

Bridging to a Corporate Network from Amazon EC2

Summary

This blueprint documents deploying Citrix C3 in a public cloud environment to deliver Windows applications from the cloud with secure, high performance access to corporate data residing behind the corporate firewall.

Citrix Labs
30 September 2009

Contents

1	Introduction	1
1.1	Disclaimer	1
1.2	Overview	1
1.3	This document	2
2	Preparing for the blueprint.....	4
2.1	Pre-requisites	4
2.2	Steps to create an instance of this blueprint.....	4
2.3	Outline	4
2.4	References.....	6
3	Creating a trust relationship.....	7
3.1	Overview	7
3.2	Set up the domains.....	7
3.3	Create a temporary AG tunnel.....	8
3.4	Create one-way trust.....	8
3.5	Close temporary AG tunnel	8
4	Set up Citrix Access Gateway tunnel on XenApp.....	9
4.1	Overview	9
4.2	Configure Access Gateway.....	9
4.3	Configure dm1.....	10
4.3.1	Remove existing Access Gateway plug-in.....	10
4.3.2	Create new user.....	10
4.3.3	Enable automatic logon	10
4.4	Install the Access Gateway plug-in.....	10
4.5	Make the Access Gateway plug-in multi-session safe	10
4.6	Verify the Access Gateway plug-in is started automatically	11
5	Set up Citrix Repeater plug-in on XenApp.....	12
5.1	Overview	12
5.2	Install the Repeater plug-in	12
5.3	Configure the Repeater plug-in.....	13
5.4	Make the Repeater plug-in multi-session safe	13
6	Verify bridge to corporate network.....	14
6.1	Overview	14
6.2	Verify single sign-on	14
6.3	Verify access to file shares.....	14
6.4	Verify traffic acceleration	14

1 Introduction

This blueprint documents deploying Citrix C3 in a public cloud environment to deliver Windows applications from the cloud with secure access to corporate data residing behind the corporate firewall. Citrix XenApp, the Citrix Access Gateway client and the Citrix Repeater client are provided in a single Amazon Machine Image (AMI) running in Amazon EC2. Customers and prospects will benefit from the ability to configure and test applications in a cloud environment without having to migrate or replicate their sensitive corporate files in the cloud. Instead, the application accesses the corporate data on-demand via the Citrix Repeater and secured via Citrix Access Gateway. The WAN acceleration benefit of the Citrix Repeater can also be easily demonstrated with this configuration.

1.1 Disclaimer

Your use of this content is at your own risk. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CITRIX AND ITS SUPPLIERS MAKE AND YOU RECEIVE NO WARRANTIES OR CONDITIONS, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, AND CITRIX AND ITS SUPPLIERS SPECIFICALLY DISCLAIM WITH RESPECT TO THE CONTENT ANY CONDITIONS OF QUALITY, AVAILABILITY, RELIABILITY, SECURITY, LACK OF VIRUSES, BUGS OR ERRORS, OR SUPPORT AND ANY IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT PERMITTED BY APPLICABLE LAW, NEITHER CITRIX, ITS SUPPLIERS SHALL BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, MULTIPLE, PUNITIVE OR OTHER DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF DATA, LOSS OF INCOME, LOSS OF OPPORTUNITY, LOST PROFITS, COSTS OF RECOVERY OR ANY OTHER DAMAGES), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, AND WHETHER OR NOT FOR BREACH OF CONTRACT, NEGLIGENCE OR OTHERWISE, AND WHETHER OR NOT CITRIX, ITS SUPPLIERS, OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

