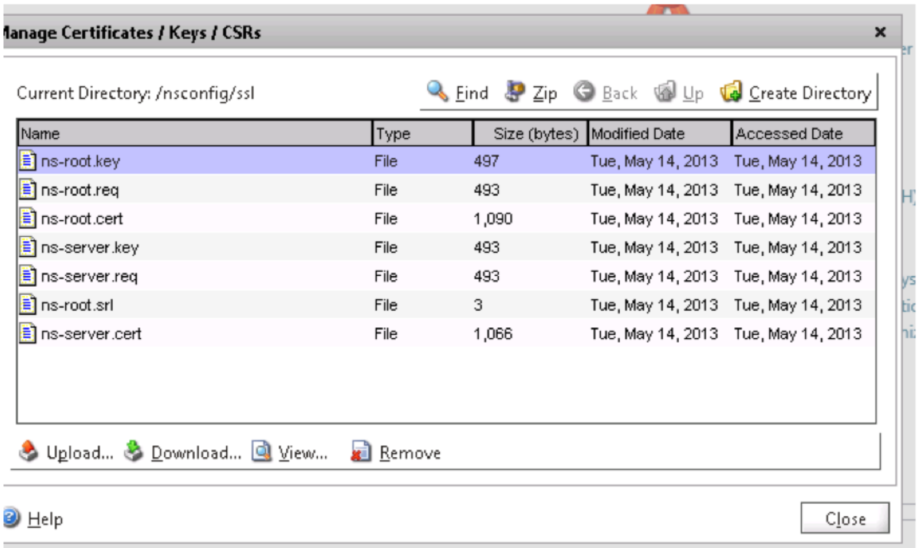
Name	State	IP Address/Domain Name	Port	Protocol	Max Cl
SF2-SSL	● Up	172.16.1.151	443	SSL	
SF1-SSL	● Up	172.16.1.150	443	SSL	

A load balancing virtual server can now be created to balance the two services created previously. This server must be an SSL server to load balance SSL services, meaning that it requires a certificate. Navigate to SSL certificates and import the certificate used for the Access Gateway URL.

Click on **Manage Certificates/Keys/CSRs** under SSL/Tools



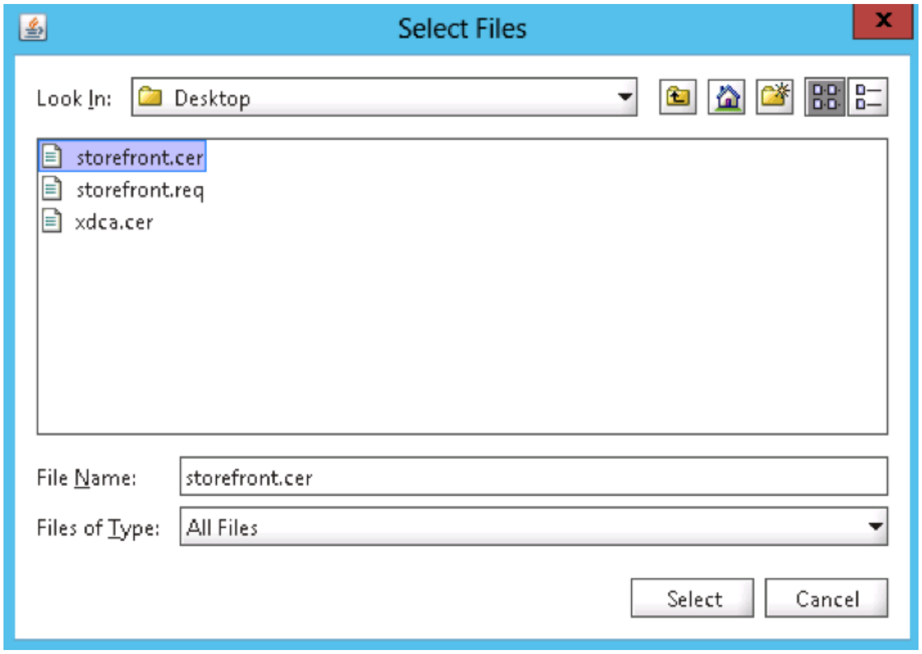
Select upload.



Current Directory: /nsconfig/ssl

Name	Type	Size (bytes)	Modified Date	Accessed Date
ns-root.key	File	497	Tue, May 14, 2013	Tue, May 14, 2013
ns-root.req	File	493	Tue, May 14, 2013	Tue, May 14, 2013
ns-root.cert	File	1,090	Tue, May 14, 2013	Tue, May 14, 2013
ns-server.key	File	493	Tue, May 14, 2013	Tue, May 14, 2013
ns-server.req	File	493	Tue, May 14, 2013	Tue, May 14, 2013
ns-root.srl	File	3	Tue, May 14, 2013	Tue, May 14, 2013
ns-server.cert	File	1,066	Tue, May 14, 2013	Tue, May 14, 2013

Upload the StoreFront certificate and any associated intermediate or root certificates.



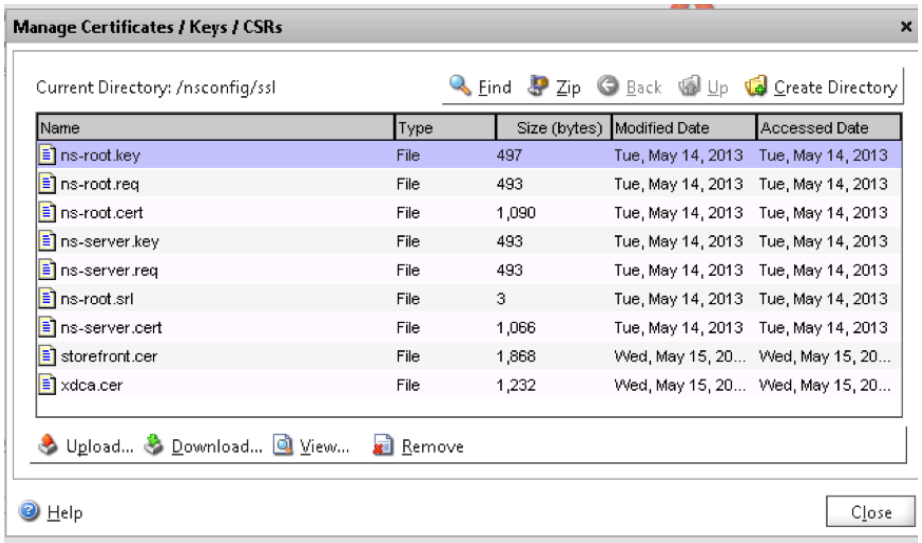
Look In: Desktop

storefront.cer
storefront.req
xdca.cer

File Name: storefront.cer

Files of Type: All Files

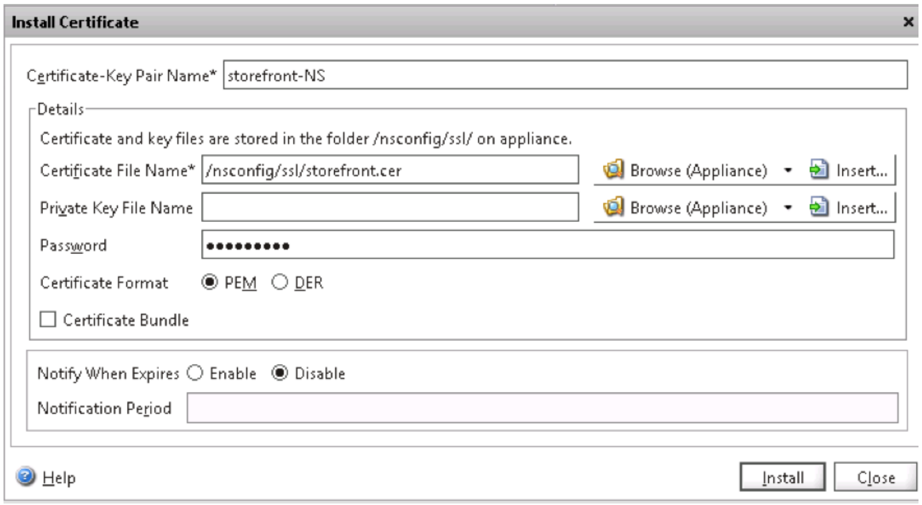
In this case, the StoreFront certificate and the CA root certificate have been uploaded.



Current Directory: /nsconfig/ssl

Name	Type	Size (bytes)	Modified Date	Accessed Date
ns-root.key	File	497	Tue, May 14, 2013	Tue, May 14, 2013
ns-root.req	File	493	Tue, May 14, 2013	Tue, May 14, 2013
ns-root.cert	File	1,090	Tue, May 14, 2013	Tue, May 14, 2013
ns-server.key	File	493	Tue, May 14, 2013	Tue, May 14, 2013
ns-server.req	File	493	Tue, May 14, 2013	Tue, May 14, 2013
ns-root.srl	File	3	Tue, May 14, 2013	Tue, May 14, 2013
ns-server.cert	File	1,066	Tue, May 14, 2013	Tue, May 14, 2013
storefront.cer	File	1,868	Wed, May 15, 20...	Wed, May 15, 20...
xdca.cer	File	1,232	Wed, May 15, 20...	Wed, May 15, 20...

Navigate to **ssl/certificates** and click **Install**. Select the certificate for StoreFront.



Install Certificate

Certificate-Key Pair Name* storefront-NS

Details

Certificate and key files are stored in the folder /nsconfig/ssl/ on appliance.

Certificate File Name* /nsconfig/ssl/storefront.cer

Private Key File Name

Password ●●●●●●●●●

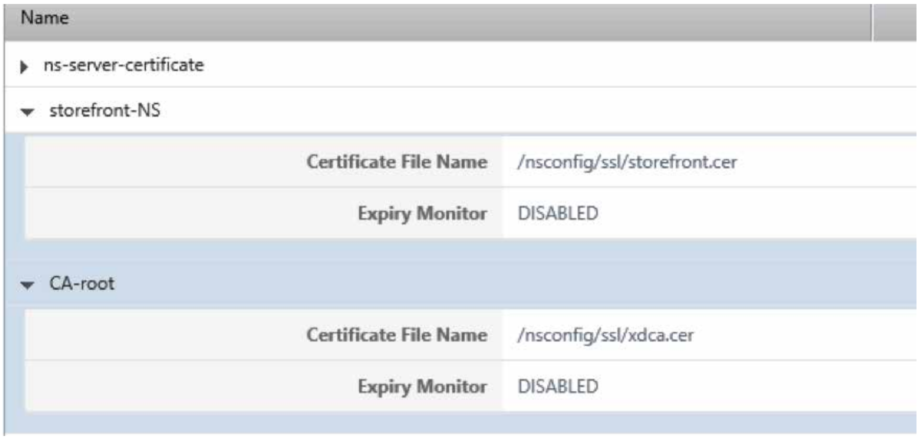
Certificate Format ● PEM ○ DER

□ Certificate Bundle

Notify When Expires ○ Enable ● Disable

Notification Period

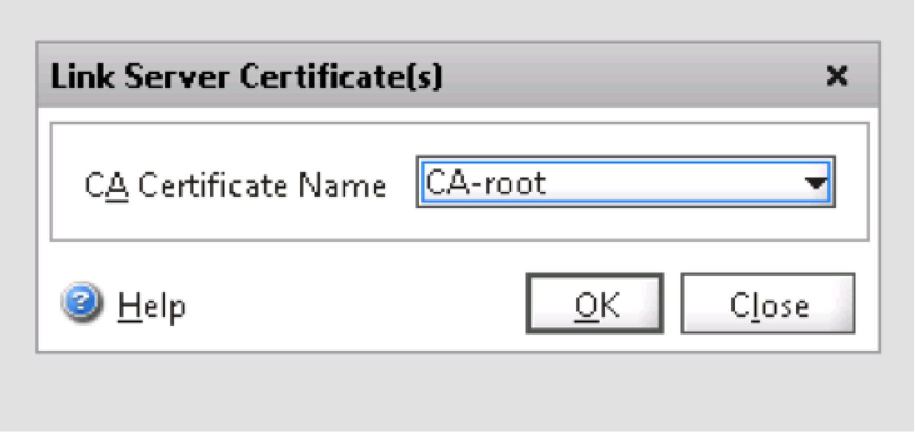
Repeat for intermediate and root certificates.



Name

- ns-server-certificate
- storefront-NS
  - Certificate File Name: /nsconfig/ssl/storefront.cer
  - Expiry Monitor: DISABLED
- CA-root
  - Certificate File Name: /nsconfig/ssl/xdca.cer
  - Expiry Monitor: DISABLED

Next select the **StoreFront certificate** and click **Link**. The root CA will be the only option for linking in this case. Click **OK**.



