STEP BY STEP:
SINGLE SIGN-ON TO AMAZON EC2-BASED .NET APPLICATIONS FROM AN ON-PREMISES WINDOWS DOMAIN

DAVE MARTINEZ

APRIL 2010

Jointly sponsored by Amazon Web Services LLC and Microsoft Corporation

This document is provided for informational purposes only and Martinez & Associates LLC makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release.

All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

TABLE OF CONTENTS

INTRODUCTION

This document provides step-by-step instructions for creating a test lab demonstrating identity federation between an on-premise Windows Server Active Directory domain and an ASP.NET web application hosted on Amazon's Elastic Compute Cloud (EC2) service, using Microsoft's Active Directory Federation Services (AD FS) technology. A companion document describing the rationale for using AD FS and EC2 together is required pre-reading, and is available here.

The document is organized in a series of scenarios, with each building on the ones before it. It is strongly recommended that the reader follow the document's instructions in the order they are presented.

The scenarios covered are:

1. **Corporate application, accessed internally:** Domain-joined Windows client (i.e. in the corporate office) accessing an Amazon EC2-hosted application operated by same company, using AD FS v1.1;
2. **Corporate application, accessed from anywhere:** External, not-domain-joined client (i.e. at the coffee shop) accessing the same EC2-hosted application, using AD FS v1.1 with an AD FS proxy. In addition to external (forms-based) authentication, the proxy also provides added security for the corporate federation server;
3. **Service provider application:** Domain-joined and external Windows clients accessing an EC2-hosted application operated by a service provider, using one AD FS v1.1 federation server for each organization (with the service provider's federation server hosted in EC2) and a federated trust between the parties;
4. **Service provider application with added security:** Same clients accessing same vendor-owned EC2-hosted application, but with an AD FS proxy deployed by the software vendor for security purposes.
5. **Corporate application, accessed internally (AD FS 2.0):** Domain-joined Windows client accessing EC2-based application owned by same organization (same as Scenario 1), but using the currently-in-beta AD FS 2.0 as the federation server and the recently-released Windows Identity Foundation (WIF) .NET libraries on the web server.

Some notes regarding this lab:

- To reduce the overall computing requirements for this lab, AD FS federation servers are deployed on the same machines as Active Directory Domain Services (AD DS) domain controllers and Active Directory Certificate Services (AD CS) certificate authorities. This configuration presents security risks. In a production environment, it is advisable to deploy federation servers, domain controllers and certificate authorities on separate machines.

- This lab includes a fully-functional Public Key Infrastructure (PKI) deployment, using Active Directory Certificate Services. PKI is a critical foundational element to a production-ready federation deployment. Note that:
  - This lab uses a single-tier certificate hierarchy. Note that a two-tier certificate hierarchy with an offline certificate authority (CA) responsible for the organization root certificate would be more secure, but is outside the scope of this lab.
  - Also, this lab uses CA-issued certificates (chained to an internal root CA certificate) for SSL server authentication. This requires distribution of the root CA certificate to all clients that access those web servers, to avoid SSL-related errors. In a production deployment, it is preferable to use certificates that chain to a third-party root certificate (from Verisign, RSA, etc.) that is already present in Windows operating systems, since this alleviates the need to distribute root CA certificates.
- This lab also includes a fully-functional Domain Name Services (DNS) deployment, using Microsoft DNS Server. DNS is also a critical foundational element to a production-ready federation deployment. Note that:
  - This lab uses fictional DNS domains, which Internet name servers resolve to the microsoft.com web site, breaking the lab functionality. Thus, the lab simulates resolution of external DNS names by using DNS forwarding from domain DNS instances to a hypothetical "Internet DNS" server that you run on one of the EC2-hosted web servers. While useful in the context of this lab, DNS forwarding is not a requirement of a functional federation deployment.
- To varying degrees, every scenario covered in this lab requires inbound Internet connectivity to the corporate federation servers, which will reside inside your organization's firewall. Before proceeding, make sure you have access to an external/internet IP address, with open ports 80 and 443 for Scenario 1, and port 443 only for Scenarios 2 through 5.
- This lab will require a total of three local computers. In this lab, Hyper-V virtualization technology in Windows Server 2008 was used to keep physical machine requirements down.
- To simplify the recording of important values you must type during configuration, please use the ***Important Values Worksheet*** on the next page.

ABOUT THE AUTHOR

Dave Martinez (dave@davemartinez.net) is Principal of Martinez & Associates, a technology consultancy based in Redmond, Washington.

IMPORTANT VALUES WORKSHEET

Machine 0: Amazon EC2 Lab Management PC

Name	Value
1. External IP address	

Machine 1: Adatum Internal Server

Name	Value
2. Adatum Administrator password	
3. Internal static IP address	
4. Alan Shen's password	
5. External IP address	

Machine 2: Domain-joined Client

Name	Value
6. Internal IP address	
7. External IP address	

Machine 3: Adatum Web Server

Name	Value
8. Elastic (public) IP address	
9. Administrator password	

Machine 4: Adatum FS Proxy

Name	Value
10. Elastic (public) IP address	

Machine 6: Trey Research Federation Server

Name	Value
11. Elastic (public) IP address	
12. Administrator password	

Machine 7: Trey Research Web Server

Name	Value
13. Elastic (public) IP address	

Machine 8: Adatum Federation Server (AD FS 2.0)

Name	Value
14. External IP address	

SCENARIO 1: CORPORATE APPLICATION, ACCESSED INTERNALLY

Alan Shen, an employee for Adatum Corporation, will use the Active Directory domain-joined computer in his office to access an ASP.NET web application hosted on Windows Server 2008 in Amazon EC2. Using AD FS provides Adatum users access to the application without any additional login requests, and without requiring that the web server be domain-joined using Amazon's Virtual Private Cloud (VPC) service.

This scenario requires three computers:

1) Adatum Internal Server

   This local machine will perform multiple server roles, including that of a domain controller, a root certificate authority, and an AD FS federation server that creates security tokens with which users access the federation application. Specifically, this machine will run:

   a) Active Directory Domain Services (domain controller)
   b) Domain Name Services (Active Directory-integrated DNS server)
   c) Active Directory Certificate Services (root CA)
   d) Internet Information Services (web server)
   e) Microsoft ASP.NET 2.0
   f) Microsoft .NET Framework 2.0
   g) Active Directory Federation Services (Adatum identity provider)

   The AD FS v1 federation server is available in Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2 (Enterprise Editions or above). This lab used a trial Windows Server 2008 R2 Enterprise Edition Hyper-V image which is available for download here.

   > *To run Hyper-V images, you will need to have a base install of Windows Server 2008 (64-bit edition) or Windows Server 2008 R2, running Hyper-V. For more information on obtaining and installing the latest version of Hyper-V, please visit the Hyper-V Homepage.*

2) Domain-joined Client

   This local domain-joined Windows client will be the machine Alan Shen uses to access the federated application. The only client requirement is Internet Explorer (version 5 and above) or another web browser with Jscript and cookies enabled. This lab used Internet Explorer 8 in a trial Windows 7 Enterprise ISO file available here.

3) Adatum Web Server

This machine, based in Amazon EC2, will host the AD FS web agent and the Adatum sample federated web application. In addition, it will act as our general-purpose “Internet DNS” server. Specifically, this machine will run:

a) Internet Information Services (web server)
b) Microsoft ASP.NET 2.0
c) Microsoft .NET Framework 2.0
d) AD FS claims-aware web agent (as opposed to the agent for NT token applications, which is not used in this guide)
e) Sample application (you will create the application files by copying content from this guide)
f) Domain Name Services (DNS server serving Internet DNS zones)

The ADFS v1 web agent is available in Windows Server 2003 R2, Windows Server 2008 and Windows Server 2008 R2 (Standard Editions or above). Amazon EC2 currently offers Windows Server 2003 R2 and Windows Server 2008 (Datacenter Edition) as guest operating systems. This lab used Windows Server 2008.

CONFIGURATION

MACHINE 1: ADATUM INTERNAL SERVER

> *The configuration steps listed below are targeted to Windows Server 2008 R2. If using a different version of Windows Server, use these steps as a guideline only.*

INITIAL INSTALL/CONFIGURATION

Install Windows Server 2008 R2 onto your server computer or virtual machine.

Log into Windows Server with the local machine Administrator account and password. This password automatically becomes the Adatum domain administrator password, once Active Directory is installed.

Record the Adatum administrator password on Line 2 of the **Important Values Worksheet**.

In the **Initial Configuration Tasks** window, click on **Provide computer name and domain**, then click **Change.** In the **computer name** field type **fs1**. Click **OK** twice, then click **Close**, then click **Restart Now**.

Log back into the machine with the Adatum administrator account and password.

CONFIGURE NETWORKING

This computer has the following networking requirements:

- *Inbound Internet connectivity (ports 80 and 443) through a static, external IP address*
- *A static internal IP address, to ensure that clients can properly access the domain DNS server*
- *A subnet mask that will allow the other local computers in this lab to see the domain controller*
- *A default gateway address in the IP address range of the subnet mask, to enable DNS forwarding*

Contact your network administrator to request a static IP address, subnet mask, default gateway, and to open ports 80 and 443 on the external IP address of the default gateway.

In the **Initial Configuration Tasks** window, click on **Configure networking**, then right-click on the **Local Area Connection** and select **Properties**. Double-click on the **Internet Protocol Version 4** list item to open TCP/IPv4 Properties. On the **General** tab, click the radio button to **Use the following IP address**. In the **IP address, Subnet mask,** and **Default Gateway** fields, type the static IPv4 address, subnet mask, and default gateway address provided by your network administrator. In the **Preferred DNS server** field, type **127.0.0.1** (which points the local DNS client to the local DNS server). Click **OK** twice.

Record your Adatum Internal Server static IP address on Line 3 of the **Important Values Worksheet**.

INSTALL/CONFIGURE ACTIVE DIRECTORY DOMAIN SERVICES (AD DS)

Close the **Initial Configuration Tasks** window; this will automatically open **Server Manager**.

In **Server Manager**, right-click on **Roles** and select **Add Roles** to start the Add Roles Wizard. On the **Select Server Roles** page, check the box next to **Active Directory Domain Services**. Click the **Add Required Features** button to allow Server Manager to add .NET Framework 3.5.1 to the installation process. Click **Next** twice, then **Install**. On the **Installation Results** page, click on the link for the **Active Directory Domain Services Installation Wizard (dcpromo.exe).**

On the **Choose a Deployment Configuration** page, select **Create a new domain in a new forest**. On the **Name the Forest Root Domain** page, type **corp.adatum.com**. On the **Set Forest Functional Level** and **Set Domain Functional Level** pages, leave the default setting of **Windows Server 2003**. On the **Additional Domain Controller Options** page, leave **DNS Server** checked. When prompted about not finding an authoritative DNS zone, click **Yes** to continue. Complete the wizard, keeping all other default values. When prompted, **restart computer**.

Once logged back into machine, click **Start > Administrative Tools > Active Directory Users and Computers**. Under **corp.adatum.com**, right-click on **Users** and select **New > Group**. In the **Group Name** field, type **Managers** and click **OK**.

Right-click **Users** again and choose **New > User**. In the First name field type **Alan.** In the **Last name** field type **Shen.** In the **User logon name** field type **alansh.** Click **Next.** Provide a password and click **Next** then **Finish.**

Record Alan Shen's password on Line 4 of the **Important Values Worksheet**.

Click on **Users**, then right-click on **Alan Shen** and select **Properties**. On the **General** tab, in the **E-mail** field type **alansh@adatum.com**. On the **Member of** tab, click **Add**. In the **Select Groups** box type **Managers** then click **Check Names**. Once verified, click **OK** twice.

IDENTIFY EXTERNAL IP ADDRESS

Identify your external IP address. You can ask your network administrator, or an alternative is to visit http://www.whatismyip.com.

Record your Adatum Internal Server external IP address on Line 5 of the **Important Values Worksheet**.

INSTALL/CONFIGURE ACTIVE DIRECTORY CERTIFICATE SERVICES (AD CS)

In **Server Manager**, right-click on **Roles** and select **Add Roles** to start the Add Roles Wizard. On the **Select Server Roles** page, check the box next to **Active Directory Certificate Services**. On the **Select Role Services** page, select **Certification Authority** and **Certification Authority Web Enrollment**. Click the **Add Required Features** button to allow Server Manager to add IIS to the installation process. On the **Specify Setup Type** page select **Enterprise** and on the **Specify CA Type** page select **Root CA**. On the **Setup Private Key** page, select **Create a new private key** and accept the default cryptography settings. On the **Configure CA Name** page, in the **Common Name for this CA** field type **Adatum Certificate Server**. Complete the wizard, keeping all other default values.

Click **Start > Run**. In the **Run** box type **mmc** and click **OK** to start the Microsoft Management Console. In the **File** menu select **Add/Remove Snap-in**. Highlight the **Certificates** snap-in and click the **Add** button; choose **computer account** and **local computer** in the following pages. Highlight the **Certificate Templates** snap-in and click **Add**. Highlight the **Certification Authority** snap-in and click **Add**; choose **local computer** in the following page and click **OK**. Click **File > Save**, and save the new MMC console (Console 1) to the machine desktop for future use.

In **Console 1**, expand **Certification Authority**. Right-click on **Adatum Certificate Server** and select **Properties**. On the **Extensions** tab for the **CRL Distribution Point (CDP)** extension, highlight the **http://** certificate revocation list location in the list. Below the list, click the **Include in CRLs** and **Include in the CDP extension of issued certificates** options and click **OK**. Click **Yes** to restart AD CS.

In **Console 1**, expand **Adatum Certificate Server**. Right-click on the **Revoked Certificates** folder and select **All Tasks > Publish**. Click **OK** to publish a new CRL with the enhanced CDP extension.

ENABLE DOUBLE ESCAPING FOR CRL WEB SITE IN IIS (WINDOWS SERVER 2008 ONLY)

> ***This task pertains only to Windows Server 2008.*** *If you are using Windows Server 2008 R2, this issue is automatically addressed by the AD CS install process.*
>
> *By default, Active Directory Certificate Services in Windows Server 2008 and above generates delta CRL files, which update on a more frequent schedule (daily) than standard CRL files (weekly). The default file name used by AD CS for a delta CRL file includes a plus ("+") sign, and in this lab, this file is accessed over the Internet. By default, IIS 7 (Windows Server 2008) and IIS 7.5 (Windows Server 2008 R2) reject URIs containing the plus character, creating an incompatibility with AD CS delta CRL files.*
>
> *To fix this, the default request filter behavior of the web site hosting the delta CRL file must be modified. AD CS in Windows Server 2008 R2 does this automatically. If using Windows Server 2008, follow the procedure below.*

Click **Start > Run**. In the **Run** box type **cmd** and click **OK** to open a command prompt. Change the directory to **c:\windows\system32\inetsrv**. At the command prompt, type the following and hit **Enter**:

```
appcmd set config "Default Web Site/CertEnroll" -
section:system.webServer/security/requestFiltering -
allowDoubleEscaping:true
```

CONFIGURE AD CS CERTIFICATE TEMPLATES

In **Console 1**, click on **Certificate Templates** in the left navigation area. In the center pane, right-click on the **Web Server** certificate template and select **Duplicate Template**. In the **Duplicate Template** dialog, leave **Windows Server 2003 Enterprise** as the minimum CA for the new template and click **OK**. In **Properties of New Template**, make the following changes:

- On the **General** tab, in the **Template display name** field type **Extranet Web Server**
- On the **Request Handling** tab, check the box next to **Allow private key to be exported**

Click **OK** to create the new template.

In the center pane, right-click on the **Web Server** certificate template and choose **Properties**. In the **Security** tab, click **Add**, and in the object names text box type **Domain Controllers** and click **Check Names**. Once verified, click **OK**. Back in the **Security** tab, highlight the **Domain Controllers** list item, then in the **Allow** column check the **Read** and **Enroll** permissions and click **OK**. Click **Start > Administrative Tools > Services**. Right-click on **Active Directory Certificate Services** and select **Restart**.

In **Console 1**, in the left navigation area, right-click on **Certificate Authority\Adatum Certificate Server\Certificate Templates** and select **New > Certificate Template to Issue**. Highlight **Extranet Web Server** from the list and click **OK**.

CREATE SERVER AUTHENTICATION CERTIFICATE

In **Console 1**, right-click on **Certificates (Local Computer)/Personal/Certificates** and select **All Tasks > Request New Certificate**. In the Certificate Enrollment Wizard, click **Next** twice, then click the blue link under **Web Server**. In **Certificate Properties**, make the following changes:

- On the **Subject** tab, in the **Subject Name** area click on the **Type** dropdown list and select **Common name**. In the **Value** field type **fs1.corp.adatum.com** and click **Add**.
- On the **General** tab, in the **Friendly name** text box type **adatum fs ssl** and click **OK**.

In the **Certificate Enrollment** window, check the box next to **Web Server** and then click the **Enroll** button, then click **Finish**. In **Console** 1, check for the new certificate with friendly name "adatum fs ssl" in **Certificates (Local Computer)/Personal/Certificates**.

CREATE AD FS TOKEN SIGNING CERTIFICATE

> *While it is possible to use the same certificate for server authentication and token signing, security best practice suggests using distinct certificates for each function. We will, however, use the same Web Server certificate template to issue the token signing certificate.*

In **Console 1**, right-click on **Certificates (Local Computer)/Personal/Certificates** and select **All Tasks > Request New Certificate.** In the Certificate Enrollment Wizard, click **Next** twice, then click the blue link under **Web Server**. In **Certificate Properties**, make the following changes:

- On the **Subject** tab, in the **Subject Name** area click on the **Type** dropdown list and select **Common name**. In the **Value** field type **Adatum Token Signing Cert1** and click **Add**.
- On the **General** tab, in the **Friendly name** text box type **adatum ts1** and click **OK**.

In the **Certificate Enrollment** window, check the box next to **Web Server** and then click the **Enroll** button, then click **Finish**. In **Console 1**, check for the new certificate with friendly name "adatum ts1" in **Certificates (Local Computer)/Personal/Certificates**.

