loadbalancer.org

Load Balancing
Microsoft AD FS

Deployment Guide
v1.2.3

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

- V7.6.4 and later

4. Microsoft Windows Versions Supported

- Windows 2008 R2 and later (AD FS 2.x – AD FS 3.x)

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.

> Note:
>
> For more details please refer to the following URL:
> http://blogs.technet.com/b/askpfeplat/archive/2014/08/25/adfs-deep-dive.aspx

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
1.0	2003 R2
1.1	2008
2.0	2008 R2
2.1	2012
3.0	2012 R2

ROLE SERVICES

The following role services can be deployed as part of the ADFS 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	The Federation Service Proxy functions act 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 (AD FS v3.0) the dedicated Proxy role service has been removed. Instead the proxy is based on WAP (Web Application Proxy).

HOW AD FS WORKS

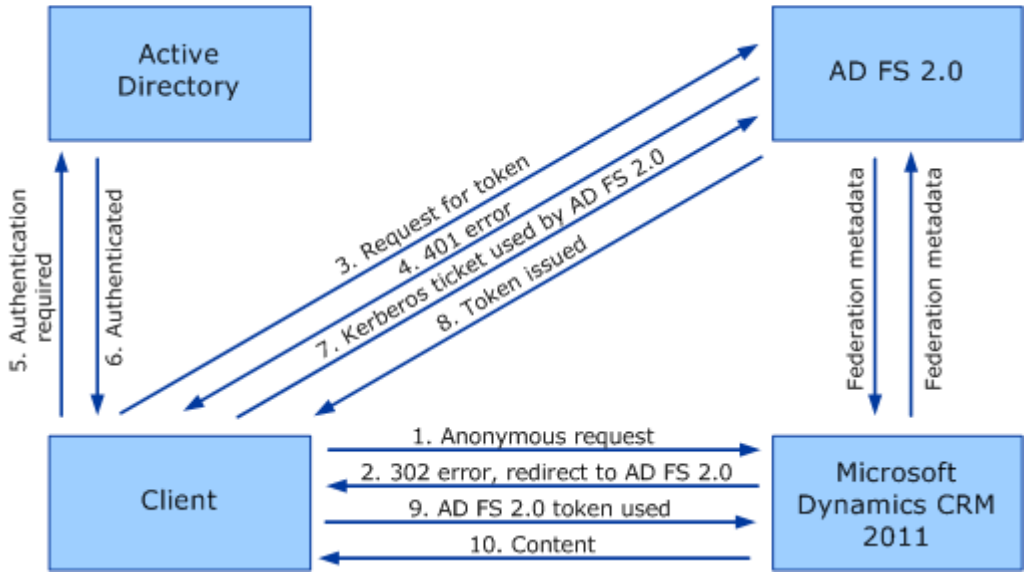
The following sections explain how AD FS authenticates internal LAN based users and external Internet based users.

A Microsoft Dynamics CRM example is used with AD FS 2.0, although the general flow is the same for other applications and different AD FS versions.

> Note:
>
> For a reference of key ADFS concepts, please refer to the following link:
> http://technet.microsoft.com/en-gb/library/ee913566.aspx

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 2.0).
3. The client sends a request for a security token to AD FS 2.0.
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 2.0 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 2.0 in step 3 and steps 4 through 7 are skipped.

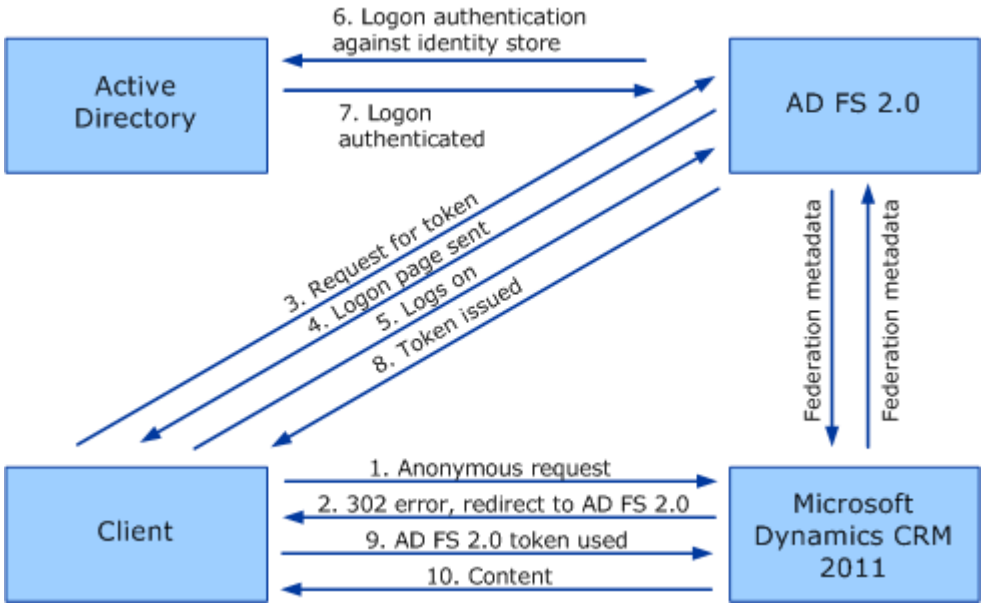
8. AD FS 2.0 provides a security token containing claims for access to Microsoft Dynamics CRM data.
9. The client sends the security token containing claims obtained from AD FS 2.0 to the Microsoft Dynamics CRM server.
10. The Microsoft Dynamics CRM server decrypts and validates the security token and presents the user with the requested information

> Note:
>
> Please refer to the following URL for more details:
> https://technet.microsoft.com/en-us/library/gg188601%28v=crm.6%29.aspx

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:
>
> Please refer to the following URL for more details:
> https://technet.microsoft.com/en-us/library/gg188603%28v=crm.6%29.aspx

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 the following link:
http://blogs.technet.com/b/askds/archive/2012/01/05/understanding-the-ad-fs-2-0-proxy.aspx

OTHER USEFUL REFERENCES

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

Office 365 SSO example:
https://technet.microsoft.com/en-us/magazine/jj631606.aspx

Sign-in Models for Office 365:
http://blogs.office.com/2014/05/13/choosing-a-sign-in-model-for-office-365/

6. Load Balancing AD FS

> Note:
>
> It's highly recommended that you have a working AD FS environment first before implementing the load balancer.