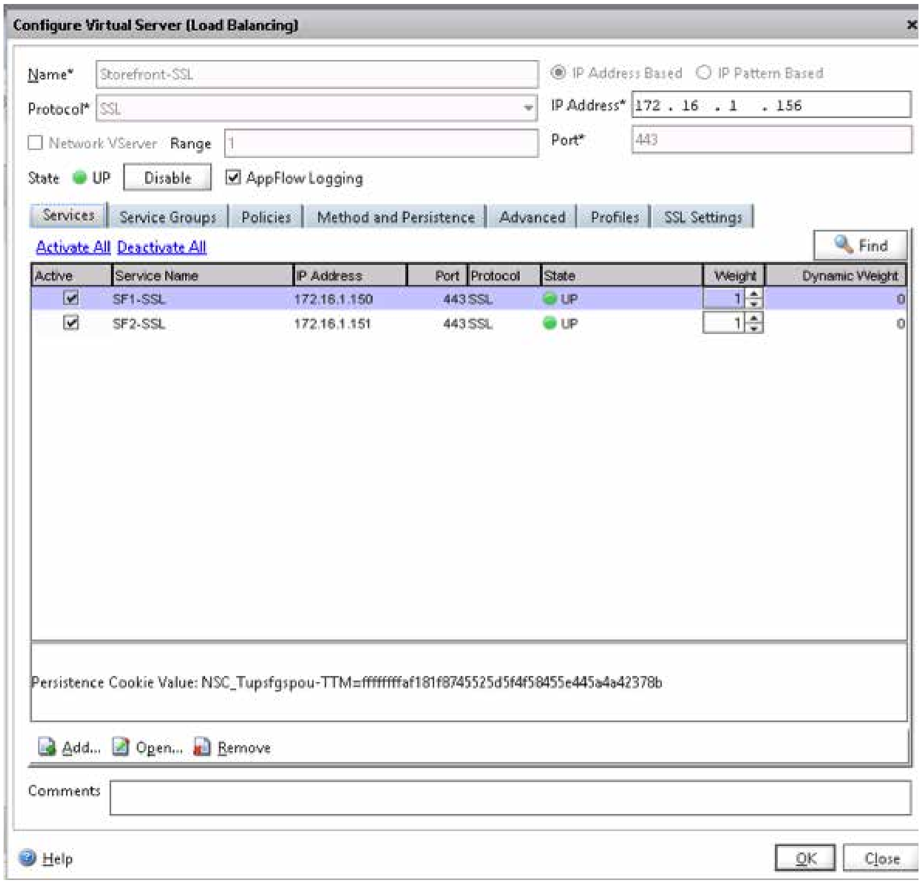
Link Server Certificate(s)

CA Certificate Name CA-root

The certificate will now be available for use on the load balancing virtual server and Access Gateway.

Go to load balancing/virtual servers and click **Add**.

Switch the protocol to SSL and enter the IP address that the virtual server will use. This is the IP address that was entered into the StoreFront configuration as the hostname. Select both StoreFront services.



Configure Virtual Server (Load Balancing)

Name* Storefront-SSL ● IP Address Based ○ IP Pattern Based

Protocol* SSL IP Address* 172 . 16 . 1 . 156

☐ Network VServer Range 1 Port* 443

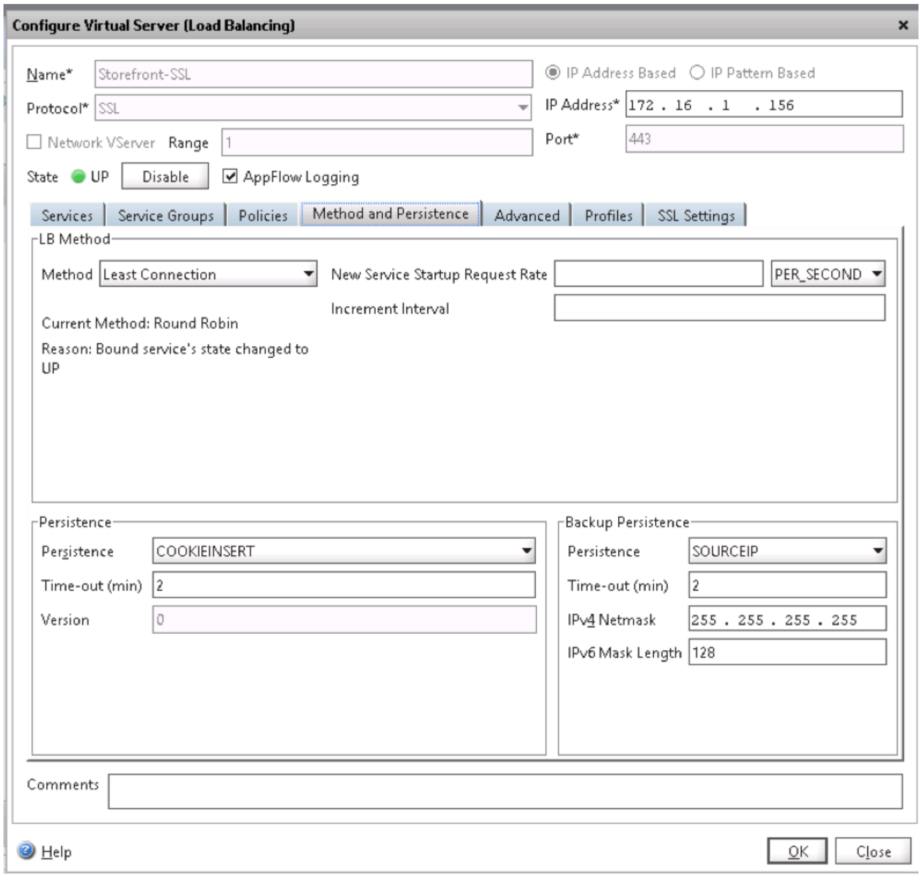
State ● UP Disable ☑ AppFlow Logging

Active	Service Name	IP Address	Port	Protocol	State	Weight	Dynamic Weight
☑	SF1-SSL	172.16.1.150	443	SSL	● UP	1	0
☑	SF2-SSL	172.16.1.151	443	SSL	● UP	1	0

Persistence Cookie Value: NSC_Tupsfgspou-TTM=ffffffffaf181f8745525d5f4f58455e445a4a42378b

Comments

Change to the method and persistence tab and specify COOKIEINSERT persistence with a SOURCEIP backup.



Configure Virtual Server (Load Balancing)

Name* Storefront-SSL

● IP Address Based ○ IP Pattern Based

Protocol* SSL

IP Address* 172 . 16 . 1 . 156

□ Network VServer Range 1

Port* 443

State UP Disable ☑ AppFlow Logging

Services | Service Groups | Policies | Method and Persistence | Advanced | Profiles | SSL Settings

LB Method

Method Least Connection

New Service Startup Request Rate PER_SECOND

Increment Interval

Current Method: Round Robin

Reason: Bound service's state changed to UP

Persistence

Persistence COOKIEINSERT

Time-out (min) 2

Version 0

Backup Persistence

Persistence SOURCEIP

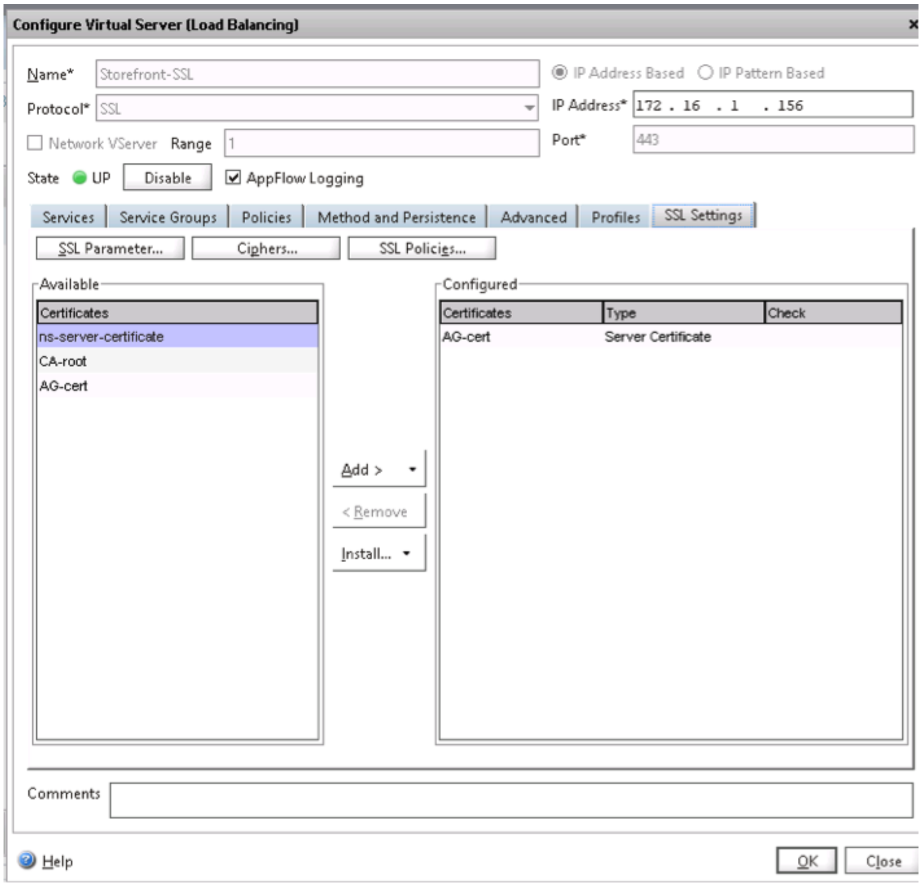
Time-out (min) 2

IPv4 Netmask 255 . 255 . 255 . 255

IPv6 Mask Length 128

Comments

Finally, under SSL settings, add the certificate for the server.



Name* Storefront-SSL ● IP Address Based ○ IP Pattern Based

Protocol* SSL IP Address* 172 . 16 . 1 . 156

□ Network VServer Range 1 Port* 443

State ● UP Disable ☑ AppFlow Logging

Available

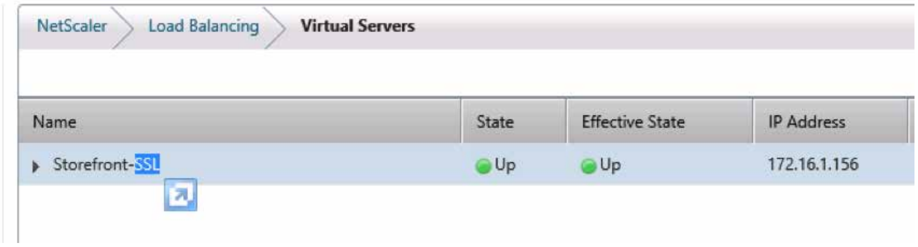
Certificates
ns-server-certificate
CA-root
AG-cert

Configured

Certificates	Type	Check
AG-cert	Server Certificate	

Comments

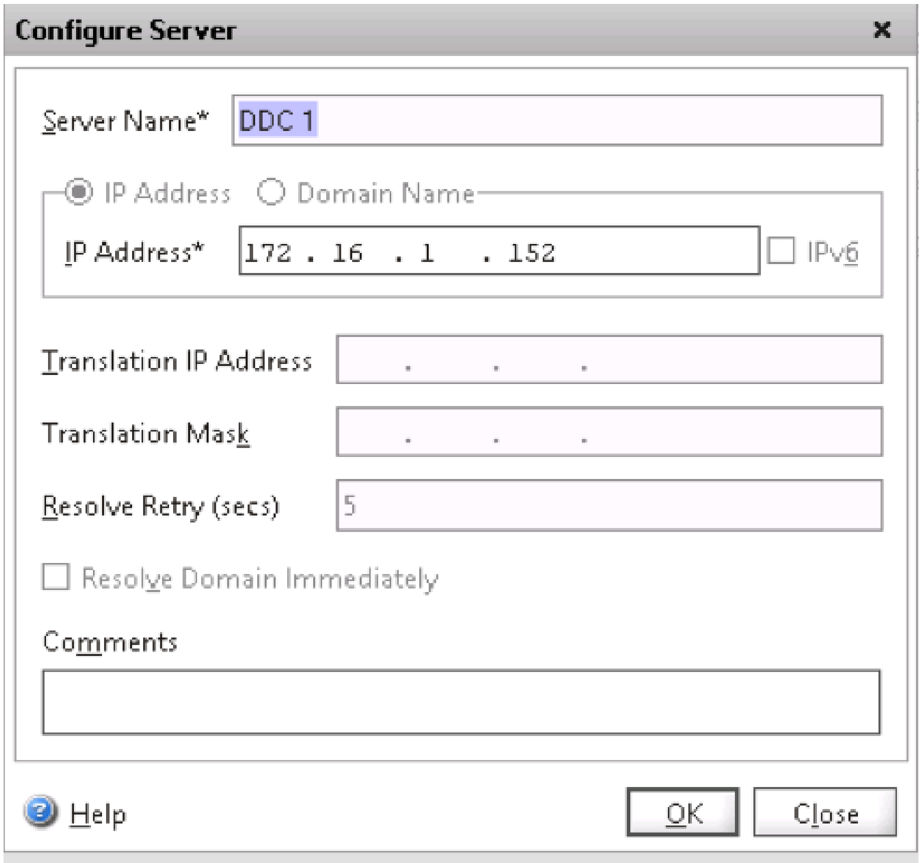
Verify that the server state is shown as **Up**.



Name	State	Effective State	IP Address
Storefront-SSL	● Up	● Up	172.16.1.156

4.4 Load balance DDCs

Next we need to configure load balancing for the DDCs. Go back to load balancing servers and add the first DDC server.



Configure Server

Server Name* DDC 1

● IP Address ○ Domain Name

IP Address* 172 . 16 . 1 . 152 □ IPv6

Translation IP Address . . .