INSTALL ACTIVE DIRECTORY FEDERATION SERVICES (AD FS)

In **Server Manager**, right-click on **Roles** and select **Add Roles** to start the Add Roles Wizard. On the **Select Server Roles** page, check the box next to **Active Directory Federation Services**. On the **Select Role Services** page, check the box next to **Federation Service**. Click the **Add Required Role Services** button to allow Server Manager to add IIS features to the installation process, and then click **Next**. On the **Choose a Server Authentication Certificate** page, highlight the existing certificate issued to **fs1.corp.adatum.com** with the intended purpose **Server Authentication** and click **Next**. On the **Choose a Token Signing Certificate** page, highlight the existing certificate issued to **Adatum Token Signing Cert1** and click **Next**. Accept all other defaults and click **Install**.

INITIAL AD FS CONFIGURATION

Click **Start > Administrative Tools > Active Directory Federation Services**. Right-click on **Account Stores** under **Federation Service/Trust Policy/My Organization** and select **New > Account Store**. In the Add Account Store Wizard, leave **AD DS** as the store type and click through to add the local AD domain.

Right-click on **My Organization/Organization Claims** and select **New > Organization claim**. In the **Claim name field** type **PriorityUsers** and click **OK**.

Right-click on **My Organization/Account Stores/Active Directory** and select **New > Group Claim Extraction**. Click **Add**, then type **Managers** into the text box and click **Check Names**. Once verified, click **OK**. In the **Map to this Organization Claim** dropdown list select **PriorityUsers**, then click **OK**.

Click on **My Organization/Account Stores/Active Directory.** In the right-hand pane, right-click on the **Email** organization claim and select **Properties**. In the **Claim Extraction Properties** dialog box, check the box next to **Enabled**, and in the **LDAP attribute** field type **mail** and click **OK**.

ADD ADATUM INTERNAL SERVER URL TO INTRANET ZONE IN DOMAIN GROUP POLICY

> *This enables domain client browsers to access the federation server at https://fs1.corp.adatum.com using Integrated Windows Authentication.*

Click **Start > Administrative Tools > Group Policy Management**. Right-click on **Forest:corp.adatum.com/Domains/corp.adatum.com/Default Domain Policy** and select **Edit**. Click on **User Configuration/Policies/Windows Settings/Internet Explorer Maintenance/Security**. In the left-hand pane, right-click on **Security Zones and Content Ratings** and select **Properties**. In the **Security Zones and Privacy** section, click the radio button next to **Import the current security zones and privacy settings**, then click **Continue**, and then click **Modify Settings**. In the **Internet Properties** window, on the **Security** tab, highlight the **Local Intranet** zone and click the **Sites** button. Click **Advanced**, then in the **Add this website to the zone** text box type **https://fs1.corp.adatum.com** and click **Add**. Click **Close**, then **OK** twice.

MACHINE 2: DOMAIN-JOINED CLIENT

> *The configuration steps listed below are targeted to Windows 7. If using a different version of Windows, use these steps as a guideline only.*

INITIAL INSTALL/CONFIGURATION

Install Windows 7 onto your client computer or virtual machine.

Click **Start > Control Panel > Network and Internet > Network and Sharing Center**. On the left side of the window, click **Change Adapter Settings.** Right-click on **Local Area Connection**, select **Status**, and then click the **Details** button. Note the IPv4 address.

Record your Domain-joined Client internal IP address on Line 6 of the **Important Values Worksheet**.

Click **Close***,* then click **Properties**. Double-click on the **Internet Protocol Version 4** list item to open TCP/IPv4 Properties. On the **General** tab, click the radio button to **Use the following DNS server address**. In the **Preferred DNS server** field, enter the value from Line 3 of the **Important Values Worksheet** and click **OK** twice.

Click **Start**. Right-click on **Computer** and select **Properties**. In the **Computer name, domain and workgroup settings** area click the link to **Change Settings**. In the **System Properties** window, on the **Computer Name** tab click the **Change** button. In the **Computer Name** field type **client.** In the **Member of** area, click the radio button for **Member of Domain**, and in the **Domain** text box type **CORP** and click **OK**. Type the Adatum domain administrator username and password from Line 2 of the **Important Values Worksheet** and click **OK**. Follow the prompts to **restart the computer**.

Log onto the computer as **CORP\Administrator**, using the password from Line 2 of the **Important Values Worksheet**.

IDENTIFY EXTERNAL IP ADDRESS

Now identify the client's external IP address. One way is to visit http://www.whatismyip.com.

Record your Domain-joined Client external IP address on Line 7 of the **Important Values Worksheet**.

CHECK CERTIFICATE/GROUP POLICY SETTINGS

Click **Start**. In the **Search programs and files** box type **mmc** and hit **Enter** to start the Microsoft Management Console. In the **File** menu select **Add/Remove Snap-in**. Highlight the **Certificates** snap-in and click the **Add** button; choose **computer account** and **local computer** in the following pages and click **OK**. Click **File > Save**, and save the new MMC console (Console 1) to the machine desktop for future use.

In **Console 1**, check in **Certificates (Local Computer)/Trusted Root Certificate Authorities/Certificates** for the presence of the **Adatum Certificate Server** root certificate. It should have been placed here automatically by the domain controller.

Open **Internet Explorer**. On the **Tools** menu, select **Internet Options**. On the **Security** tab, click on the **Local Intranet** zone icon and then click the **Sites** button. Click the **Advanced** button, and ensure that **https://fs1.corp.adatum.com** is listed as a website in this zone.

Click **Start**. Next to the Shutdown button, click the arrow and select **Switch User**. Login as **CORP\alansh**, using the password from Line 4 of the **Important Values Worksheet**.

MACHINE 3: ADATUM WEB SERVER

CREATE/CONFIGURE AMAZON EC2 ACCOUNT

> *You can access EC2 virtual machines and the EC2 Console management application on any computer with Internet access. In this lab, the external IP address of the computer used to access EC2 is used in firewall settings on EC2, to limit inbound RDP access to just the lab administrator. You can determine this machine's external IP address by visiting a site like http://www.whatismyip.com.*
>
> *Record your EC2 management external IP address on Line 1 of the **Important Values Worksheet**.*

Create an Amazon Web Services (AWS) account by visiting http://aws.amazon.com and clicking the **Sign Up Now** button.

Once complete, on the **Success/Thank You** page, click on hyperlink for **Amazon Elastic Compute Cloud (EC2),** then click the **Sign Up for Amazon EC2** button. Enter credit card information, address, and complete phone-based verification process. Click the **Complete Sign Up** button. When you see ***Thank you for signing up for Amazon Elastic Compute Cloud***, click the link for the **AWS Management Console**. Click the button to **Sign in to the AWS Console** with EC2 as the default service.

In the **EC2 Console**, in the left navigation bar select your **Region** as the location for your hosted images.

CREATE WINDOWS SERVER INSTANCE IN EC2

In the **EC2 Console**, click on the **Launch Instance** button to launch the Request Instances Wizard. Click on the **Community AMIs** tab, and in the adjacent text box type **amazon/Windows-Server2008.** Find the entry for **amazon/Windows-Server2008-i386-Base-<version#>** and click the **Select** button to its right. On the **Instance Details** page, leave the defaults selected. On the **Advanced Instance Details** page, accept the default settings. On the **Create Key Pair** page, select **Create a new Key Pair**. Enter **ADFSkey** as your key pair name, then click the yellow **Create and download your key pair** button. Save the resulting ADFSkey.pem file to your desktop. On the **Configure Firewall** page, select **Create a New Security Group**. Name the new group **Adatum Web Server**, then click on the **Select** dropdown box and **Add** the following allowed connections:

Application	Transport	Port	Source Network/CIDR[1]
RDP	TCP	3389	Lab management external IP/32[2]
HTTPS	TCP	443	Domain client external IP/32[3]
DNS	UDP	53	All Internet[4]

[1] Classless Inter-Domain Routing (CIDR) addresses allow you to scope inbound access to an EC2 instance to a specific IP address or subnet range. In this scenario, we can limit inbound access to only the Adatum domain network, or just the client computer. The CIDR portion of the IP address scopes the allowed incoming connections to your liking; for example, 1.2.3.4/32 allows only the specific IP address 1.2.3.4, while 1.2.3.4/24 allows access to any computer in the 1.2.3 subnet. To learn more about CIDR visit here.

[2] This is the external IP address of the machine being used to access the Amazon EC2 images via Remote Desktop, recorded on Line 1 of the **Important Values Worksheet**.

[3] This is the external IP address of the domain-joined client, recorded on Line 7 of the **Important Values Worksheet**.

[4] This setting is the equivalent of the address 0.0.0.0/0, and allows access from any Internet IP address. Since we're mimicking Internet DNS, we've used this setting.

Click **Continue**, then in the **Review** page click **Launch** to start the instance. Click **Close**. Click on **Instances** in the left navigation bar to see the status of your instance.

ASSOCIATE AN ELASTIC IP ADDRESS

In the **EC2 Console**, click on the **Elastic IPs** link in the left navigation area. Click the **Allocate New Address** button, then click on the **Yes, Allocate** button. Once allocated, right-click on the address and select Associate **Address**. Select the **Adatum Web Server** instance ID from the dropdown list and click **Associate**.

Record the Adatum Web Server elastic IP address on Line 8 of the **Important Values Worksheet**.

GET WINDOWS ADMINISTRATOR PASSWORD

In the **EC2 Console**, click on **Instances** in the left navigation area. Once the Status shows as "running" and your Elastic IP address is listed in the Public DNS column, right-click on the **Adatum Web Server** instance and select **Get Windows Password**. On your desktop, **open** the **ADFDSkey.PEM** file with Notepad and **copy** the entire contents of the file (including the Begin and End lines, Eg: "-----BEGIN RSA PRIVATE KEY-----"). In the **EC2 Console**, **paste** the text into the **Retrieve Default Windows Administrator Password** window. Click **inside the text box once** to enable the **Decrypt Password** button, then click **Decrypt Password**. Copy the **Computer, User and Decrypted Password** information into a text file, and save to your desktop. Click **Close** in the **Retrieve Password** window.

ACCESS INSTANCE USING REMOTE DESKTOP CONNECTION

The default RDP client in Windows XP does not support server authentication, which is required for access. To download a newer client visit here.

Click **Start > All Programs > Accessories > Communication > Remote Desktop Connection**. In the **Computer** text box copy/paste or type the **Computer Name** from your text file (for example, ec2-123-456-78-910.compute-1.amazonaws.com), then click **Connect**.

In the login dialog box that appears, type **Administrator** for user name and the **Decrypted Password** from your text file into the Password field, taking care to get capitalization correct, and click **OK**.

In the **Set Network Location** window, click on **Public Location**, then **Close**.

Optional

Once inside the instance, change the Administrator password by clicking **CTRL-ALT-END** and clicking the **Change a password** link.

Record the Adatum Web Server Administrator password on Line 9 of the **Important Values Worksheet**.

Optional

Turn off the Internet Explorer Enhanced Security Configuration for administrators. In **Server Manager**, on the **Server Summary** page under **Security Information**, click on **Configure IE ESC**. Under **Administrators,** click the **Off** radio button and click **OK**.

ADJUST CLOCK SETTINGS

> *Federation depends on the accuracy of time stamps used in signed security tokens.*

Right-click on the **Windows Taskbar** and select **Properties**. On the **Notification Area** tab, check the box to show the **Clock** and click **OK**. Right-click over the clock in the taskbar and select **Adjust Date/Time**. On the **Date and Time** tab, click the **Change time zone** button and adjust to your time zone. Click **OK** twice.

INSTALL WEB SERVER ROLE

In **Server Manager**, right-click on **Role** in the left navigation area and select **Add Roles** to start the Add Roles Wizard. On the **Select Server Roles** page, check the box next to **Web Server (IIS).** Click on the **Add Required Features** button to allow Server Manager to add the Windows Process Activation service to the install, then click **Next** twice. On the **Select Role Services** page, check the box next to **ASP.NET**, then click the **Add Required Role Services** button. Click **Next** then **Install**. Click **Close** to complete the install.

ADD RECORD FOR ADATUM INTERNAL SERVER TO HOSTS FILE

> *The web server needs to periodically access the federation server in order to download trust policy information. Therefore, the web server needs to resolve the federation server DNS name. Since the EC2-based web server is not a member of the Adatum corporate subnet, it needs to resolve the external IP address of the federation server. Here we handle this by using a host file entry. A second perimeter DNS server, or a split DNS configuration for the corp.adatum.com zone could also be used here.*

Open the **c:\Windows\system32\drivers\etc** directory folder. Right-click on the **hosts** file and select **Open**; select **Notepad** as the program and click **OK**.

Add the name and external IP address of the Adatum Internal Server from Line 5 of the **Important Values Worksheet** to the hosts file, as shown in the following example:

123.456.78.910 fs1.corp.adatum.com

Save and **close** the file. Create a shortcut to the hosts file on the desktop for future use.

INSTALL ADATUM ROOT CA CERTIFICATE

To successfully communicate with the federation server, the web server has to trust the SSL server authentication certificate at fs1.corp.adatum.com issued by the Adatum CA.

Open **Internet Explorer** and go to **https://fs1.corp.adatum.com/certsrv/**. In the **Certificate Error** page, click the link to **Continue to this website**. At the login prompt, log in as administrator with the password from Line 2 of the **Important Values Worksheet** to reach the Active Directory Certificate Services home page. At the bottom of the page, click the link to **Download a CA certificate, certificate chain, or CRL**. On the next page, click the link to **Download CA certificate**. **Save** the resulting **certnew.cer** file to the desktop.

Leave the AD CS web application open for use in upcoming steps.

Click **Start > Run**. In the **Run** box type **mmc** and click **OK** to start the Microsoft Management Console. In the **File** menu select **Add/Remove Snap-in**. Highlight the **Certificates** snap-in and click the **Add** button; choose **computer account** and **local computer** in the following pages. Highlight the **Certificates** snap-in again and click the **Add** button; choose **My user account** in the following page and click **OK**. Click **File > Save**, and save the new MMC console (Console 1) to the machine desktop for future use.

In **Console 1**, right-click **on Certificates (Local Computer)/Trusted Root Certification Authorities/Certificates** and select **All Tasks > Import** to launch the Certificate Import Wizard. On the **File to Import** page, click **Browse**, find the **certnew.cer** file on the desktop, and click **Open**. Click **Next** twice, then **Finish**, then **OK** to complete the import process.

SAVE IMAGE

To save some time later, we'll use an image of this server in this state as a starting point for a future server instance.

In the **EC2 Console**, click on **Instances** in the left navigation area, Right-click on the instance for the **Adatum Web Server** and select **Create Image (EBS AMI)**. In the **Image Name** field type **webserver** and click **Create This Image**. Click on the **View Pending Image** link to see the status of your saved image.

ADD AD FS CLAIMS-AWARE APPLICATION AGENT

In **Server Manager**, right-click on **Role** in the left navigation area and select **Add Roles** to start the Add Roles Wizard. On the **Select Server Roles** page, check the box next to **Active Directory Federation Services.** On the **Select Role Services** page, check the box next to **Claims-aware Agent**. Click **Next** then **Install**. Click **Close** to complete the install.

CREATE SAMPLE APPLICATION

You can use the sample claims-aware application provided in this document to test your federation scenarios. The claims-aware application is made up of three files:

default.aspx

web.config

default.aspx.cs

Click **Start > My Computer**. Create a new folder in **c:\inetpub** called **adfsv1app**. You will save the following files to the **c:\inetpub\adfsv1app** directory.

The sample application code and assembly steps can be found in Appendix A.

CREATE SERVER AUTHENTICATION CERTIFICATE

Back in **Internet Explorer**, click on **Home** in the upper right corner of the Certificate Services web application. Click the link to **Request a certificate**, then the link for **advanced certificate request** and finally the link to **Create and submit a request to this CA**. If prompted about the page requiring HTTPS click **OK**. If prompted to run the **Certificate Enrollment Control** add-on click **Run**.

On the **Advanced Certificate Request** page, in the **Certificate Template** dropdown select **Extranet Web Server**. In the **Identifying Information** section, in the **Name** field type **adfsv1app.adatum.com**, and leave the other fields blank. In the **Additional Options** section, in the **Friendly Name** field type **adatum web ssl** and click **Submit**. Click **Yes** to complete the request process; the certificate will be issued automatically.

Click the link to **Install this certificate** and click **Yes** on the warning dialog. In **Console 1**, click on **Certificates (Current User)/Personal/Certificates**. In the right-hand pane should be the certificate for adfsv1app.adatum.com.

MOVE SERVER AUTHENTICATION CERTIFICATE TO LOCAL COMPUTER CERTIFICATE STORE

In Windows Server 2008, the option in the AD CS Web Enrollment pages to automatically save certificates to the Local Computer certificate store was removed. AD FS requires that certificates be stored in the Local Computer certificate store. This process moves the certificate to the proper location.

In **Console 1**, right-click on the **adfsv1app.adatum.com** certificate and choose **All Tasks > Export** to launch the Certificate Export Wizard. On the **Export Private Key** page, select **Yes, export the private key**. On the **Export File Format** page, leave the default setting. After providing a password, On the **File to Export** page click **Browse**, click on **Desktop** and in the **File name** field type **adatum web ssl**. Click **Save** > **Next > Finish > OK** to complete the export process.

In **Console 1**, right-click on **Certificates (Local Computer)/Personal** and choose **All Tasks > Import** to launch the Certificate Import Wizard. On the **File to Import** page, click **Browse** and find **adatum web ssl.pfx** on the desktop. Click **Open**, then click **Next**. After typing the password, click **Next > Next > Finish > OK** to complete the import process.

ADD SAMPLE APPLICATION TO IIS

Click **Start > Administrative Tools > Internet Information Services (IIS) Manager**. Right-click on the **Sites** folder in the left navigation area and select **Add Web Site**. In the **Site name** field type **ADFSv1 app**. In the **Application Pool** field click **Select**. In the **Application pool** dropdown list select **Classic .NET AppPool** and click **OK**. In the **Content Directory** section, click on the button to the right of the **Physical path** field, browse to **c:\inetpub\adfsv1app** and click **OK**. In the **Binding** section, in the **Type** dropdown box select **https**. In the **SSL certificate** dropdown box, select **adatum web ssl** and click **OK**.

SAVE IMAGE

In the **EC2 Console**, click on **Instances** in the left navigation area, Right-click on the instance for the **Adatum Web Server** and select **Create Image (EBS AMI)**. In the **Image Name** field type **webserver2** and click **Create This Image**. Click on the **View Pending Image** link to see the status of your saved image.

ADD DNS SERVER ROLE

This web server will run a DNS Server that will serve the Internet DNS zones.