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) should 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 functional servers.

LOAD BALANCED PORTS & SERVICES

The following table shows the ports that are load balanced:

Port	Protocols	Use
443	TCP/HTTPS	All AD FS communications

PERSISTENCE (SERVER AFFINITY) REQUIREMENTS & OPTIONS

Since clients use a single TCP connection to the AD FS server to request and obtain the AD FS security token, session persistence (affinity) is not typically required for load balancing AD FS. The exception to this maybe when the application being accessed is also being load balanced. For more information please refer to the following Microsoft articles:

http://blogs.technet.com/b/speschka/archive/2011/10/28/make-sure-you-know-this-about-sharepoint-2010-claims-authentication-sticky-sessions-are-required.aspx

> Note:
>
> In this guide persistence is not used when configuring the Virtual Service. If it is required for situations such as those described above, source IP persistence can easily be enabled by modifying the VIP, setting Persistence Mode to Source IP, clicking Update and 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 it's recommended that more comprehensive checks are used.

For AD FS 2.0 a standard HTTPS negotiate check can be used that enables specific content on a particular page to read. If that content can be read the server is considered healthy.

For AD FS 3.0 which uses SNI (Server Name Indication) certificate bindings, the health-check must send the hostname inside the TLS handshake (Client Hello). The server is then able to choose the correct certificate based on this information. For this reason the standard HTTPS negotiate check cannot be used. Instead a custom script must be created that generates a correctly formed health-check. Please refer to page 19 for details of this custom script. In both cases the login page is used for the check:

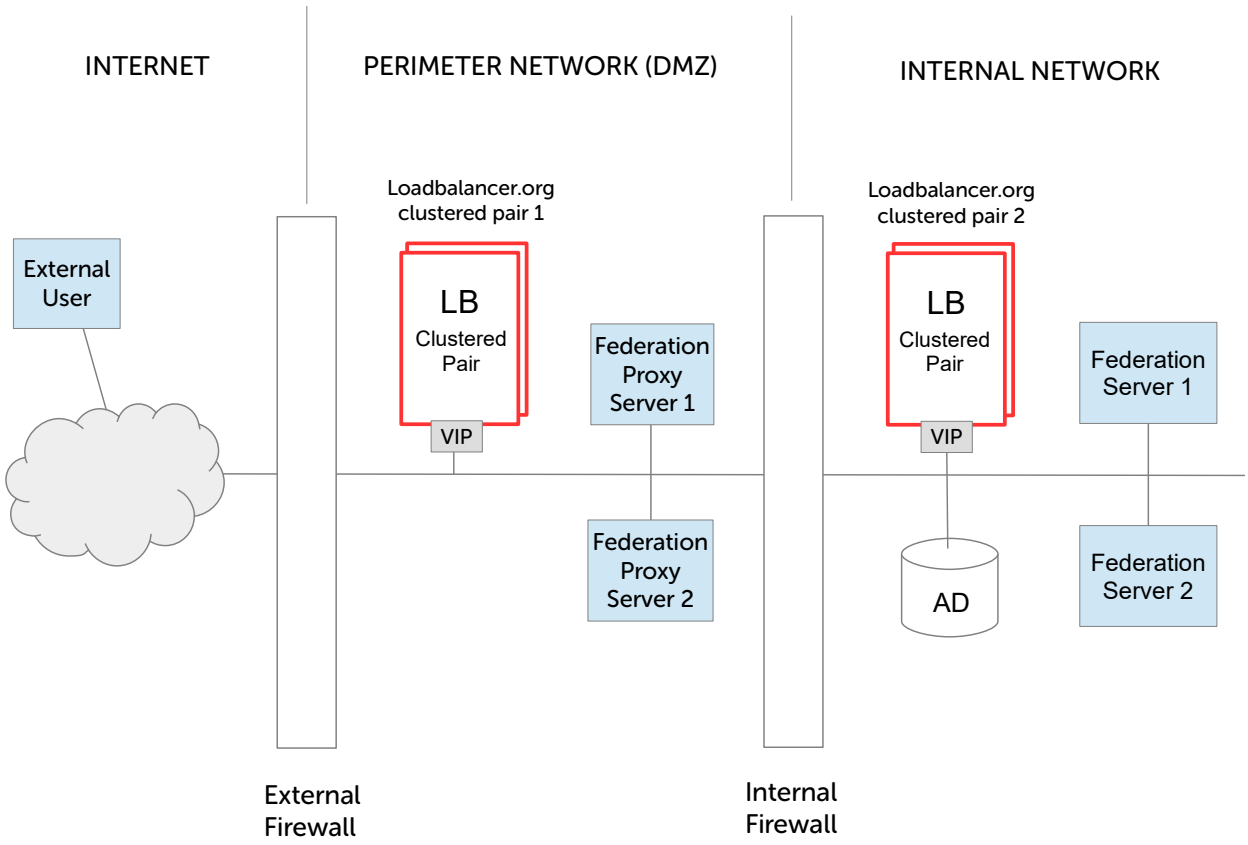
For AD FS 2.0: https://<server-fqdn>/adfs/ls/idpinitiatedsignon.aspx

For AD FS 3.0: https://<server-fqdn>adfs/ls/idpinitiatedsignon.htm

> Note:
>
> For more details on AD FS and load balancer health-checks please refer to:
> http://blogs.technet.com/b/applicationproxyblog/archive/2014/10/17/hardware-load-balancer-health-checks-and-web-application-proxy-ad-fs-2012-r2.aspx

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 recommends deploying clustered pairs for HA and resilience
- In AD FS 3.0 (Windows 2012 R2) the Federation Proxy Server role is handled by Web Application Proxy rather than a dedicated, specific role service as with AD FS 2.0