1.2 Overview

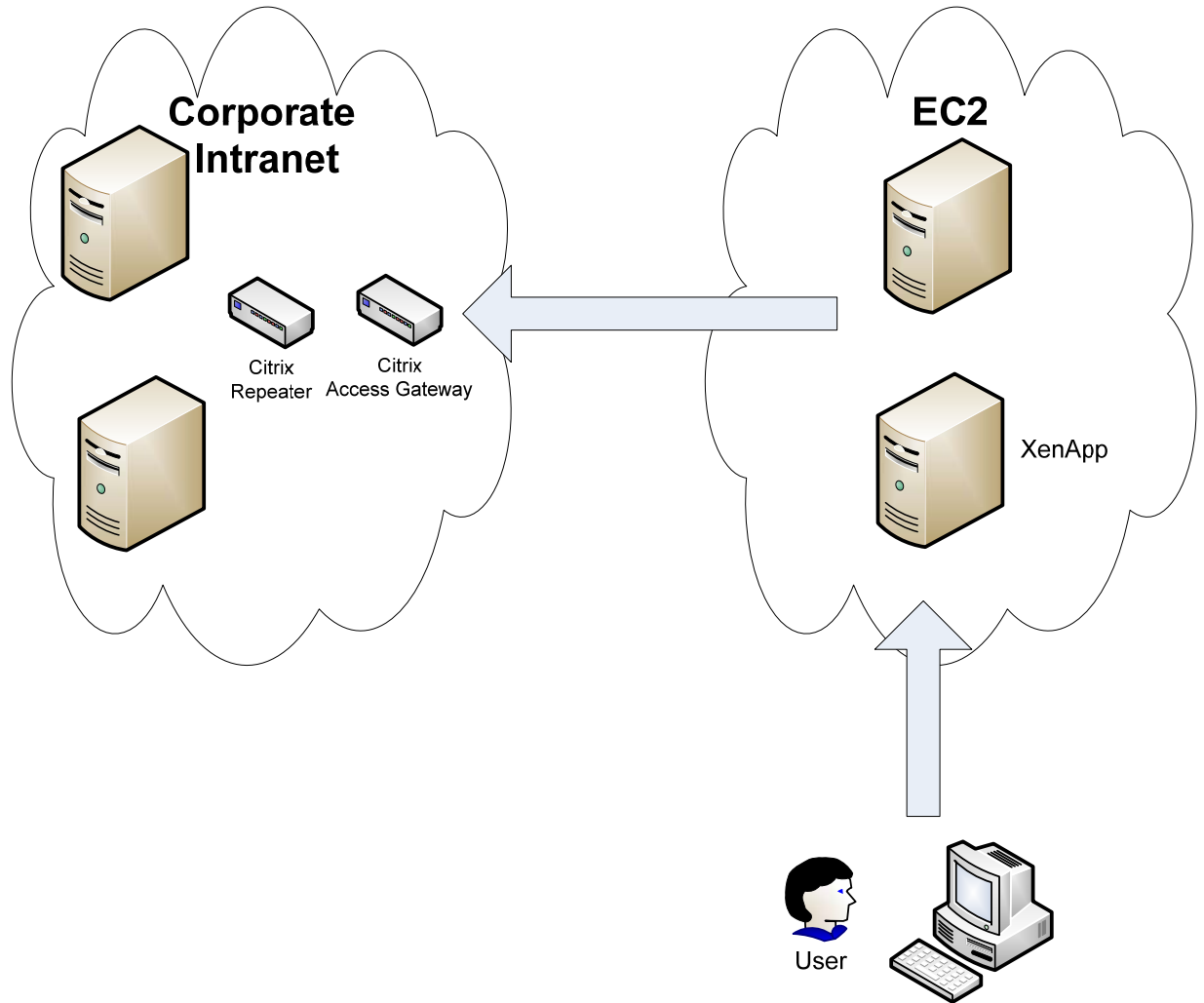
Users (corporate employees) will log on to virtual machines running XenApp in EC2. They will run published applications there and access data held in the corporate network.

In this scenario, there are 3 key problems to solve:

- Provide the applications hosted in the cloud with secured access to data that is hosted in the corporate data centre.
- Single sign-on: ensure that users authenticate once, using their enterprise credentials, and are then given access to the applications on EC2 and the data held in the enterprise.
- Ensure that the users of the applications accessing the data get optimized access to the data.

Citrix Access Gateway is used to provide secure access between the applications in the cloud and the data stored in the data centre. The Access Gateway appliance is installed at the Data Centre and the AG client is used to establish the secure connection from the cloud.

Citrix Branch Repeater is used to accelerate the data between the data centre and the cloud. A physical Branch Repeater appliance is installed at the data centre. Because EC2 doesn't yet support Citrix Branch Repeater virtual appliances, software client version of Branch Repeater is used in the cloud.



1.3 This document

In this document we explain how to:

- Create a trust relationship between a domain you create in EC2 and your corporate domain.
- Set up a Citrix Access Gateway connection on Citrix XenApp which is shared by users in all sessions.
- Set up Citrix Repeater plug-in on XenApp so that it optimizes traffic for all user sessions.

