loadbalancer.org

Load Balancing
Microsoft AD FS

Deployment Guide
v1.3.1

Table of Contents

1. About this Guide

This guide details the steps required to configure a load balanced Microsoft AD FS environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Microsoft AD FS configuration changes that are required to enable load balancing.

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the relevant Administration Manual:

- v7 Administration Manual
- v8 Administration Manual

2. Loadbalancer.org Appliances Supported

All our products can be used with AD FS. The complete list of models is shown below:

Discontinued Models	Current Models *
Enterprise R16	Enterprise R20
Enterprise VA R16	Enterprise MAX
Enterprise VA	Enterprise 10G
Enterprise R320	Enterprise Ultra
	Enterprise VA R20
	Enterprise VA MAX
	Enterprise AWS
	Enterprise AZURE **

* For full specifications of these models please refer to: http://www.loadbalancer.org/products/hardware

** Some features may not be supported, please check with Loadbalancer.org support

3. Loadbalancer.org Software Versions Supported

- v8.2.2 and later

4. Microsoft Windows Versions Supported

- Windows 2008 R2 and later (AD FS v2.0 +)

5. Active Directory Federation Services (AD FS)

INTRODUCTION

AD FS provides simplified, secured identity federation and Web single sign-on (SSO) capabilities for end users who need access to applications within an AD FS secured enterprise, in federation partner organizations, or in the cloud.

AD FS is a Web Service that authenticates users against Active Directory and provides them access to claims-aware applications. These applications are typically used through the client's web browser. The applications can be on-premises, off-premises, or even hosted by other companies.

AD FS SSO SCENARIO'S

WEB SSO

This is the most common scenario. Here users login to web applications, either off-premises or on-premises, from their browsers using their Active Directory credentials. Examples of such applications include:

- salesforce.com
- servicenow.com
- SharePoint Online (SPO)
- Office 365
- etc.

FEDERATED WEB SSO

The following scenarios are examples of Federated SSO. These scenarios aren't as common but they illustrate how AD FS can be used to collaborate with a partner, another company, or another AD forest:

- You want users from another organization to login to your web applications using their own identity credentials.
- You want to login to another organization's web applications using your own Active Directory credentials.
- You want users from another internal Active Directory forest to login to your web applications in your Active Directory using their own AD credentials without a domain and/or forest trust.
- You want to use your production Active Directory credentials to login to test web applications located in your test Active Directory environment without a domain and/or forest trust.
- You want users to be able to login to your web applications using their Google, Facebook, Live ID, Yahoo, etc. credentials.

AD FS VERSIONS

The following table lists the various versions of AD FS and in which Windows version they were initially released:

AD FS Version	Released in Windows Version
v1.0	2003 R2
v1.1	2008
v2.0	2008 R2
v2.1	2012
v3.0	2012 R2
v4.0	2016

ROLE SERVICES

The following role services can be deployed as part of the AD FS role:

Role Service	Purpose
Federation Server	Acts as an identity provider - *Authenticates users to provide security tokens to applications that trust AD FS* or Acts as a federation provider - *Consumes tokens from other identity providers and then provides security tokens to applications that trust AD FS*
Federation Server Proxy / Web Application Proxy	The Federation Service Proxy functions as an intermediary proxy service between an Internet client and a Federation Server that is located behind a firewall on a corporate network. **Note:** In Windows 2012 R2 and later, the dedicated Proxy role service has been removed. Instead, the proxy is based on WAP (Web Application Proxy).

HOW AD FS WORKS

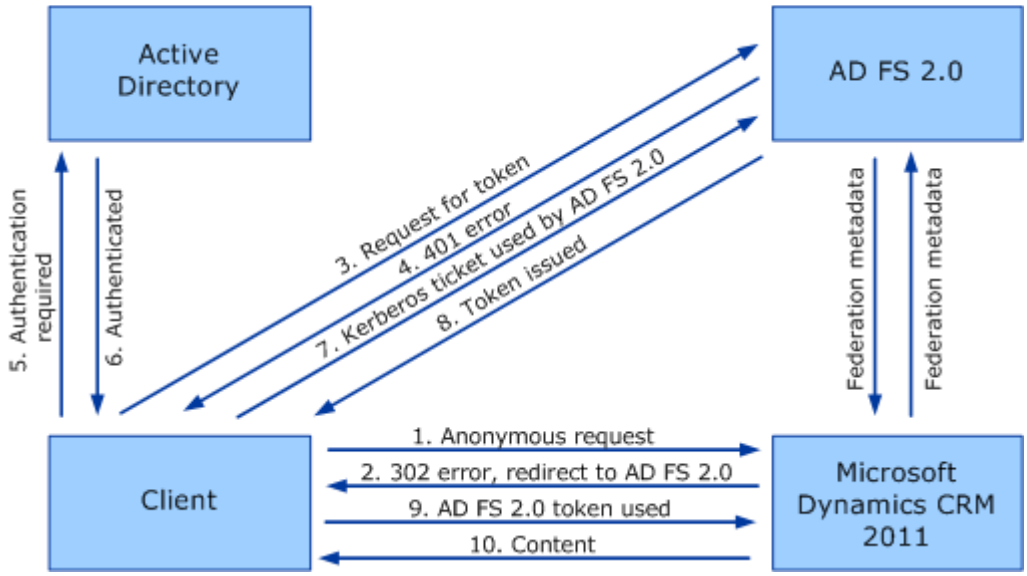
The following sections explain how AD FS authenticates internal LAN based users and external Internet based users.

A Microsoft Dynamics CRM example is used with AD FS v2.0, although the general flow is the same for other applications and different AD FS versions.

> Note:
>
> For a reference of key AD FS concepts, please refer to this URL.

INTERNAL CLIENTS

The authentication process for internal clients is shown below:



1. The client sends a request to access the Microsoft Dynamics CRM website.
2. IIS refuses the connection with an HTTP 302 error message and redirects the user to the trusted claims provider (also known as the STS) for Microsoft Dynamics CRM (AD FS v2.0).
3. The client sends a request for a security token to AD FS v2.0.
4. AD FS 2.0 returns an HTTP 401.1 error, indicating that the client must supply a Kerberos ticket.
5. The client sends a Kerberos authentication request to Active Directory.
6. Active Directory validates the client and sends a Kerberos ticket.
7. The client sends a request for a security token to AD FS v2.0 and includes the Kerberos ticket.

> Note:
>
> If the client already has a valid Kerberos ticket on the network, this ticket is sent to AD FS v2.0 in step 3 and steps 4 through 7 are skipped.

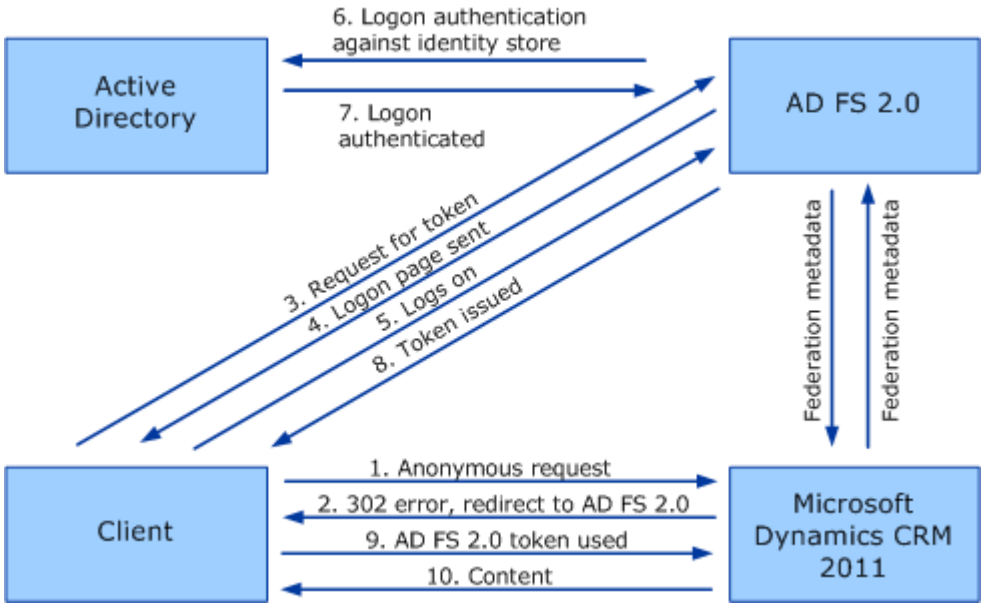
8. AD FS v2.0 provides a security token containing claims for access to Microsoft Dynamics CRM data.
9. The client sends the security token containing claims obtained from AD FS v2.0 to the Microsoft Dynamics CRM server.
10. The Microsoft Dynamics CRM server decrypts and validates the security token and presents the user with the requested information

> Note:
>
> For more information, please refer to this URL.

EXTERNAL CLIENTS

The flow for external access is largely unchanged from the flow described above for internal access. The major difference is that user authentication does not include a Kerberos ticket.

The authentication process for external clients is shown below:



> **Note:**
>
> For more information, please refer to this URL.

When an AD FS proxy is used, the client is redirected to the proxy which then connects to the internal AD FS server where authentication occurs. For more details of AD FS proxy, please refer to this URL.