In **Server Manager**, right-click on **Role** in the left navigation area and select **Add Roles** to start the Add

Roles Wizard. On the **Select Server Roles** page, check the box next to **DNS Server**. On the warning about static IP addresses, click **Install DNS Server anyway** (we have an EC2 elastic IP address, only Windows doesn’t know this). Click **Next > Next > Install**. Click **Close** to complete the install.

Click **Start > Administrative Tools > DNS**. In the left navigation area, right-click on the **Forward Lookup Zones** folder and select **New Zone** to start the New Zone Wizard. On the **Zone Type** page, leave the default setting of **Primary zone**. On the **Zone Name** page, type **adatum.com** in the text box and click **Next**. Accept the defaults on the **Zone File** and **Dynamic Updates** pages. Click **Finish**.

ADD RECORD FOR SAMPLE APPLICATION IN INTERNET DNS

In **DNS Manager**, right-click on **<Machine name>/Forward Lookup Zones/adatum.com** and select **New Host (A or AAAA)**. In the **New Host Name** field type **adfsv1app** and in the **IP address** field type the elastic IP address for the Adatum Web Server from Line 8 of the **Important Values Worksheet**. Click **Add Host > OK > Done.**

MACHINE 1: ADATUM INTERNAL SERVER

ADD SAMPLE APPLICATION TO AD FS

Right-click on **My Organization/Applications** and select **New > Application**. Enter the following in the Add Application Wizard:

- On the **Application Type** page, leave **Claims-aware application** as the application type.
- On the **Application Details** page, in the **Application display name** field type **ADFSv1 app** and in the **Application URL** field type **https://adfsv1app.adatum.com/**
- On the **Accepted Identity Claims** page, check the box next to **User principal name (UPN)**
- Click **Next** twice and then **Finish**.

Click on **ADFSv1 app** under **Applications**. In the right-hand window, right-click on the **PriorityUsers** and **Email** claims and select **Enable**.

ADD DNS FORWARDER FROM ADATUM DOMAIN DNS TO INTERNET DNS

Click **Start > Administrative Tools > DNS**. Click on **FS1** in the left navigation area, then right-click on **Forwarders** in the right-hand pane and select **Properties**. On the **Forwarders** tab, click **Edit**, then type the Adatum Web Server elastic IP address from Line 8 of the **Important Values Worksheet** and hit **Enter**. Watch for the word “validating” to change to “OK” in the Edit Forwarders window. Click **OK** twice to complete the forwarder setup.

CONFIGURE FIREWALL SETTINGS

The federation server must have inbound connectivity from the internet (port 443) in order to communicate with the EC2-based web server. However, the private keys a federation server uses to sign security tokens are sensitive items that should be protected as much as possible. To reduce the security threat the open ports represent, we use firewall rules to scope down the allowable inbound communications. Here, we do this with the Windows Server 2008 integrated firewall.

Click **Start > Administrative Tools > Windows Firewall with Advanced Security**. Click on **Inbound Rules** in the left navigation area. In the right-hand pan under **Actions**, click on **Filter by Group** and select **Filter by Secure World Wide Web Services (HTTPS)**. In the center pane, right-click on the **World Wide Web Services (HTTPS Traffic-In)** rule and select **Properties**. In the **Properties** dialog box, click on the **Scope** tab. In the **Remote IP address** section, click the radio button next to **These IP addresses:**, then click **Add**. In the **IP Address** window, in the **This IP address or subnet** field, type the elastic IP address of the Adatum Web Server from Line 8 of the **Important Values Worksheet** and click **OK**.

Click **Add** again, and in the same field type the internal IP address of the domain-joined client from Line 6 of the **Important Values Worksheet**. Click **OK** twice.

In the right-hand pane under **Actions**, click on **Filter by Group** and select **Filter by World Wide Web Services (HTTP)**. In the center pane, right click on the **World Wide Web Services (HTTP Traffic-In)** rule and select **Properties**. In the **Properties** dialog box, click on the **Scope** tab. In the **Remote IP address** section, click the radio button next to **These IP addresses:**, then click **Add**. In the **IP Address** window, in the **This IP address or subnet** field, type the elastic IP address of the Adatum Web Server from Line 8 of the **Important Values Worksheet** and click **OK**.

Port 80 is required for web server access to the Adatum CA certificate revocation list (CRL); CRLs cannot be served over HTTPS.

TEST

To test the scenario, log into the domain-joined client as Alan Shen (alansh) using the password from Line 4 of the **Important Values Worksheet**. In **Internet Explorer**, type **https://adfsv1app.adatum.com** into the address bar and hit **Enter**. You should be presented with access to the Adatum claims-aware application hosted on EC2, without being asked for a password. Scroll down to note the claims that were passed to the application, including the PriorityUsers and Email claims based on Active Directory group membership and attributes.

If you are running into errors, it’s possible that you are having certificate verification issues. Please see Appendix B for more information.

SCENARIO 2: CORPORATE APPLICATION, ACCESSED FROM ANYWHERE

This case is similar to Scenario 1, in that the scenario involves a corporate user needing federated access to an ASP.NET application hosted by their employer on Amazon EC2. However, in Scenario 2 Alan Shen needs access from a computer that is not joined to the Adatum domain – maybe the user's personal computer at home, or laptop in a coffee shop. The use of an AD FS federation server proxy (or FS proxy), which sits in a perimeter network outside the domain, enables Adatum to handle federation functions for users regardless of their physical location by proxying communication with the internal federation server.

Using an FS proxy also improves security by keeping the number of computers with inbound access to the federation server to just the web server(s) and the proxy. Without the FS proxy, all external clients would need inbound port 443 access to the federation server.

This scenario adds two additional computers to the lab.

4) Adatum FS Proxy

   This machine runs in a perimeter network and is accessible from any device with Internet connectivity. It will route user requests from the Internet to the corporate federation server. In our case, we will host this machine on Amazon EC2. Specifically, this machine will run:

   a) Internet Information Services (web server)
   b) Microsoft ASP.NET 2.0
   c) Microsoft .NET Framework 2.0
   d) Active Directory Federation Services (Adatum federation server proxy)

   The ADFS v1 FS proxy is available in Windows Server 2003 R2, Windows Server 2008 and Windows Server 2008 R2 (Enterprise Edition or above). Amazon EC2 currently offers Windows Server 2003 R2 and Windows Server 2008 (Datacenter Edition) as guest operating systems. This lab used Windows Server 2008.

   Also, in an additional effort to reduce external access to internal servers, we will host the Adatum certificate revocation list (CRL) files here on the Adatum FS Proxy. This will allow us to close port 80 inbound on the internal server.

5) External Client

   This client computer is used to access the federated application from outside the Adatum domain, to simulate the user experience from a coffee shop, internet kiosk or home-based computer. The only requirement is Internet Explorer (version 5 and above) or another web browser with Jscript and cookies enabled. In this lab, we used the computer hosting the Adatum domain Hyper-V images, which was running Windows Server 2008.

CONFIGURATION

MACHINE 1: ADATUM INTERNAL SERVER

CREATE FS PROXY CLIENT AUTH CERTIFICATE TEMPLATE

> *An FS proxy uses a client authentication certificate to securely communicate with federation servers.*

In **Console 1**, click on **Certificate Templates**. In the center pane, right-click on the **Computer** certificate template and choose **Duplicate Template**. In the **Duplicate Template** dialog, leave **Windows Server 2003 Enterprise** as the minimum CA for the new template and click **OK**.

In **Properties of New Template**, make the following changes:

- On the **General** tab, in the **Template display name** field type **Adatum Proxy Client Auth**
- On the **Request Handling** tab, check the box next to **Allow private key to be exported**
- On the **Subject Name** tab, click the radio button next to **Supply in the request**. Click **OK** in the warning about allowing user-defined subject names with automatic issuance.

Click **OK** to create the new template.

In **Console 1**, right-click on the **Certificate Authority\Adatum Certificate Server\Certificate Templates** folder, and select **New > Certificate Template to Issue**. Highlight **Adatum Proxy Client Auth** from the list and click **OK**.

ADD NEW LOCATION TO CDP EXTENSION IN ADATUM CA

> *Later we will create a new web site for Adatum's CRL files. This new web site location needs to be referenced in all certificates issued by Adatum's CA. This is done by modifying the CDP extension on the CA. For performance reasons, we'll also remove other existing CDP locations.*

In **Console 1**, right-click on **Certification Authority/Adatum Certificate Server** and select **Properties**. On the **Extensions** tab, in the **Select extension** dropdown box make sure the **CRL Distribution Point (CDP)** extension is selected. Click the **Add** button. In the **Add Location** window, in the **Location** field type **http://crl.adatum.com/**, making sure to include the forward-slash at the end. Click the **Insert** button, which adds the **<CaName>** variable (shown in the Variable dropdown list) as the next element of the address. Click on the **Variable** dropdown list and select **<CRLNameSuffix>** and click **Insert**. Click on the **Variable** dropdown list and select **<DeltaCRLAllowed>** and click **Insert**. Back up in the Location field, place the cursor at the end of the address and complete the URL by typing **.crl** and click **OK**.

The final address you added should be:

http://crl.adatum.com/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

Back on the **Extensions** tab, highlight the new location. Check the boxes next to **Include in CRLs** and **Include in the CDP extension of issued certificates.** Highlight the existing **http://<ServerDNSName>** location, and then uncheck the boxes next to **Include in CRLs** and **Include in the CDP extension of issued certificates.** Highlight the existing **ldap://** location, and then uncheck the boxes next to **Include in CRLs** and **Include in the CDP extension of issued certificates** and click **OK**. Click **Yes** to restart AD CS.

REISSUE ADATUM CRL FILE

In **Console 1,** right-click on **Certification Authority/Adatum Certificate Server/Revoked Certificates** and select **All Tasks > Publish**. Click **OK** to publish a new CRL with the enhanced CDP extension.

CREATE NEW AD FS TOKEN SIGNING CERTIFICATE

In **Console 1**, right-click on **Certificates (Local Computer)/Personal/Certificates** and select **All Tasks > Request New Certificate**. In the Certificate Enrollment Wizard, click **Next** twice, then click the blue link under **Web Server**. In **Certificate Properties** make the following changes:

- On the **Subject** tab, in the **Subject Name** area click on the **Type** dropdown list and select **Common name**. In the **Value** field type **Adatum Token Signing Cert2** and click **Add**.
- On the **General** tab, in the **Friendly name** text box type **adatum ts2** and click **OK**.

In the **Certificate Enrollment** window, check the box next to **Web Server** and then click the **Enroll** button, then click **Finish**. In **Console 1**, check for the new certificate with friendly name “adatum ts2” in **Certificates (Local Computer)/Personal/Certificates**.

REPLACE TOKEN-SIGNING CERTIFICATE IN AD FS

Click **Start > Administrative Tools > Active Directory Federation Services**. Right-click on **Federation Service** and select **Properties**. On the **General** tab in the **Token-signing certificate** section, click **Select**. Select the certificate listed as **adatum ts2** and click **OK**. Click **Yes** to complete the process.

Right-click on **Federation Service/Trust Policy** and select **Properties**. On the **Verification Certificates** tab, select the old **Adatum Token Signing Cert1** and click **Remove**, then **OK**.

MACHINE 4: ADATUM FS PROXY

CREATE NEW INSTANCE FROM *WEBSERVER* AMI

In the **EC2 Console**, click on the **AMIs** link in the left navigation area. Right-click on the **webserver** AMI shown and select **Launch Instance** to start the Request Instances Wizard. On the **Instance Details** page, leave the defaults selected. On the **Advanced Instance Details** page, accept the default settings. On the **Create Key Pair** page, leave the default to use **your existing key pair**. On the **Configure Firewall** page, select **Create a New Security Group**.

Name the new group **Adatum FS Proxy**, then click on the **Select** dropdown box and **Add** the following allowed connections:

Application	Transport	Port	Source Network/CIDR
RDP	TCP	3389	Lab management external IP/32[1]
HTTP	TCP	80	All Internet
HTTPS	TCP	443	All Internet

[1] This is the external IP address of the machine being used to access the Amazon EC2 images via Remote Desktop, recorded on Line 1 of the **Important Values Worksheet**.

Click **Continue**, then in the **Review** page click **Launch** to start the instance. Click **Close**. Click on **Instances** in the left navigation bar to see the status of your instance.

ASSOCIATE AN ELASTIC IP ADDRESS

In the **EC2 Console**, click on the **Elastic IPs** link in the left navigation area. Click the **Allocate New Address** button, then click on the **Yes, Allocate** button. Once allocated, right-click on the address and select Associate **Address**. Select the **Adatum FS Proxy** instance ID from the dropdown list and click **Associate**.

Record the Adatum FS Proxy elastic IP address on Line 10 of the **Important Values Worksheet**.

ADD CUSTOM FIREWALL PERMISSION

In the **EC2 Console**, click on **Security Groups** in the left navigation bar. Click on the **Adatum FS Proxy** security group to display its current settings. In the lower pane, **add** the following permission:

Method	Protocol	From Port	To Port	Source (IP or Group)
Custom	TCP	445	445	Internal Server external IP/32[1]

[1] This connection enables SMB over TCP, used to copy CRL files from Adatum Internal Server using the Administrator account. Use the Adatum Internal Server external IP address on Line 5 of the **Important Values Worksheet**.

MACHINE 1: ADATUM INTERNAL SERVER

MODIFY FIREWALL SETTINGS

> *We must allow the FS proxy to communicate with the federation server, and we can now close port 80.*

Click **Start > Administrative Tools > Windows Firewall with Advanced Security**. Click on **Inbound Rules** in the left navigation area. In the right-hand pan under **Actions**, click on **Filter by Group** and select **Filter by Secure World Wide Web Services (HTTPS)**. In the center pane, right-click on the **World Wide Web Services (HTTPS Traffic-In)** rule and select **Properties**. In the **Properties** dialog box, click on the **Scope** tab. In the **Remote IP address** section, click the radio button next to **These IP addresses:**, then click **Add**. In the **IP Address** window, in the **This IP address or subnet** field, type the elastic IP address of the Adatum FS Proxy from Line 10 of the **Important Values Worksheet** and click **OK**.

In the right-hand pane under **Actions**, click on **Filter by Group** and select **Filter by World Wide Web Services (HTTP)**. In the center pane, right click on the **World Wide Web Services (HTTP Traffic-In)** rule and select **Disable Rule**. This blocks all HTTP traffic into this machine.

MACHINE 4: ADATUM FS PROXY

ACCESS INSTANCE USING REMOTE DESKTOP CONNECTION

> *The EC2 Request Instances Wizard allows the creation of security groups with the most popular allowed connections. For custom permissions, we can use the Security Groups facility in the EC2 Console.*

Click **Start > All Programs > Accessories > Communication > Remote Desktop Connection**. In the **Computer** text box type the Public DNS name for the machine shown in the EC2 Console (for example, ec2-123-456-78-910.compute-1.amazonaws.com), then click **Connect**. In the login dialog box that appears, type **Administrator** for user name and the password you set for the Adatum Web Server (recorded on Line 9 of the **Important Values Worksheet**) and click **OK**.

CREATE CLIENT AUTHENTICATION CERTIFICATE

Open **Internet Explorer** and go to **https://fs1.corp.adatum.com/certsrv/**. At the login prompt, log in as administrator with the password from Line 2 of the **Important Values Worksheet** to reach the Active Directory Certificate Services home page.

Click the link to **Request a certificate**, then the link for **advanced certificate request** and finally the link to **Create and submit a request to this CA**. On the **Advanced Certificate Request** page, in the **Certificate Template** dropdown select **Adatum Proxy Client Auth**. In the **Identifying Information** section, in the **Name** field type **Adatum Proxy Client Auth**, and leave the other fields blank. In the **Additional Options** section, in the **Friendly Name** field type **proxy client auth** and click **Submit**. Click **Yes** to complete the request process; the certificate will be issued automatically.

Click the link to **Install this certificate** and click **Yes** on the warning dialog.

Leave the AD CS web application open for upcoming steps.

In **Console 1**, click on **Certificates (Current User)/Personal/Certificates**. In the right-hand pane should be the certificate for Adatum Proxy Client Auth.

MOVE CLIENT AUTHENTICATION CERTIFICATE TO LOCAL COMPUTER CERTIFICATE STORE

In **Console 1**, right-click on the **Adatum Proxy Client Auth** certificate and choose **All Tasks > Export** to launch the Certificate Export Wizard. On the **Export Private Key** page, select **Yes, export the private key**. On the **Export File Format** page, leave the default setting. After providing a password, On the **File to Export** page click **Browse**, click on **Desktop** and in the **File name** field type **adatum proxy client auth**. Click **Save** > **Next > Finish > OK** to complete the export process.

In **Console 1**, right-click on **Certificates (Local Computer)/Personal** and choose **All Tasks > Import** to launch the Certificate Import Wizard. On the **File to Import** page, click **Browse** and find **adatum proxy client auth.pfx** on the desktop. Click **Open**, then click **Next**. After typing the password, click **Next > Next > Finish > OK** to complete the import process.

CREATE SERVER AUTHENTICATION CERTIFICATE

Here you will request an SSL certificate with a name that exactly matches the internal corporate federation server. This is by design, and allows the proxy server to receive requests on behalf of the federation server.

Back in **Internet Explorer**, click on **Home** in the upper right corner of the Certificate Services web application. Click the link to **Request a certificate**, then the link for **advanced certificate request** and finally the link to **Create and submit a request to this CA**. On the **Advanced Certificate Request** page, in the **Certificate Template** dropdown select **Extranet Web Server**. In the **Identifying Information** section, in the **Name** field type **fs1.corp.adatum.com**, and leave the other fields blank. In the **Additional Options** section, in the **Friendly Name** field type **adatum proxy web ssl** and click **Submit**. Click **Yes** to complete the request process; the certificate will be issued automatically.

Click the link to **Install this certificate** and click **Yes** on the warning dialog. In **Console 1**, click on **Certificates (Current User)/Personal/Certificates**. In the right-hand pane should be the certificate for fs1.corp.adatum.com; right-click and select **Refresh** if necessary.

MOVE SERVER AUTHENTICATION CERTIFICATE TO LOCAL COMPUTER CERTIFICATE STORE

In **Console 1**, right-click on the **fs1.corp.adatum.com** certificate and choose **All Tasks > Export** to launch the Certificate Export Wizard. On the **Export Private Key** page, select **Yes, export the private key**. On the **Export File Format** page, leave the default setting. After providing a password, On the **File to Export** page click **Browse**, click on **Desktop** and in the **File name** field type **adatum proxy web ssl**. Click **Save** > **Next > Finish > OK** to complete the export process.