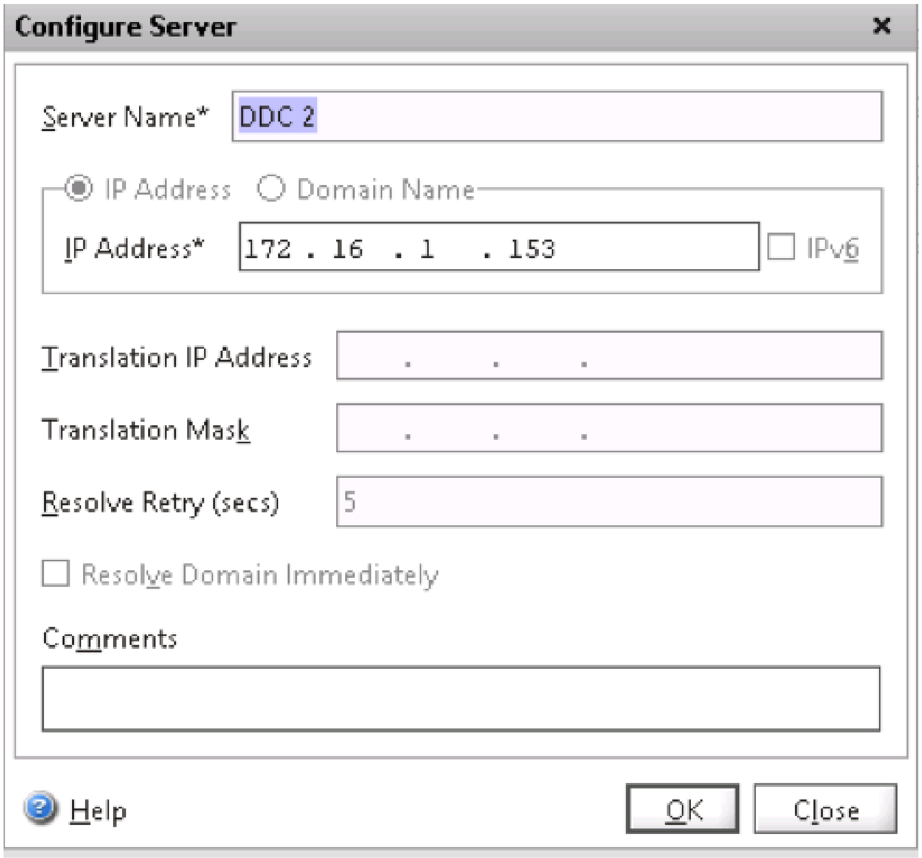
Translation Mask . . .

Resolve Retry (secs) 5

□ Resolve Domain Immediately

Comments

Repeat for DDC 2.



Configure Server

Server Name*: DDC 2

● IP Address ○ Domain Name

IP Address*: 172 . 16 . 1 . 153 □ IPv6

Translation IP Address: . . .

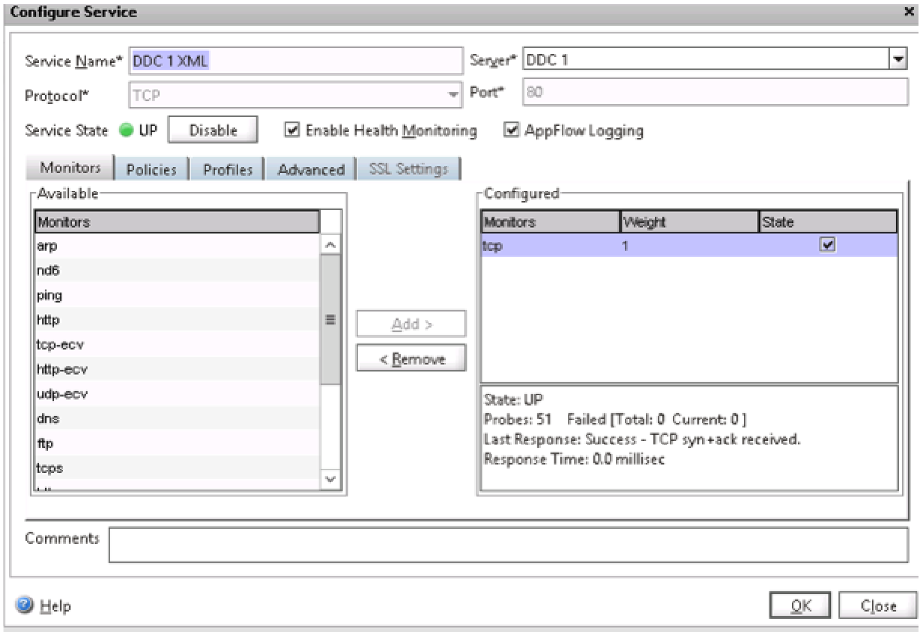
Translation Mask: . . .

Resolve Retry (secs): 5

□ Resolve Domain Immediately

Comments:

Next, create the services for XML traffic on the DDCs. In this deployment the XML service was left on port 80, the default. If the port was changed by the broker service, reflect that in the services created here.



Configure Service

Service Name* DDC 1 XML
Server* DDC 1
Protocol* TCP
Port* 80
Service State ● UP
☑ Enable Health Monitoring ☑ AppFlow Logging

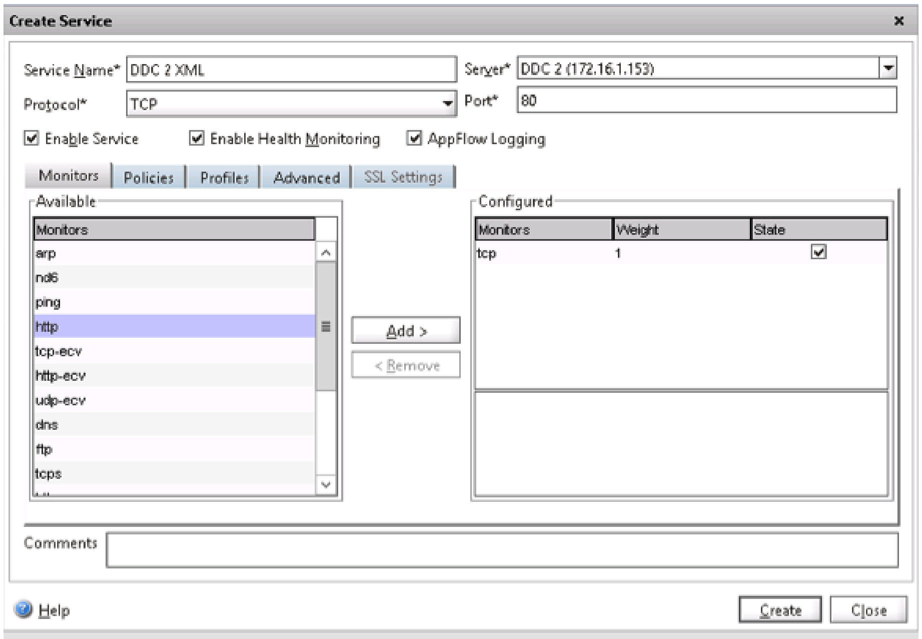
Configured:

Monitors	Weight	State
tcp	1	☑

State: UP
Probes: 51 Failed [Total: 0 Current: 0]
Last Response: Success - TCP syn+ack received.
Response Time: 0.0 millisec

Comments

Repeat for DDC 2.



Create Service

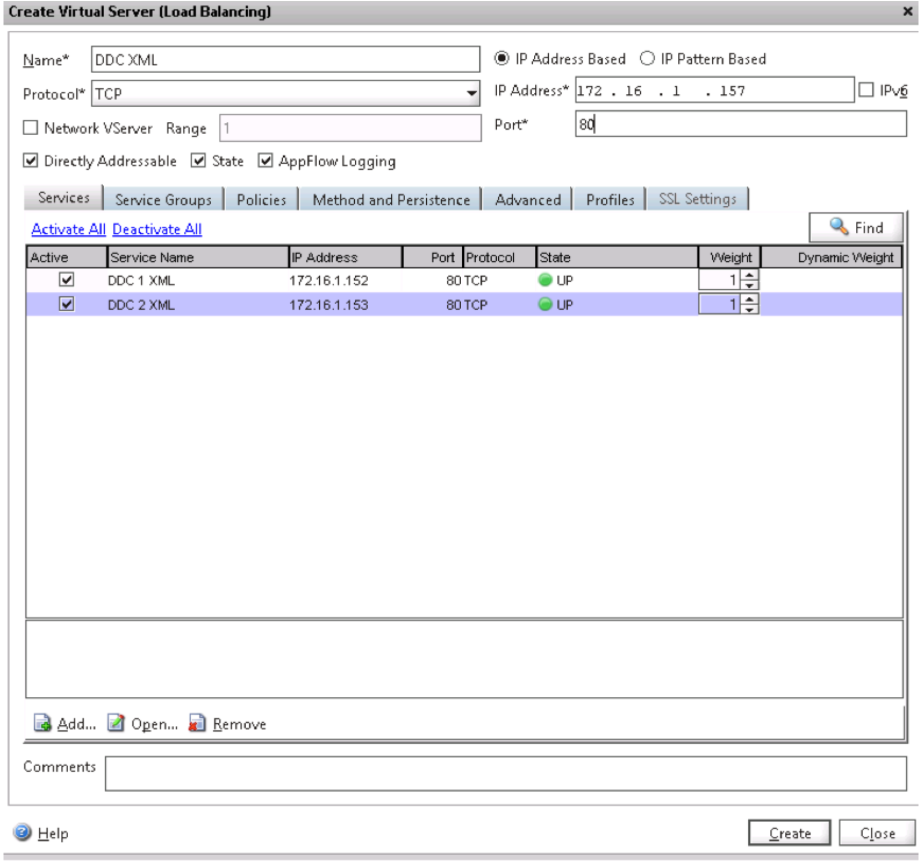
Service Name* DDC 2 XML
Server* DDC 2 (172.16.1.153)
Protocol* TCP
Port* 80
☑ Enable Service ☑ Enable Health Monitoring ☑ AppFlow Logging

Configured:

Monitors	Weight	State
tcp	1	☑

Comments

Now, create the load balancing virtual server for the XML service. This is the IP address that was entered for the delivery controller in the StoreFront configuration.



Create Virtual Server (Load Balancing)

Name*	DDC XML	● IP Address Based	○ IP Pattern Based
Protocol*	TCP	IP Address*	172 . 16 . 1 . 157 ☐ IPv6
☐ Network VServer	Range 1	Port*	80

☑ Directly Addressable ☑ State ☑ AppFlow Logging

Active	Service Name	IP Address	Port	Protocol	State	Weight	Dynamic Weight
☑	DDC 1 XML	172.16.1.152	80	TCP	● UP	1	
☑	DDC 2 XML	172.16.1.153	80	TCP	● UP	1	

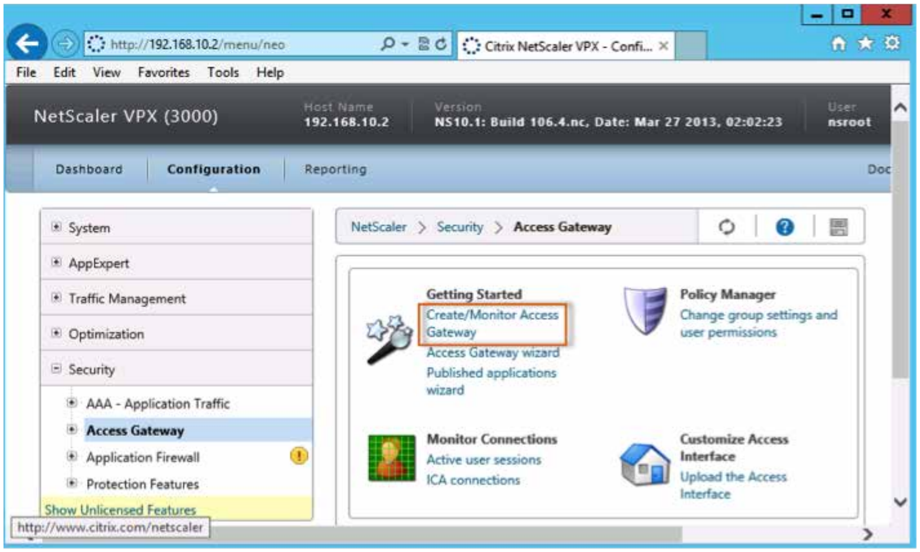
Comments

Note: Persistence isn’t required for the DDC XML service.

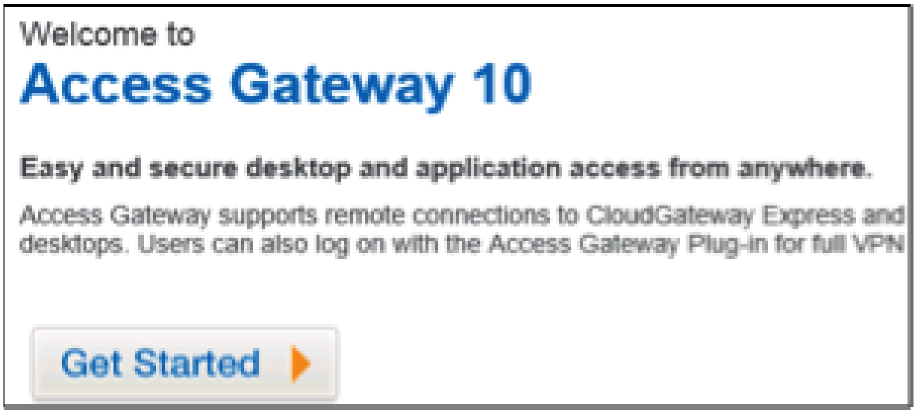
4.5 Remote access with NetScaler Access Gateway – wizard

Log into the NetScaler GUI.

Expand Security and click **Access Gateway**. Click **Create/Monitor Access Gateway**.


http://192.168.10.2/menu/neo
Citrix NetScaler VPX - Confi...
File Edit View Favorites Tools Help
NetScaler VPX (3000)
Host Name 192.168.10.2
Version NS10.1: Build 106.4.nc, Date: Mar 27 2013, 02:02:23
User nsroot
Dashboard
Configuration
Reporting
Doc
System
AppExpert
Traffic Management
Optimization
Security
AAA - Application Traffic
Access Gateway
Application Firewall
Protection Features
Show Unlicensed Features
http://www.citrix.com/netscaler
NetScaler > Security > Access Gateway
Getting Started
Create/Monitor Access Gateway
Access Gateway wizard
Published applications wizard
Policy Manager
Change group settings and user permissions
Monitor Connections
Active user sessions
ICA connections
Customize Access Interface
Upload the Access Interface

Click the **Get Started** button.


Welcome to

Access Gateway 10

Easy and secure desktop and application access from anywhere.