It is assumed the reader will use other resources to define how to set up Access Gateway and Citrix Repeater appliances, how to create Windows domains (in EC2 or otherwise), how to create and manage Amazon EC2 instances and how to configure Citrix XenApp.

1.4 Scope

This document describes how to get access to corporate data from Amazon EC2. However, it doesn't address the following issues:

- **Performance.** Sharing Access Gateway and Repeater plug-ins on each XenApp server will probably reduce the number of users you can get on each server. You won't be able to benefit from cross server compression and caching that you would get from a Citrix Repeater

appliance. The Repeater client also doesn't support cross session compression. We have done no performance testing.

- **Security of communication local to EC2.** Data sent between XenApp servers is not encrypted. Only data sent to and from the corporate network is encrypted.
- **Support.** Sharing a single Access Gateway and Repeater client between multiple user sessions on Windows Server 2003 isn't currently officially supported.
- **Audit and control.** Using shared Access Gateway and Repeater tunnels means you won't be able to audit individual user's network activity or set specific controls on their network access.
- **Bi-directional connections.** Access Gateway only supports client-initiated connections. In the scenario described in this document, it means users can only make connections from EC2 into your corporate network. Users on computers inside the corporate network can't use the same Access Gateway tunnels to make secure connections to EC2.
- **Drive mapping.** If users initiate ICA connections from within their XenApp session on EC2 to XenApp servers on the corporate network, drive mapping may not work properly. We haven't tested this and recommend you disable drive mapping on your XenApp servers for these users.

2 Preparing for the blueprint

2.1 Pre-requisites

In order to follow this blueprint you will need to have set up the following:

1. A corporate intranet with the following minimum:
 - a. A corporate domain with a Domain Controller
 - b. A file server which is a member of the corporate domain
 - c. Access Gateway (version 4.6 or later, Standard or Advanced Edition), configured for remote access to your corporate network. Please refer to the [Access Gateway Administration Guide](#) for details on how to do this.
 - d. Citrix Repeater (version 5.0.33 or higher), configured to accelerate traffic to and from your corporate network. Please refer to the [Citrix Repeater Appliance Installation and User's Guide](#) for details on how to do this.
2. An EC2 account.
 - a. See the [Amazon EC2 homepage](#) for a signup link and pointers to general documentation on EC2.
 - b. The [Citrix C3 Lab homepage](#) has a link to [getting started with EC2](#).
3. A cloud domain with the following (see section 3.2 for more details):
 - a. A domain controller (see the [Amazon documentation for creating a Windows domain in EC2](#)).
 - b. A domain member running XenApp. You'll need to create this from the Citrix C3 Lab XenApp Auth AMI (search for AMIs starting with 'citrix-c3-lab').

