# Table of Contents

- Introduction .................................................................................................................. 3
- Solution Requirements ................................................................................................. 4
- Prerequisites .................................................................................................................. 4
- Network Diagram .......................................................................................................... 5
- XenApp ............................................................................................................................ 7
  - Configuration - Web Interface .................................................................................... 7
- XenApp ............................................................................................................................. 13
  - Configuration - XenApp Plugin .................................................................................. 13
- NetScaler AGEE ............................................................................................................. 19
  - Self Signed Root CA .................................................................................................. 19
  - Private Server Certificate ......................................................................................... 21
  - Public Server Certificate ......................................................................................... 23
  - Link Public & CA Certificate ................................................................................... 25
  - Link Private & CA Certificate .................................................................................. 26
- NetScaler AGEE ............................................................................................................. 27
  - Public VIP .................................................................................................................. 27
- NetScaler AGEE ............................................................................................................. 31
  - Private VIP ................................................................................................................ 31
  - Secure Ticket Authority ............................................................................................ 35
  - Proxy Group - Web Interface .................................................................................... 36
  - Proxy Group - XenApp Plugin .................................................................................. 40
- Testing Web Interface ..................................................................................................... 45
- Testing XenApp Plugin ................................................................................................... 47
Introduction

A member of the Citrix Delivery Center™ product family, Citrix NetScaler is a purpose-built web application delivery solution that accelerates application performance up to five times while improving security and reducing web infrastructure costs. In addition to delivering web applications for thousands of corporate customers, NetScaler is also the delivery infrastructure of choice for most of the world’s largest consumer websites, touching an estimated 75 percent of all Internet users each day.

Citrix Access Gateway™, a member of the Citrix Delivery Center, is the only SSL VPN to securely deliver any application with policy-based SmartAccess control. Users will have easy-to-use secure access to all of the enterprise applications and data they need to be productive, and IT can cost effectively extend access to applications while maintaining security through SmartAccess application-level policies. With Access Gateway, organizations are empowered to cost-effectively meet the anywhere access demands of all workers – enabling flexible work options, easier outsourcing and non-employee access, and business continuity readiness – while ensuring the highest level of information security. The newest release of the company’s popular Citrix Access Gateway™ appliance now includes integration with Citrix XenDesktop™, allowing companies to deliver virtual desktops securely to thousands of end users based on their unique identity, location and security status.

Citrix XenApp™, a member of the Citrix Delivery Center™ product family, is the industry’s de facto standard for delivering Windows-based applications with the best performance, security and cost savings. XenApp is the most complete application virtualization system available with the ability to virtualize applications on both the client side and server side, delivering them on demand based on the user, the application or the location (online or offline). By centralizing applications and data in secure datacenters, IT can reduce the costs of management and support, increase data security and facilitate business continuity. XenApp Platinum Edition adds critical capabilities for application performance monitoring, secure remote access, WAN optimization and single-sign-on application security.

Citrix Delivery Center is the first solution on the market to deliver applications and desktops to any user, anytime, anywhere from a secure central location. Citrix Delivery Center’s market leading application delivery technologies - XenServer, NetScaler, XenApp and XenDesktop - enable IT to dramatically improve agility, while enabling the best performance and highest security at the lowest cost.
Solution Requirements

- ICA Proxy for XenApp Web Interface
- ICA Proxy for XenApp Plugin

Prerequisites

- Citrix NetScaler L4/7 Application Switch, version 9.0+ running Access Gateway (Quantity x 2 for High Availability)
- Citrix XenApp Server 5.0+
- Microsoft Server with Active Directory
Network Diagram

The following is the Network that was used to develop this deployment guide.

**Citrix**

"ICA Proxy for XenApp"

**Logical Network Diagram**

<table>
<thead>
<tr>
<th>VLAN Legend</th>
<th>NetScaler</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN 1</td>
<td>VLAN 1:</td>
</tr>
<tr>
<td></td>
<td>Interface 1/7, Untagged</td>
</tr>
<tr>
<td></td>
<td>NSIP: 10.217.105.53 / 24</td>
</tr>
<tr>
<td></td>
<td>SNIP: 10.217.105.3 / 24</td>
</tr>
<tr>
<td></td>
<td>VIP-SSO: 10.217.105.5 / 24</td>
</tr>
<tr>
<td>VLAN 67</td>
<td>VLAN 67:</td>
</tr>
<tr>
<td></td>
<td>Interface 1/8, Untagged</td>
</tr>
<tr>
<td></td>
<td>VIP: 67.97.253.89 / 24</td>
</tr>
</tbody>
</table>