In **Console 1**, right-click on **Certificates (Local Computer)/Personal** and choose **All Tasks > Import** to launch the Certificate Import Wizard. On the **File to Import** page, click **Browse** and find **adatum proxy web ssl.pfx** on the desktop. Click **Open**, then click **Next**. After typing the password, click **Next > Next > Finish > OK** to complete the import process.

INSTALL AD FS FEDERATION SERVER PROXY

In **Server Manager**, right-click on **Roles** and select **Add Roles** to start the Add Roles Wizard. On the **Select Server Roles** page, check the box next to **Active Directory Federation Services**. On the **Select Role Services** page, check the box next to **Federation Service Proxy**. On the **Choose a Server Authentication Certificate** page, highlight the existing certificate issued to **fs1.corp.adatum.com** and click **Next**. On the **Specify Federation Server** page, type **fs1.corp.adatum.com** and click **Validate** to check accessibility, then click **Next**. On the **Choose a Client Authentication Certificate** page, highlight the existing certificate issued to **Adatum Proxy Client Auth** and click **Next**. Click **Install**. Click **Close** to complete the install.

CREATE ADATUM CRL WEB SITE

Click **Start > Administrative Tools > Internet Information Services (IIS) Manager**. Right-click on the **Sites** folder in the left navigation area and select **Add Web Site**. In the **Site name** field type **CRL**. In the **Content Directory** section, click on the button to the right of the **Physical path** field. Browse to **c:\inetpub\**, then click the **Make New Folder** button and name the new folder **CRL** and click **OK**.

In the **Binding** section, in the **Host name** field type **crl.adatum.com** and click **OK**.

ENABLE DOUBLE ESCAPING FOR CRL WEB SITE IN IIS

<u>This task pertains both to Windows Server 2008 and Windows Server 2008 R2</u>.

As in Scenario 1, IIS default request filtering behavior must be modified to allow Adatum's delta CRL files to be properly served to clients. In this case, we are creating the web site ourselves – so we must take this step in either Windows Server 2008 or Windows Server 2008 R2. The steps used to make the modification vary by operating system.

Windows Server 2008 (either local or running on EC2)

Click **Start > Run**. In the **Run** box type **cmd** and click **OK** to open a command prompt. Change the directory to **c:\windows\system32\inetsrv**.

At the command prompt, type the following and hit **Enter**:

```
appcmd set config “CRL” -
section:system.webServer/security/requestFiltering -
allowDoubleEscaping:true
```

> *In Windows Server 2008, this process adds a web.config file to the CRL physical folder (c:\inetpub\CRL). Take care to not accidentally delete this file, as CRL checking will fail without it.*

Windows Server 2008 R2 (local only – not available in EC2)

Click **Start > Administrative Tools > Internet Information Services (IIS) Manager**. In the left navigation area under **Sites**, click on the **CRL** web site. In the center pane of the console in the **IIS** section, double-click on **Request Filtering** in Features View. In the right-hand pane, click **Edit Feature Settings**. In the **General** section of the Edit Request Filtering Settings dialog box, check the box next to **Allow double escaping** and click **OK**.

SHARE ACCESS TO CRL WEB SITE FOLDER

In I**IS Manager**, right-click on the **CRL** web site under **Sites** and select **Edit Permissions**. In the **CRL Properties** window, on the **Sharing** tab click on the **Share** button. In the **File Sharing** window, click the **Share** button. In the **Network Discovery** prompt, select **No, do not turn on network discovery**. Click **Done**, then **Close**.

MACHINE 3: ADATUM WEB SERVER

CREATE NEW *CORP.ADATUM.COM* DNS ZONE

> *The Adatum federation server endpoint URL is https://fs1.corp.adatum.com/adfs/ls/. The web server gets this URL from the federation server’s trust policy at regular intervals, and redirects client browsers to this URL to acquire security tokens. Domain-joined clients, who have access to the corp.datum.com domain and DNS zone, have no trouble (a) resolving this address, or (b) accessing this server. External clients, however, would not be able to resolve this name or access this server, since they cannot access the internal Adatum domain.*

The server access solution is to employ the FS proxy to handle external client requests, and route requests through to the internal federation server. However, this does not fix the DNS resolution problem.

By creating a corp.adatum.com Internet DNS zone, external clients can resolve the federation server endpoint URL. The zone includes only one host entry, resolving the endpoint URL to the IP address of the FS proxy sitting outside the firewall. Domain-joined clients will continue to use the corporate corp.adatum.com DNS zone to access the federation server directly.

Click **Start > Administrative Tools > DNS**. In the left navigation area, right-click on the **Forward Lookup Zones** folder and select **New Zone** to start the New Zone Wizard. On the **Zone Type** page, leave the default setting of **Primary zone**. On the **Zone Name** page, type **corp.adatum.com** in the text box and click **Next**. Accept the defaults on the **Zone File** and **Dynamic Updates** pages. Click **Finish**.

Under **Forward Lookup Zones**, right-click on **corp.adatum.com** and select **New Host (A or AAAA).** In the **New Host Name** field type **fs1** and in the **IP address** field type the elastic IP address for the **Adatum FS Proxy** from Line 10 of the **Important Values Worksheet**. Click **Add Host > OK > Done.**

ADD DNS RECORD FOR CRL WEB SITE

Under **Forward Lookup Zones**, right-click on **adatum.com** and select **New Host (A or AAAA).** In the **New Host Name** field type **crl** and in the **IP address** field type the elastic IP address for the **Adatum FS Proxy** from Line 10 of the **Important Values Worksheet**. Click **Add Host > OK > Done.**

POINT DNS CLIENT TO LOCAL DNS SERVER

The web server will use DNS to resolve the IP address of crl.adatum.com. Note that the DNS entry for fs1.corp.adatum.com (which points to the FS proxy) will not be used by this machine. Instead the hosts file entry (which points to the actual federation server) will take precedence.

Click **Start > Control Panel > Network and Sharing Center > Manage Network Connections**. Right-click on **Local Area Connection** and select **Properties**. Double-click on the **Internet Protocol Version 4** list item to open TCP/IPv4 Properties. On the **General** tab, click the radio button to **Use the following DNS server addresses**. In the **Preferred DNS server** field, type **127.0.0.1**. Click **OK** twice.

MODIFY FIREWALL SETTINGS

In the **EC2 Console**, click on **Security Groups** in the left navigation area. Click on the **Adatum Web Server** security group to display its current settings. Click the **Remove** button next to the current **HTTPS** settings. Add the following:

Method	**Protocol**	**From Port**	**To Port**	**Source (IP or Group)**
HTTPS	TCP	443	443	0.0.0.0/0

MACHINE 1: ADATUM INTERNAL SERVER

ADD FS PROXY CLIENT AUTHENTICATION CERTIFICATE TO FEDERATION SERVER POLICY

> *The federation server needs to register the public key for the client authentication certificate being used by the FS proxy, in order to verify the signature on proxy communications.*

Open **Console 1** on the desktop. Click on **Certification Authority/Adatum Certificate Server/Issued Certificates.** In the center pane, double-click on the issued certificate that used the **Adatum Proxy Client Auth** certificate template to open it. On the **Details** tab, click on the **Copy to file** button to start the Certificate Export Wizard. On the **Export File Format** page, leave the default setting. On the **File to Export** page, click **Browse**, click **Desktop** and in the **File name** field type **adatum proxy client auth public**. Click **Save > Next > Finish > OK > OK** to save **adatum proxy client auth public.cer** to the desktop

Click **Start > Administrative Tools > Active Directory Federation Services**. Right-click on **Trust Policy** under **Federation Service** and select **Properties**. On the **FSP Certificates** tab, click **Add** and select the **adatum proxy client auth public.cer** file from the desktop. Click **Open** and **OK**.

CREATE SCHEDULED TASK FOR AUTOMATIC CRL FILE SYNCHRONIZATION

In **Console 1**, right-click on **Certification Authority/Adatum Certificate Server** and select **Properties**. On the **Auditing** tab, in the **Events to audit** list, check the box next to **Revoke certificates and publish CRLs** and click **OK**.

Click **Start > Administrative Tools > Task Scheduler.** On the **Actions** menu click **Create task**. On the **General** tab, in the **Name** field type **publishcrl**. In the **Security Options** section, select **Run whether user is logged on or not**.

On the **Triggers** tab, click **New**. In the **New Trigger** dialog box, in the **Begin the task** dropdown list select **On an event.** In the **Settings** area, in the **Log** dropdown list select **Security.** In the **Source** dropdown list select **Microsoft Windows security auditing.** In the **Event ID** field type **4872** and click **OK.**

On the **Actions** tab, click **New**. In the **New Action** dialog box, in the **Action** dropdown list leave **Start a program**. In the **Program/script** text box type **robocopy**. In the **Add arguments** text box type the following:

```
c:\windows\system32\certsrv\certenroll \\fs.proxy.elastic.IP\crl
```

> *For fs.proxy.elastic.IP, use the elastic IP address for the **Adatum FS Proxy** from Line 10 of the **Important Values Worksheet**.*

Click **OK twice,** then type your domain administrator password and click **OK** to complete the task scheduling process.

In **Console 1,** right-click on **Certification Authority/Adatum Certificate Server/Revoked Certificates** and select **All Tasks > Publish**. Click **OK** to publish a new CRL. Check for success of the scheduled task by viewing the folder on the FS proxy for the CRL application (c:\Inetpub\CRL\), looking for the files such as *Adatum Certificate Server.crl* and *Adatum Certificate Server+.crl*.

MACHINE 5: EXTERNAL CLIENT

CHANGE PREFERRED DNS SERVER

Click **Start > Control Panel > Network and Sharing Center > Manage Network Connections**. Right-click on an adapter with Internet connectivity and select **Properties**. Double-click on **Internet Protocol Version 4 (TCP/IPv4)** to open TCP/IPv4 properties. On the **General** tab, click the radio button to **Use the following DNS server addresses**. In the **Preferred DNS server** field type the elastic IP address for the **Adatum Web Server** from Line 8 of the **Important Values Worksheet**. Click **OK** twice.

TEST

To test the scenario, open **Internet Explorer** on the External Client computer, type **https://adfsv1app.adatum.com** into the Address Bar and hit **Enter**. Note that instead of silent authentication, we are presented with forms-based authentication asking for our domain credentials. Log in as alansh, using the password from Line 4 of the **Important Values Worksheet.** This allows the federation server and federation server proxy to create the required security token.

Since we did not add the Adatum root CA certificate to this computer's certificate store, you must click on "Continue to this website" on each of the certificate-related security alerts that appear in the browser. Using server authentication certificates rooted at a 3rd party distributed in Windows operating systems would eliminate these errors.

If you are running into errors, it's possible that you are having certificate verification issues. Please see Appendix B for more information.

SCENARIO 3: SERVICE PROVIDER APPLICATION

In the next two scenarios, Alan Shen will access an EC2-based federated claims-aware application owned and operated by a partner organization called Trey Research. Trey Research will use AD FS to provide access to Adatum employees leveraging their existing Adatum domain credentials.

In Scenario 3, Alan Shen will access the Trey Research federated application from both a domain-joined client (contacting the Adatum federation server directly) and an external client (through the Adatum FS proxy). Trey Research will operate an AD FS federation server in EC2, giving it the ability to receive and interpret security tokens and grant access to multiple partners like Adatum simultaneously.

The scenario adds two additional computers to the lab.

6) Trey Research Federation Server

   This EC2-based machine will consume incoming security tokens from Adatum users, and generate outgoing security tokens for the Trey Research federated application's web server. Specifically, this machine will run:

   a) Active Directory Domain Services (domain controller)
   b) Domain Name Services (Active Directory-integrated DNS server)
   c) Active Directory Certificate Services (root CA)
   d) Internet Information Services (web server)
   e) Microsoft ASP.NET 2.0
   f) Microsoft .NET Framework 2.0
   g) Active Directory Federation Services (Trey Research resource partner)

   The AD FS v1 federation server is available in Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2 (Enterprise Edition or above). Amazon EC2 currently offers Windows Server 2003 R2 and Windows Server 2008 (Datacenter Edition) as guest operating systems. This lab used Windows Server 2008.

7) Trey Research Web Server

   This EC2-based machine will host the AD FS web agent and the Trey Research federated web application. Specifically, this machine will run:

   a) Internet Information Services (web server)
   b) Microsoft ASP.NET 2.0
   c) Microsoft .NET Framework 2.0
   d) AD FS v1 claims-aware web agent
   e) Sample application

The ADFS v1 web agent is available in Windows Server 2003 R2, Windows Server 2008 and Windows Server 2008 R2 (Standard Edition or above). Amazon EC2 currently offers Windows Server 2003 R2 and Windows Server 2008 (Datacenter Edition) as guest operating systems. This lab used Windows Server 2008.

CONFIGURATION

MACHINE 1: ADATUM INTERNAL SERVER

EXPORT ADATUM AD FS POLICY FILE

Click **Start > Administrative Tools > Active Directory Federation Services**. Right-click on **Federation Service/Trust Policy** in the left navigation area and select **Export Basic Partner Policy**. Click **Browse**, save the file to the desktop with the name **adatumpolicy.xml** and click **OK**. Load the file to a web-based storage solution like http://skydrive.live.com.

MACHINE 6: TREY RESEARCH FEDERATION SERVER

CREATE WINDOWS SERVER INSTANCE IN EC2

In the **EC2 Console**, click on **Instances** in the left navigation area. Click on the **Launch Instances** button to launch the Request Instances Wizard. Click on the **Community AMIs** tab, and in the adjacent text box type **amazon/Windows-Server2008.** Find the entry for **amazon/Windows-Server2008-i386-Base-<version#>** and click the **Select** button to its right. On the **Instance Details** page, leave the defaults selected. On the **Advanced Instance Details** page, accept the default settings. On the **Create Key Pair** page, leave the default to use **your existing key pair**. On the **Configure Firewall** page, select **Create a New Security Group**. Name the new group **Trey Federation Server**, then click on the **Select** dropdown box and **Add** the following allowed connections:

Application	**Transport**	**Port**	**Source Network/CIDR**
RDP	TCP	3389	Lab management external IP/32[1]
HTTPS	TCP	443	All Internet

[2] This is the external IP address of the machine being used to access the Amazon EC2 images via Remote Desktop, recorded on Line 1 of the **Important Values Worksheet**.

Click **Continue**, then in the **Review** page click **Launch** to start the instance. Click **Close**. Click on **Instances** in the left navigation bar to see the status of your instance.

ASSOCIATE AN ELASTIC IP ADDRESS

In the **EC2 Console**, click on the **Elastic IPs** link in the left navigation area. Click the **Allocate New Address** button, then click on the **Yes, Allocate** button. Once allocated, right-click on the address and select Associate **Address**. Select the **Trey Federation Server** instance ID from the dropdown list and click **Associate**.

Record the Trey Research Federation Server elastic IP address on Line 11 of the **Important Values Worksheet**.

GET WINDOWS ADMINISTRATOR PASSWORD

In the **EC2 Console**, click on **Instances** in the left navigation area. Once the Status shows as "running" and your Elastic IP address is listed in the Public DNS column, right-click on the **Trey Federation Server** instance and select **Get Windows Password**. On your desktop, **open** the **ADFDSkey.PEM** file with Notepad and **copy** the entire contents of the file (including the Begin and End lines, Eg: "-----BEGIN RSA PRIVATE KEY-----"). In the **EC2 Console**, **paste** the text into the **Retrieve Default Windows Administrator Password** window. Click **inside the text box once** to enable the **Decrypt Password** button, then click **Decrypt Password**. Copy the **Computer, User and Decrypted Password** information into a text file, and save to your desktop. Click **Close** in the **Retrieve Password** window.

ACCESS INSTANCE USING REMOTE DESKTOP CONNECTION

Click **Start > All Programs > Accessories > Communication > Remote Desktop Connection**. In the **Computer** text box copy/paste or type the **Computer Name** from your text file (for example, ec2-123-456-78-910.compute-1.amazonaws.com), then click **Connect**.

In the login dialog box that appears, type **Administrator** for user name and the **Decrypted Password** from your text file into the Password field, taking care to get capitalization correct, and click **OK**.

In the **Set Network Location** window, click on **Public Location**, then **Close**.

Optional

Once inside the instance, change the Administrator password by clicking **CTRL-ALT-END** and clicking the **Change a password** link.

Record the Trey Research Federation Server administrator password on Line 12 of the **Important Values Worksheet**.

Optional

Turn off the Internet Explorer Enhanced Security Configuration for administrators. In **Server Manager**, on the **Server Summary** page under **Security Information**, click on **Configure IE ESC**. Under **Administrators**, click the **Off** radio button and click **OK**.

INITIAL CONFIGURATION

Click **Start >All Programs > Ec2ConfigService Settings**. On the **General** tab, uncheck the box next to **Set Computer Name** and click **OK**.

In **Server Manager**, on the **Server Summary** page under **Computer Information**, click on **Change System Properties**. On the **Computer Name** tab, click the **Change** button. In the **Computer Name** field type **fs1** then click **OK**. Click **OK** twice, then click **Close**, then click **Restart Now**.

Using Remote Desktop, log back into the machine with the Administrator account and password from Line 12 of the **Important Values Worksheet**.

ADJUST CLOCK SETTINGS

Right-click on the **Windows Taskbar** and select **Properties**. On the **Notification Area** tab, check the box to show the **Clock** and click **OK**. Right-click over the clock in the taskbar and select **Adjust Date/Time**. On the **Date and Time** tab, click the **Change time zone** button and adjust to your time zone. Click **OK** twice.

INSTALL/CONFIGURE ACTIVE DIRECTORY DOMAIN SERVICES (AD DS)

> *Although this federation server will not be authenticating users, AD FS v1 federation server computers must be members of a domain. Therefore, this machine will run Active Directory Domain Services, even though the directory will contain no users, and the domain will have no other member machines.*

In **Server Manager**, right-click on **Roles** and select **Add Roles** to start the Add Roles Wizard. On the **Select Server Roles** page, check the box next to **Active Directory Domain Services**. Click **Next** twice, then **Install**. On the **Installation Results** page, click on the link for the **Active Directory Domain Services Installation Wizard (dcpromo.exe).**

On the **Choose a Deployment Configuration** page, select **Create a new domain in a new forest**. On the **Name the Forest Root Domain** page, type **treyresearch.net**. On the **Set Forest Functional Level** and **Set Domain Functional Level** pages, leave the default setting of **Windows 2000**. On the **Additional Domain Controller Options** page, leave **DNS Server** checked. On the warning about static IP addresses, click **Yes, the computer will use a dynamically assigned IP address**. When prompted about not finding an authoritative DNS zone, click **Yes** to continue. Complete the wizard, keeping all other default values. When prompted, **restart computer**.