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***

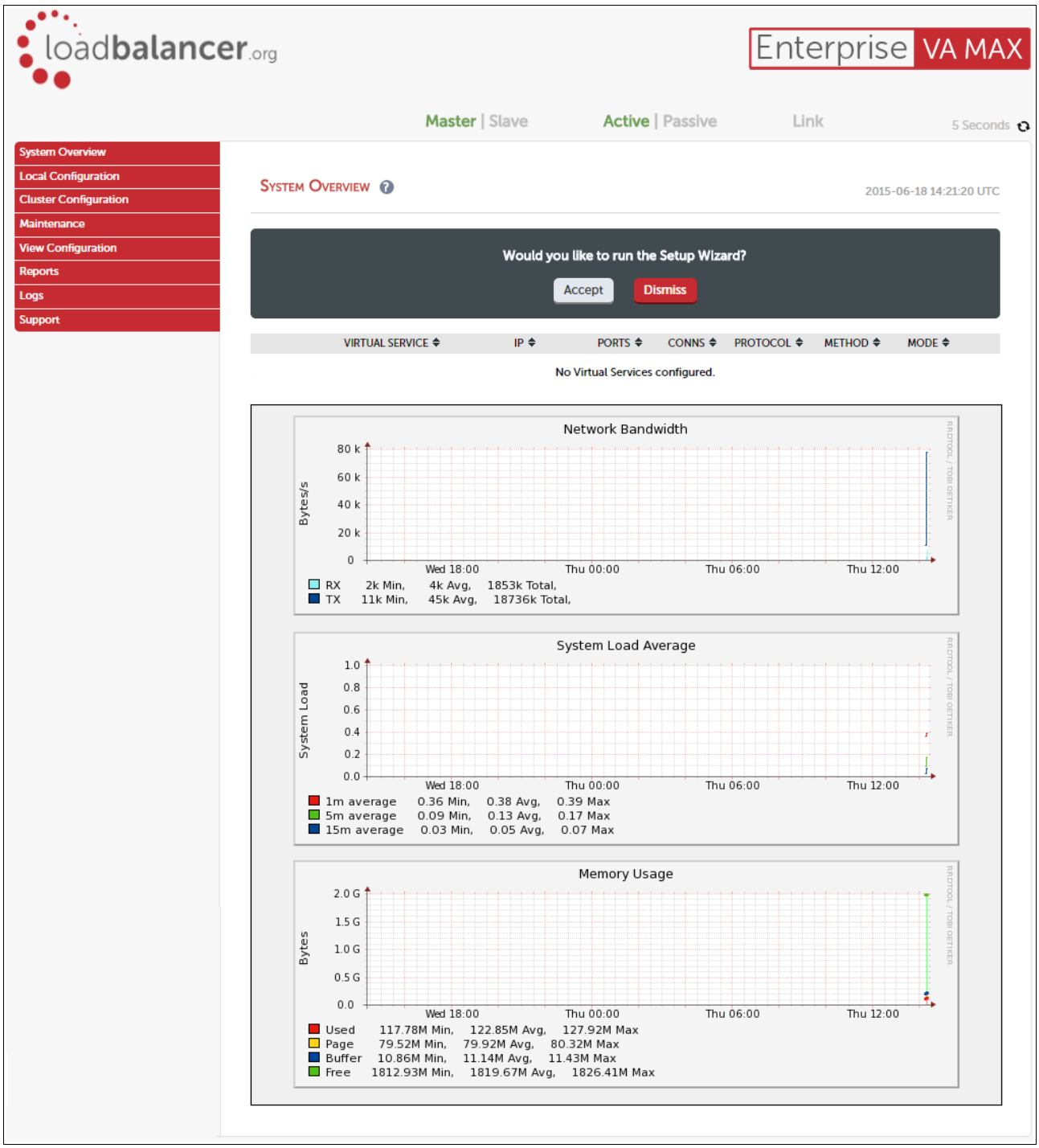
(replace 192.168.2.21 with the IP address of your load balancer if it's been changed from the default)

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:



(shows v8.2.x)

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 26.

8. Appliance & Server Configuration - AD FS 2.0

FEDERATION SERVERS

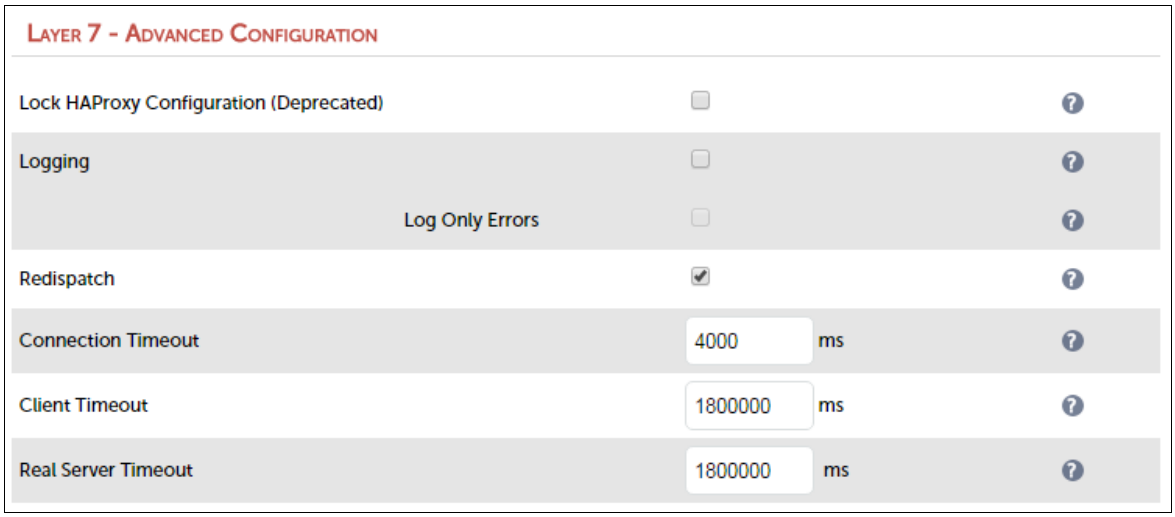
AD FS INSTALLATION & CONFIGURATION

- ADFS 2.0 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: http://www.microsoft.com/en-us/download/details.aspx?id=10909
- AD FS update rollup 3 is available here: http://support.microsoft.com/kb/2790338/en-gb
- For information on configuring the Federation Servers please refer to the following Microsoft article: https://technet.microsoft.com/en-us/library/adfs2-help-how-to-configure-a-new-federation-server%28v=ws.10%29.aspx