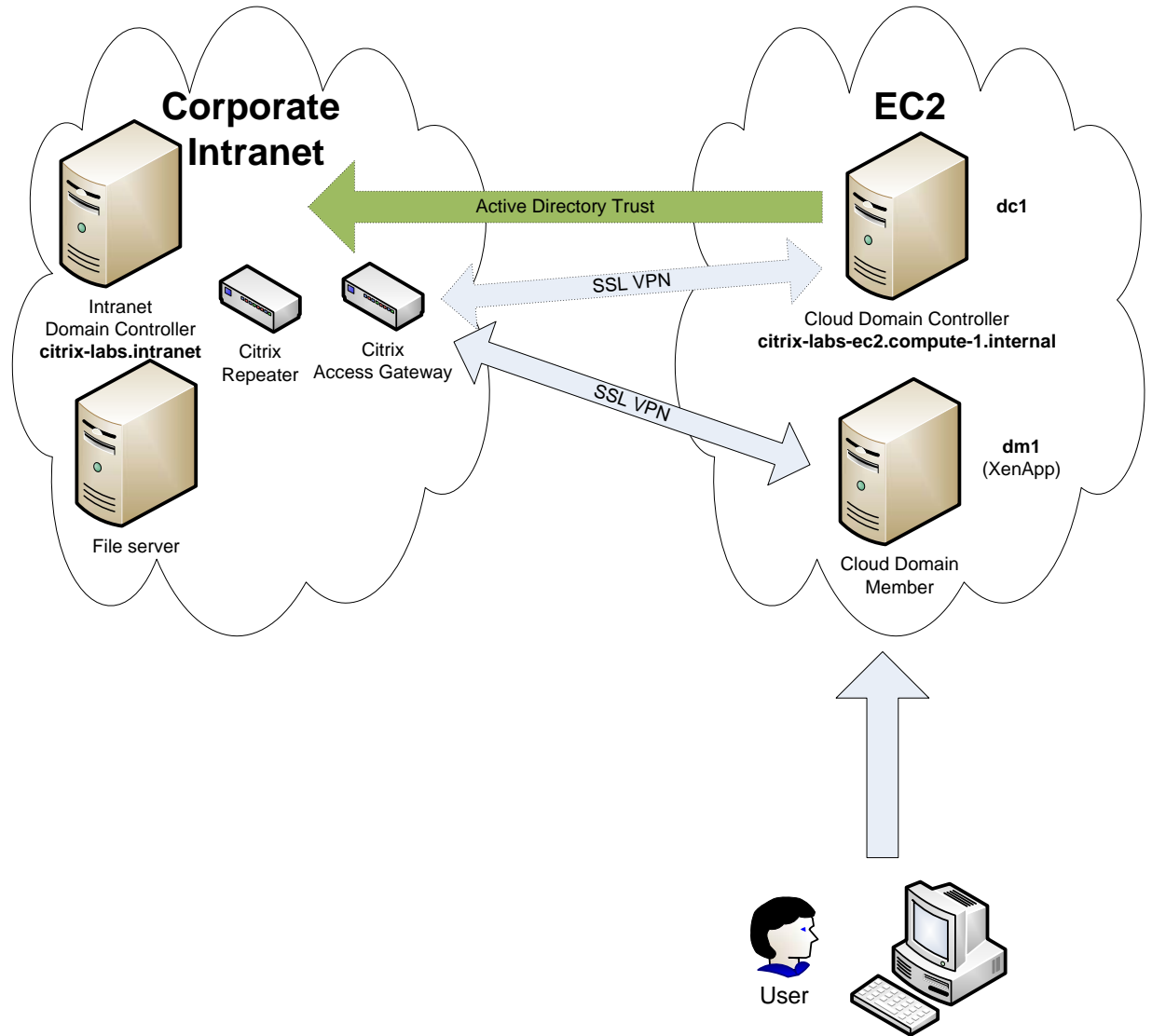
2.2 Steps to create an instance of this blueprint

This is what we're going to do:

1. Create a one-way trust between a Windows domain in EC2 and a domain on your corporate network (see section 3).
2. Create a shared Citrix Access Gateway tunnel on each domain member in EC2 (see section 4).
3. Create a shared Citrix Repeater connection on each domain member in EC2 (see section 5).

2.3 Outline

The overall schematic for the solution is shown below:



The corporate domain is called **citrix-labs.intranet** in the remainder of this document, but you should substitute the FQDN of your domain. You'll see the corporate domain controller, plus a file server which we'll use to test traffic acceleration. In front of these are the Citrix Repeater and Citrix Access Gateway appliances, configured for external access.

In EC2, you'll see two instances, **dc1** and **dm1**, both in domain **citrix-labs-ec2.compute-1.internal**. Again, you should substitute the FQDN of your chosen EC2 domain in the remainder of this document. **dc1** is the domain controller; **dm1** is a domain member running XenApp.

On **dc1** you'll create a temporary Access Gateway tunnel and then set up a permanent one-way trust (**citrix-labs.ec2.compute-1.internal** will trust **citrix-labs.intranet**).

On **dm1** you'll create a permanent Access Gateway tunnel, shared by all XenApp users. You'll also create a Citrix Repeater connection shared by all users. Users can then logon to **dm1** using their domain credentials.

2.4 References

The following documents are referenced from this document:

1. General Amazon EC2 documentation: <http://aws.amazon.com/ec2/>
2. Creating an Active Directory Domain in Amazon EC2:
<http://developer.amazonwebservices.com/connect/entry.jspa?externalID=2435>
3. [Microsoft Knowledge Base article](#) on installing Windows Server 2003 Support Tools.
4. [Amazon Tutorial](#) on attaching Windows installation media to an EC2 instance.
5. [How to turn on automatic logon](#).
6. [Sysinternals Autologons tool](#).

3 Creating a trust relationship

3.1 Overview

This section documents a method of setting up an external trust relationship from a Windows domain running in Amazon EC2 to a domain on the corporate intranet.

The effect of such a trust will be to allow a user to log onto an EC2 machine using intranet credentials. The user database in the intranet Active Directory remains there – it is not replicated out to EC2.