Private: 10.217.105.151
FQDN: srv1.xencloud.net
Primary Domain Controller

Private: 10.217.105.155
FQDN: ws2008.xencloud.net

ICA Proxy
LDAP Auth
FQDN: ns.xencloud.net
10.217.105.5
FQDN: ag.xencloud.net
67.97.253.89

CA: xencloud.net
Public Cert: ag.xencloud.net
Private Cert: ns.xencloud.net

VLAN Legend

VLAN 1:
- Interface 1/7, Untagged
- NSIP: 10.217.105.53 / 24
- SNIP: 10.217.105.3 / 24
- VIP-SSO: 10.217.105.5 / 24

VLAN 67:
- Interface 1/8, Untagged
- VIP: 67.97.253.89 / 24

Public URL
https://ag.xencloud.net
FQDN: ag.xencloud.net
67.97.253.89
Citrix
“ICA Proxy for XenApp”
Certificate Chain of Trust

1. Trusted Root CA Certificate (xencloud.net)

2. Private Server Certificate (ns.xencloud.net)

3. Public Server Certificate (ag.xencloud.net)

**NetScaler**

- Import:
  1. Trusted Root CA Certificate
  2. Private Server Certificate
  3. Public Server Certificate

**Win2k3 (S1 & DC)**

**Client**

- Import:
  1. Trusted Root CA Certificate
  2. Private Server Certificate
  3. Public Server Certificate
XenApp Configuration - Web Interface

Once you have installed Citrix XenApp you will need to configure it such that it will work with the Citrix NetScaler in an ICA Proxy deployment. Creating a Web Interface will publish the XenApp applications in a web browser to the client.

From the Access Management Console:
Citrix Resources ➜ Configuration Tools ➜ Web Interface ➜ Action ➜ Create Site.
Select XenApp Web.
Select Next.

IIS Location:
IIS Site: Default Web Site
Path: /Citrix/XenApp/
Set as the default page for IIS.
Point of Authentication:
At Access Gateway

Gateway Settings:
Authentication URL:
https://ns.xencloud.net/CitrixAuthService/AuthService.asmx

Note: ns.xencloud.net resolves to 10.217.105.5 and is the private interface of the NetScaler Access Gateway.
Specify Server Farm:
Farm Name: <your farm name>
Servers: <XenApp Hostname>

Logon Screen:
Minimal or Full
Resource Type:

Remote

Select Finish

From the Access Management Console:

Actions ➔
Manage Secure Client Access ➔
Edit Secure Client Access.
Specify Access Method:
Client IP: Default
Method: Gateway Direct

Next.

Gateway Settings:
Address: <FQDN of NetScaler Access Gateway>
Port: 443

Note: Your first thought might be to configure the private FQDN here, but that isn’t the case. According to the sentence in the dialog box, this is the FQDN that public users will use to access the applications - through the Access Gateway. Therefore, this needs to be the public FQDN of the AG, which in this example is ag.xencloud.net, and resolves to 67.97.253.89.
Secure Ticket Authority:
URL: <ip address of XenApp>/scripts/ctxsta.dll

Select Finish
XenApp
Configuration - XenApp Plugin

Once you have installed Citrix XenApp you will need to configure it such that it will work with the Citrix NetScaler in an ICA Proxy deployment. Creating a XenApp service will publish the XenApp applications through the Citrix client, such as XenApp client or Citrix Receiver.

From the Access Management Console:
Citrix Resources ➔
Configuration Tools ➔
Web Interface ➔
Action ➔
Create Site.
Select XenApp Services.
Select Next.

IIS Location:
IIS Site: Default Web Site
Path: /Citrix/PNAgent/
Confirm:
Next.
Finish.

Configure Site Now.

Specify Server Farm:
Farm Name: <your farm name>
Servers: <XenApp Hostname>
**Resource Type:**
Remote

**Confirm:**
Finish
From the Access Management Console:

- Actions ➔
- Manage Secure Client Access ➔
- Edit Secure Client Access.

Specify Access Method:

- Client IP: Default
- Method: Gateway Direct

Next.
Gateway Settings:
Address: <FQDN of NetScaler Access Gateway>
Port: 443

Note: Your first thought might be to configure the private FQDN here, but that isn’t the case. According to the sentence in the dialog box, this is the FQDN that public users will use to access the applications - through the Access Gateway. Therefore, this needs to be the public FQDN of the AG, which in this example is ag.xencloud.net, and resolves to 67.97.253.89.

