Secure Multi-tenant Desktop as a Service with NetScaler VPX
Contents

Introduction ........................................................................................................................................... 3
Reference Architecture Lab Environment ............................................................................................... 4
  Software Components ............................................................................................................................ 5
NetScaler VPX ....................................................................................................................................... 6
  Access Gateway Virtual Server .............................................................................................................. 6
  Tenant Profiles and Policies ................................................................................................................... 7
Communication Flow of a User Connection ............................................................................................. 8
Step-by-step Configuration Guide ......................................................................................................... 9
  Configuring Web Interface ................................................................................................................... 9
  Configuring the NetScaler VPX .......................................................................................................... 20
  Web Interface - Access Gateway Integration ........................................................................................ 50
  Load Balancing Web Interface and XML Services .............................................................................. 57
Appendix A: Hypervisor Host Configuration ......................................................................................... 62
Appendix B: Virtual Machine Configurations ....................................................................................... 63
Appendix C: Web Interface Requirements and Installation ................................................................. 64
Appendix D: NetScaler VPX Requirements and Installation ................................................................. 67
Introduction

The Citrix® Reference Architecture for Multi-tenant Desktop as a Service guides partners in the process of designing the new generation of Desktop as a Service (DaaS) and Software as a Service (SaaS) services.

Figure 1: Citrix Reference Architecture for Desktop as a Service

The Citrix solution for DaaS and SaaS presents users with a familiar Windows desktop and applications experience, enabled by Citrix XenApp™ 6 and the Microsoft® Windows Server® 2008 R2 - Remote Desktop Services base operating system. Service Providers can deliver these DaaS and SaaS services to users of any Citrix Receiver™ enabled end-point device over secured public internet connections with Citrix NetScaler® and Access Gateway™.

The Citrix Cloud App Delivery Group’s engineering team deployed a complete implementation of the reference architecture in their lab environment. The complete implementation of the reference architecture leverages multiple vLANs, security zones and a combination of physical and virtual server installations to enable a highly scalable, high performance and easily managed multi-tenant DaaS solution for service providers targeting small to medium businesses.

More information on the Citrix Reference Architecture for Multi-tenant Desktop as a Service can be located at http://www.citrix.com/skb/articles/RDY4015.

This document, a companion to the Citrix Reference Architecture for Multi-tenant Desktop as a Service whitepaper listed above, outlines the configuration steps a CSP will perform to configure NetScaler and Access Gateway to provide secure connections for DaaS and SaaS subscribers.
1. The firewall appliance, in front of the NetScaler VPXs, provides NAT from the external Internet to the internal Access Gateway (virtual server). It also blocks all unwanted traffic from entering the CSP environment from the public network.

2. The NetScaler VPX HA pair in the DMZ provides secure access for tenants to their desktop and application resources.

3. The Management Network hosts a load-balanced pair of Citrix XML and Web Interface servers, Active Directory Domain Controllers and a Domain Certificate Authority.

The following table provides a brief description of the software components that you will install and integrate into the DaaS environment. Together, these components provide secure access to desktops and applications. For more information on each component, please follow the provided links.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler VPX</td>
<td>NetScaler combines high-speed load balancing and content switching, data compression, content caching, SSL acceleration, network optimization, application visibility and application security on a single, comprehensive platform.</td>
</tr>
<tr>
<td>Web Interface</td>
<td>The Web Interface provides users with access to XenApp applications and content and XenDesktop virtual desktops. Users access their resources through a standard Web browser or through the Citrix online plug-in.</td>
</tr>
<tr>
<td>XML Service</td>
<td>The XML Service receives user credentials from the Web Interface and queries the server farm for a list of published applications that the user has permission to access. The XML Service retrieves this application set from the XenApp farm and returns it to the Web Interface.</td>
</tr>
<tr>
<td>Secure Ticket Authority (STA)</td>
<td>The Secure Ticket Authority (STA) is an XML Web service that exchanges XenApp server information for randomly generated tickets. The STA controls access for a Citrix Secure Gateway server.</td>
</tr>
<tr>
<td>Active Directory Domain Services (AD DS)</td>
<td>Active Directory Domain Services (AD DS) is the central location and authentication authority for users, computers, groups, printers and applications that are stored within your forest.</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>A certificate authority (CA) is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. Certificate Authorities can include well known public entities such as VeriSign or internally managed enterprise CAs running on the Windows Server platforms.</td>
</tr>
</tbody>
</table>

Table 1: Secure Access Software Components
NetScaler VPX

Citrix NetScaler is a modular platform upon which you will build several critical network security and acceleration functions. For those CSPs focused on the small to medium businesses, the Citrix Access Gateway capabilities within NetScaler are fundamental to the secure delivery of desktops and applications as a service.