OTHER USEFUL REFERENCES

How To Install AD FS 2016 For Office 365:
https://blogs.technet.microsoft.com/rmilne/2017/04/28/how-to-install-ad-fs-2016-for-office-365/

Setting up AD FS and Enabling Single Sign-On to Office 365:
https://blogs.technet.microsoft.com/canitpro/2015/09/11/step-by-step-setting-up-ad-fs-and-enabling-single-sign-on-to-office-365/

Windows 2012 R2 AD FS Federated Web SSO example:
http://blogs.technet.com/b/platformspfe/archive/2014/08/28/part-1-windows-server-2012-r2-ad-fs-federated-web-sso.aspx

6. Load Balancing AD FS

> Note:
>
> It's highly recommended that you have a working AD FS environment first before implementing the load balancer. The initial environment would normally include a single Federation Server and a single Proxy Server. If the Federation Service Name was set to **adfs.lbtestdom.com** at initial deployment, additional Federation Servers can be added to the same farm, then DNS entries must be changed so that **adfs.lbtestdom.com** points to the VIP on the load balancer rather than the primary Federation Server.

BASIC CONCEPTS

To provide resilience and high availability for your AD FS infrastructure, multiple Federation Servers and multiple Federation Proxy Servers (WAP's in Windows 2012 & later) must be deployed with a load balancer. This helps ensure that users can be authenticated and obtain access to the required systems and applications by constantly checking the health of the AD FS servers and only forwarding client authentication requests to those that are functional.

LOAD BALANCED PORTS & SERVICES

The following table shows the ports that are load balanced:

Port	Protocols	Use
443	TCP/HTTPS	AD FS communications
49443	TCP	Used for certificate authentication in AD FS v3.0 and later Note: AD FS v4.0 also supports certificate authentication over port 443. To enable this, the SSL certificate must have the SAN **certauth.your_adfs_service_name** added. In this guide, **certauth.adfs.lbtestdom.com** is used. For more details on this, please refer to this URL. For more details on certificate authentication, please refer to this URL.

PERSISTENCE (SERVER AFFINITY) REQUIREMENTS & OPTIONS

As mentioned here, Microsoft do not recommend using source IP persistence (affinity) For AD FS. However, under certain complex scenario's such as the one mentioned here, persistence may be required for the Federation Server VIP.

> Note:
>
> Source IP persistence can easily be enabled by modifying the VIP, setting *Persistence Mode* to **Source IP**, clicking **Update** and reloading/restarting HAProxy.

SERVER HEALTH CHECKING

By default the load balancer uses a TCP port connect to verify the health of back-end servers. For AD FS we recommend that more comprehensive checks are used.

For AD FS v2.0, the load balancer is configured to look for specific content on the AD FS login page: **https://<server IP address>/adfs/ls/idpinitiatedsignon.aspx**

For AD FS v3.0 prior to update rollup KB2975719, the load balancer is configured to use a script to carry out an SNI based health check that looks for specific content on the AD FS login page: **https://<server IP address>/adfs/ls/idpinitiatedsignon.htm**

For AD FS v3.0 with update rollup KB2975719 and later, the load balancer is configured to look for a HTTP 200 OK response when the built-in probe URL is read: **http://<server IP address>/adfs/probe**

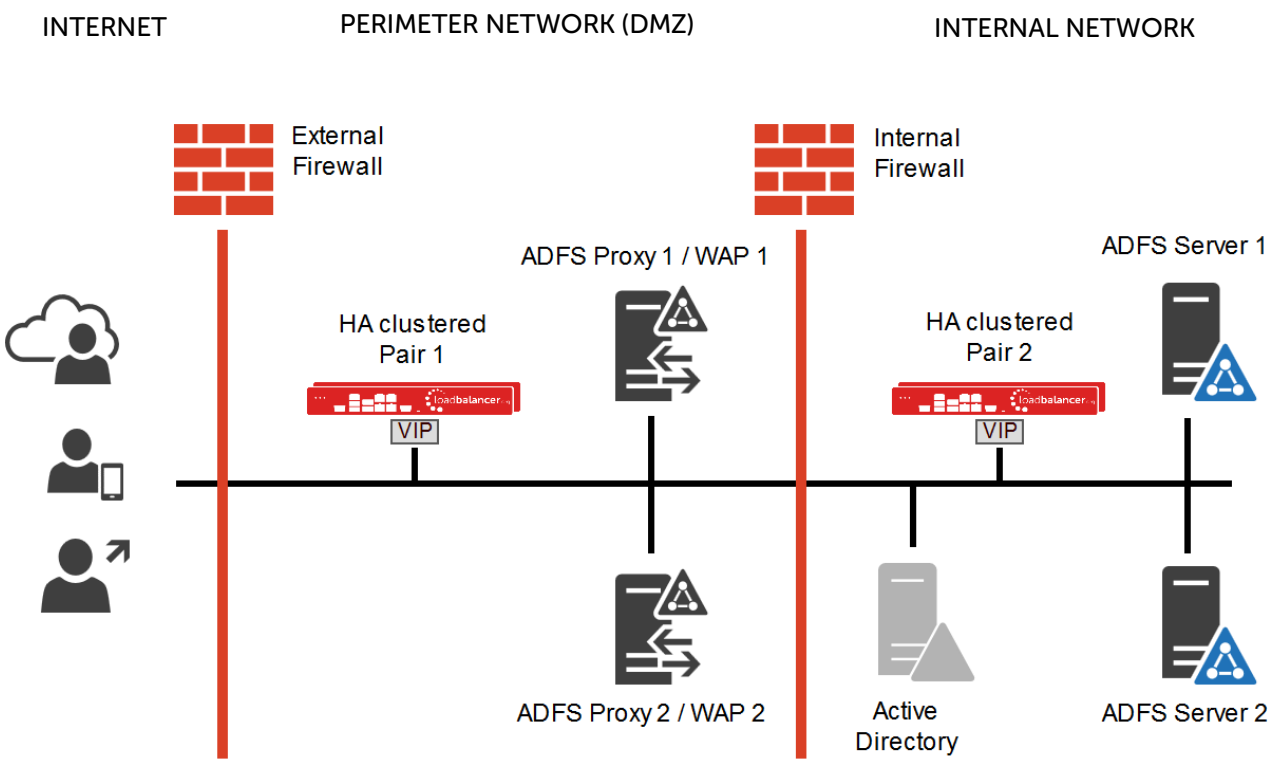
> Note:
>
> For more details about health-checks for Windows 2012 R2 please refer to this link.

SSL TERMINATION

As mentioned here, Microsoft state that SSL termination between the Proxy Servers and the Federation Servers is not supported and that SSL Termination between Client and Proxy is only supported under certain situations. For the configurations presented in this guide, SSL is terminated on the Federation & WAP servers and not the load balancer.

LOAD BALANCER DEPLOYMENT

The following diagram shows a typical load balanced AD FS deployment.



Notes:

- Load balancers can be deployed as single units or as a clustered pair. Loadbalancer.org always recommend deploying clustered pairs for HA and resilience.

- The Federation Proxy servers / WAP servers must be able to access the internal AD FS VIP on port 443 via the "Federation Service Name" specified during installation / configuration. Make sure that firewalls, routing and DNS are configured to allow this. In this guide, the Federation Service Name used is **adfs.lbtestdom.com**, so an entry for this is added to the local hosts file on each Federation Proxy Server / WAP server which resolves to the AD FS VIP on the internal LAN.

LOAD BALANCER DEPLOYMENT MODE

Layer 7 SNAT mode (HAProxy) is recommended for AD FS and is used for the configurations presented in this guide. This mode offers good performance and is simple to configure since it requires no configuration changes to the AD FS servers.

Layer 4 DR mode, NAT mode and SNAT mode can also be used if preferred. For DR mode you'll need to solve the ARP problem on each AD FS server (please see the Administration Manual and search for "DR mode considerations"), for NAT mode the default gateway of the AD FS servers must be the load balancer.

7. Loadbalancer.org Appliance – the Basics

VIRTUAL APPLIANCE DOWNLOAD & DEPLOYMENT

A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB virtual disk. The Virtual Appliance can be downloaded here.

> Note:
>
> The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance's WebUI.

> Note:
>
> Please refer to the Administration Manual and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

INITIAL NETWORK CONFIGURATION

The IP address, subnet mask, default gateway and DNS settings can be configured in several ways as detailed below:

Method 1 - Using the Network Setup Wizard at the console

After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

Method 2 - Using the WebUI

Using a browser, connect to the WebUI on the default IP address/port: **http://192.168.2.21:9080**

To set the IP address & subnet mask, use: *Local Configuration > Network Interface Configuration*

To set the default gateway, use: *Local Configuration > Routing*

To configure DNS settings, use: Local Configuration > Hostname & DNS

Method 3 - Using Linux commands

At the console, set the initial IP address using the following command:

```
ip addr add <IP address>/<mask> dev eth0
```

At the console, set the initial default gateway using the following command:

```
route add default gw <IP address> <interface>
```

At the console, set the DNS server using the following command:

```
echo nameserver <IP address> >> /etc/resolv.conf
```

> Note:
>
> If method 3 is used, you must also configure these settings using the WebUI, otherwise the settings will be lost after a reboot.