Secure Ticket Authority:
URL: <ip address of XenApp>/scripts/ctxsta.dll

Select Finish
NetScaler AGEE
Self Signed Root CA

You will need three certificates. A self signed Root CA, a public server certificate and a private server certificate.

From the NetScaler GUI:
NetScaler ➔
SSL ➔
Certificate Wizard.

Create Key:
Type: RSA
Filename: xencloudCA.key
Size: 1024
Endpoint: F4
Format: PEM

Next.

Create CSR:
Filename: xencloudCA.req
Key: xencloudCA.key
Format: PEM
Passphrase: <passphrase>
CN: xencloud.net
City: Santa Clara
Org: Citrix
Country: United States
State: California
Email: admin@xencloud.net
OU: xencloud

Next.

Note: CN of xencloud.net must match the DNS or Hosts file entry name.
Create Certificate:
Filename: xencloudCA.cer
Format: PEM
Type: Root-CA
Req: xencloudCA.req
Key: xencloudCA.key
Format: PEM
Passphrase: <passphrase>
Validity: 1800
Next.

Install Certificate:
Filename: xencloudCA.keypair
Location: Appliance
Cert File: xencloudCA.cer
Key File: xencloudCA.key
Password: <passphrase>
Format: PEM
Next.
Finish.
Private Server Certificate

The private server certificate is used for NetScaler AGEE-to-XenApp connections.

From the NetScaler GUI:
NetScaler ➔
SSL ➔
Certificate Wizard.

Create Key:
Type: RSA
Filename: xencloudNSSRV.key
Size: 1024
Endpoint: F4
Format: PEM

Next.

Create CSR:
Filename: xencloudNSSRV.req
Key: xencloudNSSRV.key
Format: PEM
Passphrase: <passphrase>
CN: ns.xencloud.net
City: Santa Clara
Org: Citrix
Country: United States
State: California
Email: admin@xencloud.net
OU: xencloud

Next.

Note: CN of ns.xencloud.net must match the DNS or Hosts file entry name.
Create Certificate:
Filename: xencloudNSSRV.cer
Format: PEM
Type: Server
Req: xencloudNSSRV.req
Validity: 1800
CA Filename: xencloudCA.cer
CA Format: PEM
CA Key: xencloudCA.key
Key Format: PEM
Passphrase: <passphrase>
CA Serial File: ns-root.srl

Next.

Install Certificate:
Filename: xencloudNSSRV.keypair
Location: Appliance
Cert File: xencloudNSSRV.cer
Key File: xencloudNSSRV.key
Password: <passphrase>
Format: PEM

Next.

Finish.
Public Server Certificate
The public server certificate is used for Client-to-AG connections.

From the NetScaler GUI:
NetScaler →
SSL →
Certificate Wizard.

Create Key:
Type: RSA
Filename: xencloudAGSRV.key
Size: 1024
Endpoint: F4
Format: PEM

Next.

Create CSR:
Filename: xencloudNAGSRV.req
Key: xencloudAGSRV.key
Format: PEM
Passphrase: <passphrase>
CN: ag.xencloud.net
City: Santa Clara
Org: Citrix
Country: United States
State: California
Email: admin@xencloud.net
OU: xencloud

Next.
Note: CN of ag.xencloud.net must match the DNS or Hosts file entry name.
Create Certificate:
Filename: xencloudAGSRV.cer
Format: PEM
Type: Server
Req: xencloudAGSRV.req
Validity: 1800
CA Filename: xencloudCA.cer
CA Format: PEM
CA Key: xencloudCA.key
Key Format: PEM
Passphrase: <passphrase>
CA Serial File: ns-root.srl

Next.

Install Certificate:
Filename: xencloudAGSRV.keypair
Location: Appliance
Cert File: xencloudAGSRV.cer
Key File: xencloudAGSRV.key
Password: <passphrase>
Format: PEM

Next.

Finish.
Link Public & CA Certificate

To establish a certificate chain of trust between the NetScaler AG and the Client, you must link the public server certificate to the self signed CA certificate.

From the NetScaler GUI:

NetScaler ➔ SSL ➔ Certificates.

Select the public certificate by the keypair name.
Name: xencloudAGSRV.keypair

Click on ‘Link;’.

Select the CA certificate.
Name: xencloudCA.keypair.
Link Private & CA Certificate

To establish a certificate chain of trust between the NetScaler AG and the XenApp server, you must link the private server certificate to the self signed CA certificate.

From the NetScaler GUI:

NetScaler ➔
SSL ➔
Certificates.

Select the private certificate by the keypair name.
Name: xencloudNSSRV.keypair

Click on ‘Link;’.