The NetScaler VPX can leverage the high availability options of the hypervisor to ensure that secure access services remain operational and reduce downtime caused by hardware failures. The virtual appliance delivers the same scalability as a physical appliance and can support 500 concurrent users per virtual machine when configured according to specification.

Access Gateway Virtual Server

The Access Gateway Enterprise Edition virtual server is an entity within a NetScaler VPX. The virtual server is the access point through which clients access services from within the CSP network. Administrators can configure multiple virtual servers on a single appliance, allowing one appliance to serve multiple user communities (tenants in our example) with differing authentication and resource access requirements.

Citrix engineers used the Access Gateway service of Citrix NetScaler VPX (Virtual Appliance) in the Citrix Cloud App Delivery lab environment to provide secure access to the DaaS environment over SSL (TCP 443) across the public internet. Access Gateway multi-tenant support can be implemented either within a single NetScaler VPX, physical appliance HA pair, or across segregated networks and vLANs with a dedicated NetScaler appliance per tenant vLAN. From a software configuration perspective, all of these scenarios are fundamentally the same considering the integration points between the DMZ and Multi-tenant DaaS network.
Tenant Profiles and Policies

Authentication, authorization and accounting (AAA) policies allow users to log on to the Access Gateway with credentials that are validated by authentication servers (e.g. LDAP, RADIUS) located in the secure network. Authorization policies determine which resources a given user can access.

In the Citrix Reference Architecture for Multi-tenant Desktop as a Service, Citrix engineers created a single Active Directory (AD) domain with multiple OUs – each OU representing one tenant. The following figure shows the AD infrastructure. The “servers” OU for each tenant contains that tenant’s dedicated XenApp servers and the “users” OU contains that tenant’s user accounts. Each tenant also has an associated AAA group and policy that will enable subscribers to securely and seamlessly logon to their DaaS and SaaS resources.

A session profile defines the settings for user’s connections and they are associated to session policies. You can create profiles separately from the policy using the configuration utility and then use the profile for multiple policies.

Integration with Web Interface

Once you have configured Access Gateway it must be associated with a Citrix Web Interface site in order for subscribers to gain access to their DaaS and SaaS subscribed services.

In this typical scenario, tenants will use a web browser or end-point running Citrix Receiver to access a secure logon point hosted by the CSP. After providing the appropriate credentials, Access Gateway directs users to their organization’s customized Citrix Web Interface in order to access their subscribed resources.
1. The user connects to the NetScaler/Access Gateway using the Fully Qualified Domain Name (FQDN) "https://agcsp.skylab.com".
   a. Upon a successful connection the Access Gateway authentication page is displayed.

After entering their username and password the following authentication process takes place:

2. The Access Gateway authenticates the user against the authentication server (AD/LDAP in this example) configured in the Authentication Policy.
3. Once authenticated, the Access Gateway passes the credentials to the Citrix Web Interface Servers.
4. The Web Interface server connects back to the Access Gateway SSL VPN virtual server utilizing the AD username and password provided by the user. The Access Gateway verifies the validity of the user by comparing the hash of the returned credentials to the hash it its session table. It returns the session policy and SSL VPN virtual server name to Web Interface. This information is then passed to the Citrix XML Service for policy verification.
5. The Web Interface Server forwards the user’s credentials to the Citrix XML Service running on the Citrix XenApp server.
6. The XML Service then authenticates the user against the Active Directory. Once successfully authenticated, the XML Service retrieves a list of resources from the Citrix XenApp farm that the users can access.
Step-by-step Configuration Guide

The following section will walk through the steps required to configure the Web Interface, NetScaler VPX and the Access Gateway virtual servers for secure access to the DaaS environment.

1. **Configuring Web Interface**
   i. Creating a Tenant XenApp Web Site
   ii. Creating a Tenant XenApp Services Site (Mobile Receiver)

2. **Configuring NetScaler VPX**
   i. Configuring the Access Gateway virtual server for multi-tenant access

3. **Web Interface – Access Gateway Integration**
   i. Configuring the XenApp Web Site to integrate with Access Gateway
   ii. Configuring the XenApp Services Site to integrate with Access Gateway

4. **Load Balancing Web Interface and XML Services**

Configuring Web Interface

For information about the installation of the Web Interface software, reference Appendix C. The following configuration steps will be conducted within the Citrix Web Interface Management Console. If multiple Web Interface servers are deployed, these steps will need to be executed on each server.

Creating a Tenant XenApp Web Site

1. Open the **Citrix Web Interface Management Console** and select the **XenApp Web Site**.
2. Select **Create Site** from the Actions pane.

