Load Balancing
Microsoft AD FS

Deployment Guide
v1.4.0
# Contents

1. About this Guide .......................................................................................................................... 4
2. Loadbalancer.org Appliances Supported .................................................................................. 4
3. Loadbalancer.org Software Versions Supported ......................................................................... 4
4. Microsoft Windows Versions Supported ................................................................................... 4
5. Active Directory Federation Services (AD FS) ........................................................................... 4
   
   Introduction ................................................................................................................................. 5
   AD FS SSO Scenarios ..................................................................................................................... 5
   Web SSO ....................................................................................................................................... 5
   Federated Web SSO ....................................................................................................................... 5
   AD FS Versions .............................................................................................................................. 5
   Role Services ................................................................................................................................ 6
   How AD FS Works ....................................................................................................................... 6
   Internal Clients ............................................................................................................................. 6
   External Clients ............................................................................................................................. 7
   Other Useful References .............................................................................................................. 8

6. Load Balancing AD FS .............................................................................................................. 9
   Basic Concepts ............................................................................................................................ 9
   Load Balanced Ports & Services .................................................................................................. 9
   Persistence (Server Affinity) Requirements & Options ............................................................... 9
   Server Health checking ................................................................................................................ 10
   SSL Termination .......................................................................................................................... 10
   Load Balancer Deployment ......................................................................................................... 10
   Load Balancer Deployment Mode .............................................................................................. 11

7. Loadbalancer.org Appliance – the Basics ................................................................................. 11
   Virtual Appliance Download & Deployment .............................................................................. 11
   Initial Network Configuration ...................................................................................................... 11
   Accessing the Web User Interface (WebUI) ................................................................................. 12
   HA Clustered Pair Configuration ............................................................................................... 13

8. Server & Appliance Configuration - AD FS 2.0 ......................................................................... 14
   Federation Servers ....................................................................................................................... 14
   Federation Server Installation & Configuration ........................................................................... 14
   Load Balancer Configuration ....................................................................................................... 14
   DNS Configuration ....................................................................................................................... 15
   Testing & Verification .................................................................................................................. 15
   Federation Proxy Servers ............................................................................................................ 16
   Proxy Server Installation & Configuration .................................................................................. 16
   Load Balancer Configuration ....................................................................................................... 16
   DNS Configuration ....................................................................................................................... 17
   Testing & Verification .................................................................................................................. 17

9. Server & Appliance Configuration - AD FS 3.0 / 4.0 / 5.0 .......................................................... 18
   Federation Servers ....................................................................................................................... 18
   Federation Server Installation & Configuration ........................................................................... 18
   Load Balancer Configuration ....................................................................................................... 20
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:

<table>
<thead>
<tr>
<th>Discontinued Models</th>
<th>Current Models *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise R16</td>
<td>Enterprise R20</td>
</tr>
<tr>
<td>Enterprise VA R16</td>
<td>Enterprise MAX</td>
</tr>
<tr>
<td>Enterprise VA</td>
<td>Enterprise 10G</td>
</tr>
<tr>
<td>Enterprise R320</td>
<td>Enterprise 40G</td>
</tr>
<tr>
<td></td>
<td>Enterprise Ultra</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA R20</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</td>
</tr>
<tr>
<td></td>
<td>Enterprise AWS</td>
</tr>
<tr>
<td></td>
<td>Enterprise AZURE **</td>
</tr>
</tbody>
</table>

* 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 Scenarios

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:

<table>
<thead>
<tr>
<th>AD FS Version</th>
<th>Released in Windows Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1.0</td>
<td>2003 R2</td>
</tr>
<tr>
<td>v1.1</td>
<td>2008</td>
</tr>
</tbody>
</table>

© Copyright Loadbalancer.org - www.loadbalancer.org - sales@loadbalancer.org
Role Services
The following role services can be deployed as part of the AD FS role:

<table>
<thead>
<tr>
<th>Role Service</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federation Server</td>
<td>Acts as an identity provider - Authenticates users to provide security tokens to applications that trust AD FS</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>Acts as a federation provider - Consumes tokens from other identity providers and then provides security tokens to applications that trust AD FS</td>
</tr>
<tr>
<td>Federation Server Proxy / Web Application Proxy</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In Windows 2012 R2 and later, the dedicated Proxy role service has been removed. Instead, the proxy is based on WAP (Web Application Proxy).</td>
</tr>
</tbody>
</table>

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:

![Authentication Process Diagram]

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:

Setting up AD FS and Enabling Single Sign-On to Office 365:

Windows 2012 R2 AD FS Federated Web SSO example:
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 (WAPs 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:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP/HTTPS</td>
<td>AD FS communications</td>
</tr>
<tr>
<td>49443</td>
<td>TCP</td>
<td>Used for certificate authentication in AD FS v3.0 and later</td>
</tr>
</tbody>
</table>

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 scenarios 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: \texttt{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: \texttt{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: \texttt{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: https://192.168.2.21:9443
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

Accessing the Web User Interface (WebUI)

1. Browse to the following URL: https://192.168.2.21:9443/lbadmin/
   (replace with your IP address if it's been changed)
   * Note the port number → 9443

2. Login to the WebUI:

   **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 below:
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 31.
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:
   
   ![Virtual Service Configuration](#)
   
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:

   ![Real Server Configuration Table](image)

   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.robtest.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.
9. Server & Appliance Configuration - AD FS 3.0 / 4.0 / 5.0

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 URs:

- 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 WAPs.

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. If 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:

![Warning]

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:
Welcome to the Active Directory Federation Services Configuration Wizard.

Before you begin configuration, you must have the following:

- An Active Directory domain administrator account.
- A publicly trusted certificate for SSL server authentication.

**AD FS prerequisites**

Select an option below:

- Create the first federation server in a federation server farm
- Add a federation server to a federation server farm

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

Specify an account with Active Directory domain administrator permissions to perform the federation service configuration.

**LBTESTDOM\administrator (Current user)**

Specify a suitable account and click **Next**

**SSL Certificate:**

**Federation Service Name:**

**Federation Service Display Name:**

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

**Specify a domain user account or group Managed Service Account.**

**Create a Group Managed Service Account**

**Account Name:**

**Use an existing domain user account or group Managed Service Account**

**Account Name:**

**Account Password:**
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:
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](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:

   ![Real Server Configuration](image)

   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.robtest.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 URLs:

- 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:

   ![Virtual Service Configuration Diagram](image)

   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:

<table>
<thead>
<tr>
<th>Health Checks</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Port</td>
<td>80</td>
</tr>
<tr>
<td>Request to send</td>
<td>adfs/probe</td>
</tr>
<tr>
<td>Response expected</td>
<td>blank</td>
</tr>
</tbody>
</table>

- 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 WAPs.

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:

   ![Real Server Configuration](image)

   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.robtest.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

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:

![Create a Clustered Pair](image)

• Once complete, the following will be displayed:

![High Availability Configuration - Master](image)

• 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.
## 14. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.4.0</td>
<td>7th August 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>RJC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added AD FS v5.0 (Win2019)</td>
<td>Support for latest version</td>
<td></td>
</tr>
</tbody>
</table>
About Loadbalancer.org

Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.

United Kingdom
Loadbalancer.org Ltd.
Compass House, North Harbour
Business Park, Portsmouth, PO6 4PS
UK:+44 (0) 330 380 1064
sales@loadbalancer.org
support@loadbalancer.org

Canada
Loadbalancer.org Appliances Ltd.
300-422 Richards Street, Vancouver,
BCV6B 2Z4, Canada
TEL:+1 302.213.0122
sales@loadbalancer.org
support@loadbalancer.org

United States
Loadbalancer.org, Inc.
4550 Linden Hill Road, Suite 201
Wilmington, DE 19808, USA
TEL: +1 833.274.2566
sales@loadbalancer.org
support@loadbalancer.org

Germany
Loadbalancer.org GmbH
Tengstraße 2780798,
München, Germany
TEL: +49 (0)89 2000 2179
sales@loadbalancer.org
support@loadbalancer.org