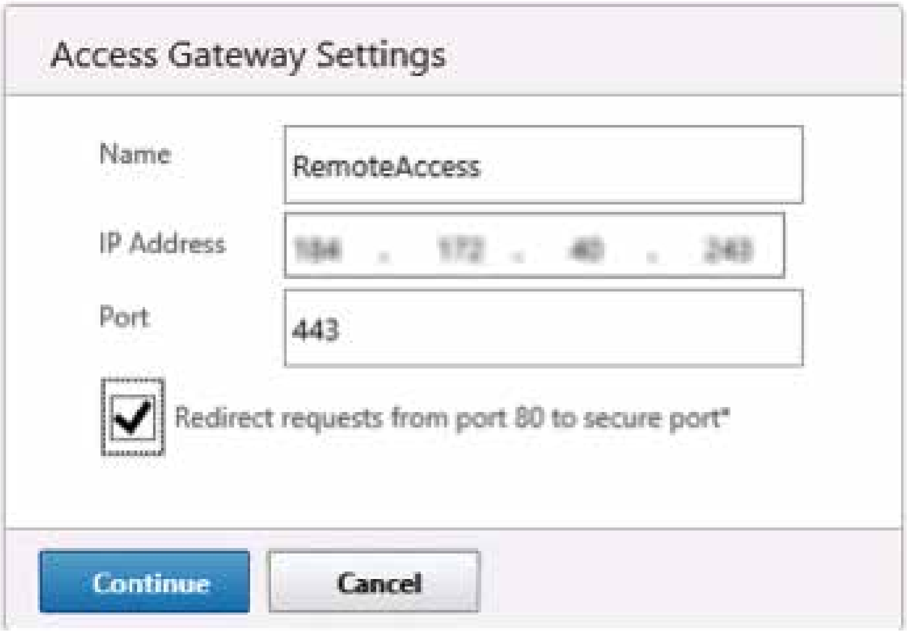
Access Gateway supports remote connections to CloudGateway Express and desktops. Users can also log on with the Access Gateway Plug-in for full VPN

Enter **RemoteAccess** for the Name.

IP Address: **<<Public IP for access>>**

Click **Redirect requests from port 80 to secure port**.

Then click **Continue**.



Access Gateway Settings

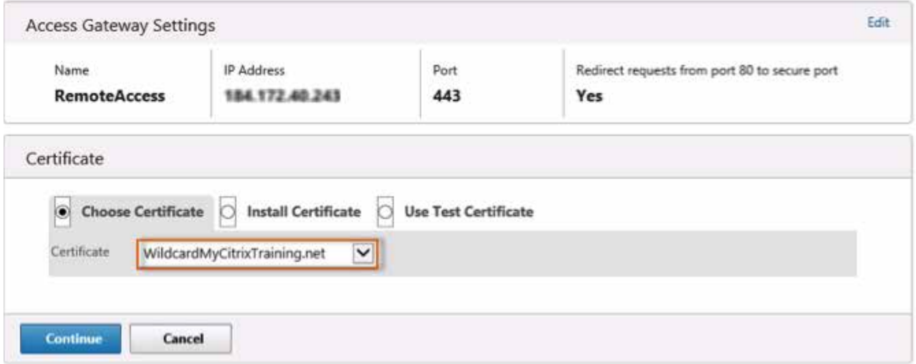
Name: RemoteAccess

IP Address: [redacted]

Port: 443

☑ Redirect requests from port 80 to secure port*

From the Certificate drop-down menu, select **the public CA certificate for the NetScaler Access Gateway** and click **Continue**.



Access Gateway Settings

Name	IP Address	Port	Redirect requests from port 80 to secure port
RemoteAccess	[redacted]	443	Yes

Certificate

● Choose Certificate ○ Install Certificate ○ Use Test Certificate

Certificate: WildcardMyCitrixTraining.net

NOTE: This certificate needs to be issued from a public CA and must be previously installed on the NetScaler appliance.

Next is authentication. If you have previously configured LDAP authentication on NetScaler, select the available authentication and skip to the next step.

Under **Authentication Settings**, click the button for **Configure New** and enter the following details:

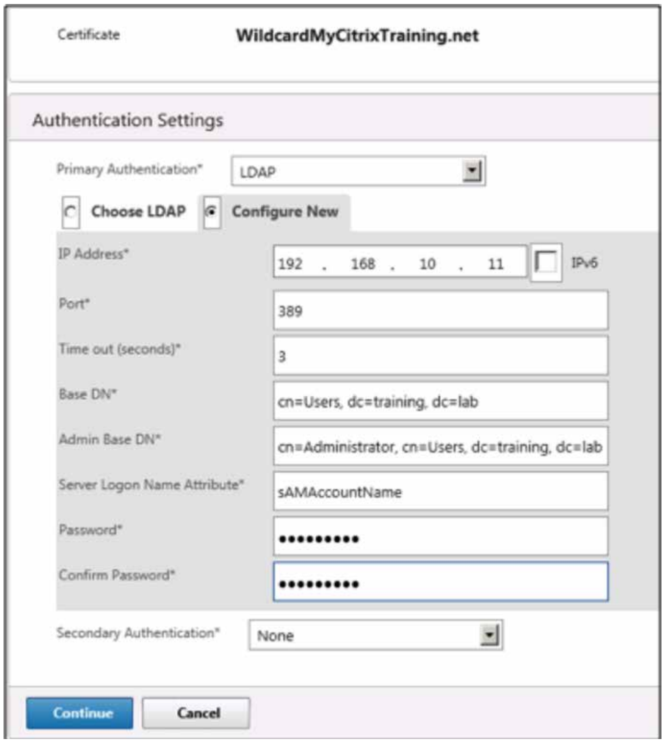
IP Address: **172.16.1.200**

Base DN: **cn=Users, dc=xd, dc=lab**

Admin Base DN: **cn=Administrator, cn=Users, dc=xd, dc=lab**

Password/Confirm Password: **Password1**

Click **Continue**.



Certificate	WildcardMyCitrixTraining.net

Authentication Settings

Primary Authentication*	LDAP
○ Choose LDAP	● Configure New
IP Address*	192 . 168 . 10 . 11 □ IPv6
Port*	389
Time out (seconds)*	3
Base DN*	cn=Users, dc=training, dc=lab
Admin Base DN*	cn=Administrator, cn=Users, dc=training, dc=lab
Server Logon Name Attribute*	sAMAccountName
Password*	•••••••••
Confirm Password*	•••••••••
Secondary Authentication*	None

Enter the following details for **Citrix Integration Settings**:

CloudGateway

Deployment Type: **Windows Storefront**

StoreFront FQDN: **storefront.xd.lab (FQDN of storefront load balancer)**

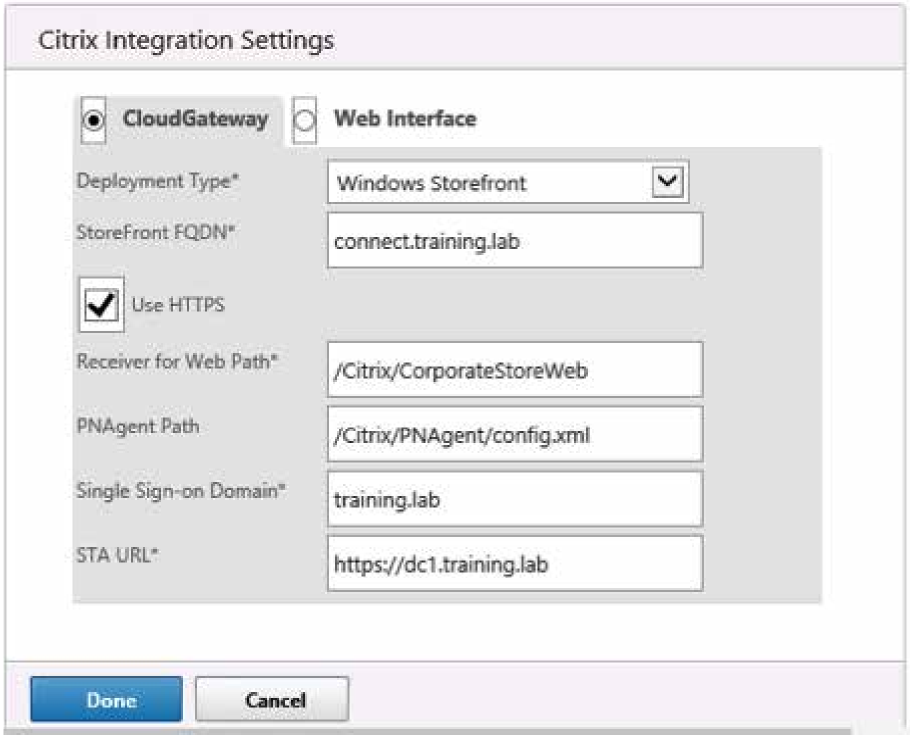
Receiver for Web Path: **/Citrix/StoreWeb** (url of receiver for web)

PNAgent Path: **/Citrix/PNAgent/config.xml**

Single Sign-on Domain: **xd.lab**

STA URL: **http://ddc1.training.lab**

Click **Done**.



Citrix Integration Settings

● CloudGateway ○ Web Interface

Deployment Type*: Windows Storefront

StoreFront FQDN*: connect.training.lab

☑ Use HTTPS

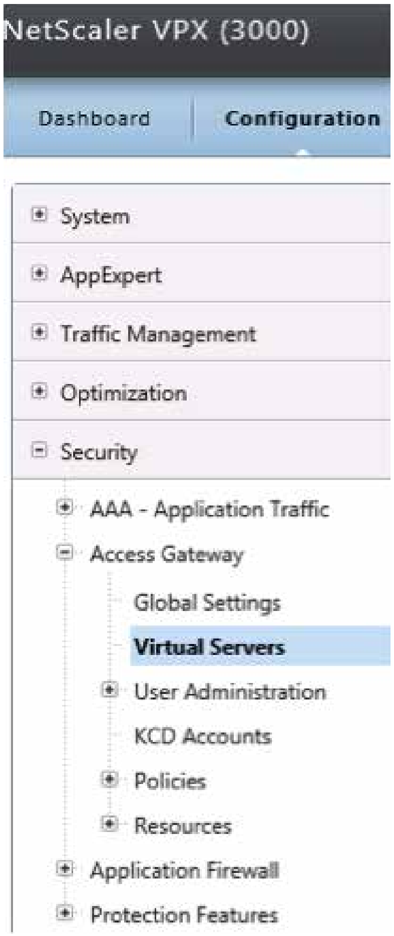
Receiver for Web Path*: /Citrix/CorporateStoreWeb

PNAgent Path: /Citrix/PNAgent/config.xml

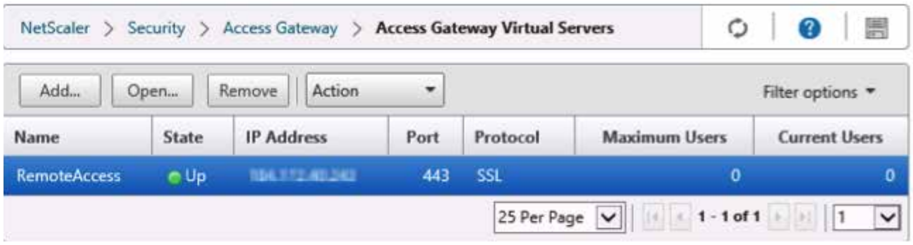
Single Sign-on Domain*: training.lab

STA URL*: https://dc1.training.lab

Under **Configuration**, go to **Security > Access Gateway > Virtual Servers.**



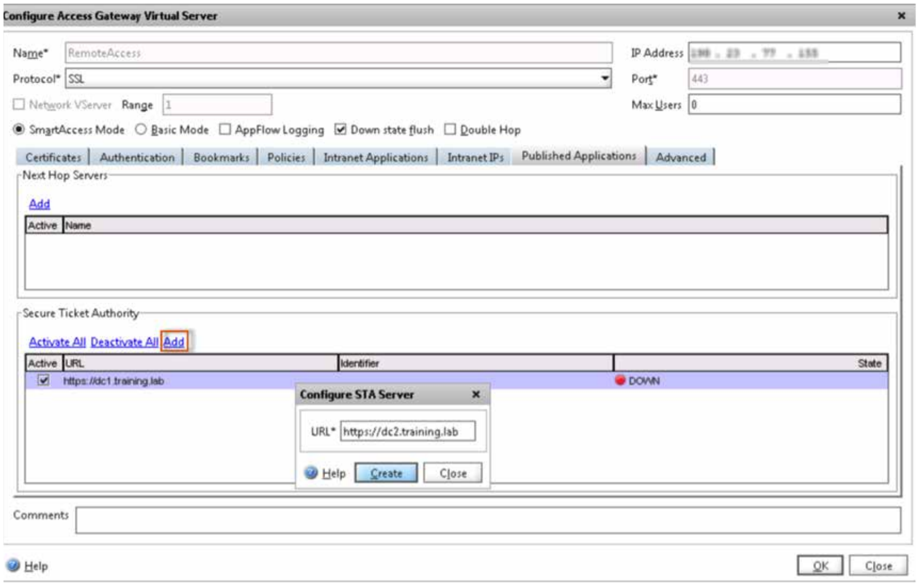
Double-click the **RemoteAccess** entry.


NetScaler > Security > Access Gateway > Access Gateway Virtual Servers
Add...
Open...
Remove
Action
Filter options
25 Per Page
1 - 1 of 1
1

Name	State	IP Address	Port	Protocol	Maximum Users	Current Users
RemoteAccess	● Up	[redacted]	443	SSL	0	0

Under **Published Applications** tab, click **Add** under Secure Ticket Authority.

Type in **http://ddc2.training.lab** and click **Create**.