ACCESSING THE WEB USER INTERFACE (WEBUI)

The WebUI can be accessed via HTTP at the following URL: **http://192.168.2.21:9080/lbadmin**
** Note the port number → **9080***

The WebUI can be accessed via HTTPS at the following URL: **https://192.168.2.21:9443/lbadmin**
** Note the port number → **9443***

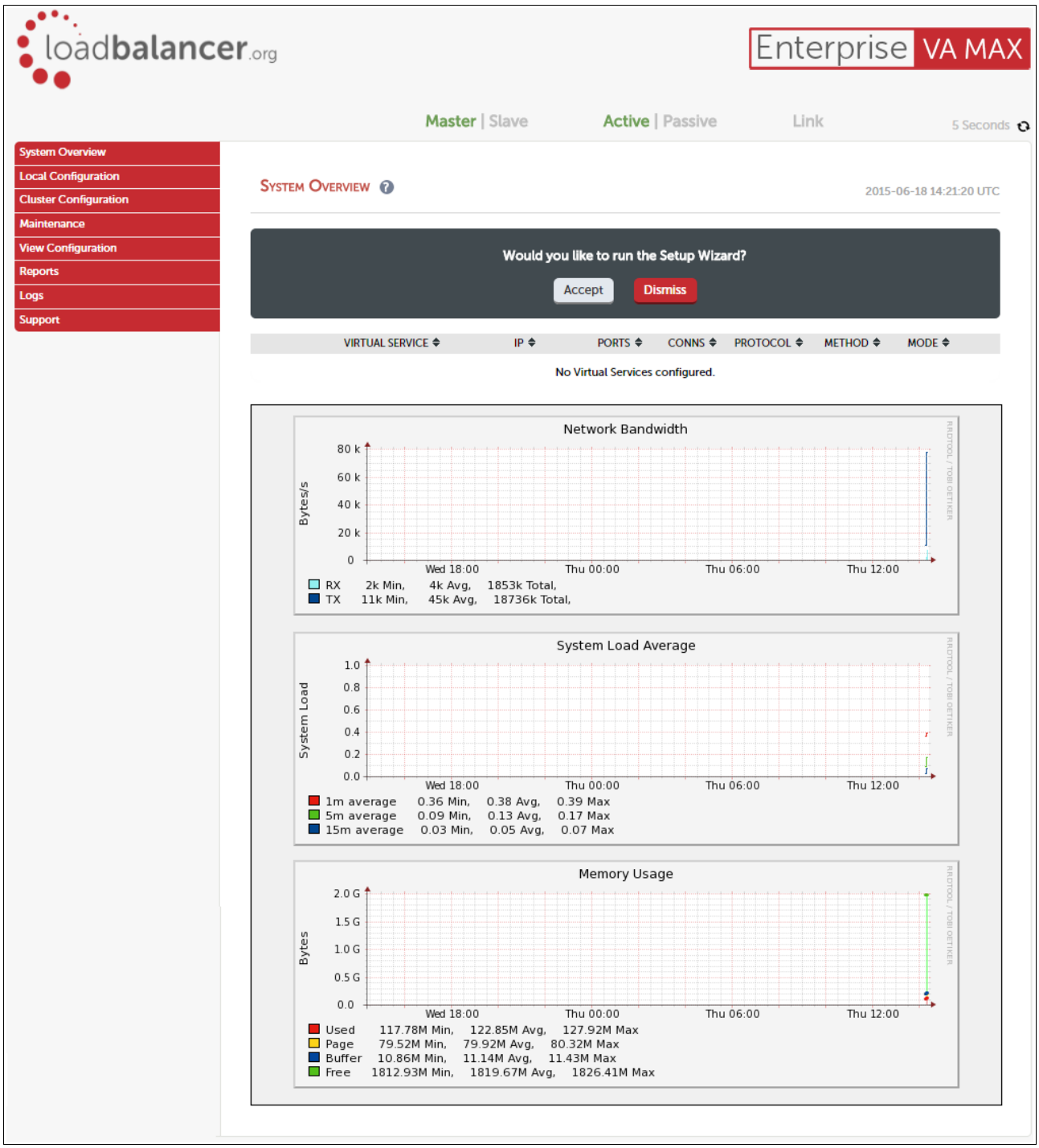
(replace 192.168.2.21 with the IP address of your load balancer if it's been changed from the default)

Login using the following credentials:

Username: loadbalancer
Password: loadbalancer

> Note:
>
> To change the password , use the WebUI menu option: *Maintenance > Passwords.*

Once logged in, the WebUI will be displayed as shown on the following page:



HA CLUSTERED PAIR CONFIGURATION

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix on page 29.

8. Server & Appliance Configuration - AD FS 2.0

FEDERATION SERVERS

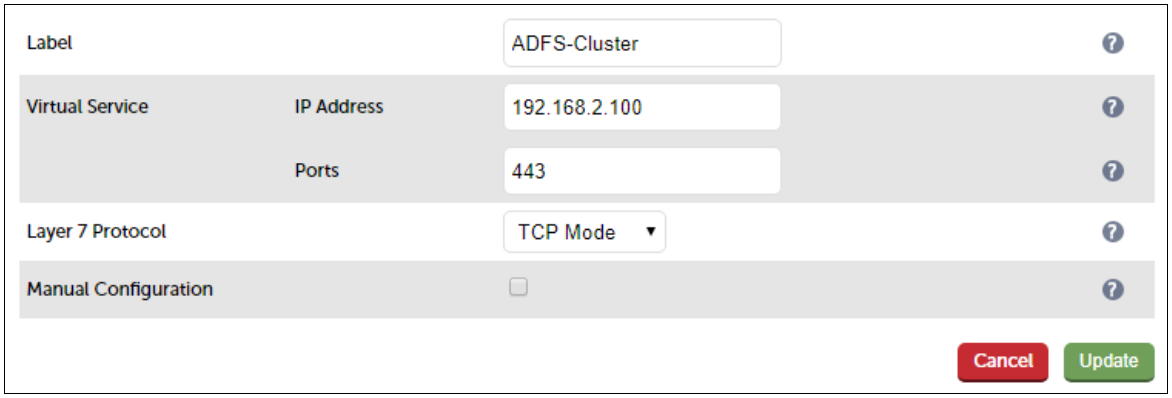
FEDERATION SERVER INSTALLATION & CONFIGURATION

- AD FS v2.0 for Windows 2008 R2 must be downloaded and installed manually on each AD FS server. If installed using Server Manager/Add Roles, v1.0 will be installed, NOT v2.0.
- AD FS v2.0 is available here
- AD FS update rollup 3 is available here
- For information on configuring the Federation Servers please refer to this URL

LOAD BALANCER CONFIGURATION

Setting up the Virtual Service (VIP)

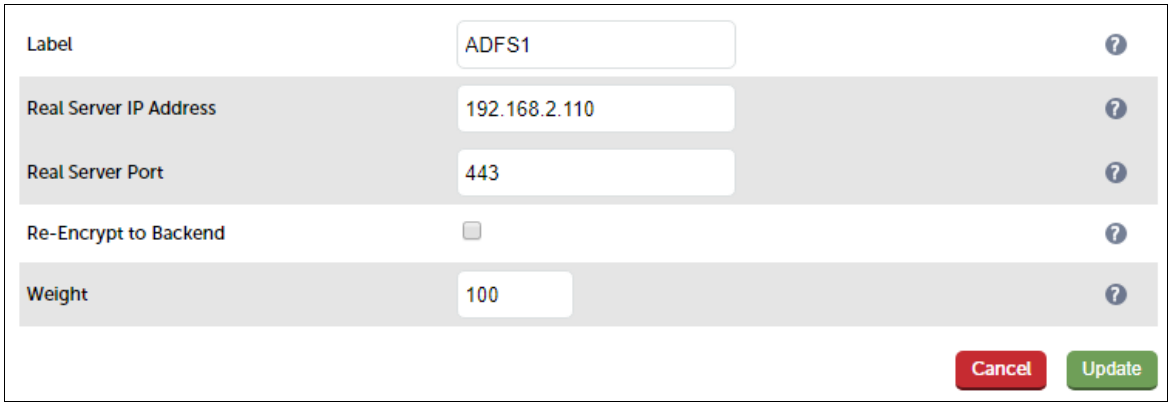
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**
2. Enter the following details:



3. Enter an appropriate name (Label) for the Virtual Service, e.g. **ADFS-Cluster**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.100**
5. Set the *Virtual Service Ports* field to **443**
6. Set *Layer 7 Protocol* to **TCP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created Virtual Service
9. Change *Persistence Mode* to **None**
10. Change *Health Checks* to **Negotiate HTTPS**
11. Set *Check Port* to **443**
12. Set *Request to Send* to **adfs/ls/idpinitiatedsignon.aspx**
13. Set *Response Expected* to **Sign-In**
14. Enable (check) the *Timeout* checkbox, set both *Client Timeout* and *Real Server Timeout* to **5m**
15. Click **Update**

Setting up the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service
2. Enter the following details:



3. Enter an appropriate name (Label) for the first AD FS server, e.g. **ADFS1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.110**
5. Set the *Real Server Port* field to **443**
6. Click **Update**
7. Now repeat for your remaining Federation server(s)

Applying the new Layer 7 Settings

1. Once the configuration is complete, use the **Restart/Reload HAProxy** button at the top of the screen to commit the changes, or use the WebUI option: *Maintenance > Restart Services*

DNS CONFIGURATION

Create a suitable DNS entry for the load balanced Federation Servers, i.e. for the VIP on the load balancer.

e.g. **adfs.lbtestdom.com**

TESTING & VERIFICATION

The load balanced AD FS servers should now be accessible using the DNS entry for the VIP. Connect to the login page from a browser.

e.g. **https://adfs.lbtestdom.com/adfs/ls/idpinitiatedsignon.aspx**

FEDERATION PROXY SERVERS

PROXY SERVER INSTALLATION & CONFIGURATION

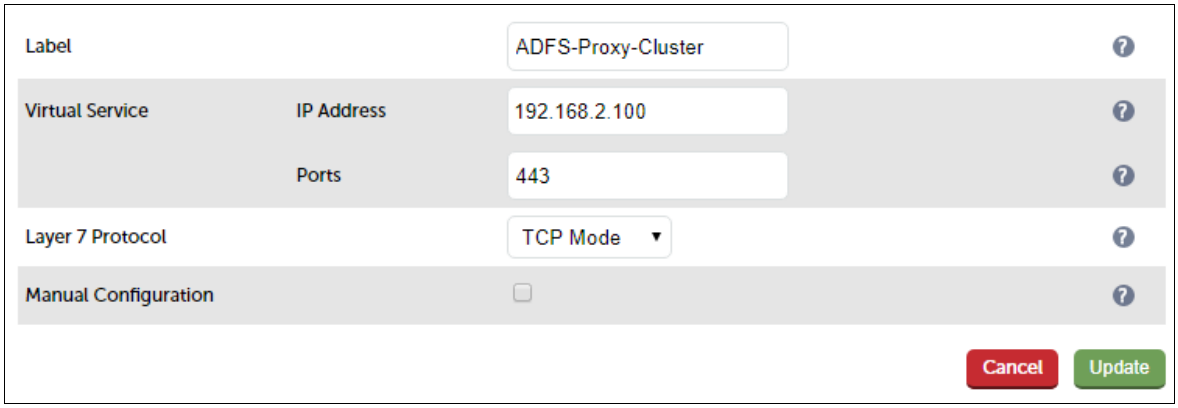
- AD FS v2.0 for Windows 2008 R2 must be downloaded and installed manually on each AD FS Proxy Server. If installed using Server Manager/Add Roles, v1.0 will be installed, NOT v2.0.
- AD FS v2.0 is available here.
- AD FS update rollup 3 is available here.