3. In the **Create Site** window, **enter** the **path** to the Tenant web site.

4. Click **Next**.
5. Select “At Access Gateway“ as the authentication method.
6. Click Next.

7. Enter the “Authentication service URL”. Tenant subscribers will be using [https://AGCSP.skylab.com] to access their resources. Note: The Authentication service URL must match https://AGCSP.skyab.com/CitrixAuthSerice/AuthService.asmx.
8. Click **Next**.

9. **Verify** the site configuration information is correct and click **Next** to create the site.

10. After the site is created, check “Configure this site now” checkbox and click **Next**.
11. **Enter** the Citrix XenApp farm name and Citrix XenApp XML server name and port. The actual XML service port depends on the options selected during the XenApp install. If the XML Service shares a port with IIS, use port 80.

12. Click **Next**
13. Choose whether the Minimal or Full logon appearance will be displayed.
14. Click Next.

15. Select Online and click Next.
16. Click **Finish** to complete the basic site configuration.
17. We will come back to the Citrix Web Interface Management Console for further configuration of the XenApp Web site after the Access Gateway virtual server is configured.
18. **Repeat** the above steps for additional tenants.
Creating a Tenant XenApp Services Site (Mobile Receiver)

1. Open the Citrix Web Interface Management console, select the XenApp Services Site

2. Select Create Site from the Actions pane.
3. In the Create Site window, enter the **path** and **name** of the Tenant mobile web site.

4. Click **Next**

5. **Verify** the configuration is correct and click **Next** to create the site.
6. After the site is created, check “Configure this site now” checkbox and click Next.

7. Enter the Citrix XenApp farm name and Citrix XenApp XML server name and port. The actual XML service port depends on the options selected during the XenApp install. If the XML Service shares a port with IIS, use port 80.
8. Select **Online** and click **Next**.

9. Click **Finish** to complete the basic site configuration.

10. We will come back to the Citrix Web Interface Management Console for further configuration of the XenApp Services site after the Access Gateway virtual server is configured.

11. Repeat the above steps for additional tenants.
Configuring the NetScaler VPX

For information about the installation of NetScaler VPX, reference Appendix D. The following configuration steps will be conducted on the NetScaler VPX appliance:

1. Creating and installing certificates
2. Creating the Access Gateway Virtual Server
3. Creating an Authentication Policy
4. Creating Tenant Session Profiles
5. Creating Session Profiles for Mobile Tenants
6. Creating Tenant Session Policies
7. Creating Tenant AAA groups

Creating and Installing Certificates

In the Citrix Cloud App Delivery lab environment tenants will be required to browse to https://agcsp.skylab.com and authenticate before they can access their desktop and application resources.

Since this DaaS environment will be accessed from public networks and the Internet, end-to-end SSL encryption is necessary in order to protect sensitive tenant information and data. In order to facilitate this, a certificate with common name of agcsp.skylab.com is required to be installed on the Citrix NetScaler.

Creating a certificate request

1. Launch the NetScaler’s administration interface and select the SSL node.
2. In the right pane of admin UI, click the Create RSA Key link.

3. In the Key Filename field, specify a name for the key file.
4. In the Key Size field, specify the size for the key file.
5. Ensure that you select the PEM key format, as shown in the screenshot above.
6. Select an appropriate PEM encoding algorithm. The selection of the PEM algorithm depends on the organizational policies.
7. Click Create.
8. Click Close.
9. In the right pane of admin UI, click the Create Certificate Request link.

10. In the Request File Name field, specify the file name of the CSR file.
11. In the Key File Name, specify the RSA key file name that you have created in the previous step.
12. Ensure that you select PEM as the key format.
13. If a password was entered in the previous step, enter the password for the key file.
14. In the Distinguished Name Fields group, specify the appropriate values for the site.
15. Click Create.
16. Click Close.
17. Using a secure FTP tool (e.g. WinCSP), **download** the newly created **request file** to your workstation. The request file can be found on the NetScaler in the `/flash/nsconfig/ssl/` directory.

18. **Submit** the **certificate** to your certificate authority.
Installing the certificate

1. Once the certificate is back from the CA, use a secure FTP program to upload the certificate to the NetScaler. Upload to the following directory: /flash/nsconfig/ssl/

2. Log on to the NetScaler. Expand the SSL folder and click on the Certificates node.
3. In the right pane, **click** the **Add** button.

4. **Provide** a meaningful name for the **key-pair name**.
5. For the Certificate File Name, **enter** the certificate file you received from the certificate authority.
6. For the Private Key File Name, use the name of key file you generated in the previous step.
7. Click **Install** to install the certificate.
Creating the Access Gateway Virtual Server

The virtual server created here will be shared among all tenants. It is not necessary to create one virtual server for each tenant, even though it can be done.