Select the CA certificate.
Name: xencloudCA.keypair.
NetScaler AGEE
Public VIP

Create the public facing VIP that users will connect to when they type in https://ag.xencloud.net into their browser URL locator.

From the NetScaler GUI:

Create Virtual Server:
Type: New
IP Address: 67.97.253.89
Port: 443
Name: ag.xencloud.net

Next.

Server Certificate:
Options: Use an installed certificate and private key pair
Certificate: xencloudAGSRV.keypair

Next.

Note:
1) ag.xencloud.net must resolve to ip address 67.97.253.89 &
2) Common Name in Server Certificate xencloudAGSRV.cer must contain ag.xencloud.net.
DNS:
DNS Server: 10.217.105.151
Note:
In this example our Active Directory Domain Controller also serves as our DNS.

Next.

Authentication:
Type: LDAP
IP: 10.217.105.151
Port: 636
Time-out: 3
Base DN: dc=xencloud,dc=net
Admin DN: cn=Administrator,cn=users,dc=xencloud,dc=net
Password: <password>
Confirm: <password>
Login Attr: sAMAccountName
Filter:
Group Attr: memberOf
Sub Attr: CN
SSL Attr: sAMAccountName
Security Type: SSL

Next.
Additional:
Authorization: Allow
Redirect:
Redirect to secure web address
Address:
https://ag.xencloud.net
Next.

Clientless Access:
Use the Access Gateway Plugin and allow access scenario fallback.

Next.

Finish.
NetScaler AGEE
Private VIP

Create the private facing VIP that XenApp will connect to when it authenticates users.

From the NetScaler GUI:
NetScaler ➔
Access Gateway ➔
Access Gateway Wizard.

Create Virtual Server:
Type: New
IP Address: 10.217.105.5
Port: 443
Name: ns.xencloud.net-vip

Next.

Server Certificate:
Options: Use an installed certificate and private key pair
Certificate: xencloudNSSRV.keypair

Next.

Note:
1) ns.xencloud.net must resolve to IP address 10.217.105.5 &
2) Common Name in Server Certificate xencloudNSSRV.cer must contain ns.xencloud.net.
DNS:
DNS Server: 10.217.105.151
Note:
In this case our Active Directory Domain Controller also serves as our DNS.

Next.

Authentication:
Type: LDAP
IP: 10.217.105.151
Port: 636
Time-out: 3
Base DN: dc=xencloud,dc=net
Admin DN: cn=Administrator,cn=users,dc=xencloud,dc=net
Password: <password>
Confirm: <password>
Login Attr: sAMAccountName
Filter:
Group Attr: memberOf
Sub Attr: CN
SSL Attr: sAMAccountName
Security Type: SSL

Next.
Additional:
Authorization: Allow
Next.

Clientless Access:
Use the Access Gateway Plugin and allow access scenario fallback.
Next.
Finish.
Secure Ticket Authority

Communication between the XenApp Server and the NetScaler AG depends on the Citrix Secure Ticket Authority. You must configure this in the NetScaler AG. In this case the CTX STA resides on the XenApp server.

From the NetScaler GUI:

NetScaler ➔ Access Gateway ➔ Virtual Servers.

Open the public vip. In this example it is ag.xencloud.net-vip at IP Address 67.97.253.89.

Select Published Applications.

Under Secure Ticket Authority, Add.

Enter the URL to the Secure Ticket Authority, in this example the same as the XenApp Server, http://10.217.105.155/scripts/ctxsta.dll

Create.

Create.
Proxy Group - Web Interface

To proxy the ICA connections from the XenApp server using the XenApp Web Interface, the NetScaler AG needs to be configured to do so. You do this by adding a group, and configure the group for proxy ICA connections via a session profile. The group name MUST match the 'memberOf' group name in the LDAP/Active Directory server. Note: The same group must be added to the LDAP/Active Directory server.

From the NetScaler GUI:

NetScaler ➔ Access Gateway ➔ Groups.

Select Add.

Group Name: <groupname>

In this example our group name is: iproxy

Create.

Select the Policies tab, Add Policy. Type in policy name, in this example it is the same as the group name: iproxy.

At Request Profile, select ‘New’ to create a new profile. In this example, the request profile is the same as the group name: iproxy.
Client Experience:
Home Page: none
Select Override Global.
Clientless Access: On.
Select Override Global.
Single Sign-on to Web Applications: Selected
Select Override Global.
Published Applications:

ICA Proxy:
On
Select Override Global

Web Interface Address:
Select Override Global

Web Interface Portal Mode:
Normal
Select Override Global

Single Sign-on Domain:
<your domain>
Select Override Global

Note: Single Sign-on Domain in this example is ‘xencloud’.