3.2 Set up the domains

Setting up the **citrix-labs.intranet** domain is outside the scope of this document.

To set up the **citrix-labs-ec2.compute-1.internal** domain, consult the guidelines in the [Amazon Tutorial](#) for setting up a Windows domain in EC2.

The starting point for the EC2 servers (both domain controller and domain member) must be an Amazon AMI with Authentication Services (see the Amazon [documentation](#) for more details).

For the domain controller, choose a vanilla Windows Server 2003 AMI.

If you wish to avoid having the domain controller running 24/7, ignore the guidelines that tell you to locate the Active Directory files on the D: drive. Instead, accept the defaults offered by the Wizard which will locate the files on the C: drive (which will be persisted if we bundle an AMI from the instance).

You should be aware that this will mean your Active Directory has limited space (the C: drive is 10 GB) but this shouldn't matter for this scenario as we only put computers into the cloud domain.

For the domain member, choose the Citrix C3 Lab XenApp AMI built from the Amazon Windows AMI with authentication (i.e. domain) support. You can find the manifest in Amazon S3 at:

```
citrix-c3-lab/XenApp5.0_LicSvr_SQLExpr_32bit_v1.1.xml
```

Instances of this AMI will think they're joined to the xencloud.net domain, which of course won't exist in your EC2 environment. You should remove your instance from the xencloud.net domain and then join it to your **citrix-labs-ec2.compute-1.internal** domain. You'll also need to rename it to **dm1**.

The rest of this document presumes you have followed the (modified) guidelines in the tutorial and set up a domain controller named **dc1** (with its own DNS server) for the **citrix-labs-ec2.compute-1.internal** domain, and a domain member named **dm1** (created from the XenApp Auth AMI).

3.2.1 Notes

If you want **dc1** and **dm1** to be able to resolve external hostnames, add a forwarding rule on **dc1**'s DNS server which forwards all requests that aren't for **citrix-labs-ec2.compute-1.internal** to Amazon's DNS server (172.16.0.23 at the time of writing).

If you want to add extra XenApp servers to your farm, use the following AMI:

```
citrix-c3-lab/XenApp5.0_ExpansionServer_32bit_v1.1.xml
```

3.3 Create a temporary AG tunnel

In order to create the one-way trust, we need to set up an Access Gateway tunnel from **dc1.citrix-labs-ec2.compute-1.internal** to the corporate network. This tunnel only needs to be in place while we create the trust – it can be closed afterwards.

To create the AG tunnel, log onto **dc1** as Administrator and point a browser to your corporate network's Access Gateway address. From there you'll be able to authenticate to AG and download the AG plug-in which will create the tunnel.

3.4 Create one-way trust

First, install the Windows Server 2003 Support Tools on **dc1** (this [Microsoft Knowledge Base article](#) tells you how). To do this, you'll need to attach the Windows Server 2003 installation media to your **dc1** instance on Amazon EC2. This [Amazon Tutorial](#) shows you how to do this.

Still logged onto **dc1** as Administrator, start a Windows Support Tools command prompt (Start → All Programs → Windows Support Tools → Command Prompt).

Type the following command to establish an external trust from **citrix-labs-ec2.compute-1.internal** to **citrix-labs.intranet**:

```
> netdom trust citrix-labs-ec2.compute-1.internal /d:citrix-labs.intranet /add /userD Administrator /passwordD *
```

This will prompt you for the **citrix-labs.intranet** Administrator password as it establishes both sides of the trust relationship.

To verify the trust has been correctly established:

```
> netdom trust citrix-labs-ec2.compute-1.internal /d:citrix-labs.intranet /verify /userD Administrator /passwordD *
```

Again, you'll need to enter the **citrix-labs.intranet** Administrator password.

3.5 Close temporary AG tunnel

You can now close the AG tunnel on **dc1.citrix-labs-ec2.compute-1.internal** as we don't need to access the corporate network any more from **dc1**.