1. In the NetScaler administration UI, expand the Access Gateway folder, and select the Virtual Servers node.

1. Click Add in the right pane to create a virtual server.
2. Enter a Name for the virtual server.
3. Enter a unique internal IP Address.
4. Select the Certificates tab; add the certificate just created to the virtual server.
5. Select the **Published Applications** tab and click the **Add** button.
6. **Enter the IP or FQDN** of the Secure Ticket Authority. If the STA or XML server is a load-balanced entity, use the virtual server IP or FQDN. Please see [load balancing section](#) on how to create load-balanced virtual servers. It is recommended practice to select your XML Service or Data Collector servers to host the STA role. In this environment the backup data collector was selected for the STA. If the XML service on the STA server is running on a port other than 80, insert the port number in the URL.
Creating an Authentication Policy

1. Select the Policies folder.

2. Select the Authentication node. In the right pane, select the Servers tab.
3. Click Add at the bottom to create a new Authentication server.
4. **Enter** the **Name** of the authentication server.
5. **Enter** the **IP Address** of the domain controller.
6. **Enter** domain connection **settings**.
7. Click **Create**.
8. Now select the Policies tab and click Add.

9. In the “Create Authentication Policy” window, Enter the name of policy.
10. In the server dropdown box, select the name of the authentication server just created.
11. Enter “ns_true” in the Expression section.
Creating Tenant Session Profiles

1. **Select** the **Session** node under the policies folder.

2. In the Right pane, **select** the **Profile Tab** and **click** the **Add** button to create a new profile.
3. In the “Create Access Gateway Session Profile” window, enter the name of profile.
4. **Select** the Client Experience Tab.
   a. Split Tunnel is set to **ON**.
   b. Clientless Access set to **Allow**.
   c. **Single Sign-on** to web Application is **checked**.
   d. **Single Sign-on** with windows is **checked**.

5. Select the Security Tab.
7. Select the Published Applications Tab.
   a. Verify that ICA Proxy is ON
   b. Enter the Web Interface or the WI load-balanced virtual server address created
      in the Creating a Tenant XenApp Web Site section.
   c. Web Interface Portal Mode - NORMAL
   d. Single Sign-on Domain name
8. Repeat the steps for each tenant.
Creating Session Profiles for Mobile Tenants

1. **Select** the **Session** node under the policy node.

2. In the Right pane, **select** the **Profiles** tab and select **Add** to create a new profile.
3. In the “Create Access Gateway Session Profile” window, enter a name for a profile
4. Select the Client Experience tab
5. Split Tunnel is set to **ON**
6. Clientless Access set to **Allow**
7. **Single Sign-on** to web Application is checked
8. **Single Sign-on** with windows is checked
9. Select the **Security** tab.
10. Set Default Authorization to **ALLOW**.

11. Select the **Published Applications** tab.
12. Set ICA Proxy to **ON**.
13. Enter the **Web Interface** or the **WI load-balanced virtual server** address created in the Creating a Tenant XenApp Services Site section.
14. Web Interface Portal Mode – **NORMAL**.
15. **Enter** the Domain name.
16. Repeat for each additional tenant.
1. Select the Policies tab and click the Add at the bottom.
2. In the “Create Access Gateway Session Policy” window, enter the following information:
   a. Enter a name for the policy.
   b. Select the profile just created from the request Profile dropdown box.
   c. Enter “ns_true” in the expression section.
3. Repeat steps for each additional tenant.
1. **Select** the Policies tab and **click** the **Add** button.
2. In the “Create Access Gateway Session Policy” window, enter the following information:
   a. Name for the policy.
   b. Select the profile just created from the Request Profile dropdown box.
   c. Click the Add next to the Match Any Expression.

3. Enter `REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver` expression.
4. Click OK.
5. After the expression is added, the Policy window will look like this.
6. Click **Create** to create the policy.
7. Repeat for each additional tenant.
Creating Tenant AAA groups

AAA groups provide security for a distributed Internet environment by allowing any client with the proper credentials to connect securely to protected application servers from anywhere on the Internet. This feature incorporates the three security features of authentication, authorization, and auditing. Authentication enables the NetScaler appliance to verify the client’s credentials, either locally or with a third-party authentication server, and allow only approved users to access protected servers. Authorization enables the appliance to verify which content on a protected server it should allow each user to access. Auditing enables the appliance to keep a record of each user’s activity on a protected server.

1. From the NetScaler administration console select the Groups node under the Access Gateway folder.

2. In the right pane, click the Add button at the bottom.
3. Within the pop window, enter the name of the group. Make sure that the Group Name exactly matches the name of the AD security group that Tenant users belong to. The above figure shows the AAA group Tenant1SG matches exactly to the security group Tenant1SG in Active Directory.