- When running the wizard, the Federation Service Name should be the load balanced VIP of the Federation Servers.
- For information on configuring the Proxy Servers please refer to this URL.
- The Federation Proxy servers must be able to access the internal AD FS VIP on port 443 via the "Federation Service Name" specified during installation / configuration. Make sure that firewalls, routing and DNS are configured to allow this. In this guide, the Federation Service Name used is **adfs.lbtestdom.com**, so an entry for this is added to the local hosts file on each Federation Proxy Server which resolves to the AD FS VIP on the internal LAN.

LOAD BALANCER CONFIGURATION

Setting up the Virtual Service (VIP)

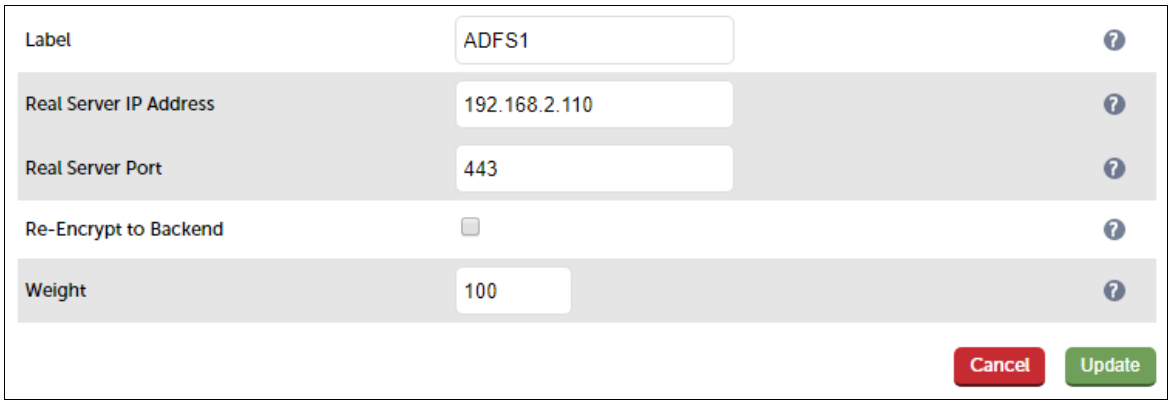
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**
2. Enter the following details:



3. Enter an appropriate name (Label) for the Virtual Service, e.g. **ADFS-Proxy-Cluster**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.100**
5. Set the *Virtual Service Ports* field to **443**
6. Set the *Layer 7 Protocol* to **TCP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created Virtual Service
9. Change *Persistence Mode* to **None**
10. Change *Health Checks* to **Negotiate HTTPS**
11. Set *Check Port* to **443**
12. Set *Request to Send* to **adfs/ls/idpinitiatedsignon.aspx**
13. Set *Response Expected* to **Sign-In**
14. Enable (check) the *Timeout* checkbox, set both *Client Timeout* and *Real Server Timeout* to **5m**
15. Click **Update**

Setting up the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service
2. Enter the following details:



3. Enter an appropriate name (Label) for the first AD FS server, e.g. **ADFS1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.110**
5. Set the *Real Server Port* field to **443**
6. Click **Update**
7. Now repeat for your remaining Federation Proxy server(s)

Applying the new Layer 7 Settings

1. Once the configuration is complete, use the **Restart/Reload HAProxy** button at the top of the screen to commit the changes, or use the WebUI option: *Maintenance > Restart Services*

DNS CONFIGURATION

Create a suitable DNS entry for the load balanced Proxy Servers, i.e. for the VIP on the load balancer.

e.g. **adfs.robstest.com**

TESTING & VERIFICATION

The load balanced AD FS servers should now be accessible using the DNS entry for the VIP. Connect to the login page from a browser.

e.g. **https://adfs.robstest.com/adfs/ls/idpinitiatedsignon.aspx**

9. Server & Appliance Configuration - AD FS 3.0 / 4.0

FEDERATION SERVERS

FEDERATION SERVER INSTALLATION & CONFIGURATION

The key points of the installation process are covered below. For more details, please also refer to the following Microsoft URL's:

- How to Build Your AD FS Lab
- How To Install AD FS 2016 For Office 365

STEP 1 – Prepare AD FS Certificates

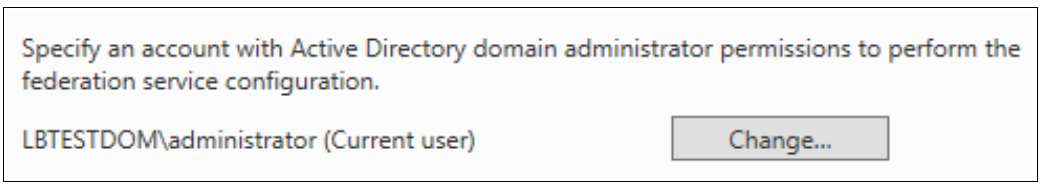
In this guide an Internal CA was used to issue the certificate. As mentioned here the Private Key must be exportable so that the certificate and private key can be exported from the first Federation Server, and used on other Federation Servers and on the WAP's.

> Note:
>
> In this guide, the Common Name is set to **adfs.lbtestdom.com**. As mentioned on page 9, for AD FS v4.0 and later, an additional SAN can be added (**certuth.adfs.lbtestdom.com**) to allow certificate authentication over port 443. It this is not done, certificate authentication occurs over TCP 49443. In this scenario, port 49443 must be included in the VIP.
>
> The following warning is displayed for AD FS v4.0+ if the additional SAN is not included:
>
> ⚠ The SSL certificate subject alternative names do not support host name 'certauth.adfs.lbtestdom.com'. Configuring certificate authentication binding on port '49443' and hostname 'adfs.lbtestdom.com'.

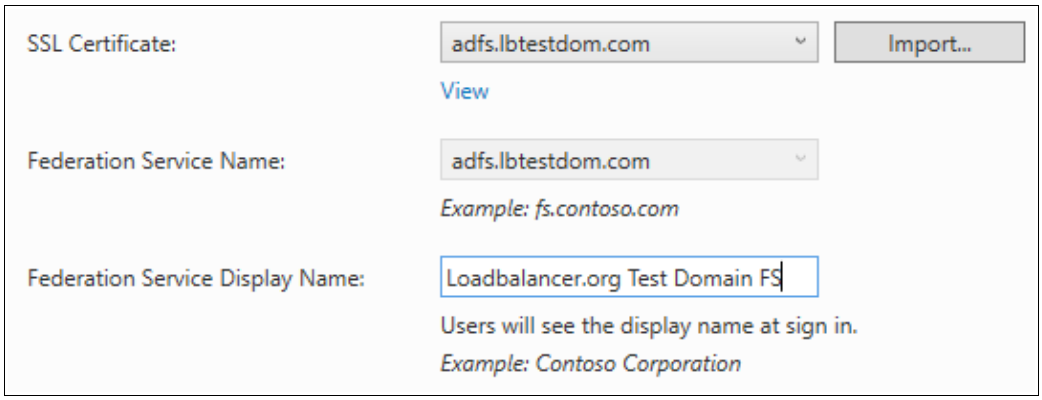
STEP 2 – Install AD FS on the first (Primary) Federation Server

Use *Server Manager > Add Roles and Features* to install AD FS, then run the Configuration Wizard:

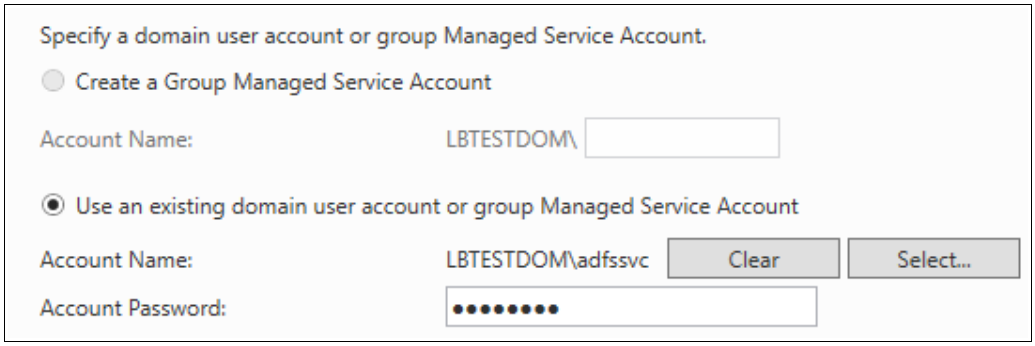
Select *Create the first federation server in federation server farm* and click **Next**