Configure Access Gateway Virtual Server

Name* RemoteAccess

IP Address [redacted]

Protocol* SSL

Port* 443

□ Network VServer Range 1

Max Users 0

● SmartAccess Mode ○ Basic Mode □ AppFlow Logging ☑ Down state flush □ Double Hop

Next Hop Servers

Active	Name

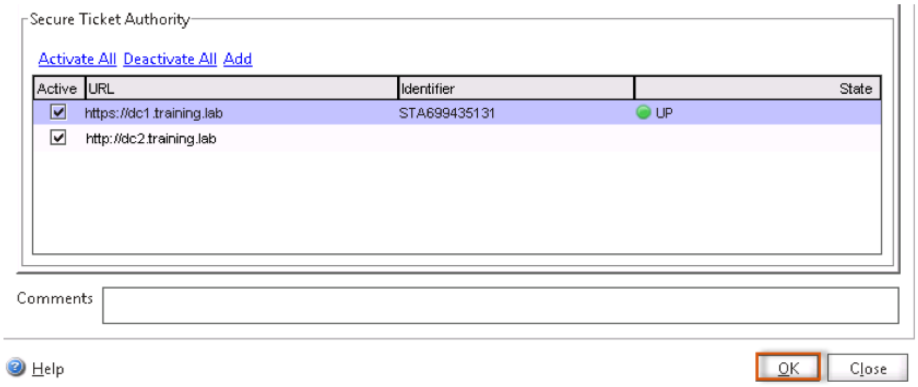
Secure Ticket Authority

Active	URL	Identifier	State
☑	https://dc1.training.lab		DOWN

Configure STA Server

URL* https://dc2.training.lab

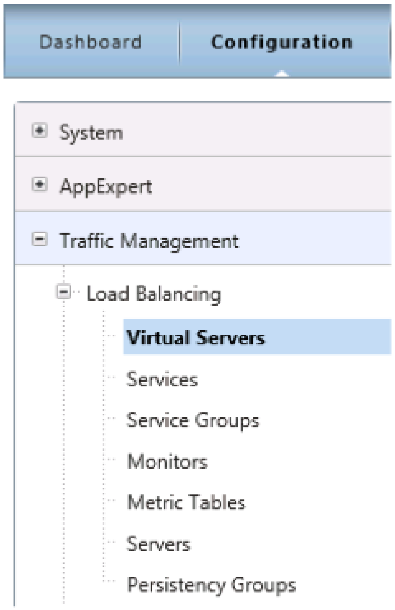
Click **OK**.



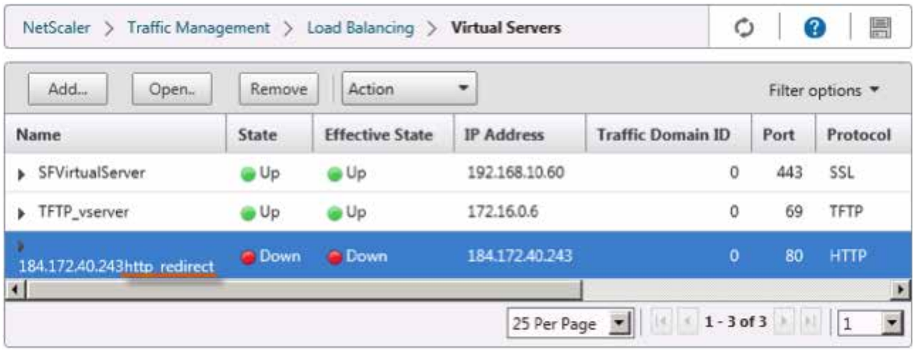
Secure Ticket Authority

Active	URL	Identifier	State
☑	https://dc1.training.lab	STA699435131	UP
☑	http://dc2.training.lab		

Go to **Traffic Management > Load Balancing > Virtual Servers**.

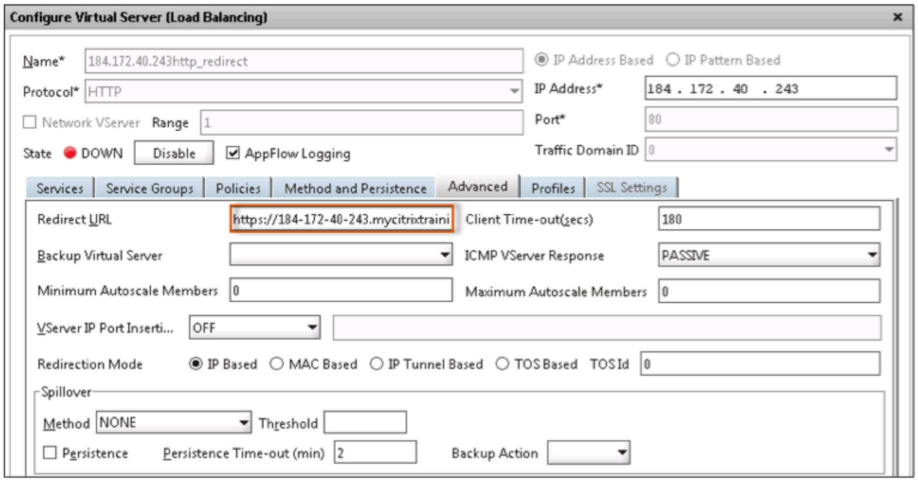


Double-click the entry with the name that contains **http_redirect**. This was created as part of the wizard.


NetScaler > Traffic Management > Load Balancing > Virtual Servers
Add...
Open..
Remove
Action
Filter options
25 Per Page
1 - 3 of 3
1

Name	State	Effective State	IP Address	Traffic Domain ID	Port	Protocol
SFVirtualServer	Up	Up	192.168.10.60	0	443	SSL
TFTP_vserver	Up	Up	172.16.0.6	0	69	TFTP
184.172.40.243http_redirect	Down	Down	184.172.40.243	0	80	HTTP

Click the Advanced tab and change the **Redirect URL** to be in the format **https://externally-accessible-FQDN** based on the IP address that was there.



Configure Virtual Server (Load Balancing)

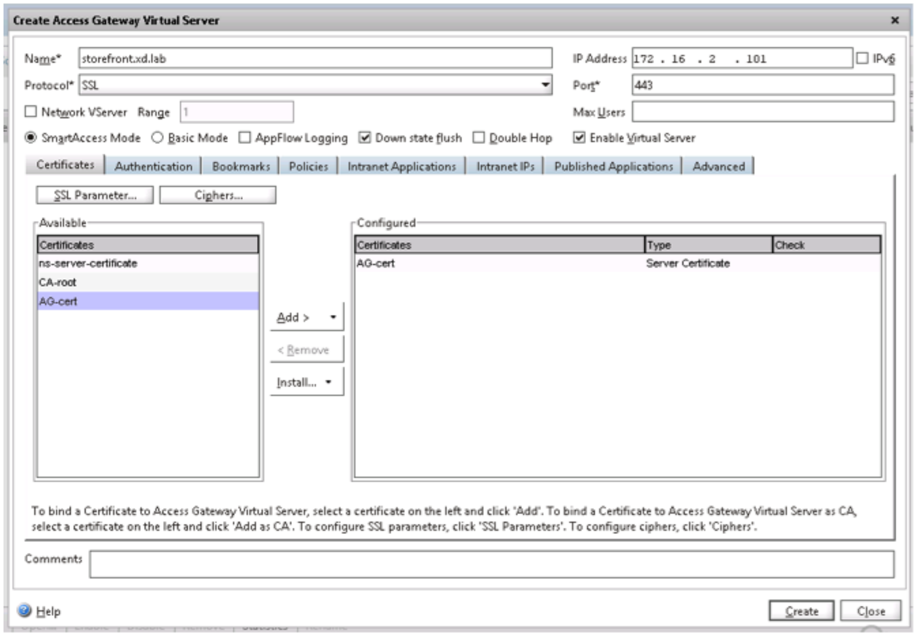
Name* 184.172.40.243http_redirect ● IP Address Based ○ IP Pattern Based
Protocol* HTTP IP Address* 184 . 172 . 40 . 243
□ Network VServer Range 1 Port* 80
State ● DOWN Disable ☑ AppFlow Logging Traffic Domain ID 0

Redirect URL https://184-172-40-243.mycitrixtraini Client Time-out(secs) 180
Backup Virtual Server ICMP VServer Response PASSIVE
Minimum Autoscale Members 0 Maximum Autoscale Members 0
VServer IP Port Inserti... OFF
Redirection Mode ● IP Based ○ MAC Based ○ IP Tunnel Based ○ TOS Based TOS Id 0
Spillover
Method NONE Threshold
□ Persistence Persistence Time-out (min) 2 Backup Action

4.6 Remote access with NetScaler Access Gateway – manual setup

Now that load balancing is configured, Access Gateway can be configured. In this deployment, a second subnet was configured to act as the "WAN." This subnet contains only the Access Gateway VIP, a NetScaler SNIP and a client access machine. The subnet used is 172.16.2.x/24. First configure a SNIP on this subnet; in this guide 172.16.2.100 was used. Then go to **Access Gateways/virtual servers** and click **Add**.

Name the server using the common name of the certificate, give it a VIP and assign the StoreFront certificate and click **Create**.



Create Access Gateway Virtual Server

Name* storefront.xd.lab IP Address 172 . 16 . 2 . 101 □ IPv6
Protocol* SSL Port* 443
□ Network VServer Range 1 Max Users
● SmartAccess Mode ○ Basic Mode □ AppFlow Logging ☑ Down state flush □ Double Hop ☑ Enable Virtual Server

Available

Certificates
ns-server-certificate
CA-root
AG-cert

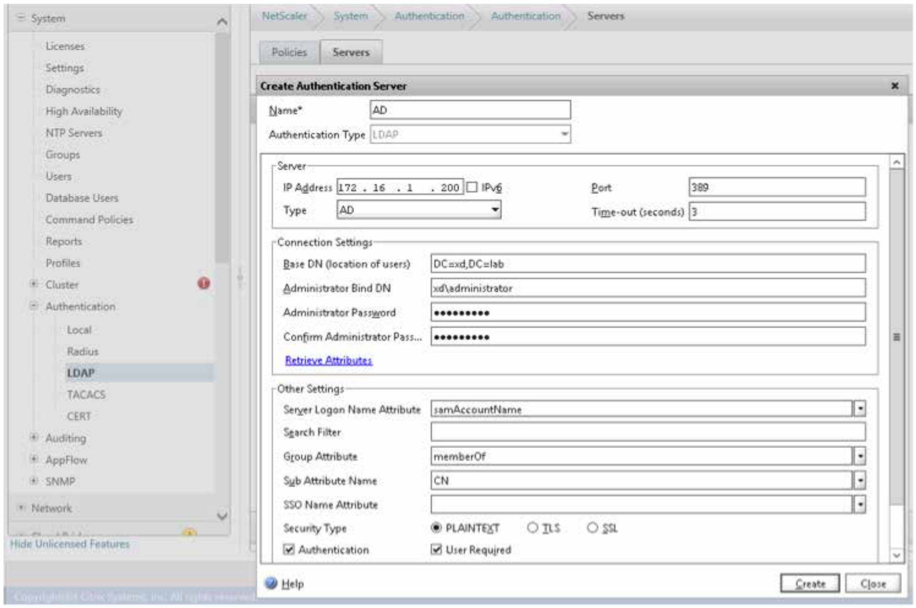
Configured

Certificates	Type	Check
AG-cert	Server Certificate	

To bind a Certificate to Access Gateway Virtual Server, select a certificate on the left and click 'Add'. To bind a Certificate to Access Gateway Virtual Server as CA, select a certificate on the left and click 'Add as CA'. To configure SSL parameters, click 'SSL Parameters'. To configure ciphers, click 'Ciphers'.

Comments

We want Access Gateway to be able to authenticate users with Active Directory, so we added LDAP authentication to the system. Go to the **system/authentication/ldap/servers** tab and click **Add**. Fill in the domain controller information and click **Create**.



Create Authentication Server

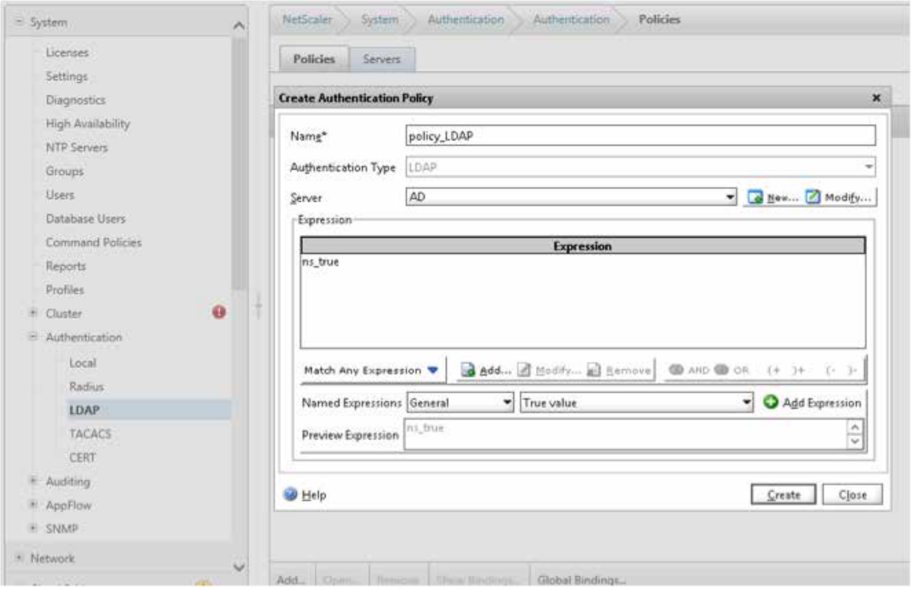
Name* AD
Authentication Type LDAP

Server
IP Address 172 . 16 . 1 . 200 □ IPv6
Port 389
Type AD
Time-out (seconds) 3

Connection Settings
Base DN (location of users) DC=xd,DC=lab
Administrator Bind DN xd\administrator
Administrator Password •••••••••
Confirm Administrator Pass... •••••••••
Retrieve Attributes

Other Settings
Server Logon Name Attribute samAccountName
Search Filter
Group Attribute memberOf
Sub Attribute Name CN
SSO Name Attribute
Security Type ● PLAINTEXT ○ TLS ○ SSL
☑ Authentication ☑ User Required

Now switch over to the **Policies** tab and click **Add**. Add the **ns_true** expression to the policy and click **Create**.