4. Select the Policies tab and click the Session icon. Click Insert Policy and insert the session policies created in the step above. It is important that the “mobile policy” is higher in priority than the access session policy.

5. Repeat for each tenant.
Web Interface - Access Gateway Integration

XenApp Web Site Access Gateway Integration

The following section will walk through the configuration changes required on the Web Interface Web Site in order to complete the integration with the Access Gateway virtual server.

1. Logon on the Citrix Web Interface Management Console.
2. Select the Tenant XenApp Web Interface Site and select Secure Access.
3. Change the access method to **Gateway Direct**.
4. Click **Next**.

5. Enter the **FQDN** of the **Access Gateway**. Click **Next**
6. Enter the URL of the Secure Ticket Authority. It is recommended practice to select your XML Service or Data Collector servers to host the STA role. In this environment the backup data collector was selected for the STA. If the XML service on the STA server is running on a port other than 80, insert the port number in the URL.

7. Click OK and Finish.

8. Repeat for each additional tenant.
XenApp Services Site Access Gateway Integration

The following section will walk through the configuration changes required on the Web Interface Services Site in order to complete the integration with the Access Gateway virtual server.

1. **Logon** on the Citrix Web Interface Management Console.
2. Select the Tenant **XenApp Service** Interface Site and click the **Secure Access** link.
3. Change the access method to **Gateway Direct**.
4. Click **Next**.

5. Enter the **FQDN** of the **Access Gateway**. Click **Next**
6. Enter the URL of the Secure Ticket Authority. It is recommended practice to select your XML Service or Data Collector servers to host the STA role. In this environment the backup data collector was selected for the STA. If the XML service on the STA server is running on a port other than 80, insert the port number in the URL.

7. Click OK and Finish.

8. Your configured site should look like the following graphic.
1. Select “Authentication Methods” in the right pane

2. In the pop up window, change the default authentication to “Pass-Through”

3. Repeat for each tenant.
Load Balancing Web Interface and XML Services

NetScaler load balancing services is a core component responsible for distributing incoming traffic among servers hosting the same content. In this environment, the content consists of tenant Web Interface sites and services, and Citrix XML Servers. By balancing requests across multiple servers, the NetScaler prevents any server from becoming a single point of failure, thus improving overall availability and responsiveness. In a multi-tenant DaaS environment, these services are critical in ensuring that Service Provider HA, DR and performance SLA requirements are met.

The next section details the steps to create Web Interface and XML Server load-balanced services on the NetScaler VPX virtual appliance.

1. From within the Netscaler administration UI. Click on the Load Balancing folder.
2. In the right pane click on the “Load Balancing wizard for Citrix XenApp” link, the following window will appear.
3. Click Next.

4. Enter the **IP Address** and **port** of the Web Interface virtual server. This IP address needs to be an address that is accessible from the NetScaler.

5. Enter the **IP Addresses** and **ports** of the Web Interface servers. Since the NetScalers will communicate with the Web Interface servers over port 443, the certificates created earlier will need to be installed on the Web Interface servers.

6. Click **Next**.
7. **Enter** the **IP Address** of the XML Server virtual server. This IP address needs to be an address that is accessible from the NetScaler. Enter the port the XML Service is configured on, in this case port 8080 is used.

8. **Enter** the **IP Addresses** of the XML Servers.

9. **Click** **Next**

10. This completes the Load Balancing configuration of the Web Interface and XML virtual servers.

**Verifying Load Balancing Configuration**

1. From within the Netscaler administration UI, **Click** on the **Load Balancing** folder.
2. **Click** on the **Virtual Servers** object.
3. **Verify** that the Virtual Servers were created and that their **State** and **Effective State** are **UP**.
4. From within the Netscaler administration UI, **Click** on the **Load Balancing** folder.
5. **Click** on the **Service Groups** object.
6. **Verify** that the Service Groups were created and that their **State** and **Effective State** are **UP**.

7. From within the Netscaler administration UI, **Click** on the **Load Balancing** folder.
8. **Click** on the **Monitors** object.
9. **Verify** that the Monitors were created and that their **State** is **UP**.

10. From within the Netscaler administration UI, **Click** on the **Load Balancing** folder.
11. **Click** on the **Servers** object.
12. **Verify** that the Servers were created and that their **State** is **ENABLED**.
13. The last step is to create DNS **Host records** for the Access Gateway, Web interface and XML virtual servers.
Appendix A: Hypervisor Host Configuration

The Citrix DaaS solution is hypervisor agnostic, any of the following hypervisors can be used for the infrastructure or the XenApp servers used to deliver the shared hosted desktops:

**Citrix XenServer**

Citrix® XenServer® is a complete, managed server virtualization platform built on the powerful Xen® hypervisor. Xen technology is widely acknowledged as the fastest and most secure virtualization software in the industry. XenServer is designed for efficient management of Windows® and Linux® virtual servers and delivers cost-effective server consolidation and business continuity. More information on XenServer can be obtained at the company website.