Select Ok.

Under named expressions, select True Value, Add Expression.

Then Create.
The iproxy profile should now be bound to the iproxy group.
Proxy Group - XenApp Plugin

To proxy the ICA connections from the XenApp server using the XenApp Plugin on the users device, the NetScaler AG needs to be configured to do so. You do this by adding a group, and configure the group for proxy ICA connections via a session profile. The group name MUST match the 'memberOf' group name in the LDAP/Active Directory server. Note: The same group must be added to the LDAP/Active Directory server.

From the NetScaler GUI:

NetScaler → Access Gateway → Groups.

Select Add.
Group Name: <groupname>
In this example our group name is: iproxy2
Create.

Select the Policies tab, Add Policy. Type in policy name, in this example it is the same as the group name: iproxy2.

At Request Profile, select ‘New’ to create a new profile. In this example, the request profile is the same as the group name: iproxy2.

Note: by now you notice that you need two groups with associated policies. One for Web Interface clients (groupname iproxy) and one for XenApp Plugin clients (groupname iproxy2)
**Client Experience:**

- Home Page: none
  - Select Override Global.
- Clientless Access: On.
  - Select Override Global.
- Single Sign-on to Web Applications: Selected
  - Select Override Global.
Published Applications:

ICA Proxy:
On
Select Override Global

Web Interface Address:
Select Override Global

Web Interface Portal Mode:
Normal
Select Override Global

Single Sign-on Domain:
<your domain>
Select Override Global

Note: Single Sign-on Domain in this example is ‘xencloud’.

Select Ok.

Under named expressions, select True Value, Add Expression.

Then Create.
The iproxy2 profile should now be bound to the iproxy2 group.
Testing Web Interface

Once you have installed all of the components of this solution, you should test it, by publishing a test application such as Notepad, in XenApp, then connect and see if Single Sign-On works, and that the application launches.

From a web browser, enter the FQDN of the public vip:

In this example it is:
https://ag.xencloud.net

Enter login credentials, which are consequently configured in Active Directory. Because we have configured this solution for Single Sign-On, you should only have to do this one time.

Web Interface:
Wait for the Web Interface to load.
Application:
At this point you should see the Web Interface with the application that is published for this user.
Launch the application.

Application Delivery:
The application should be delivered or proxied from XenApp, through the NetScaler Access Gateway, to the end user.
Testing XenApp Plugin

Once you have installed all of the components of this solution, you should test it, by publishing a test application such as Notepad, in XenApp, then connect with Citrix XenApp Client and see if Single Sign-On works, and that the application launches.

Download the Citrix:
Open a web browser, and navigate to the downloads section of http://citrix.com.
Download and install the XenApp Plugin for Hosted Apps.

Enter login credentials, which are consequently configured in Active Directory. Because we have configured this solution for Single Sign-On, you should only have to do this one time.

Server Address:
Configure the Server Address to point to the AG public VIP.
In this example:
https://ag.xencloud.net/Citrix/PNAgent/config.xml
Application:
At this point you should see the Citrix XenApp Client with the application that is published for this user.

Launch the application.

Application Delivery:
The application should be delivered or proxied from XenApp, through the Citrix Access Gateway, to the end user.
About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is the leading provider of virtualization, networking and software as a service technologies for more than 230,000 organizations worldwide. Its Citrix Delivery Center, Citrix Cloud Center (C3) and Citrix Online Services product families radically simplify computing for millions of users, delivering applications as an on-demand service to any user, in any location on any device. Citrix customers include the world’s largest Internet companies, 99 percent of Fortune Global 500 enterprises, and hundreds of thousands of small businesses and consumers worldwide. Citrix partners with over 10,000 companies worldwide in more than 100 countries. Founded in 1989, annual revenue in 2008 was $1.6 billion.

The information in this publication is subject to change without notice.

THIS PUBLICATION IS PROVIDED “AS IS” WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. CITRIX SYSTEMS, INC. (“CITRIX”), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

This publication contains information protected by copyright. Except for internal distribution, no part of this publication may be photocopied or reproduced in any form without prior written consent from Citrix.

The exclusive warranty for Citrix products, if any, is stated in the product documentation accompanying such products. Citrix does not warrant products other than its own.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

© 2009 Citrix Systems, Inc., 851 West Cypress Creek Road, Ft. Lauderdale, Florida 33309-2009 U.S.A. All rights reserved.