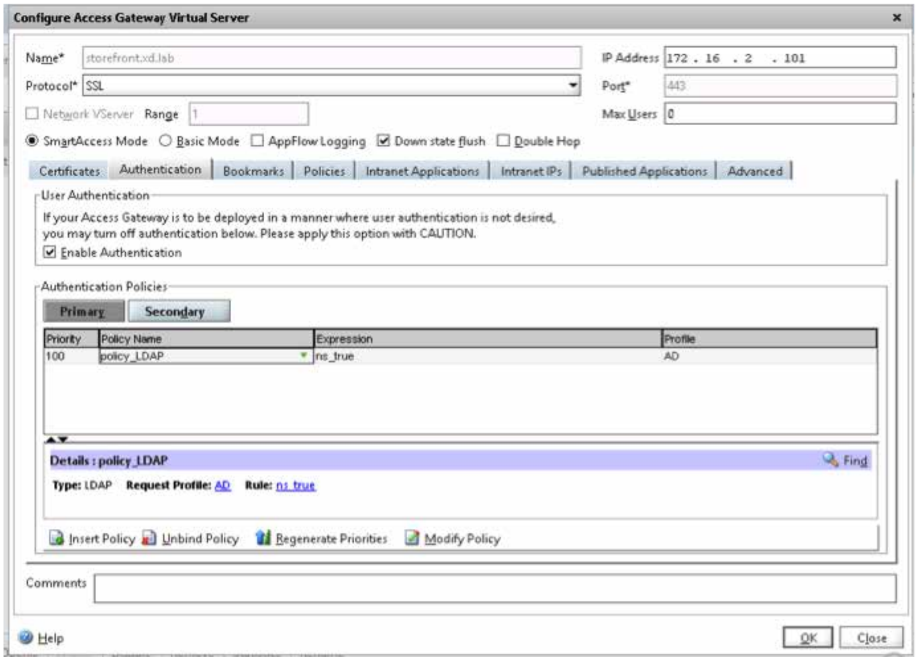
Create Authentication Policy

Name* policy_LDAP
Authentication Type LDAP
Server AD

Expression
Expression
ns_true

Named Expressions General True value
Preview Expression ns_true

Now go back to the Access Gateway virtual server and switch to the **authentication** tab, and click **Insert Policy**. Select the policy we just created and click **OK**.



Configure Access Gateway Virtual Server

Name* storefront.xd.lab
IP Address 172 . 16 . 2 . 101
Protocol* SSL
Port* 443
□ Network VServer Range 1
Max Users 0

● SmartAccess Mode ○ Basic Mode □ AppFlow Logging ☑ Down state flush □ Double Hop

User Authentication

If your Access Gateway is to be deployed in a manner where user authentication is not desired, you may turn off authentication below. Please apply this option with CAUTION.

☑ Enable Authentication

Authentication Policies

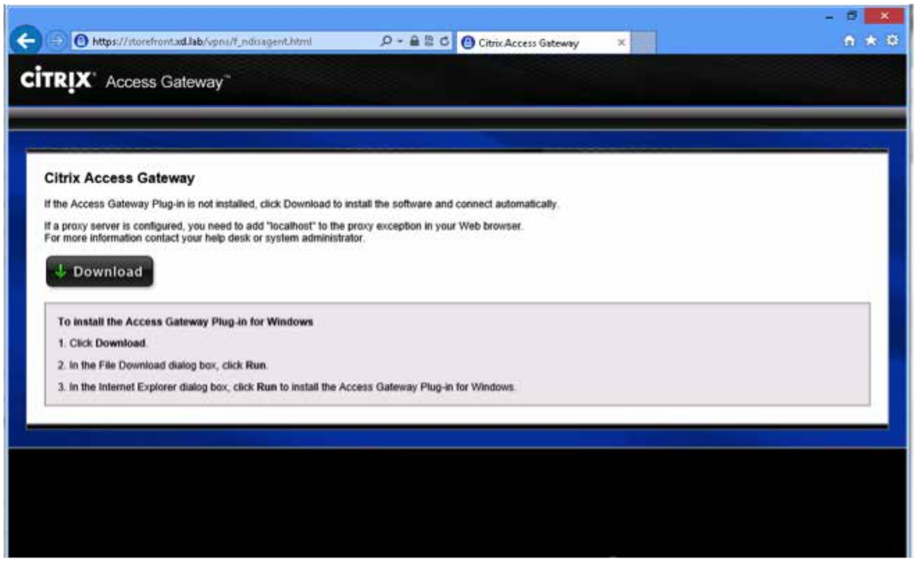
Priority	Policy Name	Expression	Profile
100	policy_LDAP	ns_true	AD

Details : policy_LDAP

Type: LDAP Request Profile: AD Rule: ns_true

Comments

At this point we should be able to log into NetScaler Access Gateway.



https://storefront.xd.lab/vpns/f_ndisagent.html

Citrix Access Gateway

If the Access Gateway Plug-in is not installed, click Download to install the software and connect automatically.

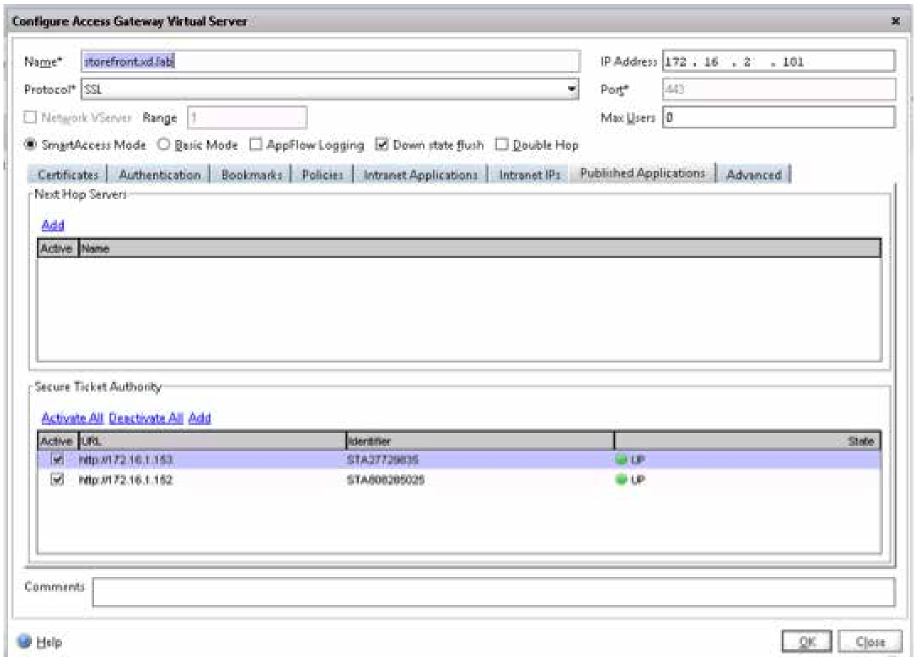
If a proxy server is configured, you need to add "localhost" to the proxy exception in your Web browser.
For more information contact your help desk or system administrator.

To install the Access Gateway Plug-in for Windows

1. Click **Download**.
2. In the File Download dialog box, click **Run**.
3. In the Internet Explorer dialog box, click **Run** to install the Access Gateway Plug-in for Windows.

You land on the NetScaler Access Gateway portal because there is no session policy defined to forward the session. That will be the next step. This step verifies that the certificate is valid and that the authentication works.

Back on the StoreFront Access Gateway virtual server, add the two DDs as STAs. Go to the **Published Applications** tab, and under **Secure Ticket Authority** enter http:// followed by the IP address of the servers. Once entered, each entry should appear up with an identifier listed.



Configure Access Gateway Virtual Server

Name* storefront.xd.lab

IP Address 172 . 16 . 2 . 101

Protocol* SSL

Port* 443

□ Network VServer Range 1

Max Users 0

● SmartAccess Mode ○ Basic Mode □ AppFlow Logging ☑ Down state flush □ Double Hop

Next Hop Servers

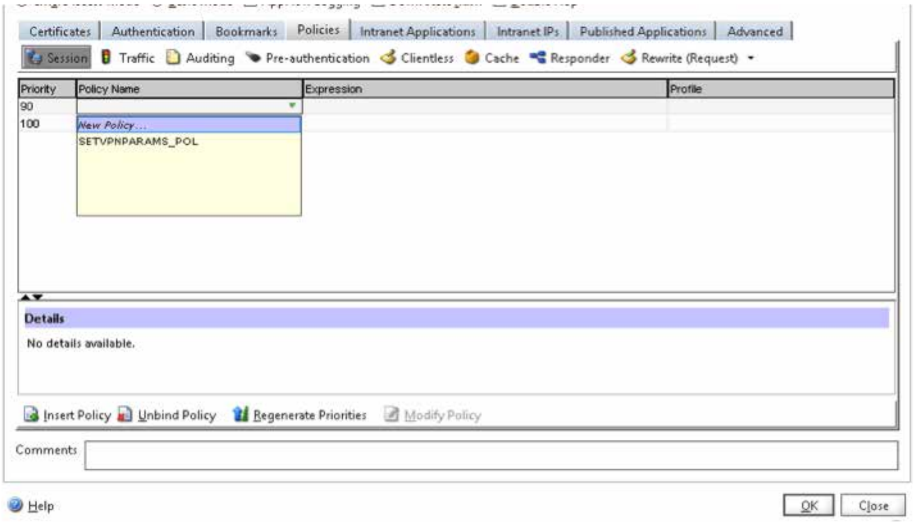
Active	Name

Secure Ticket Authority

Active	URL	Identifier	State
☑	http://172.16.1.153	STA27729835	● UP
☑	http://172.16.1.152	STA808285025	● UP

Comments

Navigate to the **Policies** tab and click Insert Policy. Select **New Policy**. Name the policy. Next to **Request Profile**, select **New**.



Priority	Policy Name	Expression	Profile
90			
100			

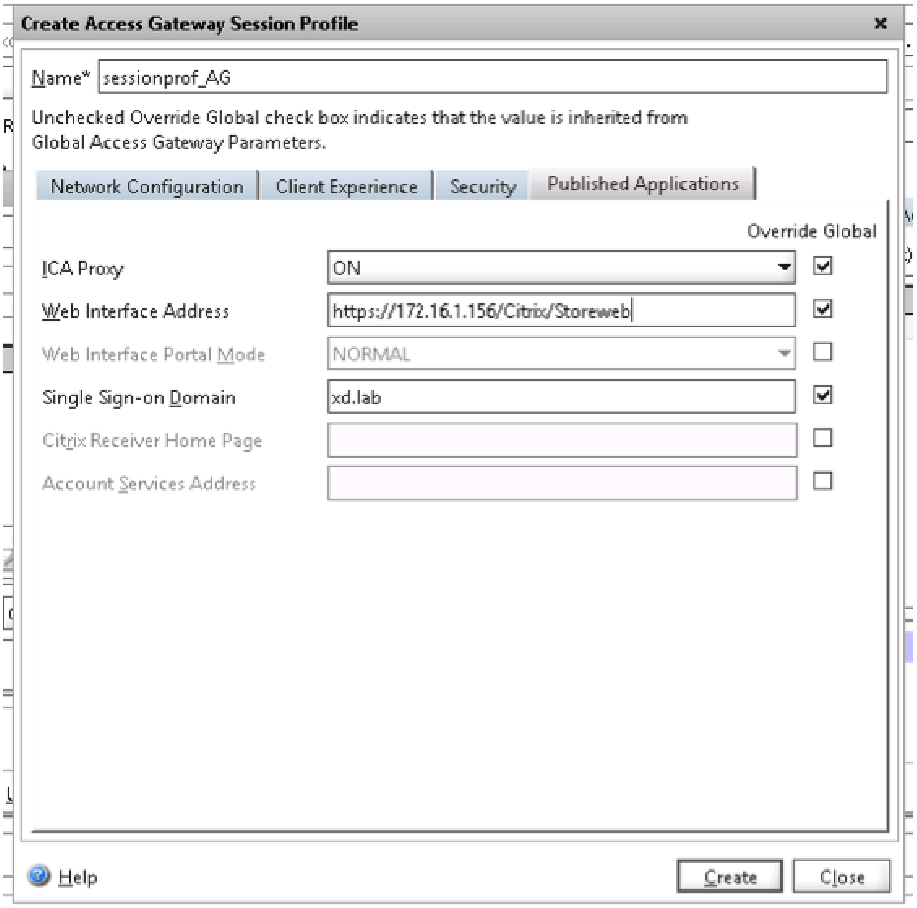
New Policy...
SETVPNPARAMS_POL

Details

No details available.

Comments

Switch to the **Published Applications** tab and make the following changes:

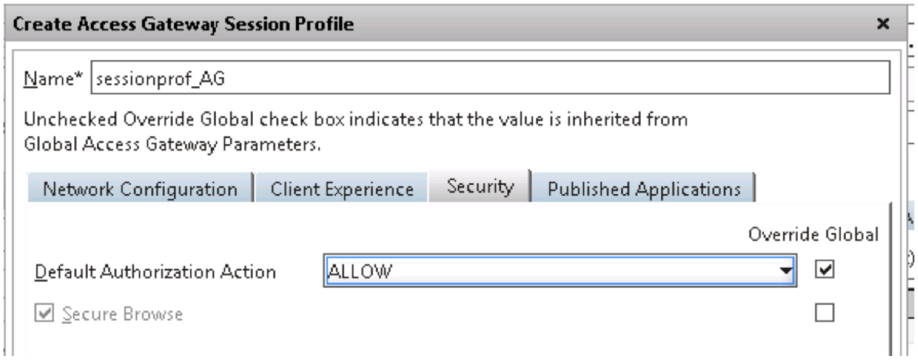


Name* sessionprof_AG

Unchecked Override Global check box indicates that the value is inherited from Global Access Gateway Parameters.