**Microsoft Hyper-V**

Microsoft Windows Server 2008 R2 Hyper-V builds on the architecture and functions of Windows Server 2008 Hyper-V by adding multiple new features that enhance product flexibility. Hyper-V is available in a Standard, Server Core and free Hyper-V Server 2008 R2 versions. More information on Hyper-V can be obtained at the company website.

**VMware vSphere**

VMware vSphere consists of the management infrastructure or virtual center server software and the hypervisor software that virtualizes the hardware resources on the servers. It offers features like Distributed resource scheduler, vMotion, HA, Storage vMotion, VMFS, and a mutlipathing storage layer. More information on vSphere can be obtained at the company website.

The following server types were used to host the infrastructure for the entire Citrix DaaS solution.

**Server Hardware used in the Citrix lab implementation**

2 x HP DL360
Dual – Quad core Intel E5335 @ 2.00 GHz
16GB – PC3 1066MHz
6 x 1Gbe NICs

10 x HP DL380
Dual – Quad core Intel E5335 @ 2.00 GHz
96GB – PC3 1066MHz
6 x 1Gbe NICs
## Appendix B: Virtual Machine Configurations

### NetScaler VPX Configuration

<table>
<thead>
<tr>
<th>Hypervisor</th>
<th>XenServer 5.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>NetScaler VPX 9.3</td>
</tr>
<tr>
<td>Server 1</td>
<td>4vCPU, 4 GB RAM</td>
</tr>
<tr>
<td>Server 2</td>
<td>4vCPU, 4 GB RAM</td>
</tr>
</tbody>
</table>

### Web Interface Server Configuration

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Microsoft Windows Server 2008 R2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed Roles/Features</td>
<td>Internet Information Services 7.5</td>
</tr>
<tr>
<td>Additional Software</td>
<td>.NET Framework 3.5 with Service Pack 1</td>
</tr>
<tr>
<td></td>
<td>Visual J#.NET 2.0 Second Edition</td>
</tr>
<tr>
<td></td>
<td>ASP.NET 2.0</td>
</tr>
<tr>
<td></td>
<td>Web Interface 5.3</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>XenServer 5.6</td>
</tr>
<tr>
<td>Server</td>
<td>4 vCPU, 4GB RAM</td>
</tr>
</tbody>
</table>

### Active Directory Server Configuration

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Microsoft Windows Server 2008 R2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed Roles</td>
<td>Active Directory Services</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>XenServer 5.6</td>
</tr>
<tr>
<td>Virtual Server Specifications</td>
<td>4 vCPU w/ 4GB RAM</td>
</tr>
</tbody>
</table>

### Data Collector / XML Server Configuration

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Microsoft Windows Server 2008 R2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed Roles/Features</td>
<td>During a wizard-based XenApp installation, the Server Role Manager (using the Server Role Installer), automatically installs all prerequisite software and Windows Server roles.</td>
</tr>
<tr>
<td>Additional Software</td>
<td>XenApp 6</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>XenServer 5.6</td>
</tr>
<tr>
<td>Server</td>
<td>4 vCPU, 8GB RAM</td>
</tr>
</tbody>
</table>
## Appendix C: Web Interface Requirements and Installation

### Web Interface Server Requirements

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Web server</th>
<th>Runtime/JDK</th>
<th>Servlet engine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 R2 x64</td>
<td>Internet Information Services 7.5</td>
<td>.NET Framework 3.5 with Service Pack 1</td>
<td>N/A</td>
</tr>
<tr>
<td>Windows Server 2008 x64 Editions with Service Pack 2</td>
<td>Internet Information Services 7.0</td>
<td>Visual J#.NET 2.0 Second Edition</td>
<td>ASP.NET 2.0</td>
</tr>
<tr>
<td>Windows Server 2008 x86 with Service Pack 2</td>
<td>Internet Information Services 6.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003 R2 x86 with Service Pack 2</td>
<td>Internet Information Services 6.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003 Standard Edition x86 with Service Pack 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003 Enterprise Edition x86 with Service Pack 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003 R2 Standard Edition x86 with Service Pack 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003 R2 Standard Edition x64 with Service Pack 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003 Standard Edition x86 with Service Pack 2</td>
<td>Apache 2.2.x</td>
<td>Java 1.6.x</td>
<td>Apache Tomcat 6.0.x</td>
</tr>
</tbody>
</table>
To install the Web Interface on Microsoft Internet Information Services

Before installing the Web Interface, you must configure your server to add the Web server role and install IIS and ASP.NET.