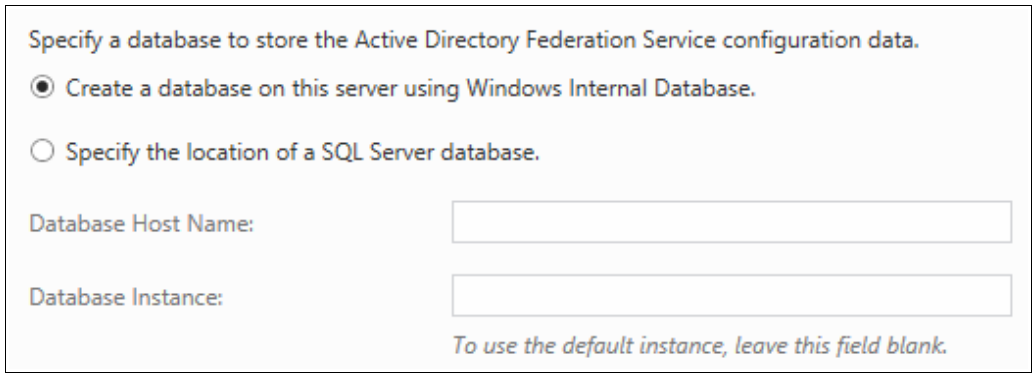
Specify a suitable account and click **Next**



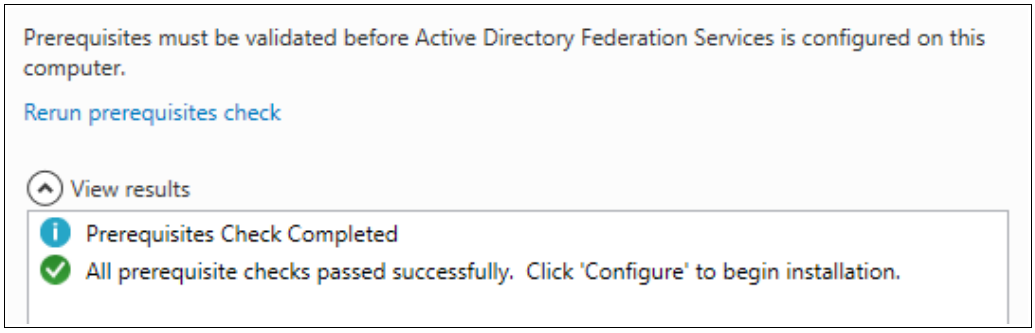
Choose the certificate created in Step 1, enter a display name and click **Next**



Choose a suitable service account and click **Next**



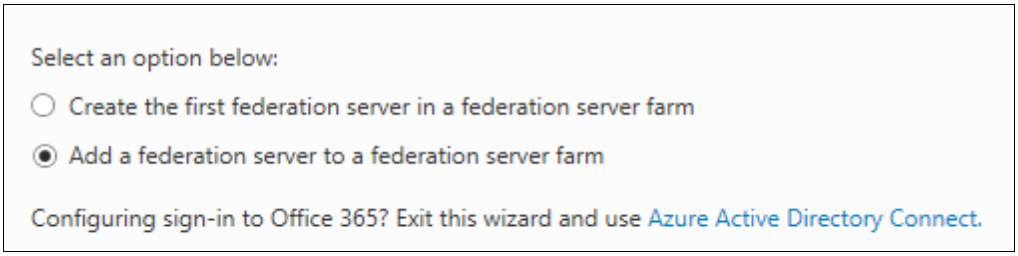
Choose where configuration data will be stored and click **Next**



As mentioned, click **Configure** to begin the installation

STEP 3 – Install AD FS on the remaining Federation Server(s)

Use *Server Manager > Add Roles and Features* to install AD FS, then run the Configuration Wizard:

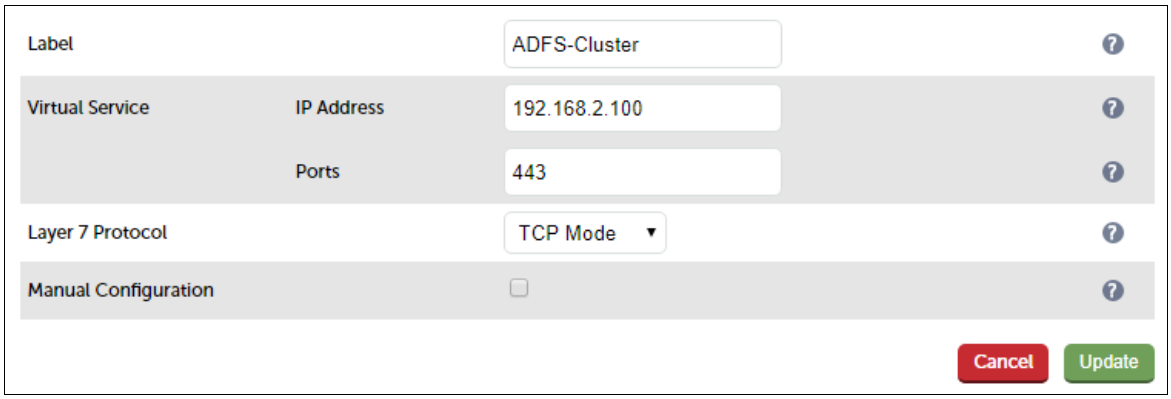


In this case, select *Add a federation server to the federation server farm* and click **Next** , then continue through the remaining screens until the installation & configuration is complete.

LOAD BALANCER CONFIGURATION

Setting up the Virtual Service (VIP)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**
2. Enter the following details:



3. Enter an appropriate name (Label) for the Virtual Service, e.g. **ADFS-Cluster**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.100**
5. Set the *Virtual Service Ports* field to **443**

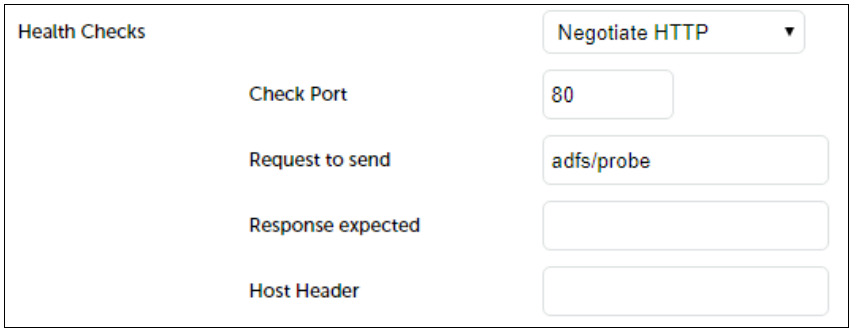
> Note:
>
> If you don't have the SAN **certauth.your_adfs_service_name** added to your SSL certificate, make sure port 49443 is also included in the VIP, i.e. set the *Virtual Service Ports* field to: **443, 49443** rather than: **443**

6. Set the *Layer 7 Protocol* to **TCP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created Virtual Service
9. Enable (check) the *Timeout* checkbox, set both *Client Timeout* and *Real Server Timeout* to **5m**
10. Click **Update**

Configure the Health-check for Windows 2012 R2 with KB2975719 & Later

> Note:
>
> Update rollup KB2975719 was released in August 2014, so the health-check configuration presented in this section should be used in most if not all cases.

1. Click **Modify** next to the newly created Virtual Service
2. Configure the health check settings as shown below, this will configure the load balancer to look for an **HTTP 200 OK** response from each server:



   - Change *Health Checks* to **Negotiate HTTP**
   - Set *Check Port* to **80**
   - Set *Request to send* to **adfs/probe**
   - Leave *Response Expected* blank

3. Click **Update**

Configure the Health-check for Windows 2012 R2 prior to KB2975719

The **adfs/probe** option above does not exist in older versions of Windows. In this case, the load balancer's built-in SNI check must be used instead as described below:

1. Edit the file: **/var/lib/loadbalancer.org/check/sni-check-v2.sh**

   This can be done using an editor on the appliance such as **vim** or **vi** if you're familiar with Linux or by using the built-in editor available in **WinSCP**. **WinSCP** is a free Windows utility that enables files in a Linux filesystem to be easily created, viewed and modified from a Windows PC/server. It's available here: http://winscp.net/eng/download.php

   Set the SNI host and URI parameters at the top of the file to the required values, e.g.

   SNI_HOST="adfs.lbtestdom.com"
   SNI_URI="adfs/ls/idpinitiatedsignon.htm"

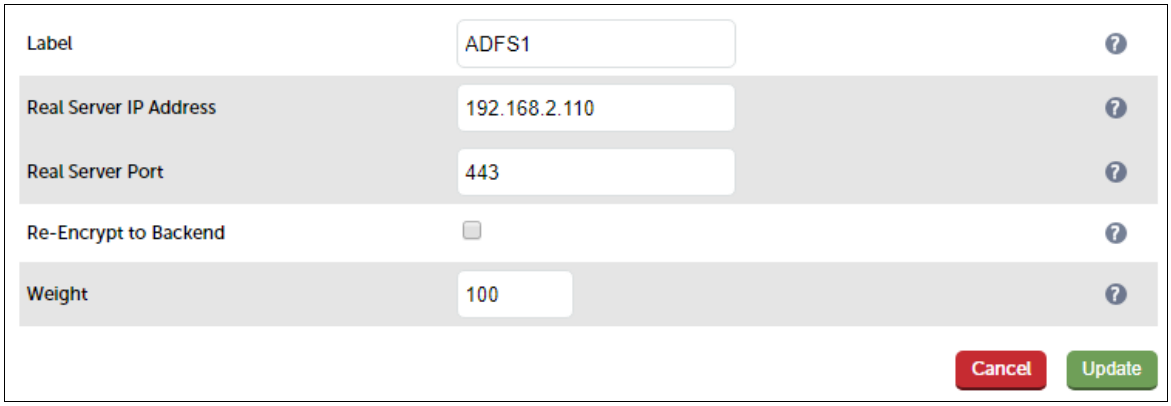
   > Note:
   >
   > This SNI URI is the default AD FS sign-in URI and should not normally need changing.