ICA Proxy	ON	☑
Web Interface Address	https://172.16.1.156/Citrix/Storeweb	☑
Web Interface Portal Mode	NORMAL	□
Single Sign-on Domain	xd.lab	☑
Citrix Receiver Home Page		□
Account Services Address		□

Click the **Security** tab and set the **Default Authorization Action** to **ALLOW**.

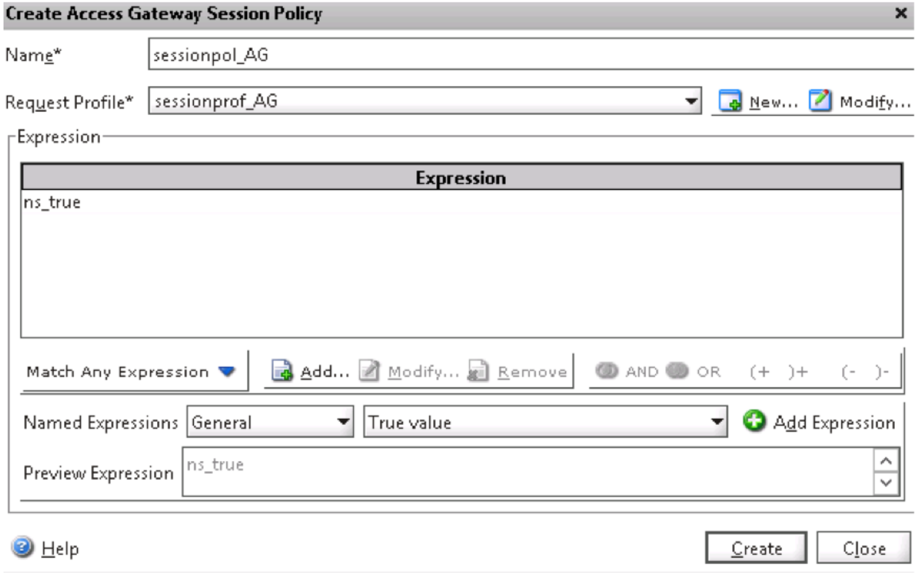


Name* sessionprof_AG

Unchecked Override Global check box indicates that the value is inherited from Global Access Gateway Parameters.

Default Authorization Action	ALLOW	☑
☑ Secure Browse		□

Add the **ns_true** expression to the policy and click **Create**.



Create Access Gateway Session Policy

Name* sessionpol_AG

Request Profile* sessionprof_AG

Expression

Expression
ns_true

Match Any Expression

Named Expressions General | True value

Preview Expression ns_true

Now test it out….

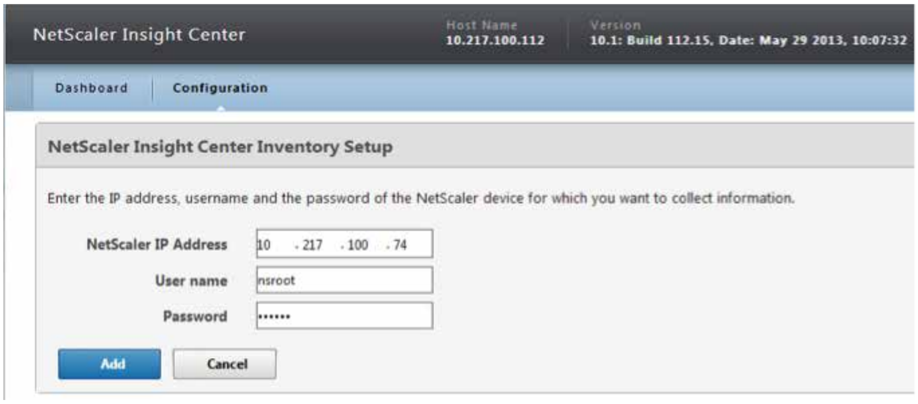
You should be able to log in, be forwarded to Citrix Receiver, see applications and launch applications.

5. Uncompromised monitoring

NetScaler Insight Center is an industry-first application that consolidates end-to-end web application data with Citrix virtual desktop infrastructure performance data in one place for further detailed analysis. This section shows how to configure NetScaler Insight Center to monitor the XenDesktop 7 deployment.

5.1 NetScaler Insight Center configuration and screens

Log into the NetScaler Insight Center GUI, navigate to **Configuration** and under **Inventory**, click **Add**. Enter the IP, username and password of the NetScaler appliance from which you want to collect AppFlow data.



NetScaler Insight Center

Host Name 10.217.100.112

Version 10.1: Build 112.15, Date: May 29 2013, 10:07:32

NetScaler Insight Center Inventory Setup

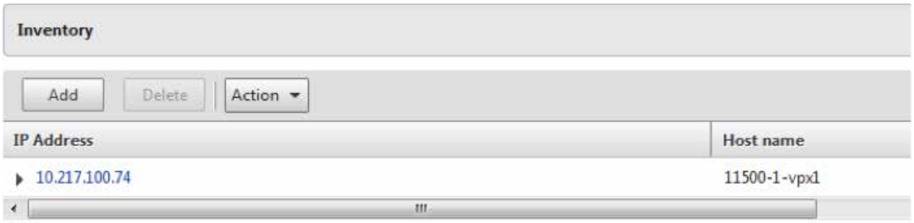
Enter the IP address, username and the password of the NetScaler device for which you want to collect information.

NetScaler IP Address 10 . 217 . 100 . 74

User name nsroot

Password ••••••

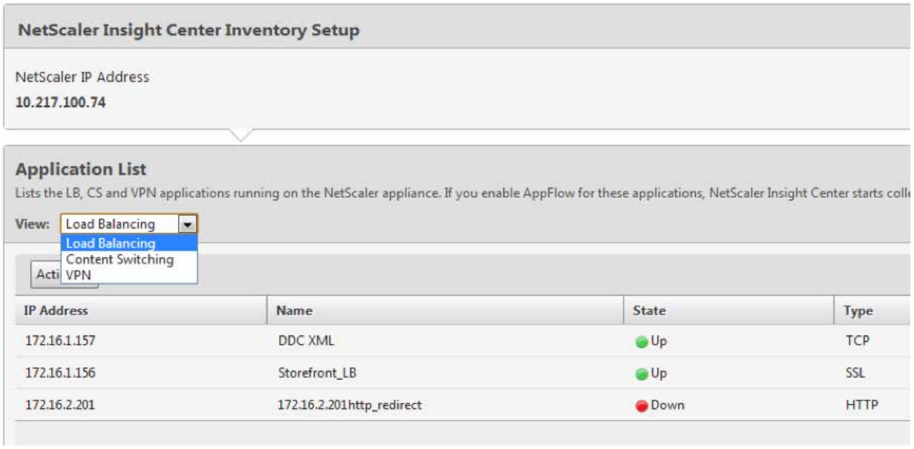
Click **Add**. Return to the **Inventory** screen, and the NetScaler appliance should be listed with its IP address and hostname.



Inventory

IP Address	Host name
10.217.100.74	11500-1-vpx1

Click on the IP address of the NetScaler appliance. All load balancing vServers, content switching vServers and NetScaler Access Gateway vServers should be shown on the **Applications List**.



NetScaler Insight Center Inventory Setup

NetScaler IP Address
10.217.100.74

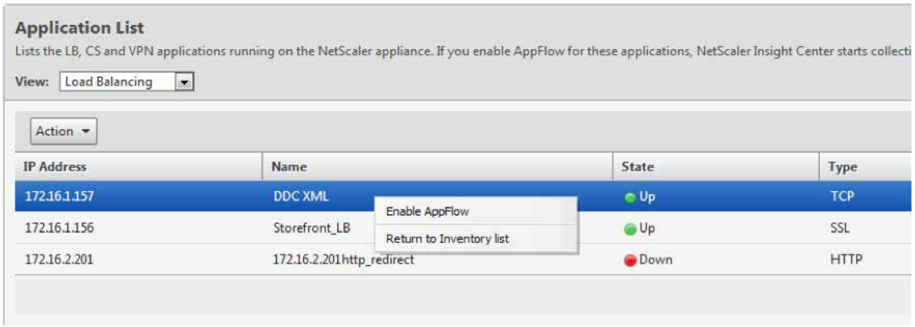
Application List

Lists the LB, CS and VPN applications running on the NetScaler appliance. If you enable AppFlow for these applications, NetScaler Insight Center starts coll

View: Load Balancing

IP Address	Name	State	Type
172.16.1.157	DDC XML	● Up	TCP
172.16.1.156	Storefront_LB	● Up	SSL
172.16.2.201	172.16.2.201http_redirect	● Down	HTTP

Navigate to the IP address and service for which you want to enable AppFlow logging, right click and select **Enable AppFlow**.



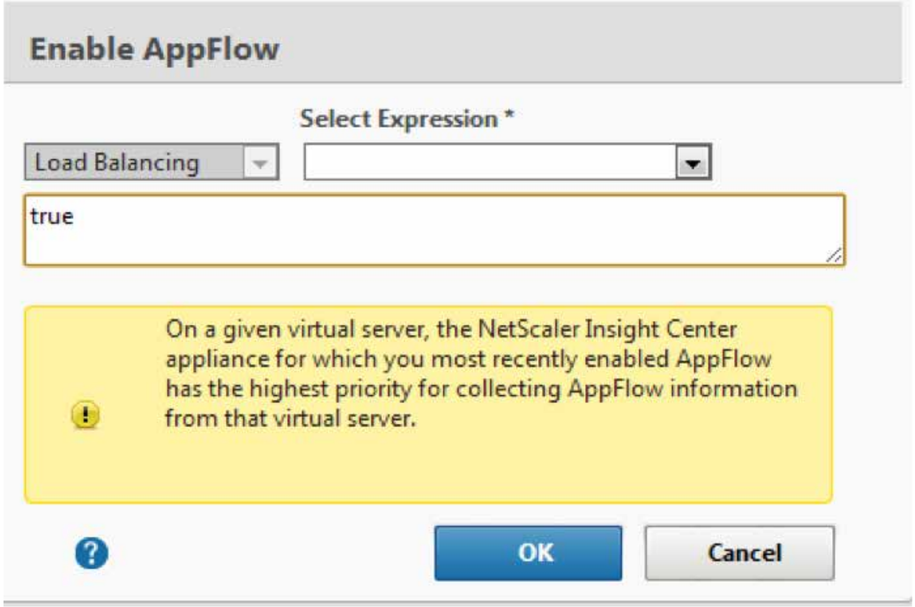
Application List

Lists the LB, CS and VPN applications running on the NetScaler appliance. If you enable AppFlow for these applications, NetScaler Insight Center starts collecti

View: Load Balancing

IP Address	Name	State	Type
172.16.1.157	DDC XML	● Up	TCP
172.16.1.156	Storefront_LB	● Up	SSL
172.16.2.201	172.16.2.201http_redirect	● Down	HTTP

You need to define an expression for the logging. This enables you to gather data only when a specific expression is true. To record all data from the vServer, enter **true** as the expression.



Enable AppFlow

Select Expression *

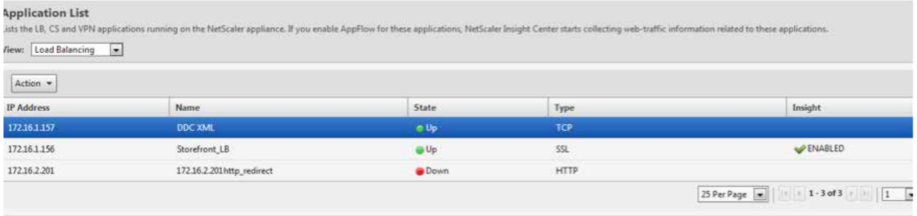
Load Balancing

true

On a given virtual server, the NetScaler Insight Center appliance for which you most recently enabled AppFlow has the highest priority for collecting AppFlow information from that virtual server.

Click **OK**.

Now there should be a green check mark with **ENABLED** under the insight column header. In the screenshot below, AppFlow logging has been enabled for the StoreFront load balancing vServer.



Application List

Lists the LB, CS and VPN applications running on the NetScaler appliance. If you enable AppFlow for these applications, NetScaler Insight Center starts collecting web-traffic information related to these applications.

View: Load Balancing

IP Address	Name	State	Type	Insight
172.16.1.157	DDC XML	● Up	TCP	
172.16.1.156	Storefront_LB	● Up	SSL	✓ ENABLED
172.16.2.201	172.16.2.201http_redirect	● Down	HTTP	

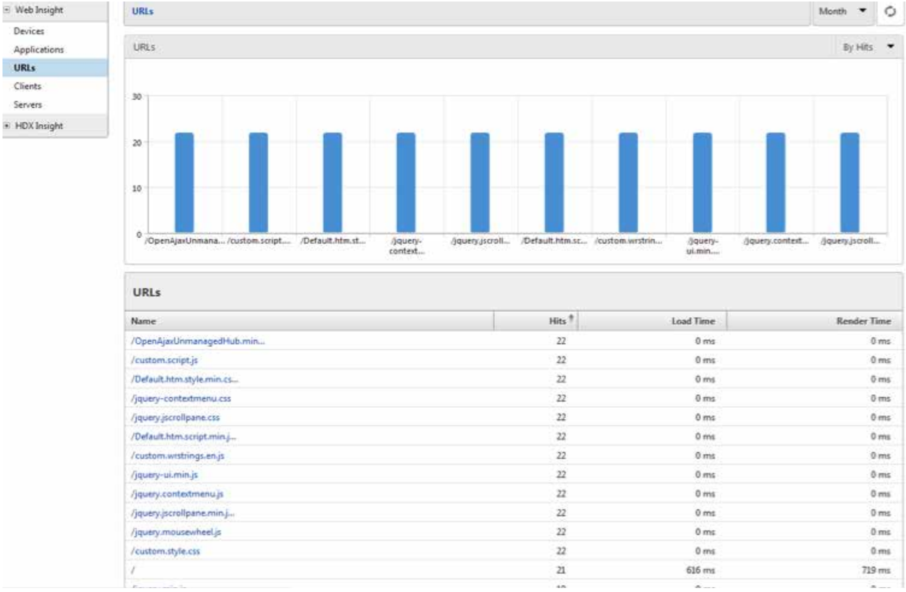
25 Per Page 1 - 3 of 3 1

NOTE: AppFlow logging must also be enabled on the NetScaler side to enable logging in Insight.