LOAD BALANCER CONFIGURATION

Configuring Layer 7 Timeout Settings

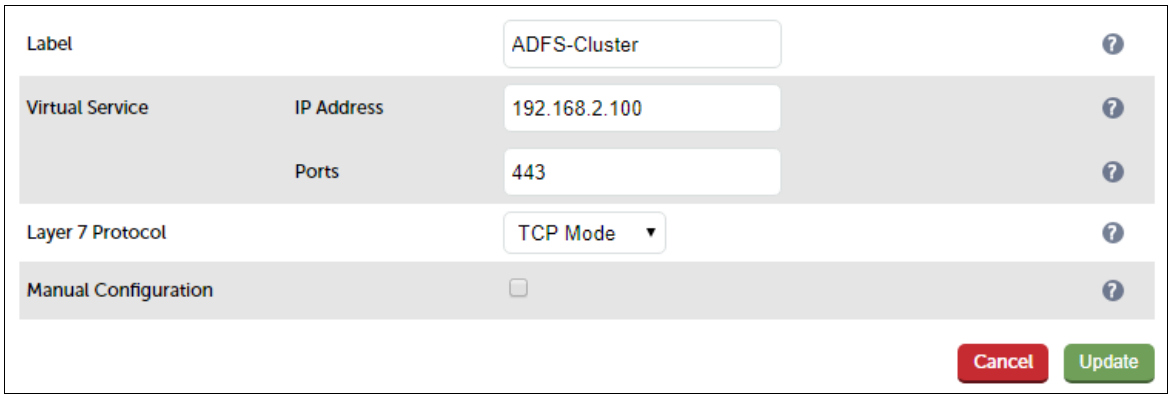
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Advanced Configuration*
2. Set the client and server timeouts as shown below:



3. Set *Client Timeout* to 1800000 , i.e. 30minutes
   *Note: You can also enter **30m** rather than 1800000*
4. Set *Real Server Timeout* to 1800000 , i.e. 30minutes
   *Note: You can also enter **30m** rather than 1800000*
5. Click **Update**

Setting up the Virtual Service (VIP)

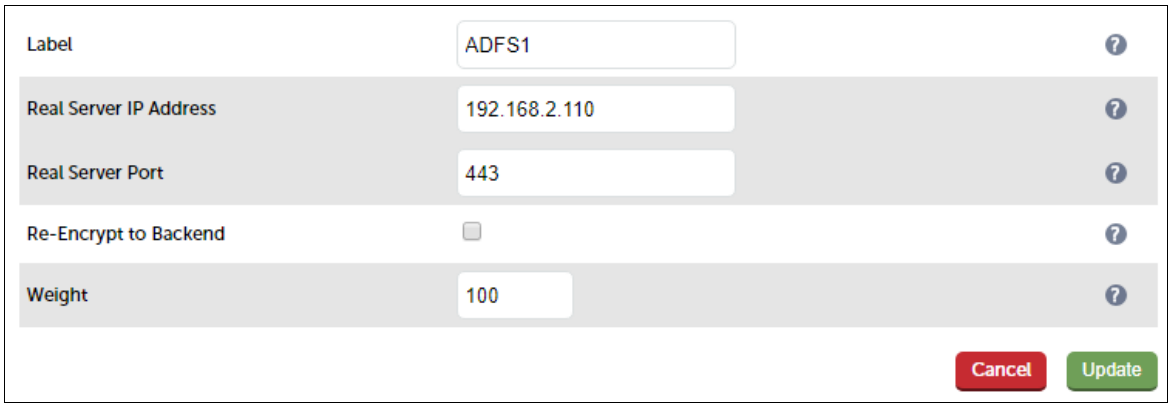
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**
2. Enter the following details:



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 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. Ensure *Check Port* is set to **443**
12. Set *Request to Send* to **adfs/ls/idpinitiatedsignon.aspx**
13. Set *Response Expected* to **Sign-In**
14. 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 AD FS 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.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**

FEDERATION PROXY SERVERS

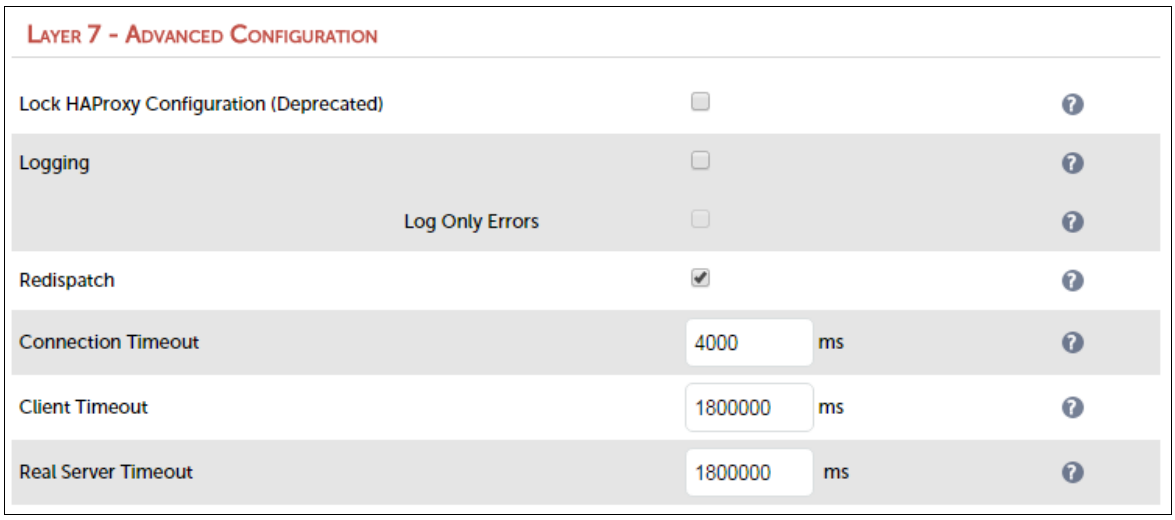
AD FS INSTALLATION & CONFIGURATION

- ADFS 2.0 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: http://www.microsoft.com/en-us/download/details.aspx?id=10909
  AD FS update rollup 3 is available here: http://support.microsoft.com/kb/2790338/en-gb
- 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 the following Microsoft article:
  https://technet.microsoft.com/en-us/library/adfs2-help-how-to-configure-a-new-federation-server-proxy%28v=ws.10%29.aspx