To use IIS 7.x on Windows Server 2008, install the **Web Server (IIS)** role and then enable the following role services:

- **Web Server > Application Development > ASP.NET**
- **Management Tools > IIS 6 Management Compatibility > IIS 6 Metabase Compatibility**

If you plan to enable pass-through, pass-through with smart card, and/or smart card authentication, you also need to install the following role services:

- For pass-through and pass-through with smart card authentication, enable **Web Server > Security > Windows Authentication**
- For smart card authentication, enable **Web Server > Security > Client Certificate Mapping Authentication**

To use IIS 6.0 on Windows Server 2003, add the **Application server (IIS, ASP.NET)** role and enable ASP.NET.

On IIS, each site is assigned to an application pool. The application pool configuration contains a setting that determines the maximum number of worker processes. If you change the default value of one, you might not be able to run the Web Interface.

After configuring your server role, ensure that .NET Framework 3.5 with Service Pack 1 and Visual J#.NET 2.0 Second Edition are installed.

1. Log on as an administrator.

If you are installing the Web Interface from the XenApp or XenDesktop installation media, insert the disc in your Web server’s optical drive.

If you downloaded the Web Interface from the Citrix Web site, copy the file WebInterface.exe to your Web server.

2. Navigate to and double-click the file WebInterface.exe.

3. Select your language from the list. The language of your operating system is detected and appears as the default selection. Click **OK**.

4. On the **Welcome** page, click **Next**.

5. On the **License Agreement** page, select **I accept the license agreement** and click **Next**.
6. On the **Installation Location** page, browse to an installation location for the Web Interface (the default is C:\Program Files (x86)\Citrix\Web Interface\). Click **Next**.

7. On the **Location of Clients** page, select **Copy the clients to this computer**. Click **Browse** to search the installation media or your network for the Citrix client setup files.

Setup copies the contents of the \Citrix Receiver and Plug-ins folder on the installation media or network share to the Web Interface \Clients folder, typically C:\Program Files (x86)\Citrix\Web Interface\Version\Clients. All Web sites created by the installation process assume that the Web server contains the client files in this directory structure.

If you do not want to copy the clients to the Web server during Web Interface installation, select **Skip this step**. You can copy the clients to the server later.

8. Click **Next** to continue and click **Next** again to confirm that you are ready to begin the installation.

9. When the installation is complete, click **Finish**.

10. On the Windows **Start** menu, click **All Programs > Citrix > Management Consoles > Citrix Web Interface Management** to access the Citrix Web Interface Management console and begin creating and configuring your sites.
## Appendix D: NetScaler VPX Requirements and Installation

### Hypervisor Hardware Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2 or more 64-bit x86 CPUs with virtualization assist (Intel-VT or AMD-V) enabled</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> To run NetScaler VPX, hardware support for virtualization must be enabled on the host. Make sure that the BIOS option for virtualization support is not disabled. Consult your BIOS documentation for more details.</td>
</tr>
<tr>
<td>RAM</td>
<td>3 gigabytes (GB)</td>
</tr>
<tr>
<td>Disk space</td>
<td>Locally attached storage (PATA, SATA, SCSI) with 40 GB of disk space</td>
</tr>
<tr>
<td>Network Interface Card (NIC)</td>
<td>1 one gigabits per second (Gbps) NIC; 2 one Gbps NICs recommended</td>
</tr>
</tbody>
</table>


For information about installing VMware ESX, see [http://www.vmware.com/](http://www.vmware.com/).


### Installing NetScaler Virtual Appliances on XenServer by Using XenCenter

After you have installed and configured XenServer and XenCenter, you can use XenCenter to install virtual appliances on XenServer. The number of virtual appliances that you can install depends on the amount of memory available on the hardware that is running XenServer.

**To install NetScaler virtual appliances on XenServer by using XenCenter**
1. Start XenCenter on your workstation.

2. On the Server menu, click Add.

3. In the Add New Server dialog box, in the Hostname text box, type the IP address or DNS name of the XenServer that you want to connect to.

4. In the User Name and Password text boxes, type the administrator credentials, and then click Connect. The XenServer name appears in the navigation pane with a green circle, which indicates that the XenServer is connected.

5. In the navigation pane, click the name of the XenServer on which you want to install NetScaler VPX.

6. On the VM menu, click Import.

7. In the Import dialog box, in Import file name, browse to the location at which you saved the NetScaler VPX .xva image file. Make sure that the Exported VM option is selected, and then click Next.