Using Remote Desktop, log back into the machine with the **TREYRESEARCH\administrator** account and the password from Line 12 of the **Important Values Worksheet**.

ADD DNS FORWARDER FROM TREY RESEARCH DOMAIN DNS TO INTERNET DNS

> *This is required so that the federation server can resolve the Adatum CRL location DNS name.*

Click **Start > Administrative Tools > DNS**. Click on **FS1** in the left navigation area, then right-click on **Forwarders** in the right-hand pane and select **Properties**. On the **Forwarders** tab, click **Edit.** In the **Click here to add an IP address or DNS name** field, type the Adatum Web Server elastic IP address from Line 8 of the **Important Values Worksheet** and hit **Enter**. Highlight any other forwarders previously listed and click **Down** to make your new forwarder is the first one listed. Click **OK** twice.

INSTALL/CONFIGURE ACTIVE DIRECTORY CERTIFICATE SERVICES (AD CS)

In **Server Manager**, right-click on **Roles** and select **Add Roles** to start the Add Roles Wizard. On the **Select Server Roles** page, check the box next to **Active Directory Certificate Services**. On the **Select Role Services** page, select **Certification Authority** and **Certification Authority Web Enrollment**. Click the **Add Required Features** button to allow Server Manager to add IIS to the installation process. On the **Specify Setup Type** page select **Enterprise** and on the **Specify CA Type** page select **Root CA**. On the **Setup Private Key** page, select **Create a new private key** and accept the default cryptography settings. On the **Configure CA Name** page, in the **Common Name for this CA** field type **Trey Certificate Server**. Complete the wizard, keeping all other default values. Click **Close** to finish the install.

Click **Start > Run**. In the **Run** box type **mmc** and click **OK** to start the Microsoft Management Console. In the **File** menu select **Add/Remove Snap-in**. Highlight the **Certificates** snap-in and click the **Add** button; choose **computer account** and **local computer** in the following pages. Highlight the **Certificate Templates** snap-in and click **Add**. Highlight the **Certification Authority** snap-in and click **Add**; choose **local computer** in the following page and click **OK**. Click **File > Save**, and save the new MMC console (Console 1) to the machine desktop for future use.

ENABLE DOUBLE ESCAPING FOR CRL WEB SITE IN IIS

Click **Start > Run**. In the **Run** box type **cmd** and click **OK** to open a command prompt. Change the directory to **c:\windows\system32\inetsrv**. At the command prompt, type the following and hit **Enter**:

```
appcmd set config “Default Web Site/CertEnroll” -
section:system.webServer/security/requestFiltering -
allowDoubleEscaping:true
```

CONFIGURE AD CS CERTIFICATE TEMPLATES

In **Console 1**, click on **Certificate Templates** in the left navigation area. In the center pane, right-click on the **Web Server** certificate template and select **Duplicate Template**.

In the **Duplicate Template** dialog, leave **Windows Server 2003 Enterprise** as the minimum CA for the new template and click **OK**. In **Properties of New Template**, make the following changes:

- On the **General** tab, in the **Template display name** field type **Extranet Web Server**
- On the **Request Handling** tab, check the box next to **Allow private key to be exported**

Click **OK** to create the new template.

In the center pane, right-click on the **Web Server** certificate template and choose **Properties**. In the **Security** tab, click **Add**, and in the object names text box type **Domain Controllers** and click **Check Names**. Once verified, click **OK**. Back in the **Security** tab, highlight the **Domain Controllers** list item, then in the **Allow** column check the **Read** and **Enroll** permissions and click **OK**. Click **Start > Administrative Tools > Services**. Right-click on **Active Directory Certificate Services** and select **Restart**.

In **Console 1**, in the left navigation area, right-click on **Certificate Authority\Trey Certificate Server\Certificate Templates** and select **New > Certificate Template to Issue**. Highlight **Extranet Web Server** from the list and click **OK**.

CREATE SERVER AUTHENTICATION CERTIFICATE

In **Console 1**, right-click on **Certificates (Local Computer)/Personal/Certificates** and select **All Tasks > Request New Certificate**. In the Certificate Enrollment Wizard, click **Next**, then click the blue link under **Web Server**. In **Certificate Properties**, make the following changes:

- On the **Subject** tab, in the **Subject Name** area click on the **Type** dropdown list and select **Common name**. In the **Value** field type **fs1.treyresearch.net** and click **Add**.
- On the **General** tab, in the **Friendly name** text box type **trey fs ssl** and click **OK**.

In the **Certificate Enrollment** window, check the box next to **Web Server** and then click the **Enroll** button, then click **Finish**. In **Console** 1, check for the new certificate with friendly name “trey fs ssl” in **Certificates (Local Computer)/Personal/Certificates**.

CREATE AD FS TOKEN SIGNING CERTIFICATE

In **Console 1**, right-click on **Certificates (Local Computer)/Personal/Certificates** and select **All Tasks > Request New Certificate.** In the Certificate Enrollment Wizard, click **Next**, then click the blue link under **Web Server**. In **Certificate Properties**, make the following changes:

- On the **Subject** tab, in the **Subject Name** area click on the **Type** dropdown list and select **Common name**. In the **Value** field type **Trey Token Signing Cert1** and click **Add**.
- On the **General** tab, in the **Friendly name** text box type **trey ts1** and click **OK**.

In the **Certificate Enrollment** window, check the box next to **Web Server** and then click the **Enroll** button, then click **Finish**. In **Console 1**, check for the new certificate with friendly name “trey ts1” in **Certificates (Local Computer)/Personal/Certificates**.

ADD ADATUM ROOT CA CERTIFICATE

> *The Trey Research federation server needs the root CA certificate for Adatum in order to perform token-signing certificate CRL verification.*

Open **Internet Explorer** and in the address bar type **http://crl.adatum.com/fs1.corp.adatum.com_Adatum%20Certificate%20Server.crt**. In the **File Download – Security Warning** box click **Save**, and save the file to the desktop. Click **Close**.

In **Console 1**, right-click on **Certificates (Local Computer)/Trusted Root Certification Authorities/Certificates** and select **All Tasks > Import** to launch the Certificate Import Wizard. On the **File to Import** page, click **Browse**, find the Adatum root CA certificate file on the desktop, and click **Open**. Click **Next > Next > Finish > OK** to complete the import process.

INSTALL ACTIVE DIRECTORY FEDERATION SERVICES (AD FS)

In **Server Manager**, right-click on **Roles** and select **Add Roles** to start the Add Roles Wizard. On the **Select Server Roles** page, check the box next to **Active Directory Federation Services**. On the **Select Role Services** page, check the box next to **Federation Service**. Click the **Add Required Role Services** button to allow Server Manager to add IIS features to the installation process, and then click **Next**. On the **Choose a Server Authentication Certificate** page, highlight the existing certificate issued to **fs1.treyresearch.net** with the intended purpose **Server Authentication** and click **Next**. On the **Choose a Token Signing Certificate** page, highlight the existing certificate issued to **Trey Token Signing Cert1** and click **Next**. Accept all other defaults and click **Install**.

INITIAL AD FS CONFIGURATION

Click **Start > Administrative Tools > Active Directory Federation Services**. Right-click on **Account Stores** under **Federation Service/Trust Policy/My Organization** and select **New > Account Store**. In the Add Account Store Wizard, leave **AD DS** as the store type and click through to add the local AD domain.

Right-click on **My Organization/Organization Claims** and select **New > Organization claim**. In the **Claim name field** type **GoldUsers** and click **OK**.

EXPORT TREY RESEARCH AD FS POLICY FILE

Click **Start > Administrative Tools > Active Directory Federation Services**. Right-click on **Federation Service/Trust Policy** in the left navigation area and select **Export Basic Partner Policy**. Click **Browse**, save the file to the desktop with the name **adatumpolicy.xml** and click **OK**. Load the file to a web-based storage solution like http://skydrive.live.com.

MACHINE 7: TREY RESEARCH WEB SERVER

CREATE NEW INSTANCE FROM *WEBSERVER2* AMI

One could use the existing Adatum Web Server to host the Trey Research federated application. However, since each application requires SSL server authentication certificates with different DNS suffixes (adatum.com, treyresearch.net) and EC2 does not offer multiple IP addresses per single machine instance, using the same server would require either:

- *using a multi-domain certificate (which AD CS does not issue), or*
- *using a port other than 443 for SSL communication with one of the applications (which can cause trouble when clients are limited to 443 only for HTTPS)*

Therefore, this lab uses dedicated web servers for each organization and port 443 exclusively.

In the **EC2 Console**, click on the **AMIs** link in the left navigation area. Right-click on the **webserver2** AMI shown and select **Launch Instance** to start the Request Instances Wizard. On the **Instance Details** page, leave the defaults selected. On the **Advanced Instance Details** page, accept the default settings. On the **Create Key Pair** page, leave the default to use **your existing key pair**. On the **Configure Firewall** page, select **Create a New Security Group**. Name the new group **Trey Web Server**, then click on the **Select** dropdown box and **Add** the following allowed connections:

Application	Transport	Port	Source Network/CIDR
RDP	TCP	3389	Lab management external IP/32[1]
HTTPS	TCP	443	All Internet

[1] This is the external IP address of the machine being used to access the Amazon EC2 images via Remote Desktop, recorded on Line 1 of the **Important Values Worksheet**.

Click **Continue**, then in the **Review** page click **Launch** to start the instance. Click **Close**. Click on **Instances** in the left navigation bar to see the status of your instance.

ASSOCIATE AN ELASTIC IP ADDRESS

In the **EC2 Console**, click on the **Elastic IPs** link in the left navigation area. Click the **Allocate New Address** button, then click on the **Yes, Allocate** button. Once allocated, right-click on the address and select Associate **Address**. Select the **Trey Web Server** instance ID from the dropdown list and click **Associate**.

Record the Trey Research Web Server elastic IP address on Line 13 of the **Important Values Worksheet**.

ACCESS INSTANCE USING REMOTE DESKTOP CONNECTION

Click **Start > All Programs > Accessories > Communication > Remote Desktop Connection**. In the **Computer** text box type the Public DNS name for the machine shown in the EC2 Console (for example, ec2-123-456-78-910.compute-1.amazonaws.com), then click **Connect**. In the login dialog box that appears, type **Administrator** for user name and the password you set for the Adatum Web Server (recorded on Line 9 of the **Important Values Worksheet**) and click **OK**.

ADD RECORD FOR TREY FEDERATION SERVER TO HOSTS FILE

Double-click the shortcut on the desktop for the **hosts** file; select **Notepad** as the program and click **OK**. Add the name and external IP address of the Trey Federation Server from Line 11 of the **Important Values Worksheet**, as shown in the following example:

123.456.78.910   fs1.treyresearch.net

Save and **close** the file.

INSTALL TREY RESEARCH ROOT CA CERTIFICATE

Open **Internet Explorer** and go to **https:// fs1.treyresearch.net/certsrv /.** In the **Certificate Error** page, click the link to **Continue to this website**. At the login prompt, log in as administrator with the password from Line 12 of the **Important Values Worksheet** to reach the Active Directory Certificate Services home page. At the bottom of the page, click the link to **Download a CA certificate, certificate chain, or CRL**. On the next page, click the link to **Download CA certificate**. **Save** the resulting **certnew.cer** file to the desktop; click **Yes** to overwrite the previous one there.

Leave the AD CS web application open for use in upcoming steps.

In **Console 1**, right-click **on Certificates (Local Computer)/Trusted Root Certification Authorities/Certificates** and select **All Tasks > Import** to launch the Certificate Import Wizard. On the **File to Import** page, click **Browse**, find the **certnew.cer** file on the desktop, and click **Open**. Click **Next** twice, then **Finish**, then **OK** to complete the import process.

CREATE SERVER AUTHENTICATION CERTIFICATE

Back in **Internet Explorer**, click on **Home** in the upper right corner of the Certificate Services web application. Click the link to **Request a certificate**, then the link for **advanced certificate request** and finally the link to **Create and submit a request to this CA**. If prompted about the page requiring HTTPS click **OK**. If prompted to run the **Certificate Enrollment Control** add-on click **Run**.

On the **Advanced Certificate Request** page, in the **Certificate Template** dropdown select **Extranet Web Server**. In the **Identifying Information** section, in the **Name** field type **adfsv1app.treyresearch.net**, and leave the other fields blank. In the **Additional Options** section, in the **Friendly Name** field type **trey web ssl** and click **Submit**. Click **Yes** to complete the request process; the certificate will be issued automatically.

Click the link to **Install this certificate** and click **Yes** on the warning dialog. In **Console 1**, click on **Certificates (Current User)/Personal/Certificates**. In the right-hand pane should be the certificate for adfsv1app.treyresearch.net.

MOVE SERVER AUTHENTICATION CERTIFICATE TO LOCAL COMPUTER CERTIFICATE STORE

In **Console 1**, right-click on the **adfsv1app.adatum.com** certificate and choose **All Tasks > Export** to launch the Certificate Export Wizard. On the **Export Private Key** page, select **Yes, export the private key**. On the **Export File Format** page, leave the default setting. After providing a password, On the **File to Export** page click **Browse**, click on **Desktop** and in the **File name** field type **trey web ssl**. Click **Save** > **Next > Finish > OK** to complete the export process.

In **Console 1**, right-click on **Certificates (Local Computer)/Personal** and choose **All Tasks > Import** to launch the Certificate Import Wizard. On the **File to Import** page, click **Browse** and find **trey web ssl.pfx** on the desktop. Click **Open**, then click **Next**. After typing the password, click **Next > Next > Finish > OK** to complete the import process.

EDIT SAMPLE APPLICATION

> *The sample application (which is already on this machine, from the original machine image) needs to be changed from belonging to Adatum to Trey Research.*

Click **Start > Administrative Tools > Internet Information Services (IIS) Manager**. In the **Sites** folder, right-click on **ADFSv1 app** and choose **Edit Bindings**. Highlight the **HTTPS** entry and then click the **Edit** button. In the **SSL Certificate** dropdown box, select **trey web ssl** and click **OK**, then click **Close**. In the application properties window, make the following changes:

Right-click on the **ADFSv1 app** web site and select **Explore**. Right-click on **default.aspx** (not default.aspx.cs) and select **Edit**. On the **Edit** menu, select **Replace**. Type **Adatum** in the **Find what** field, **Trey Research** in the **Replace with** field, and click **Replace All**. Close the Replace tool. Save and close default.aspx.

Right-click on **web.config** and select **Edit**. In the **<websso>** section, replace the current **<returnurl>** entry with **<returnurl>https://adfsv1app.treyresearch.net/</returnurl>.** Replace the current **<fs>** entry with **<fs>https://fs1.treyresearch.net/adfs/fs/federationserverservice.asmx</fs>.** Save and close web.config.

MACHINE 3: ADATUM WEB SERVER

ADD *TREYRESEARCH.NET* ZONE AND RECORDS TO INTERNET DNS

Click **Start > Administrative Tools > DNS**. In the left navigation area, right-click on the **Forward Lookup Zones** folder and select **New Zone** to start the New Zone Wizard. On the **Zone Type** page, leave the default setting of **Primary zone**. On the **Zone Name** page, type **treyresearch.net** in the text box and click **Next**. Accept the defaults on the **Zone File** and **Dynamic Updates** pages. Click **Finish**.

Under **Forward Lookup Zones**, right-click on **treyresearch.net** and select **New Host (A or AAAA).** In the **New Host Name** field type **fs1** and in the **IP address** field type the elastic IP address for the **Trey Research Federation Server** from Line 11 of the **Important Values Worksheet**. Click **Add Host > OK.** In the **New Host Name** field type **adfsv1app** and in the **IP address** field type the elastic IP address for the Trey Research Web Server from Line 13 of the **Important Values Worksheet**. Click **Add Host > OK > Done.**

MACHINE 1: ADATUM INTERNAL SERVER

ADD TREY RESEARCH AS A RESOURCE PARTNER

Download the **treypolicy.xml** file you created on the Trey Research Federation Server earlier from your preferred Internet-based storage solution. Save to your desktop.

Click **Start > Administrative Tools > Active Directory Federation Services**. Right-click on **Federation Service/Trust Policy/Partner Organizations/Resource Partners** and select **New > Resource Partner** to start the Add Resource Partner Wizard. On the **Import Policy File** page, click **Yes** then **Browse** to **treypolicy.xml** and click **Open**, then click **Next**. On the **Resource Partner Details** page, change the Display name to **Trey Research** and click **Next**. In the **Federation Scenario** page, leave **Federated Web SSO** selected. In the **Account Partner Identity Claims** page, leave the **UPN** and **E-mail** claims selected. In the **Select UPN Suffix** page, leave the default **pass through all UPN suffixes unchanged** selected. In the **Select E-mail Suffix** page, leave the default **pass through all E-mail suffixes unchanged** selected. Click **Next > Finish** to complete the wizard.

Right-click on **Partner Organizations/Resource Partners/Trey Research** and select **New > Outgoing Group Claim Mapping**. Leave **PriorityUsers** as the **Organization Group Claim**. In the **Outgoing group claim name** field type **CliamInTransit** and click **OK**.

ADD TREY RESEARCH ROOT CA CERTIFICATE TO END USER DESKTOPS WITH GROUP POLICY

> *To avoid SSL certificate warnings, client desktops need to trust the SSL certificates used by Trey Research at the application and federation server.*

Open **Internet Explorer** and in the address bar type **https://fs1.treyresearch.net/certenroll/fs1.treyresearch.net_Trey%20Certificate%20Server.crt**. In the **Certificate Error** page, click the link to **Continue to this website**. In the **File Download – Security Warning** box click **Save**, and save the file to the desktop. Click **Close**.

Click **Start > Administrative Tools > Group Policy Management**. Right-click on **Forest:corp.adatum.com/Domains/corp.adatum.com/Default Domain Policy** and select **Edit**. Under **Computer Configuration/Policies/Windows Settings/Security Settings/Public Key Policies**, right-click on **Trusted Root Certification Authorities** and choose **Import** to start the Certificate Import Wizard. On the **File to Import** page, click **Browse** and select the Trey root CA certificate you just downloaded from the desktop and click **Open**. Click **Next > Next > Finish > OK** to complete the import process.