LOAD BALANCER CONFIGURATION

Configuring Layer 7 Timeout Settings

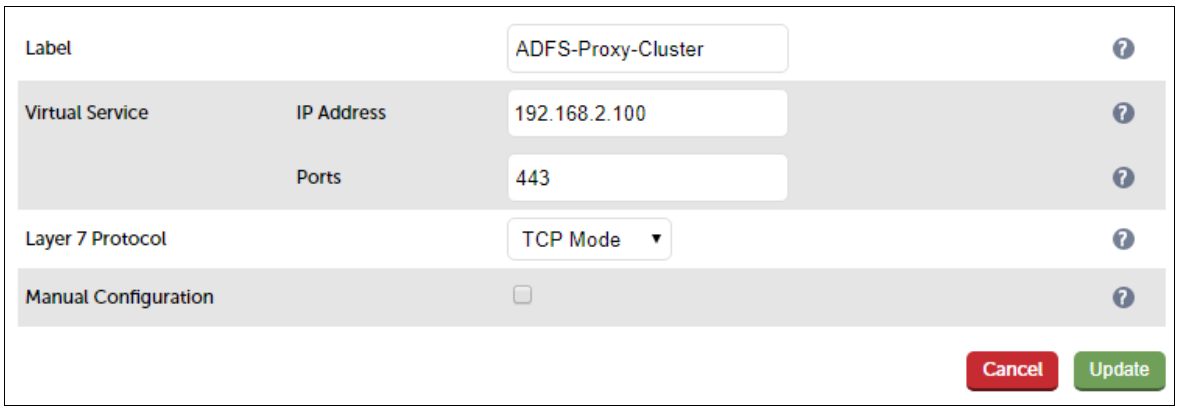
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Advanced Configuration*
2. Set the client and server timeouts as shown below:



3. Set *Client Timeout* to 1800000 , i.e. 30minutes
   *Note: You can also enter **30m** rather than 1800000*
4. Set *Real Server Timeout* to 1800000 , i.e. 30minutes
   *Note: You can also enter **30m** rather than 1800000*
5. Click **Update**

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:

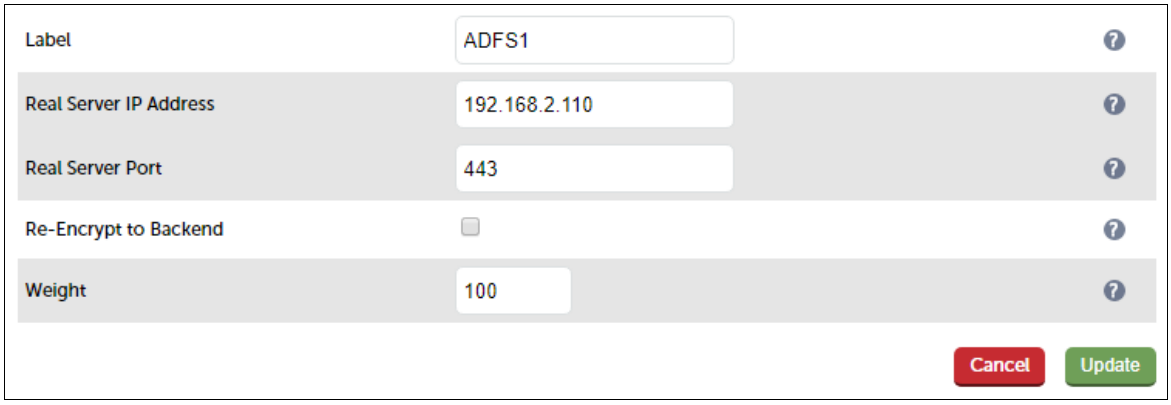


3. Enter an appropriate name (Label) for the Virtual Service, e.g. **ADFS-Proxy-Cluster**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.100**
5. Set the *Virtual Service Ports* field to **443**
6. Set the *Layer 7 Protocol* to **TCP Mode**
7. Click **Update**
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. Ensure *Check Port* is set to **443**
12. Set *Request to Send* to **adfs/ls/idpinitiatedsignon.aspx**

13. Set *Response Expected* to **Sign-In**
14. 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 AD FS 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.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. Appliance & Server Configuration - AD FS 3.0

FEDERATION SERVERS

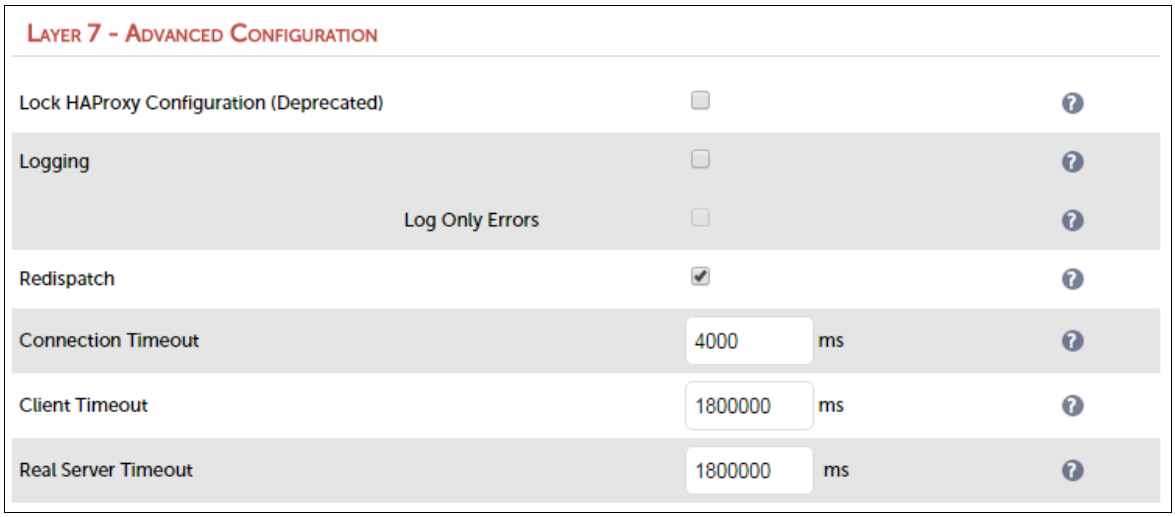
AD FS INSTALLATION & CONFIGURATION

- Use Server Manager to install the AD FS Server Role on each Federation Server
- For more information on configuring AD FS please refer to the following Microsoft articles:
  http://blogs.technet.com/b/askpfeplat/archive/2013/12/09/how-to-build-your-adfs-lab-on-server-2012-part-1.aspx
  http://blogs.technet.com/b/rmilne/archive/2014/04/28/how-to-install-adfs-2012-r2-for-office-365.aspx