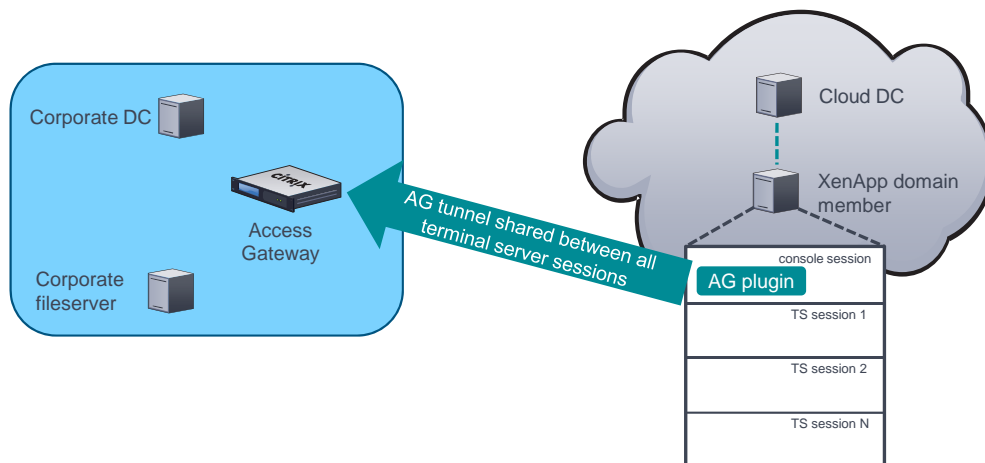
4 Set up Citrix Access Gateway tunnel on XenApp

4.1 Overview

In order to get seamless access to computers on the corporate network from XenApp EC2 instances, it's necessary to set up an Access Gateway tunnel on each instance. It's assumed that you already have an Access Gateway providing remote access to your corporate network.

Each EC2 XenApp instance is a member of the **citrix-labs-ec2.compute-1.internal** domain and creates its own connection back to the corporate network. These instructions are for a single instance, **dm1.citrix-labs-ec2.compute-1.internal**, but the same applies to any other domain members you create.

The idea is to set up a single Access Gateway connection in **dm1**'s console session, which all other sessions on the instance then share for accessing computers on the corporate network.



Briefly, it works like this:

1. Create accounts on Access Gateway and **dm1** with the same name and password.
2. Configure AG so when someone logs onto **dm1**, the AG plug-in is started automatically and authenticates to AG using their Windows username and password.
3. Auto logon the user to the console session on **dm1** when the machine boots – hence starting the AG plug-in and creating the tunnel.
4. Wrap the AG plug-in so only the user setting up the tunnel runs the AG client – subsequent users don't create new tunnels but share the initial one.

The rest of this section describes these steps in more detail.

4.2 Configure Access Gateway

On your Access Gateway appliance, do the following:

1. Create a user that your tunnel will authenticate as.
2. Ensure "Enable single sign-on with Windows" is checked in the user's group's properties. On the Access Policy Manager tab, right click the user's group (e.g. Default) and select Properties. You'll see the setting there – make sure it's checked.

4.3 Configure dm1

4.3.1 Remove existing Access Gateway plug-in

If there's an Access Gateway plug-in already installed, uninstall it and reboot.

4.3.2 Create new user

1. Connect to the console on **dm1** (mstsc /console).
2. Logon as Administrator.
3. Create a new user with the same name and password as the user you created on Access Gateway. Make sure you create a local account, not a domain account.
 - a. Uncheck "User must change password at next logon."
 - b. Check "Password never expires."
4. Make the user a member of the local Administrators group (otherwise, the tunnel doesn't get shared by all users on the machine).

4.3.3 Enable automatic logon

Arrange for the user you created to be logged on automatically. Don't reboot yet if Windows asks you to (we'll reboot later on).

Follow the instructions in the following document: <http://support.microsoft.com/kb/315231>. Use the user name and password of the user you created in the previous section. Make sure you set **ForceAutoLogon**.

In addition, you need to create an extra registry entry in `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` called **DefaultDomain**. This should contain a string value and be set to the name of your computer, in capitals (i.e. its NETBIOS name).

Note that you'll be storing the user's password in the Windows registry in plain text. If you want the password encrypted, use the [Sysinternals Autologons tool](#) instead of following the Microsoft KB article.

4.4 Install the Access Gateway plug-in

Browse to your corporate network's Access Gateway and login to the web page. From there you'll be able to download and install the Access Gateway plug-in.

Now you can reboot **dm1**.