8. Select the XenServer on which you want to install the virtual appliance, and then click Next.

9. Select the local storage repository in which to store the virtual appliance, and then click Import to begin the import process.

10. You can add, modify, or delete virtual network interfaces as required. When finished, click Next.

11. Click Finish to complete the import process.

Note: To view the status of the import process, click the Log tab.

12. If you want to install another virtual appliance, repeat steps 5 through 11.

Installing NetScaler Virtual Appliances on VMware ESX 4.0

After you have installed and configured VMware ESX 4.0, you can use VMware vSphere client to install virtual appliances on the VMware ESX. The number of virtual appliances that you can install depends on the amount of memory available on the hardware that is running VMware ESX.

To install NetScaler virtual appliances on VMware ESX 4.0 by using VMware vSphere Client

1. Start the VMware vSphere client on your workstation.

2. In the IP address / Name text box, type the IP address of the VMware ESX server that you want to connect to.
3. In the **User Name** and **Password** text boxes, type the administrator credentials, and then click **Login**.

4. On the **File** menu, click **Deploy OVF Template**.

5. In the **Deploy OVF Template** dialog box, in **Deploy from file**, browse to the location at which you saved the NetScaler VPX setup files, select the .ovf file, and click **Next**.

6. Map the networks shown in the VPX OVF template to the networks that you configured on the ESX host. Click **Next** to start installing VPX on VMware ESX. When installation is complete, a pop-up window informs you of the successful installation.

7. You are now ready to start the NetScaler VPX. In the navigation pane, select the NetScaler VPX that you have just installed and, from the right-click menu, select **Power On**. Click the **Console** tab to emulate a console port.

8. If you want to install another virtual appliance, repeat steps 4 through 6.

**Installing NetScaler VPX on Microsoft Server 2008 R2**

After you have enabled the Hyper-V role on Microsoft Server 2008 R2 and extracted the VPX files, you can use Hyper-V Manager to install NetScaler VPX. After you import the virtual machine, you need to configure the virtual NICs by associating them to the virtual networks created by Hyper-V.

You can configure a maximum of eight virtual NICs. Even if the physical NIC is DOWN, the virtual appliance assumes that the virtual NIC is UP, because it can still communicate with the other virtual appliances on the same host (server).

**Note:** You cannot change any settings while the virtual appliance is running. Shut down the virtual appliance and then make changes.

**To install NetScaler VPX on Microsoft Server 2008 R2 by using Hyper-V Manager**

1. To start Hyper-V Manager, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.

2. In the navigation pane, under **Hyper-V Manager**, select the server on which you want to install NetScaler VPX.

3. On the **Action** menu, click **Import Virtual Machine**.

4. In the **Import Virtual Machine** dialog box, in **Location**, specify the path of the folder that contains the NetScaler VPX software files, and then select **Copy the virtual machine (create a new unique ID)**. This folder is the parent folder that contains the Snapshots, Virtual Hard Disks, and Virtual Machines folders.
Note: If you received a compressed file, make sure that you extract the files into a folder before you specify the path to the folder.

5. Click Import.

6. Verify that the virtual appliance that you imported is listed under Virtual Machines.

7. To install another virtual appliance, repeat steps 2 through 6.

Important: Make sure that you extract the files to a different folder in step 4.

To configure NetScaler VPX

1. Right-click the virtual appliance that you previously installed, and then select Start.

2. Access the console by double-clicking the virtual appliance.

3. Type the NetScaler IP address, subnet mask, and gateway for your virtual appliance.

You have completed the basic configuration of your virtual appliance. Type the IP address in a Web browser to access the virtual appliance.

Obtain VPX license files. For more information about VPX licenses, see the NetScaler VPX Licensing Guide at http://support.citrix.com/article/ctx122426.
About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is a leading provider of virtual computing solutions that help people work and play from anywhere on any device. More than 230,000 enterprises rely on Citrix to create better ways for people, IT and business to work through virtual meetings, desktops and datacenters. Citrix virtualization, networking and cloud solutions deliver over 100 million corporate desktops and touch 75 percent of Internet users each day. Citrix partners with over 10,000 companies in 100 countries. Annual revenue in 2010 was $1.87 billion. Learn more at www.citrix.com.

©2011 Citrix Systems, Inc. All rights reserved. Branch Repeater™, Citrix®, Citrix Access Gateway™, Citrix Merchandising™ Server, Citrix Provisioning Services™, Citrix Receiver™, EdgeSight®, HDX™, ICA®, NetScaler®, VPX™, XenApp™, XenDesktop®, and XenServer® are trademarks or registered trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. Xen® is a trademark of Citrix Systems, Inc. managed on behalf of Xen.org, and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.