LOAD BALANCER CONFIGURATION

Configuring Layer 7 Timeout Settings

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Advanced Configuration*
2. Set the client and server timeouts as shown below:



3. Set *Client Timeout* to 1800000 , i.e. 30minutes
   Note: You can also enter 30m rather than 1800000
4. Set *Real Server Timeout* to 1800000 , i.e. 30minutes
   Note: You can also enter 30m rather than 1800000
5. Click **Update**

Setting up the SNI Health Check

1. Using an editor, create a file named **adfs-check.sh** in **/var/lib/loadbalancer.org/check/**
2. 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

> Note:
>
> From v8.2.2, the appliance includes an external health check script called "sni-check.sh". The contents of this file are identical to the content detailed in the next step. Therefore, for v8.2.2, select the external check script "sni-check.sh" rather than creating a new file, then modify this file to suit your environment as described below:

3. Copy/paste the following into the file:

```
#!/bin/bash
# Script to check SNI enabled servers are healthy
# $3 contains the IP address of the real server and is passed by the
# calling program (HAProxy)

REAL_SERVER_IP=$3
SNI_HOST="adfs.robstest.com"
SNI_URI="adfs/ls/idpinitiatedsignon.htm"
CHECK_VALUE="Sign in"

# check if previous instance of health check is running & kill if req'd
PIDFILE="/var/run/sni-check-$SNI_HOST.pid"
if [ -f $PIDFILE ]
then
        kill -9 `cat $PIDFILE` > /dev/null 2>&1
fi

# write the process ID to the PID file
echo "$$" > $PIDFILE

# check that the ADFS login page is accessible
CURL_OUTPUT=$(/usr/bin/curl -k -m 5 --resolve \
$SNI_HOST:443:$REAL_SERVER_IP \
https://$SNI_HOST/$SNI_URI)

if [[ $CURL_OUTPUT == *$CHECK_VALUE* ]]
then
        exit 0
else
        exit 1
fi
```

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

```
SNI_HOST="adfs.robstest.com"
SNI_URI="adfs/ls/idpinitiatedsignon.htm"
```

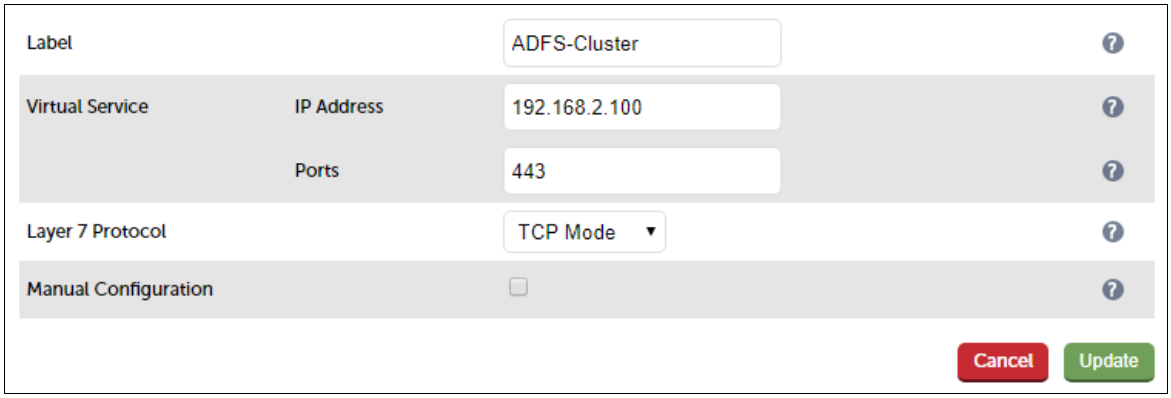
> Note:
>
> This SNI URI is the default ADFS sign-in URI and should not normally need changing.

5. Save the file
6. Set the file permissions to 755, under WinSCP right click the file, click properties and set the permissions as shown below:

7. The file is selected when configuring the VIPs

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:



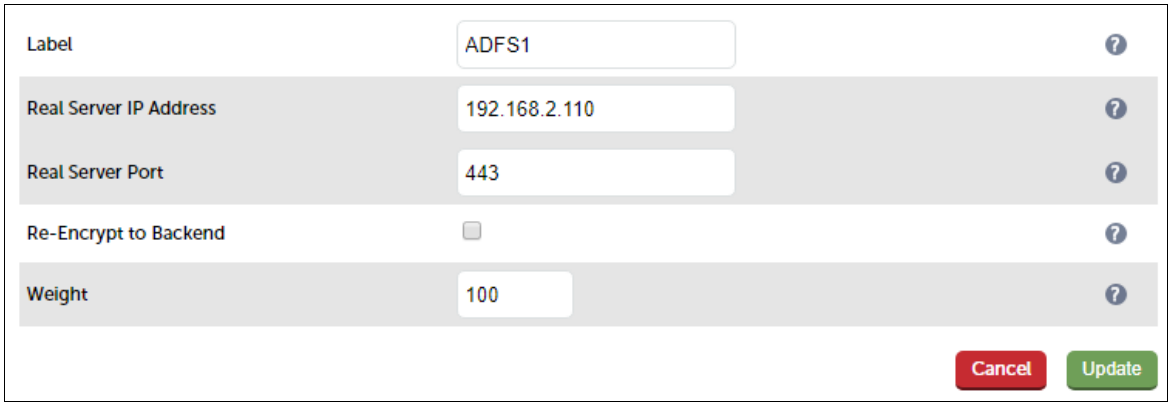
3. Enter an appropriate name (Label) for the Virtual Service, e.g. **ADFS-Cluster**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.100**
5. Set the *Virtual Service Ports* field to **443**
6. Set the *Layer 7 Protocol* to **TCP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created Virtual Service
9. Change *Persistence Mode* to **None**
10. Change *Health Checks* to **External Check**
11. Set *Check Script* to **sni-check.sh**

> Note:
>
> sni-check.sh is listed by default for v8.2.2 and later, for earlier versions it will appear once it has been created as described on page 19.