4.5 Make the Access Gateway plug-in multi-session safe

1. Connect to the console on **dm1** again.
2. Logon as the user you created.
 - a. The user should already have been auto logged on to the console so you'll be connected to the existing session.
3. Open a Windows Explorer window to `C:\Program Files\Citrix\Access Gateway`.
4. Rename `cag_plugin.exe` to `cag_plugin_orig.exe`
5. Open [TODO: plugin_wrapper.zip link](#)

- a. Copy plugin_wrapper.exe from the zip file to cag_plugin.exe in C:\Program Files\Citrix\Access Gateway
 - b. Copy plugin_wrapper.exe.config from the zip file to cag_plugin.exe.config in C:\Program Files\Citrix\Access Gateway
6. Edit C:\Program Files\Citrix\Access Gateway\cag_plugin.exe.config and change “fred” to the name of the user you created (keep the “\” at the start).
5. Run All Programs → Citrix → Citrix Access Clients → Citrix Access Gateway
 - a. Enter the address of your Access Gateway.
 - b. If you get a warning about your Access Gateway’s certificate not being trusted, either install its root certificate or accept the warning and check the box “Do not show me this message again”.
7. Log in to Access Gateway using the username and password you created.
8. Reboot **dm1** again.

4.6 Verify the Access Gateway plug-in is started automatically

1. Connect to the console on **dm1** again.
2. Logon as the user you created.
 - a. The user should already have been auto logged on to the console so you’ll be connected to the existing session.
3. You should see that the AG client is already connected (look for an icon in the system tray).
 - a. If there’s no icon shown in the system tray, you may actually be connected but the icon is missing (this happens very occasionally).
4. Verify you can access computers on the internal corporate network (e.g. ping your corporate domain controller).

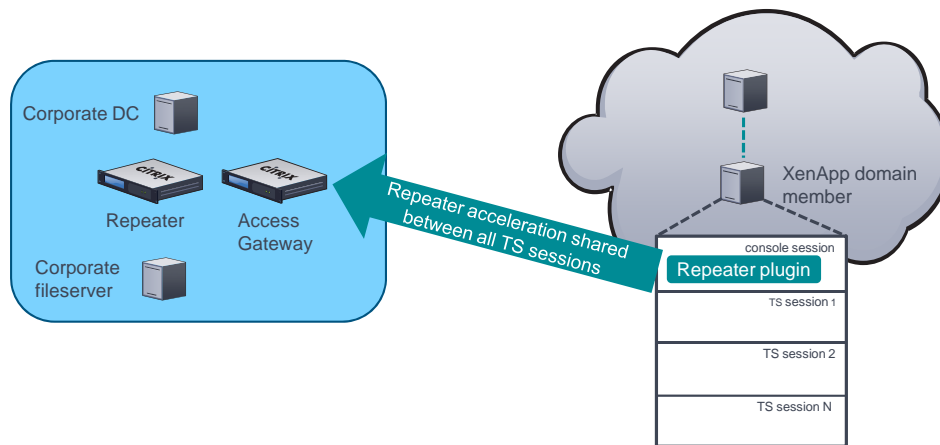
5 Set up Citrix Repeater plug-in on XenApp

5.1 Overview

In order to leverage Citrix Repeater acceleration between the corporate network and XenApp EC2 instances, it's necessary to set up the Repeater plug-in on each instance. It's assumed that you already have a Citrix Repeater appliance providing acceleration services to your corporate network.

Each EC2 XenApp instance creates its own Repeater connection back to the corporate network. These instructions are for a single instance, **dm1.citrix-labs-ec2.compute-1.internal**, but the same applies to any other domain members you create.

The idea is the same as for Access Gateway connection sharing. We create a single Repeater connection in **dm1**'s console session, which all other sessions on the instance then share for traffic acceleration to and from the corporate network.



5.2 Install the Repeater plug-in

1. Connect to the console on **dm1** again.
2. Logon as the user you created for the Access Gateway tunnel in section 4.3.2.
 - a. The user should already have been auto logged on to the console so you'll be connected to the existing session.
3. Download the Repeater plug-in from <http://www.citrix.com/downloads>.
 - a. Select **Citrix Branch Repeater** as the project.
 - b. Click **Log in for More Downloads**.
 - c. Log in with your *My Citrix* user name and password, or register for a new account.
 - d. Under **Clients** you'll find **Repeater Plug-in**.
 - e. Click through to download the .msi file.
 - f. Save the .msi to somewhere on the C: drive.
 - g. Download and install the Microsoft Orca MSI Editor, available as part of the [Windows SDK](#). Note this is a large download (300Mb). Once you've downloaded the Windows SDK, run Orca.msi to install Orca.
4. Run Orca: **Start** → **All Programs** → **Orca**
5. Select **File** → **Open** from the menu.