> *In this lab, domain-wide Group Policy updating results in the Adatum Internal Server also getting the Trey root CA installed. However, this isn't a requirement - only clients require the Trey root CA to avoid certificate warnings.*

MACHINE 6: TREY RESEARCH FEDERATION SERVER

ADD SAMPLE APPLICATION TO AD FS

Click **Start > Administrative Tools > Active Directory Federation Services**. Right-click on **Applications** under **Federation Service/Trust Policy/My Organization** and select **New > Application**. Enter the following in the Add Application Wizard:

- On the **Application Type** page, leave **Claims-aware application** as the application type.
- On the **Application Details** page, in the **Application display name** field type **ADFSv1 app** and in the **Application URL** field type **https://adfsv1app.treyresearch.net/**
- On the **Accepted Identity Claims** page, check the box next to **User principal name (UPN)** and **E-mail**
- Click **Next** twice and then **Finish**.

Click on **ADFSv1 app** under **Applications**. In the right-hand window, right-click on the **GoldUsers** group claim and select **Enable**.

ADD ADATUM AS AN ACCOUNT PARTNER

Download the **adatumpolicy.xml** file you created on the Adatum Internal Server earlier from your preferred Internet-based storage solution. Save to your desktop.

Right-click on **Federation Service/Trust Policy/Partner Organizations/Account Partners** and select **New > Account Partner** to start the Add Account Partner Wizard. On the **Import Policy File** page, click **Yes** then **Browse** to **adatumpolicy.xml** and click **Open**, then click **Next**. On the **Resource Partner Details** page, leave the default settings. On the **Account Partner Verification Certificate** page, leave **Use the verification certificate in the import policy file** selected. On the **Federation Scenario** page, leave **Federated Web SSO** selected. In the Account Partner Identity Claims page, leave **UPN** and **E-mail** claims selected. In the **Accepted UPN Suffixes** page, in the **Add a new suffix** field type **corp.adatum.com** and click Add, then Next. In the **Accepted E-mail Suffixes** page, in the **Add a new suffix** field type **adatum.com** and click **Add**, then **Next > Next > Finish** to complete the wizard.

Under **Partner Organizations/Account Partners**, right-click on **Adatum** and choose **New > Incoming Group Claim Mapping**. In the **Incoming group claim name** field type **ClaimInTransit**. Leave **GoldUsers** as the **Organization Group Claim** and click **OK**.

MODIFY FIREWALL SETTINGS

> *The Trey Research web server needs to read CRL information from the Trey Research CA, which is running on this machine. Since CRLs cannot be accessed via HTTPS, Port 80 must be opened (but can be scoped to only this web server).*

In the Amazon **EC2 Console**, click on **Security Groups** in the left navigation bar. Click on the **Trey Federation Server** row to display its current settings. In the lower pane, add the following firewall permission and click Save:

Connection Method	Protocol	From Port	To Port	Source (IP or Group)
HTTP	TCP	80	80	Trey web server external IP/32[1]

[1] This is the elastic IP address for the **Trey Research Web Server** from Line 13 of the **Important Values Worksheet**.

MACHINE 2: DOMAIN-JOINED CLIENT

UPDATE GROUP POLICY SETTINGS

Click **Start**. In the **search** field type **cmd** and hit **Enter** to open a command prompt. At the prompt type **gpupdate /force** to ensure the Trey Research root CA certificate is installed on the client machine.

TEST

Before testing on either the domain-joined or external client, you should clear browser cookies, to reinitiate the complete federation process. In **Internet Explorer** click **Tools > Internet Options**. On the **General** tab under **Browsing history**, click the **Delete** button. Make sure the box next to **Cookies** is checked and click **Delete**.

To test the scenario, open **Internet Explorer** in the domain-joined client, type **https://adfsv1app.treyresearch.net/** in the address bar and hit **Enter**. Note that the Trey Research federation server provides a home realm discovery service to redirect users without security tokens to the proper identity provider. In the dropdown, choose **Adatum**, since Alan Shen in an Adatum user.

Silent Integrated Windows Authentication ensures that the user is not asked for credentials when domain joined. When the application is shown, scroll to the bottom of the page. Note that the group claim “PriorityUsers” was transformed to “GoldUsers” by the federation servers. Claim transformation allows for increased flexibility when sending claims to partner organizations.

To further test the scenario, open **Internet Explorer** on the External Client computer and type **https://adfsv1app.treyresearch.net/** into the Address Bar and hit **Enter**. Note that instead of silent authentication, we are presented with forms-based authentication asking for our domain credentials. Login as alansh using the password from Line 4 of the **Important Values Worksheet.**

If you are running into errors, it’s possible that you are having certificate verification issues. Please see Appendix B for more information.

SCENARIO 4: SERVICE PROVIDER APPLICATION WITH ADDED SECURITY

This scenario is essentially the same as Scenario 3, with the difference being the addition of an AD FS proxy to the Trey Research AD FS deployment in Amazon EC2. By using the AD FS proxy, Trey Research can limit direct access to its federation server to only its web servers and the proxy server, instead of allowing all inbound clients to access the federation server. Since the federation server issues security tokens used by the web servers, it is a high-value resource that should be protected.

This scenario does not require any additional machines. While earlier we used a separate machine for the Adatum FS proxy, the proxy can be installed on the same machine as our Trey Research Web Server, as long as the Default Web Site in IIS is available (which it is). However, to enable hosting of multiple SSL web sites on the same web server, we will use a wildcard certificate and custom IIS configuration; this is discussed in detail below.

CONFIGURATION

MACHINE 6: TREY RESEARCH FEDERATION SERVER

CREATE FS PROXY CLIENT AUTH CERTIFICATE TEMPLATE

In **Console 1**, click on **Certificate Templates**. In the center pane, right-click on the **Computer** certificate template and choose **Duplicate Template**. In the **Duplicate Template** dialog, leave **Windows Server 2003 Enterprise** as the minimum CA for the new template and click **OK**. In **Properties of New Template**, make the following changes:

- On the **General** tab, in the **Template display name** field type **Trey Proxy Client Auth**
- On the **Request Handling** tab, check the box next to **Allow private key to be exported**
- On the **Subject Name** tab, click the radio button next to **Supply in the request**. Click **OK** in the warning about allowing user-defined subject names with automatic issuance.

Click **OK** to create the new template.

In **Console 1**, right-click on the **Certificate Authority\Trey Certificate Server\Certificate Templates** folder, and select **New > Certificate Template to Issue**. Highlight **Trey Proxy Client Auth** from the list and click **OK**.

MACHINE 7: TREY RESEARCH WEB SERVER

CREATE WILDCARD SERVER AUTHENTICATION CERTIFICATE

> *Both the Trey Research FS proxy and the Trey Research sample application require SSL server authentication certificates. It is generally not possible to support multiple SSL applications on the same web server, unless the applications use different ports (which has its issues) or different IP addresses (which isn't possible in EC2).*
>
> *To overcome this limitation, it is possible to use a single SSL certificate for multiple applications simultaneously – if that certificate supports multiple domains, or if the certificate is a wildcard SSL certificate. A wildcard SSL certificate would be issued, for example, to* ****.treyresearch.net****, and thus be appropriate for any applications using that DNS suffix.*
>
> *In this lab, we will use wildcard certificates in conjunction with host headers to run the FS proxy (fs1.treyresearch.net) and sample application (adfsv1app.treyresearch.net) on the same web server. The special configuration steps are not supported in the IIS Manager interface; instead we will use command-line scripts, as described by Microsoft here.*

Open **Internet Explorer** and go to **https:// fs1.treyresearch.net/certsrv /.** At the login prompt, log in as administrator with the password from Line 12 of the **Important Values Worksheet** to reach the Active Directory Certificate Services home page. Click the link to **Request a certificate**, then the link for **advanced certificate request** and finally the link to **Create and submit a request to this CA**.

On the **Advanced Certificate Request** page, in the **Certificate Template** dropdown select **Extranet Web Server**. In the **Identifying Information** section, in the **Name** field type ***.treyresearch.net**, and leave the other fields blank. In the **Additional Options** section, in the **Friendly Name** field type **trey wild ssl** and click **Submit**. Click **Yes** to complete the request process; the certificate will be issued automatically.

Click the link to **Install this certificate** and click **Yes** on the warning dialog. In **Console 1**, click on **Certificates (Current User)/Personal/Certificates**. In the right-hand pane should be the certificate for *.treyresearch.net.

> *Leave the AD CS web application open for use in upcoming steps.*

MOVE WILDCARD CERTIFICATE TO LOCAL COMPUTER CERTIFICATE STORE

In **Console 1**, right-click on the ***.treyresearch.net** certificate and choose **All Tasks > Export** to launch the Certificate Export Wizard. On the **Export Private Key** page, select **Yes, export the private key**. On the **Export File Format** page, leave the default setting. After providing a password, On the **File to Export** page click **Browse**, click on **Desktop** and in the **File name** field type **trey wild ssl**. Click **Save** > **Next > Finish > OK** to complete the export process.

In **Console 1**, right-click on **Certificates (Local Computer)/Personal** and choose **All Tasks > Import** to launch the Certificate Import Wizard. On the **File to Import** page, click **Browse** and find **trey wild ssl.pfx** on the desktop. Click **Open**, then click **Next**. After typing the password, click **Next > Next > Finish > OK** to complete the import process.

CREATE CLIENT AUTHENTICATION CERTIFICATE

Back in **Internet Explorer**, click on **Home** in the upper right corner of the Certificate Services web application. Click the link to **Request a certificate**, then the link for **advanced certificate request** and finally the link to **Create and submit a request to this CA**. On the **Advanced Certificate Request** page, in the **Certificate Template** dropdown select **Trey Proxy Client Auth**.

> *If the template isn't yet showing in the dropdown list, you can speed the process by restarting the Active Directory Certificate Services service on the Trey Research Federation Server.*

In the **Identifying Information** section, in the **Name** field type **Trey Proxy Client Auth**, and leave the other fields blank. In the **Additional Options** section, in the **Friendly Name** field type **proxy client auth** and click **Submit**. Click **Yes** to complete the request process; the certificate will be issued automatically.

Click the link to **Install this certificate** and click **Yes** on the warning dialog. In **Console 1**, click on **Certificates (Current User)/Personal/Certificates**. In the right-hand pane should be the certificate for Trey Proxy Client Auth.

MOVE CLIENT AUTHENTICATION CERTIFICATE TO LOCAL COMPUTER CERTIFICATE STORE

In **Console 1**, right-click on the **Trey Proxy Client Auth** certificate and choose **All Tasks > Export** to launch the Certificate Export Wizard. On the **Export Private Key** page, select **Yes, export the private key**. On the **Export File Format** page, leave the default setting. After providing a password, On the **File to Export** page click **Browse**, click on **Desktop** and in the **File name** field type **trey proxy client auth**. Click **Save** > **Next > Finish > OK** to complete the export process.

In **Console 1**, right-click on **Certificates (Local Computer)/Personal** and choose **All Tasks > Import** to launch the Certificate Import Wizard. On the **File to Import** page, click **Browse** and find **trey proxy client auth.pfx** on the desktop. Click **Open**, then click **Next**. After typing the password, click **Next > Next > Finish > OK** to complete the import process.

INSTALL AD FS FEDERATION SERVER PROXY

In **Server Manager**, click on **Roles** in the left navigation area. In the right-hand pane under **Active Directory Federation Services**, click the link to **Add Role Services**. On the **Select Role Services** page, check the box next to **Federation Service Proxy**. On the **Choose a Server Authentication Certificate** page, highlight the existing certificate issued to ***.treyresearch.net** and click **Next**. On the **Specify**

Federation Server page, type **fs1.treyresearch.net** and click **Validate** to check accessibility, then click **Next**. On the **Choose a Client Authentication Certificate** page, highlight the existing certificate issued to **Trey Proxy Client Auth** and click **Next**. Click **Install**. Click **Close** to complete the install.

APPLY WILDCARD CERTIFICATE TO SAMPLE APPLICATION

Click **Start > Administrative Tools > Internet Information Services (IIS) Manager**. In the **Sites** folder, right-click on **ADFSv1 app** and choose **Edit Bindings**. Highlight the **HTTPS** entry and then click the **Edit** button. In the **SSL Certificate** dropdown box, select **trey wild ssl** and click **OK**, then click **Close**.

CONFIGURE SERVER BINDINGS FOR SSL HOST HEADERS

These are the steps to set up multiple applications to use the wildcard certificate with host headers, which isn’t possible through the IIS Manager interface. The steps add a new HTTPS binding with a host header to each web site, and then delete the previous HTTPS binding that doesn’t include a host header.

Click **Start > Run**. In the **Run** box type **cmd** and click **OK** to open a command prompt. Change the directory to **c:\windows\system32\inetsrv**. At the command prompt, type the following and hit **Enter**:

```
appcmd set site /site.name:“Default Web Site”
/+bindings.[protocol=’https’,bindingInformation=’*:443:fs1.treyre
search.net’]
```

You should see the following response:

```
SITE object “Default Web Site” changed
```

Type the following and hit **Enter**:

```
appcmd set site /site.name:“Default Web Site” /-
bindings.[protocol=’https’,bindingInformation=’*:443:’]
```

Type the following and hit **Enter**:

```
appcmd set site /site.name:“ADFSv1 app”
/+bindings.[protocol=’https’,bindingInformation=’*:443:adfsv1app.
treyresearch.net’]
```

Type the following and hit **Enter**:

```
appcmd set site /site.name:“ADFSv1 app” /-
bindings.[protocol=’https’,bindingInformation=’*:443:’]
```

In **Internet Explorer**, in the **Sites** folder, right-click on **Default Web Site** and select **Manage Web Site > Start**.

MACHINE 6: TREY RESEARCH FEDERATION SERVER

ADD FS PROXY CLIENT AUTHENTICATION CERTIFICATE TO FEDERATION SERVER POLICY

Open **Console 1** on the desktop. Click on **Certification Authority/Trey Certificate Server/Issued Certificates.** In the center pane, double-click on the issued certificate that used the **Trey Proxy Client Auth** certificate template to open it. On the **Details** tab, click on the **Copy to file** button to start the Certificate Export Wizard. On the **Export File Format** page, leave the default setting. On the **File to Export** page, click **Browse**, click **Desktop** and in the **File name** field type **trey proxy client auth public**. Click **Save > Next > Finish > OK > OK** to save **trey proxy client auth public.cer** to the desktop

Click **Start > Administrative Tools > Active Directory Federation Services**. Right-click on **Trust Policy** under **Federation Service** and select **Properties**. On the **FSP Certificates** tab, click **Add** and select the **trey proxy client auth public.cer** file from the desktop. Click **Open** and **OK**.

MODIFY FIREWALL SETTINGS

> *We can now reduce the scope of allowed inbound connections to the federation server to just the web server and FS proxy – which in this case happen to be the same machine. Other client requests will be handled by the proxy.*

In the Amazon **EC2 Console**, click on **Security Groups** in the left navigation bar. Click on the **Trey Federation Server** row to display its current settings. In the lower pane, click the **Remove** button next to the current **HTTPS** setting. **Add** the following setting and click **Save**:

Connection Method	Protocol	From Port	To Port	Source (IP or Group)
HTTPS	TCP	443	443	Trey web server external IP/32[1]

[1] This is the elastic IP address for the Trey Research Web Server from Line 13 of the **Important Values Worksheet**.

MACHINE 3: ADATUM WEB SERVER

EDIT DNS ADDRESS FOR TREY RESEARCH FEDERATION SERVER IN INTERNET DNS

Click **Start > Administrative Tools > DNS**. Under **Forward Lookup Zones**, click on **treyresearch.net.** In the right-hand pane, right-click on the record for **fs1** and select **Properties**. In the **IP address** field type the elastic IP address for the **Trey Research Web Server** from Line 13 of the **Important Values Worksheet**. Click **OK.** This redirects all client inbound traffic to the proxy instead of the federation server

MACHINE 1: ADATUM INTERNAL SERVER

CLEAR DNS CACHE

Click **Start > Administrative Tools > DNS**. Click on **FS1** in the left navigation area. In the **Action** menu, select **Clear Cache** to ensure that the new DNS record for *fs1.treyresearch.net* (pointing to the FS proxy) is used instead of the previous entry.

MACHINE 2: DOMAIN-JOINED CLIENT

CLEAR INTERNET EXPLORER DNS CACHE

Click **Start**. In the **search** field type **cmd** and hit **Enter** to open a command prompt. At the prompt type type **ipconfig /flushdns** to make sure Internet Explorer uses the new DNS listing for *fs1.treyresearch.net*.

TEST

Before testing on either the domain-joined or external client, you should clear browser cookies, to reinitiate the complete federation process. In **Internet Explorer** click **Tools > Internet Options**. On the **General** tab under **Browsing history**, click the **Delete** button. Make sure the box next to **Cookies** is checked and click **Delete**.

To test, open **Internet Explorer** on the domain-joined client, type **https://adfsv1app.treyresearch.net** in the address bar and hit **Enter**. The home realm discovery page and all security token requests and responses will be handled in this scenario by the Trey Research FS proxy, which allows the federation server to scope down its inbound access to just communication from the proxy and web servers. You can also test with the External Client; run **ipconfig /flushdns** to make sure IE uses DNS properly.

SCENARIO 5: CORPORATE APPLICATION, ACCESSED INTERNALLY (AD FS 2.0)

This scenario is the same as Scenario 1, but using different software. We will install the beta release of AD FS 2.0 (formerly known as "Geneva" Server) and use it as our security token issuer. On the application side, we will use the recently-released Windows Identity Foundation (formerly known as "Geneva" Framework) on the web server, and use it to support our claims-aware application.

These updated components of Microsoft's claims-based application access model represent a substantial upgrade in capability and flexibility over AD FS v1. To learn more about these improvements, visit the "Geneva" site on Microsoft Connect.

The scenario adds one additional computer to the lab.

8) Adatum Federation Server (AD FS 2.0)

    This local machine will create security tokens for users to give the federation application. Since Adatum already has a domain controller, we will leverage that existing deployment. In total, this machine will run:

    a) Internet Information Services 7 (web server)
    b) Microsoft .NET Framework 3.5
    c) Active Directory Federation Services 2.0 (Adatum identity provider)

    The AD FS 2.0 federation server (currently in beta) is available as a download from Microsoft here. Supported operating systems are Windows Server 2008 Service Pack 2 and Windows Server 2008 R2. This lab used the trial Windows Server 2008 R2 Enterprise Edition Hyper-V image which is available for download here.