Repeat the process for any other load balancing vServers, then use the dropdown menu to switch to content switching vServers or VPN. The VPN category will list all NetScaler Access Gateway appliances. If the gateway runs in ICA proxy mode instead of VPN, check the **ICA** box when you complete the expression **true**.

Now navigate to the dashboard view and confirm that you can see the data gathered from NetScaler Access Gateway. In this example there is logging enabled on the StoreFront load balancing vServer, and several types of information are available, such as:

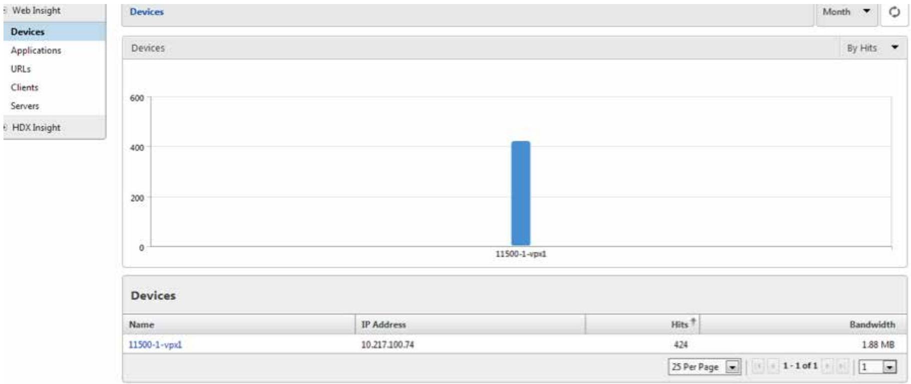
URLs



URLs

Name	Hits	Load Time	Render Time
/OpenAjaxUnmanagedHub.min...	22	0 ms	0 ms
/custom.script.js	22	0 ms	0 ms
/Default.htm.style.min.cs...	22	0 ms	0 ms
/jquery-contextmenu.css	22	0 ms	0 ms
/jquery.jscrollpane.css	22	0 ms	0 ms
/Default.htm.script.min.j...	22	0 ms	0 ms
/custom.wrstrings.en.js	22	0 ms	0 ms
/jquery-ui.min.js	22	0 ms	0 ms
/jquery.contextmenu.js	22	0 ms	0 ms
/jquery.jscrollpane.min.j...	22	0 ms	0 ms
/jquery.mousewheel.js	22	0 ms	0 ms
/custom.style.css	22	0 ms	0 ms
/	21	616 ms	719 ms

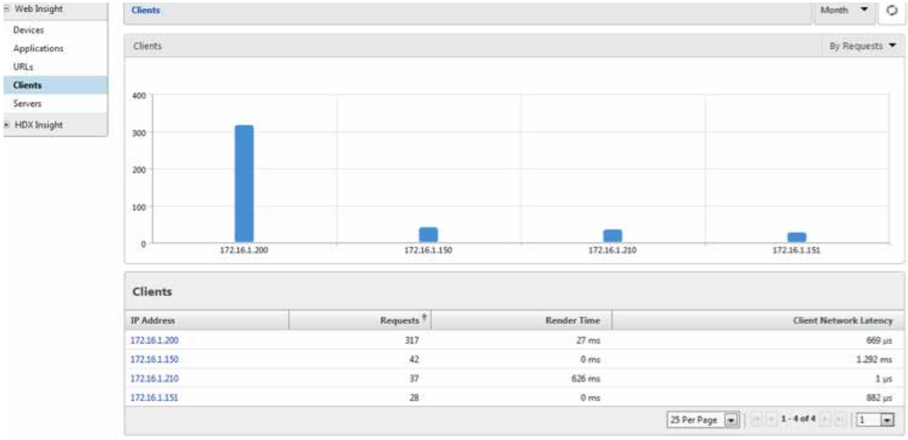
Devices (the NetScaler instances that are in use, by number of hits)



Devices

Name	IP Address	Hits	Bandwidth
11500-1-vpx1	10.217.100.74	424	1.88 MB

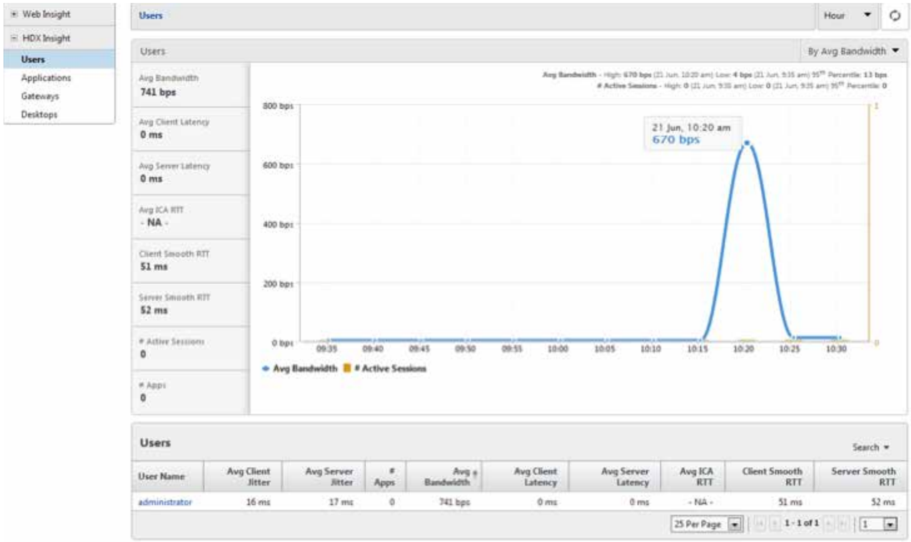
Clients (Infrastructure servers that NetScaler is contacting. 150,151 are StoreFront servers, 200 is DNS resolutions, etc.)



Clients

IP Address	Requests	Render Time	Client Network Latency
172.16.1.200	317	27 ms	669 µs
172.16.1.150	42	0 ms	1.292 ms
172.16.1.210	37	626 ms	1 µs
172.16.1.151	28	0 ms	882 µs

The HDX Insight portion of NetScaler Insight Center keeps detailed information about user ICA sessions. The following chart shows the average bandwidth, latency, RTT, etc., for a specific user.



Avg Bandwidth
741 bps

Avg Client Latency
0 ms

Avg Server Latency
0 ms

Avg ICA RTT
- NA -

Client Smooth RTT
51 ms

Server Smooth RTT
52 ms

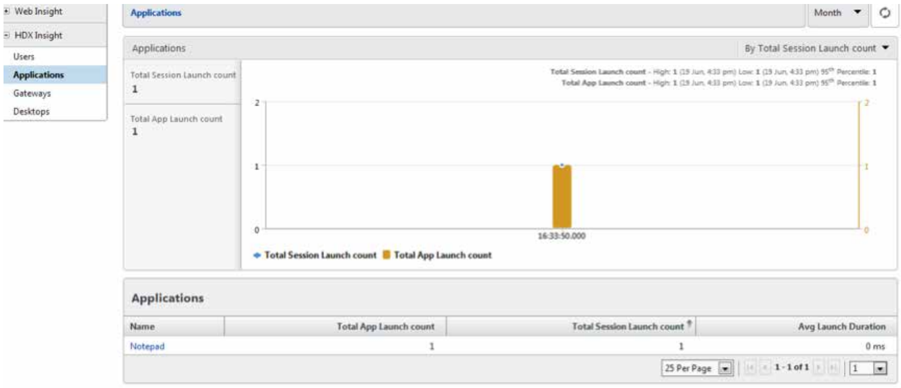
Active Sessions
0

Apps
0

Users

User Name	Avg Client Jitter	Avg Server Jitter	# Apps	Avg Bandwidth	Avg Client Latency	Avg Server Latency	Avg ICA RTT	Client Smooth RTT	Server Smooth RTT
administrator	16 ms	17 ms	0	741 bps	0 ms	0 ms	- NA -	51 ms	52 ms

Application launch history



Total Session Launch count
1

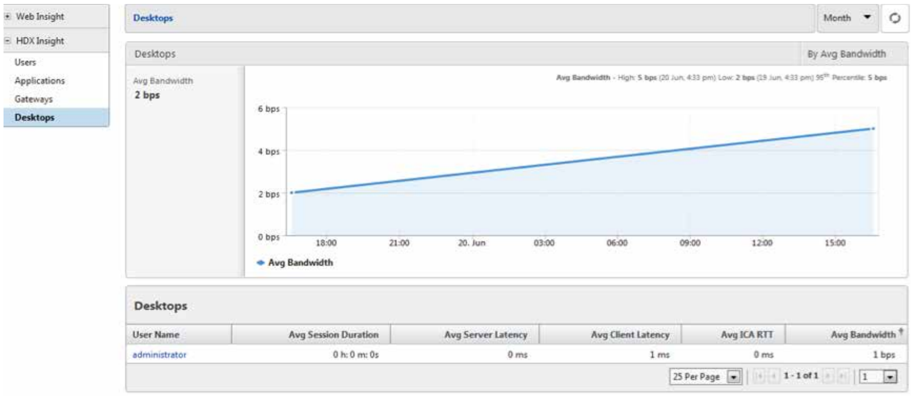
Total App Launch count
1

Total Session Launch count - High: 1 (19 Jun, 4:33 pm) Low: 1 (19 Jun, 4:33 pm) 95th Percentile: 1
Total App Launch count - High: 1 (19 Jun, 4:33 pm) Low: 1 (19 Jun, 4:33 pm) 95th Percentile: 1

Applications

Name	Total App Launch count	Total Session Launch count	Avg Launch Duration
Notepad	1	1	0 ms

Desktop performance and bandwidth



Avg Bandwidth
2 bps

Avg Bandwidth - High: 5 bps (20 Jun, 4:33 pm) Low: 2 bps (19 Jun, 4:33 pm) 95th Percentile: 5 bps

Desktops

User Name	Avg Session Duration	Avg Server Latency	Avg Client Latency	Avg ICA RTT	Avg Bandwidth
administrator	0 h: 0 m: 0s	0 ms	1 ms	0 ms	1 bps

6. Considerations and troubleshooting

- The StoreFront servers on SSL are particularly sensitive to the persistence settings on the load balancer.
- In this deployment, modifications have been made to the host's file on the StoreFront servers to resolve the FQDN of Access Gateway. These machines also had NetScaler Access Gateway set as their default to reach the IP on the external subnet.

7. Tables and references

7.1 Design decisions – overview

The best practice architecture uses two StoreFront servers and two DDCs for scale and availability. The two StoreFront servers are then configured behind a VIP on the load balancer. Users access the StoreFront service via the VIP. This provides increased availability to the control plane.

Decision point	Design decision	Justification
Management Servers		
Number of management servers	1 (1 for virtual desktop infrastructure, 0 for storage, 0 for monitoring, 1 for load balancer management software)	High availability
Deployment location		You can easily add another set of management servers to the cluster without reconfiguring the entire infrastructure.
Deployment hypervisor	XenServer 6.0.2	
Management server VM properties	CPU: 2 x vCPURAM: 40 GB RAM NIC: 2 1gbE NIC (Vlan 100) HDD: 100GB	

Decision point	Design decision	Justification
Monitoring VM	NetScaler Insight Center 10.1. Storage: 120gB CPU: 2x vCPU RAM: 4gB	
Operating system	RHEL 6 (64-bit)	
Management servers – load balancing		
Load balancing used	Yes	
Load balancer	NetScaler SDX 11500, w/ 1 VPX instance	
VIP (FQDN)		
SSL encryption	Yes	
MySQL database		
Number of MySQL servers (VM)	1	
Deployment hypervisor	XenServer 6.0.2	
Management server VM properties	CPU: 2 x vCPU RAM: 6 GB RAM NIC: 1 x NIC (vLAN 100) HDD: 100GB	
Operating system	RHEL 6 (64-bit)	
MySQL version	MySQL 5.6	
Replication	No Master: Slave:	

7.1. Design – zone architecture (Phoenix)

We've labeled this deployment the Phoenix zone and it has 3 VLAN's: Internal, DMZ, and Client. There's also an L3 router and a couple L2 switches, all completely virtualized. This deployment highlights only one zone but each zone can be replicated using different IP subnets. Each zone can be clustered. The isolation between tenants is provided by switch-based security zones.

Availability zone(s) – 1 (it is always recommended to go with two availability zones)		
Phoenix		
Deployment location	Phoenix, AZ	
Network mode	Basic (L3 network model)	The L3 network model is simple to manage and does not restrict the number of accounts. It also reduces the complexity of network management.
External DNS server(s)		
Internal DNS server(s)		
vLAN range		
Guest CIDR		
Public		
Domain		

7.2. Design decisions - networking

Decision point	Design decision	Justification
Distribution switch	Cisco Nexus 7000	

8. Conclusion

To conclude, it is quite apparent from this guide that the NetScaler ADC best optimizes your XenApp/XenDesktop deployment, as follows:

- Best end-user experience with the NetScaler ADC
- End-to-end application visibility with NetScaler Insight Center
- Enhanced security with the NetScaler ADC built-in firewall
- End-to-end support from a single vendor

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix
Citrix (NASDAQ:CTXS) is the cloud company that enables mobile workstyles—empowering people to work and collaborate from anywhere, easily and securely. With market-leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration and data sharing, Citrix helps organizations achieve the speed and agility necessary to succeed in a mobile and dynamic world. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally. Annual revenue in 2012 was $2.59 billion. Learn more at www.citrix.com.