2. Save the file
3. Now click **Modify** next to the newly created Virtual Service

4. Change *Health Checks* to **External Check**
5. Change *Check Script* to **sni-check-v2.sh**
6. Click **Update**

Setting up the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service
2. Enter the following details:



3. Enter an appropriate name (Label) for the first AD FS server, e.g. **ADFS1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.110**
5. Set the *Real Server Port* field to **443**

> Note:
>
> If you included port 49443 in the VIP, leave the *Real Server Port* field blank.

6. Click **Update**
7. Now repeat for your remaining Federation server(s)

Applying the new Layer 7 Settings

1. Once the configuration is complete, use the **Restart/Reload HAProxy** button at the top of the screen to commit the changes, or use the WebUI option: *Maintenance > Restart Services*

DNS CONFIGURATION

Create a suitable DNS entry for the load balanced AD FS servers, i.e. for the VIP on the load balancer.

e.g. **adfs.lbtestdom.com**

If your SSL certificate includes the additional SAN for certificate authentication, you'll also need a suitable DNS entry for this.

e.g. **certauth.adfs.lbtestdom.com**

TESTING & VERIFICATION

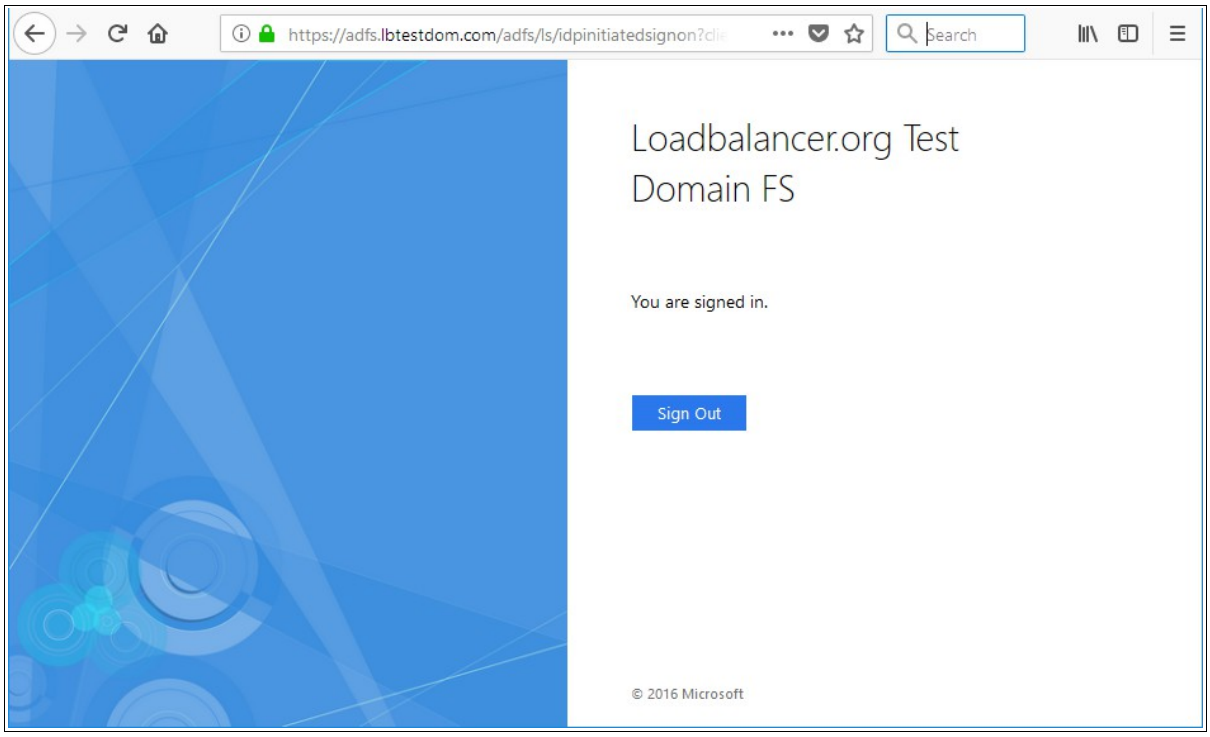
The load balanced AD FS servers should now be accessible using the DNS entry for the VIP. Connect to

the login page from a browser.

e.g. **https://adfs.robstest.com/adfs/ls/idpinitiatedsignon.htm**

> Note:
>
> As mentioned here, the Sign In page is disabled by default in AD FS 2016 (AD FS v4.0) and later. To manually enable it, use the following PowerShell command on the Primary Federation Server:
>
> ```
> Set-AdfsProperties -EnableIdPInitiatedSignonPage $true
> ```

Login as prompted. Once logged in, your browser should display something similar to the following:



WEB APPLICATION PROXY (WAP) SERVERS

WAP SERVER INSTALLATION & CONFIGURATION

The key points of the installation process are covered below. For more details, please also refer to the following Microsoft URL's:

- How to Build Your AD FS Lab
- How To Install AD FS 2016 For Office 365

> Note:
>
> The WAP servers must be able to access the internal AD FS VIP on port 443 via the "Federation Service Name" specified during installation / configuration. Make sure that firewalls, routing and DNS are configured to allow this. In this guide, the Federation Service Name used is **adfs.lbtestdom.com**, so an entry for this is added to the local hosts file on each WAP server

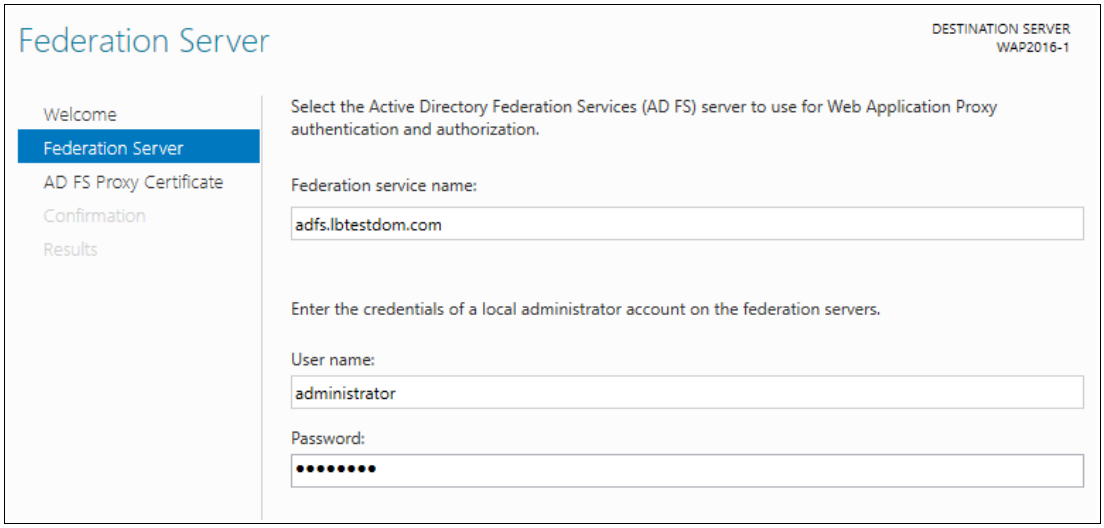
> which resolves to the AD FS VIP on the internal LAN.

STEP 1 – Prepare the SSL Certificate

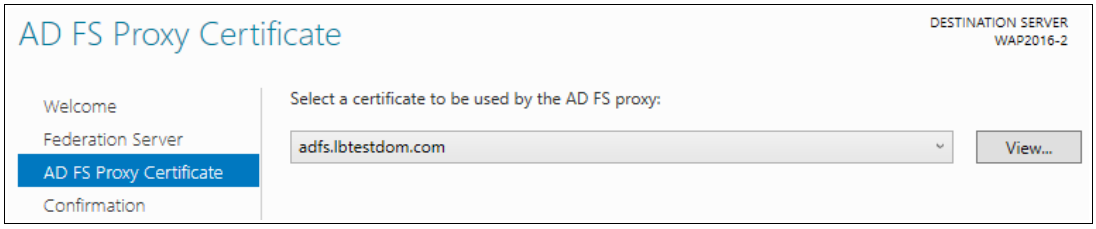
Export the certificate & private key from one of the Federation Servers, then import the certificate into the local computer account certificate store on each WAP server. This will ensure the certificate is ready to use when the configuration wizard is run.