12. 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 AD FS 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.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.htm**

FEDERATION PROXY SERVERS (WEB APPLICATION PROXIES)

AD FS INSTALLATION & CONFIGURATION

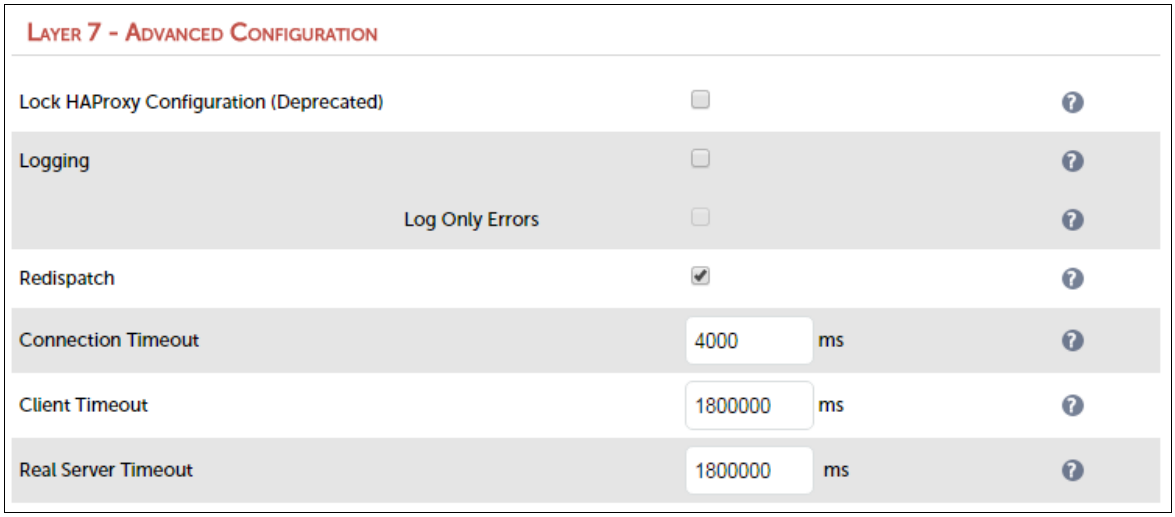
- Use Server Manager to install the Web Application Proxy Server Role on each Proxy Server
- When specifying the Federation Service Name, this should be the load balanced VIP of the Federation Servers
- For more information on configuring Web Application Proxy for AD FS please refer to the following Microsoft articles:

http://blogs.technet.com/b/askpfeplat/archive/2013/12/09/how-to-build-your-adfs-lab-on-server-2012-part-1.aspx
http://blogs.technet.com/b/rmilne/archive/2014/04/28/how-to-install-adfs-2012-r2-for-office-365_1320_part-2.aspx

LOAD BALANCER CONFIGURATION

Configuring Layer 7 Timeout Settings

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Advanced Configuration*
2. Set the client and server timeouts as shown below:



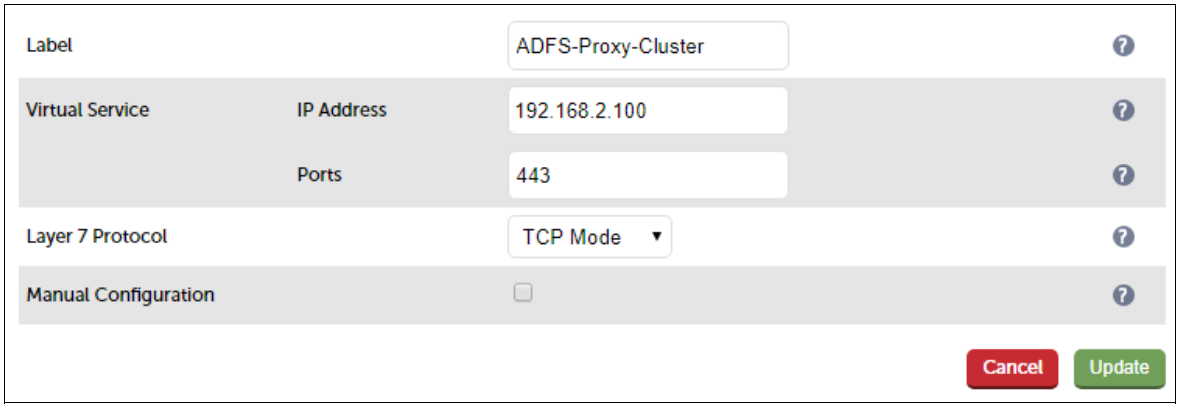
3. Set *Client Timeout* to 1800000 , i.e. 30minutes
   *Note: You can also enter **30m** rather than 1800000*
4. Set *Real Server Timeout* to 1800000 , i.e. 30minutes
   *Note: You can also enter **30m** rather than 1800000*
5. Click **Update**

Setting up the SNI Health Check

1. Configure the SNI health-check script as described on page 19.

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:



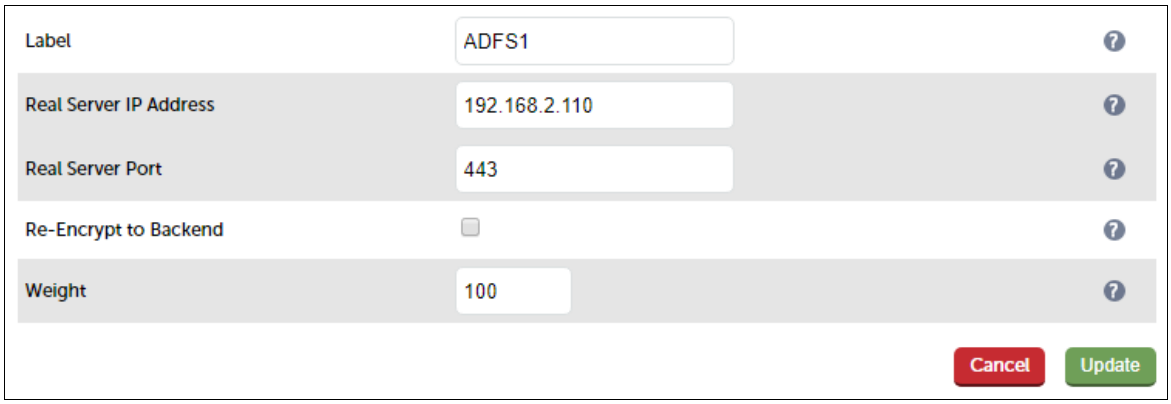
3. Enter an appropriate name (Label) for the Virtual Service, e.g. **ADFS-Proxy-Cluster**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.100**
5. Set the *Virtual Service Ports* field to **443**
6. Set the *Layer 7 Protocol* to **TCP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created Virtual Service
9. Change *Persistence Mode* to **None**
10. Change *Health Checks* to **External Check**
11. Set *Check Script* to **sni-check.sh**