In addition, this scenario installs the Windows Identity Foundation (WIF) onto the Adatum Web Server, or Machine 3. The following components are added:

a) Windows Identity Foundation (.NET libraries for claims-aware applications)
b) WIF SDK with sample applications

The .NET Framework 3.5, a required component, is already installed on the EC2 base Windows machine images.

Windows Identity Foundation (released November 2009) is available as a download from Microsoft. Supported operating systems are Windows Server 2003 Service Pack 2, Windows Server 2008 Service Pack 2, Windows Server 2008 R2, Windows Vista and Windows 7. Amazon EC2 currently offers Windows Server 2003 R2 Service Pack 2 and Windows Server 2008 Service Pack 2 as guest operating systems. This lab uses our existing Adatum Web Server, which is running Windows Server 2008 Service Pack 2. Therefore, our download locations are here for the runtime and here for the SDK.

CONFIGURATION

MACHINE 1: ADATUM INTERNAL SERVER

MODIFY AD CS CERTIFICATE TEMPLATE PERMISSIONS

Open **Console 1** from the desktop**.** Click on **Certificate Templates** in the left navigation area. In the center pane, right-click on the **Web Server** certificate template and choose **Properties**. On the **Security** tab, click **Add**, and in the object names text box type **Domain Computers** and click **Check Names**. Once verified, click **OK**. Back in the **Security** tab, highlight the **Domain Computers** list item, then in the **Allow** column check the **Read** and **Enroll** permissions and click **OK**.

MACHINE 8: ADATUM FEDERATION SERVER (AD FS 2.0)

The configuration steps listed below are targeted to Windows Server 2008 R2. If using a different version of Windows Server, use these steps as a guideline only.

INITIAL INSTALL

Install Windows Server 2008 R2 on your server computer or virtual machine.

If you use the Windows Server 2008 R2 trial VHD for both the domain controller and a member server on the same network, those machines will have the same security identifier (SID), potentially causing domain-related issues later. To defend against this, run Sysprep on the second VHD instance as follows:

*Navigate to the **c:\Windows\System32\sysprep** folder and double-click on **sysprep.exe** to open the System Preparation Tool. In the **System Cleanup Action** dropdown box, leave **Enter System Out-of-Box Experience** selected. In the **Shutdown Options** dropdown box, select **Reboot** and click **OK**. Accept the defaults through the rest of the process.*

CONFIGURE NETWORKING

> *This computer requires inbound Internet connectivity through a static, external IP address through port 443, to allow the EC2-based web server to communicate with the AD FS federation server. Contact your network administrator to request a static IP address, and to open port 443 on the external IP address.*

In the **Initial Configuration Tasks** window, click on **Configure networking**, then right-click on the **Local Area Connection** and select **Properties**. Double-click on the **Internet Protocol Version 4** list item to open TCP/IPv4 Properties. On the **General** tab, click the radio button to **Use the following DNS server address**. In the **Preferred DNS server** field, type the static domain IP address of the Adatum Internal Server from Line 3 of the **Important Values Worksheet** and click **OK** twice.

In **Initial Configuration Tasks**, click on **Provide computer name and domain**, then click **Change** and type **fs2** in the computer name field. In the **Member of** area, click the radio button for **Member of Domain**, and in the **Domain** text box type **CORP** and click **OK**. Type the Adatum domain administrator username and password from Line 2 of the **Important Values Worksheet** and click **OK**. Follow prompts to restart computer.

Log back into the machine with the **CORP\administrator** account using the password from Line 2 of the **Important Values Worksheet**.

Optional

Turn off the Internet Explorer Enhanced Security Configuration for administrators. In **Server Manager**, on the **Server Summary** page under **Security Information**, click on **Configure IE ESC**. Under **Administrators,** click the **Off** radio button and click **OK**.

IDENTIFY EXTERNAL IP ADDRESS

Identify your external IP address. You can ask your network administrator, or an alternative is to visit http://www.whatismyip.com.

Record your Adatum Federation Server (AD FS 2.0) external IP address on Line 14 of the **Important Values Worksheet**.

CREATE SERVER AUTHENTICATION CERTIFICATE

Click **Start > Run**. In the **Run** box type **mmc** and click **OK** to start the Microsoft Management Console. In the **File** menu select **Add/Remove Snap-in**. Highlight the **Certificates** snap-in and click the **Add** button; choose **computer account** and **local computer** in the following pages and click **OK**. Click **File > Save**, and save the new MMC console (Console 1) to the machine desktop for future use.

In **Console 1**, right-click on **Certificates (Local Computer)/Personal** and select **All Tasks > Request New Certificate**. In the Certificate Enrollment Wizard, click **Next** twice, then click the blue link under **Web Server**.

> *If the Web Server template isn't yet showing, you can speed the process by restarting the Active Directory Certificate Services service on the Adatum Internal Server.*

In **Certificate Properties**, make the following changes:

- On the **Subject** tab, in the **Subject Name** area click on the **Type** dropdown list and select **Common name**. In the **Value** field type **fs2.corp.adatum.com** and click **Add**.
- On the **General** tab, in the **Friendly name** text box type **adatum fs2 ssl** and click **OK**.

In the **Certificate Enrollment** window, check the box next to **Web Server** and then click the **Enroll** button, then click **Finish**. In **Console 1**, check for the new certificate with friendly name "adatum fs2 ssl" in **Certificates (Local Computer)/Personal/Certificates**.

CREATE AD FS TOKEN SIGNING CERTIFICATE

In **Console 1**, right-click on **Certificates (Local Computer)/Personal** and select **All Tasks > Request New Certificate.** In the Certificate Enrollment Wizard, click **Next** twice, then click the blue link under **Web Server**. In **Certificate Properties**, make the following changes:

- On the **Subject** tab, in the **Subject Name** area click on the **Type** dropdown list and select **Common name**. In the **Value** field type **Adatum Token Signing Cert3** and click **Add**.
- On the **General** tab, in the **Friendly name** text box type **adatum ts3** and click **OK**.

In the **Certificate Enrollment** window, check the box next to **Web Server** and then click the **Enroll** button, then click **Finish**. In **Console 1**, check for the new certificate with friendly name "adatum ts3" in **Certificates (Local Computer)/Personal/Certificates**.

MODIFY READ PERMISSION TO TOKEN SIGNING PRIVATE KEY

> *AD FS 2.0 runs using the Network Service account, which needs access to the token signing certificate private key in order to use it for signing security tokens and federation metadata.*

Computer)/Personal/Certificates and select **All Tasks > Manage Private Keys**. Click **Add**, and in the object text box type **Network Service** and click **Check Names.** Once verified, click **OK** twice.

INSTALL AD FS 2.0

Download the AD FS 2.0 installation media from here and save to your machine. Run the saved file to start the AD FS 2.0 Installation Wizard. The AD FS 2.0 installer automatically installs .NET Framework 3.5 and IIS 7.5 in Windows Server 2008 R2.When the wizard completes, click **Finish** to automatically start the AD FS 2.0 Management console.

In the **AD FS 2.0 Management** console, click the link in the center pane to launch the **AD FS 2.0 Federation Server Configuration Wizard**. On the **Welcome** page, leave the default to **Create a new Federation Service**. On the **Select Stand-Alone or Farm Deployment** page, select **Stand-alone federation server**. In the **Specify the Federation Service Name** page, in the **SSL certificate** dropdown box select **adatum fs2 ssl**. Click **Next** twice to begin the configuration process, then **Close**.

ADD TOKEN SIGNING CERTIFICATE IN AD FS

Click **Start > Administrative Tools > Windows PowerShell Modules**. At the PowerShell command prompt, type the following and hit **Enter**:

```
Set-ADFSProperties -AutoCertificateRollover $false
```

This will disable the automatic certificate rollover feature in AD FS, a prerequisite to adding a token signing certificate. Leave PowerShell open for later use.

In the **AD FS 2.0 Management** console, click on **AD FS 2.0/Service/Certificates** in the left navigation area. In the right-hand pane under **Actions** click the link to **Add Token-Signing Certificate**. In the new window, select the **adatum ts3** certificate and click **OK**. Back in the center pane of **AD FS 2.0 Management**, in the **Token-signing** section, right-click on **Adatum Token Signing Cert3** and select **Set as Primary**, then click **Yes**. Right-click on the other listed token-signing certificate (**CN=ADFS Signing…**) and select **Delete**.

In the PowerShell command window, at the command prompt type the following and hit **Enter**:

```
Set-ADFSProperties -AutoCertificateRollover $true
```

MACHINE 3: ADATUM WEB SERVER

ADD RECORD FOR ADATUM FEDERATION SERVER (AD FS 2.0) TO HOSTS FILE

> *This web server will access the Adatum Federation Server (AD FS 2.0) to automatically get federation trust policy data. This data could be manually exchanged, thus eliminating the need for the web server and federation server to communicate directly, and eliminating the need for inbound HTTPS connectivity to the federation server. However, the approach used here allows for automated, periodic updating of trust policy information.*

Double-click the shortcut on the desktop for the **hosts** file; select **Notepad** as the program and click **OK**. Add the name and external IP address of the Adatum Federation Server (AD FS 2.0) from **Line 14** of the **Important Values Worksheet**, as shown in the following example:

123.456.78.910 fs2.corp.adatum.com

Save and **close** the file.

CREATE WILDCARD SERVER AUTHENTICATION CERTIFICATE

> *As in Scenario 4, this web server will now use a wildcard SSL server authentication certificate and host headers, to allow secure access to the Adatum AD FS v1 and AD FS 2.0 apps simultaneously.*

Open **Internet Explorer** and go to **https://fs1.corp.adatum.com/certsrv/**. At the login prompt, log in as administrator with the password from on Line 2 of the **Important Values Worksheet** to reach the Active Directory Certificate Services home page. Click the link to **Request a certificate**, then the link for **advanced certificate request** and finally the link to **Create and submit a request to this CA**.

On the **Advanced Certificate Request** page, in the **Certificate Template** dropdown select **Extranet Web Server**. In the **Identifying Information** section, in the **Name** field type ***.adatum.com**, and leave the other fields blank. In the **Additional Options** section, in the **Friendly Name** field type **adatum wild ssl** and click **Submit**. Click **Yes** to complete the request process; the certificate will be issued automatically.

Click the link to **Install this certificate** and click **Yes** on the warning dialog. In **Console 1**, click on **Certificates (Current User)/Personal/Certificates**. In the right-hand pane should be the certificate for *.adatum.com.

> *Leave the AD CS web application open for use in upcoming steps.*

MOVE WILDCARD CERTIFICATE TO LOCAL COMPUTER CERTIFICATE STORE

In **Console 1**, right-click on the ***.adatum.com** certificate and choose **All Tasks > Export** to launch the Certificate Export Wizard. On the **Export Private Key** page, select **Yes, export the private key**. On the **Export File Format** page, leave the default setting. After providing a password, On the **File to Export** page click **Browse**, click on **Desktop** and in the **File name** field type **adatum wild ssl**. Click **Save** > **Next > Finish > OK** to complete the export process.

In **Console 1**, right-click on **Certificates (Local Computer)/Personal** and choose **All Tasks > Import** to launch the Certificate Import Wizard. On the **File to Import** page, click **Browse** and find **adatum wild ssl.pfx** on the desktop. Click **Open**, then click **Next**. After typing the password, click **Next > Next > Finish > OK** to complete the import process.

INSTALL WINDOWS IDENTITY FOUNDATION RUNTIME AND SDK

Download the **Windows Identity Foundation runtime** here. Make sure to pick the media with the words **Windows6.0** in the title. In the **Download Complete** window click **Open** to start the installation. When the wizard completes, click **Close**.

Download the **Windows Identity Foundation SDK** here. In the **Download Complete** window click **Run** twice to start the Setup Wizard. Accept all of the defaults in the wizard. Click **Finish**.

ADD AD FS 2.0 SAMPLE APPLICATION TO IIS

> *We will use a sample application installed on the machine with the WIF SDK.*

Click **Start > Administrative Tools > Internet Information Services (IIS) Manager**. Right-click on the **Sites** folder in the left navigation area and select **Add Web Site**. In the **Site name** field type **ADFSv2 app**. In the **Content Directory** section, click on the button to the right of the **Physical path** field, browse to **c:\Program Files\Windows Identity Foundation SDK\v3.5\Samples\Quick Start\Using Managed STS\ClaimsAwareWebAppWithManagedSTS** and click **OK**. In the **Binding** section, in the **Type** dropdown box select **https**. In the **SSL certificate** dropdown box, select **adatum wild ssl** and click **OK,** then **Yes**. This will automatically assign **adatum wild ssl** to both the ADVSv1 and ADFSv2 applications.

CONFIGURE SERVER BINDINGS FOR SSL HOST HEADERS

Click **Start > Run**. In the **Run** box type **cmd** and click **OK** to open a command prompt. Change the directory to **c:\windows\system32\inetsrv**. At the command prompt, type the following and hit **Enter**:

```
appcmd set site /site.name:"ADFSv1 app"
/+bindings.[protocol='https',bindingInformation='*:443:adfsv1app.
adatum.com']
```

You should see the following response:

```
SITE object "Default Web Site" changed
```

Type the following and hit **Enter**:

```
appcmd set site /site.name:"ADFSv1 app" /-
bindings.[protocol='https',bindingInformation='*:443:']
```

Type the following and hit **Enter**:

```
appcmd set site /site.name:"ADFSv2 app"
/+bindings.[protocol='https',bindingInformation='*:443:adfsv2app.
adatum.com']
```

Type the following and hit **Enter**:

```
appcmd set site /site.name:"ADFSv2 app" /-
bindings.[protocol='https',bindingInformation='*:443:']
```

In **Internet Explorer**, in the **Sites** folder, right-click on **ADFSv2 app** and select **Manage Web Site > Start**.

ADD RECORD FOR AD FS 2.0 SAMPLE APPLICATION IN INTERNET DNS

Click **Start > Administrative Tools > DNS**. Right-click on **<Machine name>/Forward Lookup Zones/adatum.com** and select **New Host (A or AAAA)**. In the **New Host Name** field type **adfsv2app** and in the **IP address** field type the elastic IP address for the Adatum Web Server from Line 8 of the **Important Values Worksheet**. Click **Add Host > OK > Done.**

RUN WINDOWS IDENTITY FOUNDATION FEDERATION UTILITY

> *This tool automatically modifies an application's web.config file to support claims. It can be run standalone (as we're doing here) or launched from inside Visual Studio.*

Click **Start > Administrative Tools > Windows Identity Foundation Federation Utility** to launch the Federation Utility Wizard. On the **Welcome** page, in the **Application configuration location** section click Browse and navigate to **c:\Program Files\Windows Identity Foundation SDK\v3.5\Samples\Quick Start\Using Managed STS\ClaimsAwareWebAppWithManagedSTS/web.config** and click **Open**. In the **Application URI** field type **https://adfsv2app.adatum.com/** and click **Next.** On the **Security Token Service** page, select **Use an existing STS**. In the **STS WS-Federation metadata document location** field, type **https://fs2.corp.adatum.com/FederationMetadata/2007-06/FederationMetadata.xml** and click **Test Location**. Once you see the xml file, click **Next**. On the **Security Token Encryption** page, leave the default **No encryption** setting. Click **Next > Next > Finish > OK**.

MACHINE 8: ADATUM FEDERATION SERVER (AD FS 2.0)

ADD SAMPLE APPLICATION AS A RELYING PARTY TRUST

Click **Start > Administrative Tools > AD FS 2.0 Management**. In the center pane, click on the link to **Add a trusted relying party** to start the Add Relying Party Trust Wizard. On the **Select Data Source** page, in the **federation metadata address** field type **https://adfsv2app.adatum.com/FederationMetadata/2007-06/FederationMetadata.xml** and click **Next**. Click **Next > Next > Next > Close** to complete the wizard and automatically open the **Edit Claim Rules** window.

On the **Issuance Transform Rules** tab, click **Add Rule** to start the Add Transform Claim Rule Wizard. On the **Choose Rule Type** page, leave the default **Send LDAP Attributes as Claims** selected and click **Next**. On the **Configure Claim Rule** page, in the **Claim rule name** field type **Rule1**. In the **Attribute store** dropdown box select **Active Directory**. In the **LDAP Attribute** dropdown box, select **Display-Name**, and in the adjoining **Outgoing Claim Type** dropdown box select **Name**. Click **Finish**.

On the **Issuance Transform Rules** tab, click **Add Rule** again. On the **Choose Rule Type** page, select **Send Group Membership as a Claim** and click **Next**. On the **Configure Claim Rule** page, in the **Claim rule name** field type **Rule2**. Click the **Browse** button, and in the object name text box type **Managers** and click **Check Names**. Once verified, click **OK**. In the **Outgoing Claim Type** dropdown box select **Role**. In the **Outgoing claim value** field type **PriorityUsers**. Click **Finish** and **OK**.

CONFIGURE FIREWALL SETTINGS

Click **Start > Administrative Tools > Windows Firewall with Advanced Security**. Click on **Inbound Rules** in the left navigation area. In the right-hand pan under **Actions**, click on **Filter by Group** and select **Filter by Secure World Wide Web Services (HTTPS)**. In the center pane, right-click on the **World Wide Web Services (HTTPS Traffic-In)** rule and select **Properties**. In the **Properties** dialog box, click on the **Scope** tab. In the **Remote IP address** section, click the radio button next to **These IP addresses:**, then click **Add**. In the **IP Address** window, in the **This IP address or subnet** field, type the elastic IP address of the Adatum Web Server from Line 8 of the **Important Values Worksheet** and click **OK**.

Click **Add** again, and in the same field type the internal IP address of the domain-joined client from Line 6 of the **Important Values Worksheet**. Click **OK** twice.

In AD FS 2.0, the FS proxy server (which is not being used here) handles more functionality than in AD FS v1. In addition to the prior capability of handling external client token requests, the server can now also be a proxy for web servers requesting trust policy information. This allows administrators to scope down internet traffic inbound to the federation server to only the FS proxy, and not include individual web servers (as we have done above).