STEP 2 – Install & Configure Web Application Proxy (WAP) on the each WAP Server

Use *Server Manager > Add Roles and Features* to install Web Application Proxy, then run the Configuration Wizard:



Enter the *Federation service name* and the user credentials and click **Next**

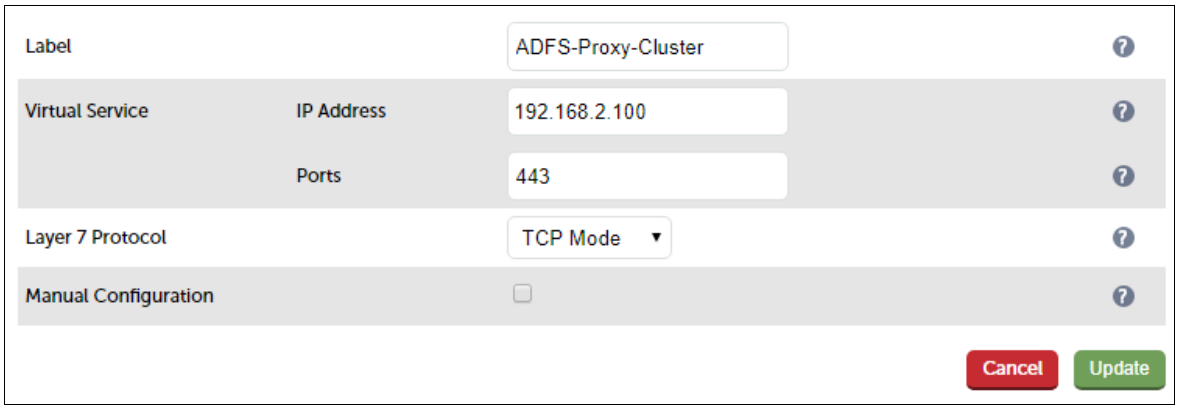


Select the certificate to be used by the Proxy and click **Next**, then click **Configure** to start the configuration

LOAD BALANCER CONFIGURATION

Setting up the Virtual Service (VIP)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**
2. Enter the following details:



3. Enter an appropriate name (Label) for the Virtual Service, e.g. **ADFS-Proxy-Cluster**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.100**
5. Set the *Virtual Service Ports* field to **443**

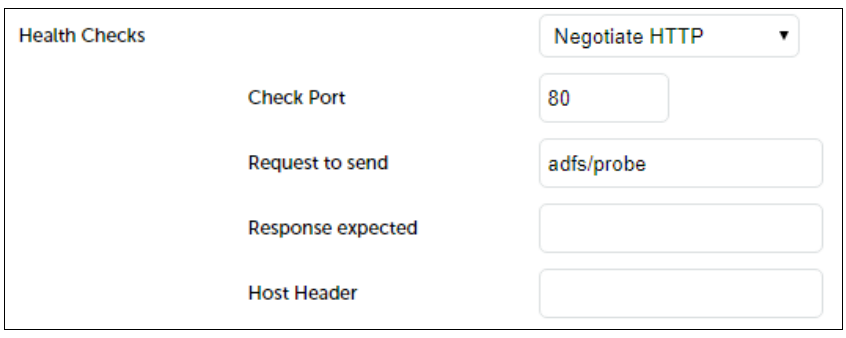
> Note:
>
> If you don't have the SAN **certauth.your_adfs_service_name** added to your SSL certificate, make sure port 49443 is also included in the VIP, i.e. set the *Virtual Service Ports* field to: **443, 49443** rather than: **443**

6. Set the *Layer 7 Protocol* to **TCP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created Virtual Service
9. Enable (check) the *Timeout* checkbox, set both *Client Timeout* and *Real Server Timeout* to **5m**
10. Click **Update**

Configure the Health-check for Windows 2012 R2 with KB2975719 & Later

> Note:
>
> Update rollup KB2975719 was released in August 2014, so the health-check configuration presented in this section should be used in most if not all cases.

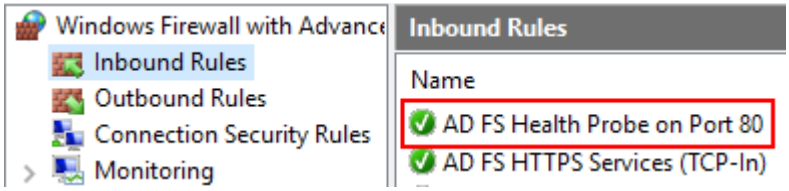
1. Click **Modify** next to the newly created Virtual Service
2. Configure the health check settings as shown below, this will configure the load balancer to look for an **HTTP 200 OK** response from each server:



- Change *Health Checks* to **Negotiate HTTP**

- Set *Check Port* to **80**
- Set *Request to send* to **adfs/probe**
- Leave *Response Expected* blank

> Note:
>
> As mentioned here, you'll need to create an inbound rule to open port 80 on the firewall of each WAP server for this health-check to work. For the Federation servers this is configured automatically, but not for the WAP's.



3. Click **Update**

Configure the Health-check for Windows 2012 R2 prior to KB2975719

The **adfs/probe** option above does not exist in older versions of AD FS. In this case, the load balancer's built-in SNI check must be used instead as described below:

1. Modify the file: **/var/lib/loadbalancer.org/check/sni-check-v2.sh**

   This can be done using an editor on the appliance such as **vim** or **vi** if you're familiar with Linux or by using the built-in editor available in **WinSCP**. **WinSCP** is a free Windows utility that enables files in a Linux filesystem to be easily created, viewed and modified from a Windows PC/server. It's available here: **http://winscp.net/eng/download.php**

   Set the SNI host and URI parameters at the top of the file to the required values, e.g.

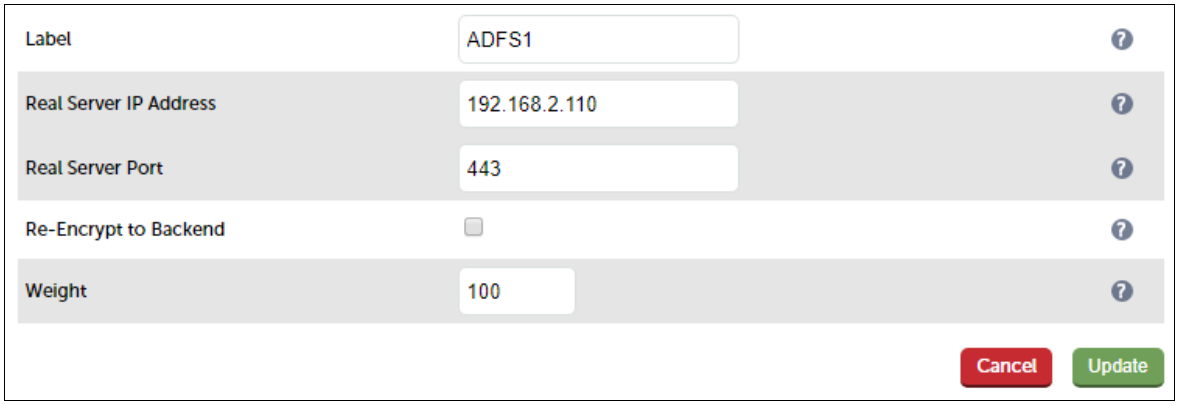
   SNI_HOST="adfs.lbtestdom.com"
   SNI_URI="adfs/ls/idpinitiatedsignon.htm"

   > Note:
   >
   > This SNI URI is the default AD FS sign-in URI and should not normally need changing.

2. Save the file
3. Now click **Modify** next to the newly created Virtual Service
4. Change *Health Checks* to **External Check**
5. Change *Check Script* to **sni-check-v2.sh**
6. Click **Update**

Setting up the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service
2. Enter the following details:



3. Enter an appropriate name (Label) for the first AD FS server, e.g. **ADFS1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.110**
5. Set the *Real Server Port* field to **443**

> Note:
>
> If you included port 49443 in the VIP, leave the *Real Server Port* field blank.

6. Click **Update**
7. Now repeat for your remaining WAP server(s)

Applying the new Layer 7 Settings

1. Once the configuration is complete, use the **Restart/Reload HAProxy** button at the top of the screen to commit the changes, or use the WebUI option: *Maintenance > Restart Services*

DNS CONFIGURATION

Create a suitable DNS entry for the load balanced AD FS servers, i.e. for the VIP on the load balancer.

e.g. **adfs.lbtestdom.com**

If your SSL certificate includes the additional SAN for certificate authentication, you'll also need a suitable DNS entry for this.

e.g. **certauth.adfs.lbtestdom.com**

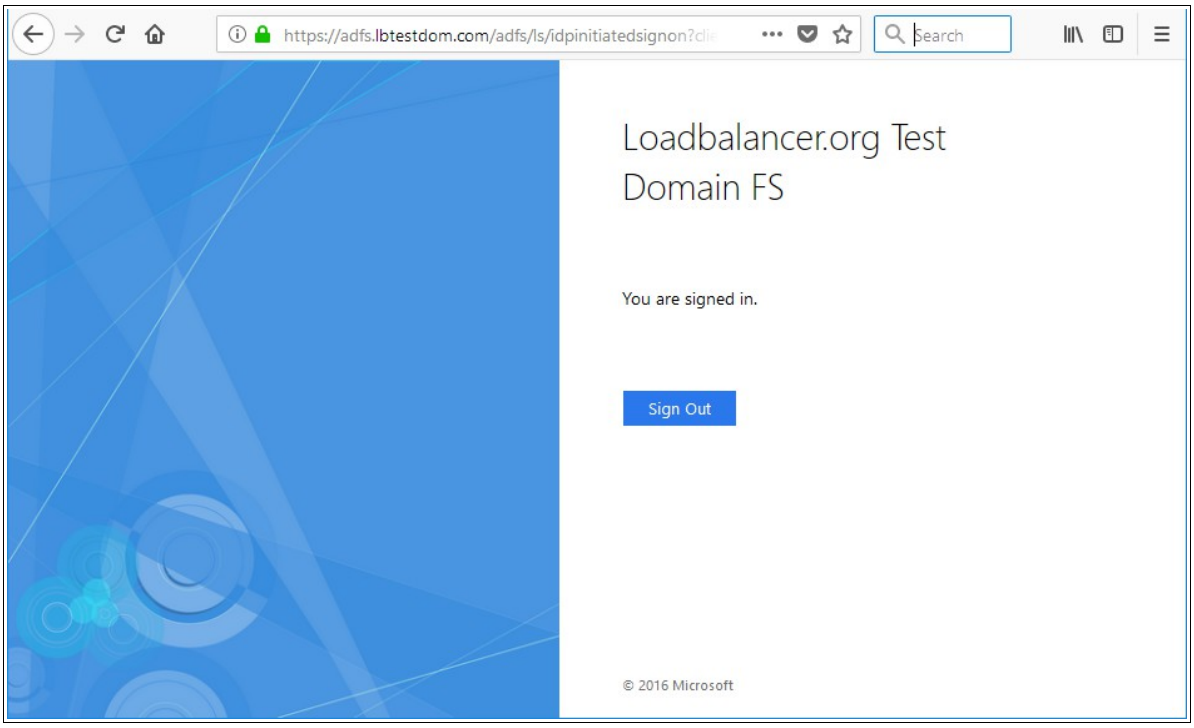
> Note:
>
> The WAP servers must be able to access the internal AD FS VIP on port 443 via the "Federation Service Name" specified during installation / configuration. Make sure that firewalls, routing and DNS are configured to allow this. In this guide, the Federation Service Name used is **adfs.lbtestdom.com**, so an entry for this is added to the local hosts file on each WAP server which resolves to the AD FS VIP on the internal LAN.