> Note:
>
> sni-check.sh is listed by default for v8.2.2 and later, for earlier versions it will appear once it has been created as described on page 19.

12. 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 AD FS 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.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.htm**

10. Technical Support

For more details about configuring the appliance and assistance with designing your deployment please don't hesitate to contact the support team using the following email address: 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 Server 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

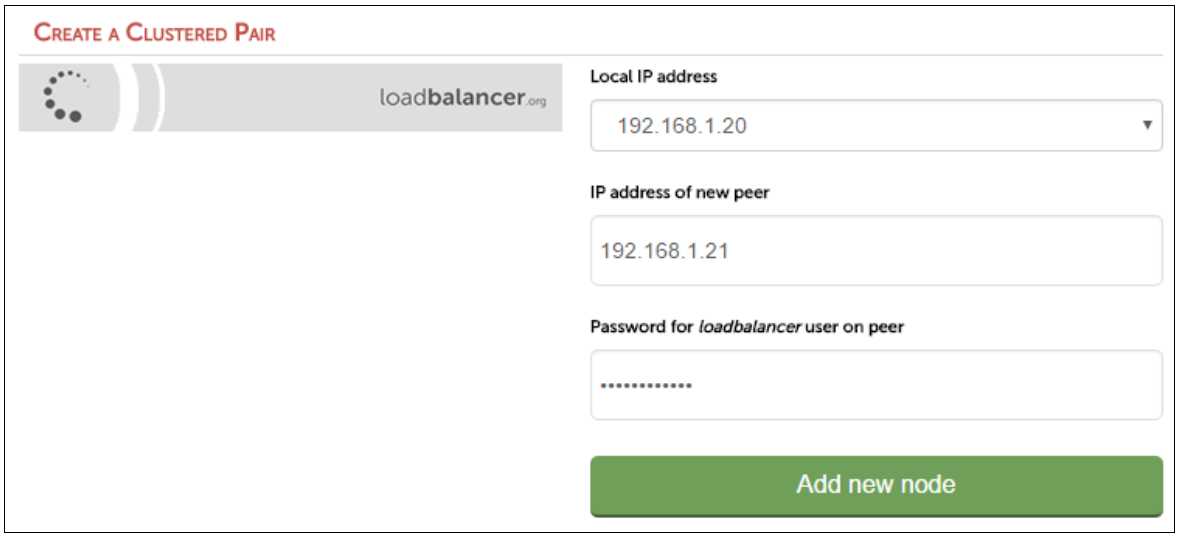
Version 7:

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

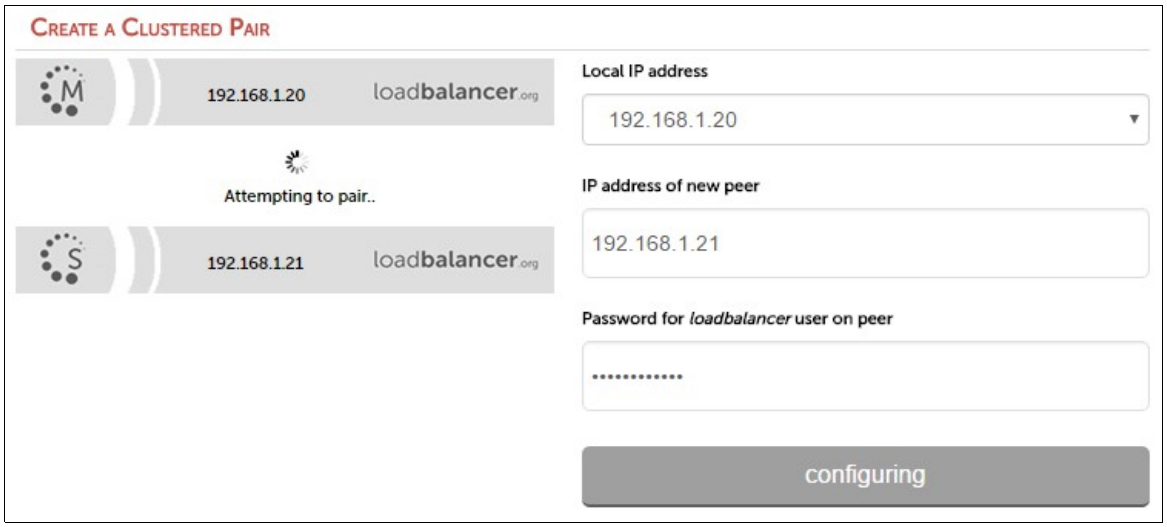
Version 8:

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

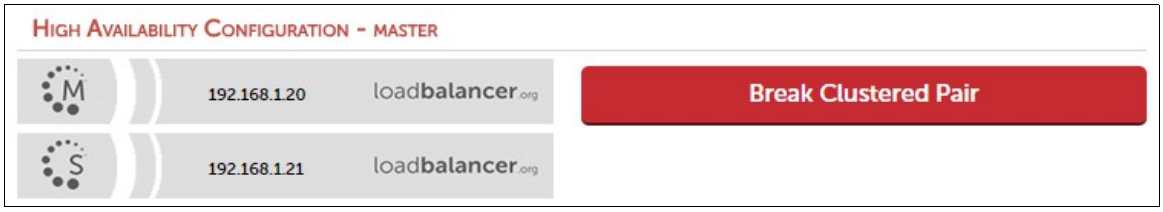
- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: *Cluster Configuration > High-Availability Configuration*



- 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