MACHINE 1: ADATUM INTERNAL SERVER

ADD ADATUM FEDERATION SERVER (AD FS 2.0) URL TO INTRANET ZONE IN GROUP POLICY

Click **Start > Administrative Tools > Group Policy Management**. Right-click on **Forest:corp.adatum.com/Domains/corp.adatum.com/Default Domain Policy** and select **Edit**. Click on **User Configuration/Policies/Windows Settings/Internet Explorer Maintenance/Security**. In the left-hand pane, right-click on **Security Zones and Content Ratings** and select **Properties**. In the **Security Zones and Privacy** section, click the radio button next to **Import the current security zones and privacy settings**, then click **Continue**, and then click **Modify Settings**. In the **Internet Properties** window, on the **Security** tab, highlight the **Local Intranet** zone and click the **Sites** button. Click **Advanced**, then in the **Add this website to the zone** text box type **https://fs2.corp.adatum.com** and click **Add**. Click **Close**, then **OK** twice.

MACHINE 2: DOMAIN-JOINED CLIENT

UPDATE GROUP POLICY SETTINGS

Click **Start**. In the **search** field type **cmd** and hit **Enter** to open a command prompt. At the prompt type **gpupdate /force** to ensure the IE Intranet Zone is updated on the client machine.

TEST

To test the scenario, open **Internet Explorer** in the domain-joined client, type **https://adfsv2app.adatum.com** in the Address Bar and hit **Enter**. You should be presented with access to the WIF sample claims-aware application hosted on EC2, without being asked for a password. Note the claims that were passed to the application, including the PriorityUsers claim that was based on Active Directory group membership.

If you are running into errors, it's possible that you are having certificate verification issues. Please see Appendix B for more information.

APPENDIX A: SAMPLE FEDERATED APPLICATION FILES

Start Notepad.

Copy/paste this entire Appendix into a new text file. Then download the text file to the desktop of your EC2-based Adatum Web Server. A web-based storage service such as http://skydrive.live.com can be useful here.

On the Adatum Web Server, **open** the text file in Notepad.

DEFAULT.ASPX

Copy the following section to the clipboard:

```
<%@ Page Language="C#" AutoEventWireup="true"  CodeFile="Default.aspx.cs" Inherits="_Default"
%>
<%@ OutputCache Location="None" %>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" >

<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title> Claims-aware Sample Application</title>
<style>
<!--
.pagetitle   { font-family: Verdana; font-size: 18pt; font-weight: bold;}
.propertyTable td { border: 1px solid; padding: 0px 4px 0px 4px}
.propertyTable th { border: 1px solid; padding: 0px 4px 0px 4px; font-weight: bold;
background-color: #cccccc ; text-align: left }
.propertyTable { border-collapse: collapse;}
td.l{ width: 200px }
tr.s{ background-color: #eeeeee }
.banner      { margin-bottom: 18px }
.propertyHead { margin-top: 18px; font-size: 12pt; font-family: Arial; font-weight: bold;
margin-top: 18}
.abbrev { color: #0066FF; font-style: italic }
-->
```

```
</style>
</head>

<body>
<form ID="Form1" runat=server>

<div class=banner>
<div class=pagetitle>Adatum SSO Sample (ADFSv1)</div>
[ <asp:HyperLink ID=SignOutUrl runat=server>Sign Out</asp:HyperLink> | <a
href="<%=Context.Request.Url.GetLeftPart(UriPartial.Path)%>">Refresh without viewstate
data</a>]
</div>

<div class=propertyHead>Page Information</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table runat=server ID=PageTable CssClass=propertyTable>
<asp:TableHeaderRow>
<asp:TableHeaderCell>Name</asp:TableHeaderCell>
<asp:TableHeaderCell>Value</asp:TableHeaderCell>
<asp:TableHeaderCell>Type</asp:TableHeaderCell>
</asp:TableHeaderRow>
</asp:Table>
</div>

<div class=propertyHead>User.Identity</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=IdentityTable runat=server>
<asp:TableHeaderRow>
<asp:TableHeaderCell>Name</asp:TableHeaderCell>
<asp:TableHeaderCell>Value</asp:TableHeaderCell>
<asp:TableHeaderCell>Type</asp:TableHeaderCell>
</asp:TableHeaderRow>
</asp:Table>
</div>

<div class=propertyHead>(IIdentity)User.Identity</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=BaseIdentityTable runat=server>
```

```
<asp:TableHeaderRow>

<asp:TableHeaderCell>Name</asp:TableHeaderCell>

<asp:TableHeaderCell>Value</asp:TableHeaderCell>

<asp:TableHeaderCell>Type</asp:TableHeaderCell>

</asp:TableHeaderRow>

</asp:Table>

</div>


<div class=propertyHead>(SingleSignOnIdentity)User.Identity</div>

<div style="padding-left: 10px; padding-top: 10px">

<asp:Table CssClass="propertyTable" ID=SSOIdentityTable runat=server>

<asp:TableHeaderRow>

<asp:TableHeaderCell>Name</asp:TableHeaderCell>

<asp:TableHeaderCell>Value</asp:TableHeaderCell>

<asp:TableHeaderCell>Type</asp:TableHeaderCell>

</asp:TableHeaderRow>

</asp:Table>

</div>


<div class=propertyHead>SingleSignOnIdentity.SecurityPropertyCollection</div>

<div style="padding-left: 10px; padding-top: 10px">

<asp:Table CssClass="propertyTable" ID=SecurityPropertyTable runat=server>

<asp:TableHeaderRow>

<asp:TableHeaderCell>Uri</asp:TableHeaderCell>

<asp:TableHeaderCell>Claim Type</asp:TableHeaderCell>

<asp:TableHeaderCell>Claim Value</asp:TableHeaderCell>

</asp:TableHeaderRow>

</asp:Table>

</div>


<div class=propertyHead>(IPrincipal)User.IsInRole(...)</div>

<div style="padding-left: 10px; padding-top: 10px">

<asp:Table CssClass="propertyTable" ID=RolesTable runat=server>

</asp:Table>


<div style="padding-top: 10px">

<table>

<tr><td>Roles to check (semicolon separated):</td></tr>
```

```
<tr><td><asp:TextBox ID=Roles Columns=55 runat=server/></td><td align=right><asp:Button
UseSubmitBehavior=true ID=GetRoles runat=server Text="Check Roles"
OnClick="GoGetRoles"/></td></tr>
</table>
</div>

</div>
</form>
</body>

</html>
```

On the desktop, right-click and select **New > Text Document**. **Double-click** on the file to open it, then **paste** the clipboard contents into the file. Click **File > Save As.** In the **Save as Type** dropdown box, select **All Files** and save the file as **default.aspx** in the **c:\inetpub\adfsv1app** directory.

> *Saving directly into this folder (as opposed to drag-and-drop from the desktop, for example) will ensure that web-friendly ACLs are set on the files.*

WEB.CONFIG

Copy the following section to the clipboard:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
   <configSections>
      <sectionGroup name="system.web">
              <section name="websso"
                       type="System.Web.Security.SingleSignOn.WebSsoConfigurationHandler,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null" />
      </sectionGroup>
   </configSections>

   <system.web>

    <sessionState mode="Off" />
    <compilation defaultLanguage="c#" debug="true">
       <assemblies>
          <add assembly="System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null"/>
          <add assembly="System.Web.Security.SingleSignOn.ClaimTransforms, Version=1.0.0.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35, Custom=null"/>
       </assemblies>
    </compilation>

    <customErrors mode="Off"/>

    <authentication mode="None" />

    <httpModules>
        <add
            name="Identity Federation Services Application Authentication Module"
            type="System.Web.Security.SingleSignOn.WebSsoAuthenticationModule,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null" />
    </httpModules>

       <websso>
        <authenticationrequired />
        <eventloglevel>55</eventloglevel>
        <auditsuccess>2</auditsuccess>
        <urls>
          <returnurl>https://adfsv1app.adatum.com/</returnurl>
        </urls>
        <cookies writecookies="true">
          <path>/</path>
          <lifetime>240</lifetime>
        </cookies>
    <fs>https://fs1.corp.adatum.com/adfs/fs/federationserverservice.asmx</fs>
      </websso>



</system.web>
```

```
   <system.diagnostics>
      <switches>
  <add name="WebSsoDebugLevel" value="255" /> <!-- Change to 255 to enable full debug logging
-->
      </switches>
      <trace autoflush="true" indentsize="3">
         <listeners>
            <add name="LSLogListener"
type="System.Web.Security.SingleSignOn.BoundedSizeLogFileTraceListener,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null"
initializeData="c:\ADFS_app_logs\adfsv1app.log" />
         </listeners>
      </trace>
   </system.diagnostics>

</configuration>
```

On the desktop, double-click on the **New Text Document**, then paste the clipboard contents into the file. Click **File > Save As.** In the **Save as Type** dropdown box, select **All Files** and save the file as **web.config** in the **c:\inetpub\adfsv1app** directory.

DEFAULT.ASPX.CS

Copy the following section to the clipboard:

```
using System;
using System.Data;
using System.Collections.Generic;
using System.Configuration;
using System.Reflection;
using System.Web;
using System.Web.Security;
using System.Web.UI;
using System.Web.UI.WebControls;
using System.Web.UI.WebControls.WebParts;
using System.Web.UI.HtmlControls;
using System.Security;
using System.Security.Principal;


using System.Web.Security.SingleSignOn;
using System.Web.Security.SingleSignOn.Authorization;


public partial class _Default : System.Web.UI.Page
{
    const string NullValue = "<span class=\"abbrev\" title=\"Null Reference, or not
applicable\"><b>null</b></span>";


    static Dictionary<string, string> s_abbreviationMap;


    static _Default()
    {
        s_abbreviationMap = new Dictionary<string, string>();
        //
        // Add any abbreviations here. Make sure that prefixes of
        // replacements occur *after* the longer replacement key.
        //
        s_abbreviationMap.Add("System.Web.Security.SingleSignOn.Authorization", "SSO.Auth");
        s_abbreviationMap.Add("System.Web.Security.SingleSignOn", "SSO");
        s_abbreviationMap.Add("System", "S");
    }


    protected void Page_Load(object sender, EventArgs e)
    {
        SingleSignOnIdentity ssoId = User.Identity as SingleSignOnIdentity;


        //
        // Get some property tables initialized.
        //
        PagePropertyLoad();
        IdentityLoad();
        BaseIdentityLoad();
        SSOIdentityLoad(ssoId);
        SecurityPropertyTableLoad(ssoId);


        //
```

```
            // Filling in the roles table
            // requires a peek at the viewstate
            // since we have a text box driving this.
            //
            if (!IsPostBack)
            {
                UpdateRolesTable(new string[] { });
            }
            else
            {
                GoGetRoles(null, null);
            }

            //
            // Get the right links for SSO
            //
            if (ssoId == null)
            {
                SignOutUrl.Text = "Single Sign On isn't installed...";
                SignOutUrl.Enabled = false;
            }
            else
            {
                if (ssoId.IsAuthenticated == false)
                {
                    SignOutUrl.Text = "Sign In (you aren't authenticated)";
                    SignOutUrl.NavigateUrl = ssoId.SignInUrl;
                }
                else
                    SignOutUrl.NavigateUrl = ssoId.SignOutUrl;
            }
        }

        void SecurityPropertyTableLoad(SingleSignOnIdentity ssoId)
        {
            Table t = SecurityPropertyTable;

            if (ssoId == null)
            {
                AddNullValueRow(t);
                return;
            }

            //
            // Go through each of the security properties provided.
            //
            bool alternating = false;
            foreach (SecurityProperty securityProperty in ssoId.SecurityPropertyCollection)
            {
                t.Rows.Add(CreateRow(securityProperty.Uri, securityProperty.Name,
    securityProperty.Value, alternating));
                alternating = !alternating;
            }
        }

        void UpdateRolesTable(string[] roles)
        {
            Table t = RolesTable;

            t.Rows.Clear();

            bool alternating = false;
            foreach (string s in roles)
            {
                string role = s.Trim();
                t.Rows.Add(CreatePropertyRow(role, User.IsInRole(role), alternating));

                alternating = !alternating;
            }
        }

        void IdentityLoad()
        {
            Table propertyTable = IdentityTable;

            if (User.Identity == null)
            {
                AddNullValueRow(propertyTable);
            }
            else
            {
                propertyTable.Rows.Add(CreatePropertyRow("Type name",
    User.Identity.GetType().FullName));
            }
        }

        void SSOIdentityLoad(SingleSignOnIdentity ssoId)
        {
            Table propertyTable = SSOIdentityTable;

            if (ssoId != null)
            {
                PropertyInfo[] props = ssoId.GetType().GetProperties(BindingFlags.Instance |
    BindingFlags.Public | BindingFlags.DeclaredOnly);
                AddPropertyRows(propertyTable, ssoId, props);
            }
            else
            {
                AddNullValueRow(propertyTable);
            }
        }

        void PagePropertyLoad()
        {
            Table propertyTable = PageTable;

            string leftSidePath = Request.Url.GetLeftPart(UriPartial.Path);

            propertyTable.Rows.Add(CreatePropertyRow("Simplified Path", leftSidePath));
        }

        void BaseIdentityLoad()
        {
            Table propertyTable = BaseIdentityTable;
            IIdentity identity = User.Identity;

            if (identity != null)
            {
                PropertyInfo[] props = typeof(IIdentity).GetProperties(BindingFlags.Instance |
    BindingFlags.Public | BindingFlags.DeclaredOnly);
                AddPropertyRows(propertyTable, identity, props);
            }
            else
            {
                AddNullValueRow(propertyTable);
            }
        }

        void AddNullValueRow(Table table)
        {
            TableCell cell = new TableCell();
            cell.Text = NullValue;

            TableRow row = new TableRow();
            row.CssClass = "s";
            row.Cells.Add(cell);

            table.Rows.Clear();
            table.Rows.Add(row);
        }

        void AddPropertyRows(Table propertyTable, object obj, PropertyInfo[] props)
        {
            bool alternating = false;

            foreach (PropertyInfo p in props)
            {
                string name = p.Name;
                object val = p.GetValue(obj, null);

                propertyTable.Rows.Add(CreatePropertyRow(name, val, alternating));
                alternating = !alternating;
            }
        }

        TableRow CreatePropertyRow(string propertyName, object propertyValue)
        {
            return CreatePropertyRow(propertyName, propertyValue, false);
        }

        TableRow CreatePropertyRow(string propertyName, object value, bool alternating)
        {
            if (value == null)
                return CreateRow(propertyName, null, null, alternating);
            else
                return CreateRow(propertyName, value.ToString(), value.GetType().FullName ,
    alternating);
        }

        TableRow CreateRow(string s1, string s2, string s3, bool alternating)
        {
            TableCell first = new TableCell();
            first.CssClass = "l";
            first.Text = Abbreviate(s1);

            TableCell second = new TableCell();
            second.Text = Abbreviate(s2);

            TableCell third = new TableCell();
            third.Text = Abbreviate(s3);

            TableRow row = new TableRow();
            if (alternating)
                row.CssClass = "s";
            row.Cells.Add(first);
            row.Cells.Add(second);
            row.Cells.Add(third);

            return row;
        }
        private string Abbreviate(string s)

        {

            if (s == null)

                return NullValue;


            string retVal = s;

            foreach (KeyValuePair<string, string> pair in s_abbreviationMap)

            {

                //

                // We only get one replacement per abbreviation call.

                // First one wins.

                //

                if (retVal.IndexOf(pair.Key) != -1)

                {

                    string replacedValue = string.Format("<span class=\"abbrev\" 
    title=\"{0}\">{1}</span>", pair.Key, pair.Value);

                    retVal = retVal.Replace(pair.Key, replacedValue);

                    break;

                }

            }

            return retVal;

        }


        //

        // ASP.NET server side callback

        //

        protected void GoGetRoles(object sender, EventArgs ea)

        {

            string[] roles = Roles.Text.Split(';');

            UpdateRolesTable(roles);

        }

    }
```

On the desktop, double-click on the **New Text Document**, then paste the clipboard contents into the file. Click **File > Save As.** In the **Save as Type** dropdown box, select **All Files** and save the file as **default.aspx.cs** in the **c:\inetpub\adfsv1app** directory.

APPENDIX B: CERTIFICATE VERIFICATION TROUBLESHOOTING

In this lab, the most common reasons for errors have to do with checking the certification revocation list (CRL) for the Adatum certificate authority (CA), to verify that the AD FS token-singing certificate has not been revoked. There are a number of ways that CRL checking can break, leading to testing errors:

- If the Adatum Internal Server (which hosts our Adatum CA) is a Hyper-V image, and in a Saved state at the time it is supposed to issue a CRL or delta CRL, it will not automatically issue the skipped CRL file upon being restored to a Running state. The old, expired CRL file will not be replaced, and CRL checking will fail. This can be fixed by going to **Start > Administrative Tools > Services** and restarting the **Active Directory Certificate Services** service.
- If the Adatum FS Proxy (which hosts our Adatum CRL files, starting in Scenarios 2) is in a Stopped (Amazon EC2) or Saved (Hyper-V) state when a new CRL file is issued by the Adatum CA, it will not receive the new CRL file. If a web server accesses the CRL web site before it's been updated with the fresh CRL files, it will retrieve old CRL files that will break the test. However, the robocopy command used to copy the files reruns continuously every 30 seconds until it succeeds in transferring the files, meaning the fresh CRL files should be in place approximately two minutes after the Adatum FS Proxy is restored to a Running state.
- CRL files are cached on the web server(s) until they expire. If you cannot get the web server to properly perform the CRL check and the solutions above have not solved the problem, then a way to "start over" is to delete the CRL cache on the web server. Do the following:
  - Log into the Adatum Web Server or the Trey Research Web Server – whichever is the destination of your testing.
  - Click **Start > Computer** and click through to **c:\Windows\ServiceProfiles\NetworkService**.
  - Click on the **Organize** dropdown list and select **Folder and Search Options**.
  - On the **View** tab, click to fill the radio button next to **Show Hidden Files and Folders** and click **OK**.
  - Continue clicking through to **c:\Windows\ServiceProfiles\NetworkService\AppData\LocalLow\Microsoft\CryptUrlCache**.
  - Delete all the content of both the **Content** and **Metadata** subfolders in the CryprUrlCache folder.
  - Empty the Recycle Bin on the desktop.
  - In **IIS Manager**, in the left pane click on the connection to the local web server (*IP-abcd….*). In the right-hand pane under **Actions** click **Restart**.

The easiest way to avoid these issues is to not put any of the machines in this lab into a Saved or Stopped state during your testing.