TESTING & VERIFICATION

The load balanced AD FS servers should now be accessible using the DNS entry for the VIP. Connect to the login page from a browser.

e.g. **https://adfs.robstest.com/adfs/ls/idpinitiatedsignon.htm**

Login as prompted. Once logged in, your browser should display something similar to the following:



10. Technical Support

If you have any questions regarding the appliance or would like assistance designing your deployment, please don't hesitate to contact our support team: support@loadbalancer.org.

11. Further Documentation

The Administration Manual contains much more information about configuring and deploying the appliance. It's available here: http://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf

12. Conclusion

Loadbalancer.org appliances provide a very cost effective and flexible solution for highly available load balanced Active Directory Federation Services environments.

13. Appendix

1 - CLUSTERED PAIR CONFIGURATION – ADDING A SLAVE UNIT

If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant section below for more details:

> Note:
>
> A number of settings are not replicated as part of the master/slave pairing process and therefore must be manually configured on the slave appliance. These are listed below:
>
> - Hostname & DNS settings
> - Network settings including IP addresses, bonding configuration and VLANs
> - Routing configuration including default gateways and static routes
> - Date & time settings
> - Physical – Advanced Configuration settings including Internet Proxy IP address & port, Firewall table size, SMTP relay and Syslog server
> - SNMP settings
> - Graphing settings
> - Firewall Script & Firewall Lockdown Script settings
> - Software updates

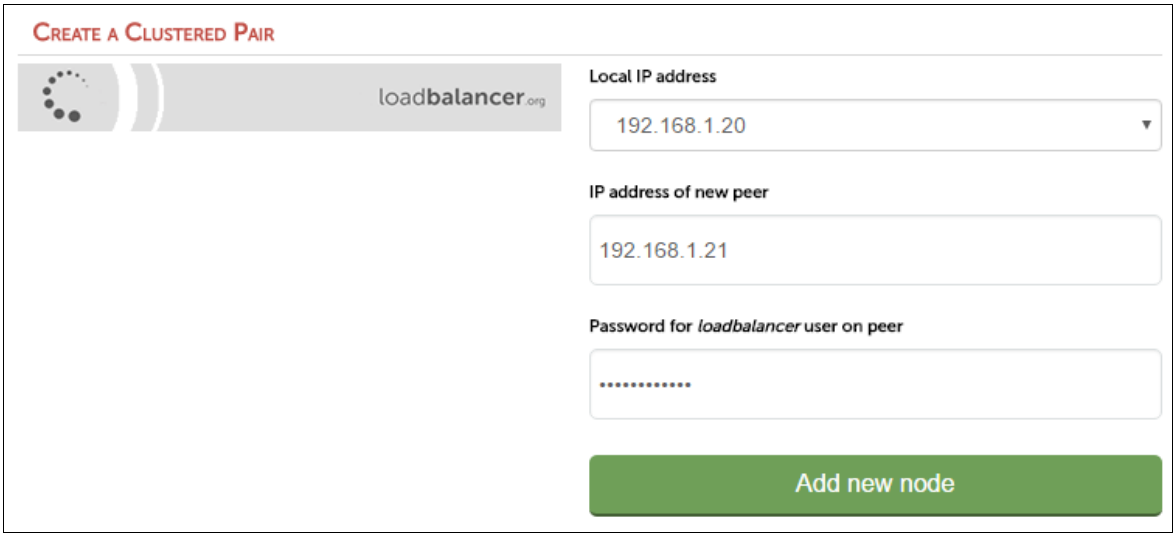
Version 7:

Please refer to **Chapter 8 – Appliance Clustering for HA** in the v7 Administration Manual.

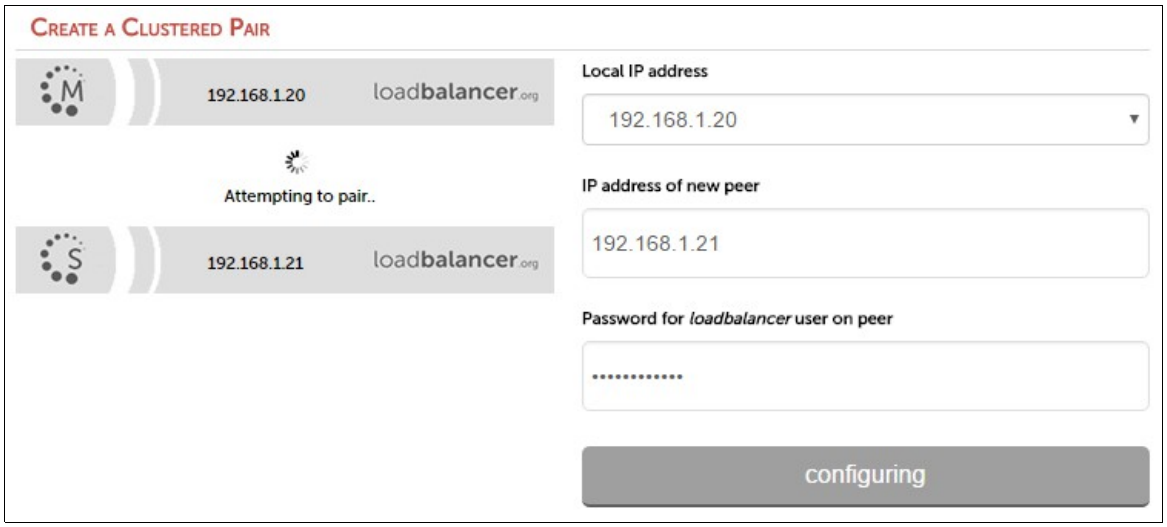
Version 8:

To add a slave node – i.e. create a highly available clustered pair:

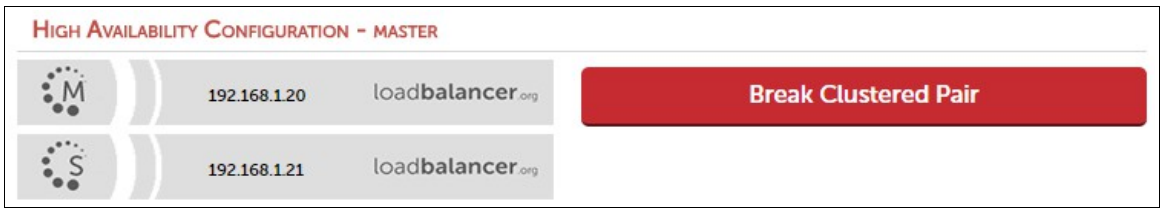
- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: *Cluster Configuration > High-Availability Configuration*



- Specify the IP address and the *loadbalancer* users password (the default is 'loadbalancer') for the slave (peer) appliance as shown above
- Click **Add new node**
- The pairing process now commences as shown below:



- Once complete, the following will be displayed:



- To finalize the configuration, restart heartbeat and any other services as prompted in the blue message box at the top of the screen

> Note:
>
> Clicking the **Restart Heartbeat** button on the master appliance will also automatically restart heartbeat on the slave appliance.

> Note:
>
> Please refer to chapter 9 – Appliance Clustering for HA in the Administration Manual for more detailed information on configuring HA with 2 appliances.

2 - COMPANY CONTACT INFORMATION

Website	URL: www.loadbalancer.org
North America (US)	Loadbalancer.org, Inc. 4250 Lancaster Pike, Suite 120 Wilmington DE 19805 USA Tel: +1 888.867.9504 Fax: +1 302.213.0122 Email (sales): sales@loadbalancer.org Email (support): support@loadbalancer.org
North America (Canada)	Loadbalancer.org Ltd 300-422 Richards Street Vancouver, BC V6B 2Z4 Canada Tel: +1 866.998.0508 Fax: +1 302.213.0122 Email (sales): sales@loadbalancer.org Email (support): support@loadbalancer.org
Europe (UK)	Loadbalancer.org Ltd. Compass House North Harbour Business Park Portsmouth, PO6 4PS UK Tel: +44 (0)330 3801064 Fax: +44 (0)870 4327672 Email (sales): sales@loadbalancer.org Email (support): support@loadbalancer.org
Europe (Germany)	Loadbalancer.org GmbH Tengstraße 27 D-80798 München Germany Tel: +49 (0)89 2000 2179 Fax: +49 (0)30 920 383 6495 Email (sales): vertrieb@loadbalancer.org Email (support): support@loadbalancer.org