6. Open the Repeater plug-in .msi.
7. Click on **LaunchCondition** in the left-hand pane.
8. Click on **VersionNT=500 OR VersionNT=501 OR VersionNT=600** in the right-hand pane.
9. Append **OR VersionNT=502** so the full entry reads **VersionNT=500 OR VersionNT=501 OR VersionNT=600 OR VersionNT=502**
10. Select **File → Save**.
11. Exit Orca.
12. Install the (modified) Repeater .msi
 - a. Accept all the defaults.
13. Reboot when the installer asks you to.

5.3 Configure the Repeater plug-in

1. Connect to the console on **dm1** again.
2. Logon as the user you created for the Access Gateway tunnel in section 4.3.2.
 - a. The user should already have been auto logged on to the console so you'll be connected to the existing session.
3. Double click the Repeater plug-in icon in the system tray.
4. Click on the **Configuration** tab.
5. Type in the signalling address of your Citrix Repeater appliance.
6. Click on **Save**.
7. In **Acceleration Rules**, you should see the Repeater plug-in connect to the Repeater appliance and then establish an accelerated link.

5.4 Make the Repeater plug-in multi-session safe

1. Open a Windows Explorer window to C:\Program Files\Citrix\Citrix Accelerator.
2. Rename CitrixAcceleratorUI.exe to CitrixAcceleratorUI_orig.exe
3. Open [TODO: plugin_wrapper.zip link](#)
 - a. Copy plugin_wrapper.exe from the zip file to CitrixAcceleratorUI.exe in C:\Program Files\Citrix\Citrix Accelerator
 - b. Copy plugin_wrapper.exe.config from the zip file to CitrixAcceleratorUI.exe.config in C:\Program Files\Citrix\Citrix Accelerator
4. Edit C:\Program Files\Citrix\Citrix Accelerator\CitrixAcceleratorUI.exe.config
 - a. Change “\fred” to the name of the user you created (keep the “\” at the start).
 - b. Change “C:\Program Files\Citrix\Access Gateway” to “C:\Program Files\Citrix\Citrix Accelerator”
 - c. Change “cag_plugin_orig.exe” to “CitrixAcceleratorUI_orig.exe”
5. Reboot **dm1** again.

6 Verify bridge to corporate network

6.1 Overview

In this section, we'll verify you can now access the corporate network from EC2.

6.2 Verify single sign-on

1. Configure your EC2 account to allow ports 1494 and 2598 ingress to your instances.
2. Configure **dm1** to allow your corporate domain users to logon
 - a. Logon to **dm1** as an administrator.
 - b. Add the Domain Users from your corporate domain to the Remote Desktop Users group on **dm1**.
 - c. For the purposes of testing, we'll connect to a desktop on **dm1**, so we'll need to allow non-administrators to start desktops (you can disable this later if you want).
 - i. Run **Start → Administrative Tools → Terminal Services Configuration**
 - ii. Double click on ICA-tcp in the right-hand pane.
 - iii. Select the ICA Settings tab.
 - iv. Uncheck "Non-administrators only launch published applications".
 - v. Click OK.
3. Start Citrix Program Neighborhood Classic on your local computer¹.
4. Create a Custom ICA connection
 - a. Create a server connection.
 - b. Use the public IP address of **dm1** as the server name.
5. Double click the connection you created.
6. Verify you can logon to **dm1** using your corporate domain credentials.

6.3 Verify access to file shares

Once you've logged on to **dm1** using your corporate domain credentials, use Windows Explorer to view a file share in the corporate domain. Make sure the file share is protected so only domain users can get access it.

Verify that you can see the file share and that you aren't prompted to enter your domain credentials again.

6.4 Verify traffic acceleration

1. Logon to **dm1** using Citrix Program Neighborhood and your corporate domain credentials.
2. In another window, logon to the console on **dm1** and logon as local Administrator.
3. In the corporate domain session, copy a large file from a file share on the corporate domain to somewhere on the local disk.
4. In the local Administrator session, verify that the traffic is being accelerated
 - a. Double click the Citrix Accelerator Manager icon from the system tray.
 - b. Click on the Performance tab.
 - c. You should see a graph of accelerated traffic, with statistics below it.
 - d. The compression ratio should be above 1:1.

¹ An alternative way of creating a direct connection to **dm1** is to write an ICA file containing **dm1**'s public IP address.