Progress®
Kemp® LoadMaster®

Deployment Guide AD FS v3

Generated on: 18 December 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 5

Chapter 2: Template 6

Chapter 3: Load Balancing AD FS 7

Load Balancing Internal AD FS Servers 8

Load Balancing AD FS Proxy (WAP) Servers 9

Using LoadMaster to Proxy External Clients to AD FS Servers 11

Chapter 4: Prerequisites 14

DNS 14

AD FS SSL Certificate Import on LoadMaster 15

Chapter 5: Enable Subnet Originating Requests Globally 16

Chapter 6: VS Configuration 18

Create a VS using a Template 18

AD FS Internal Farm VS Recommended API Settings (optional) 19

AD FS Proxy Farm VS Recommended API Settings (optional) 20

AD FS Progress Kemp as Proxy VS Recommended API Settings (optional) 21

Chapter 7: References 23

1

Introduction

Active Directory Federation Services (AD FS) is a Microsoft identity access solution. It was an optional component of Microsoft Windows Server® 2003 R2. It is now built into Windows Server® 2008, Windows Server® 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019. AD FS helps to establish trust relationships and reduces the need for provisioning and managing user accounts. Its implementation provides clients (internal or external to the trusted internal LAN) with simplified access to systems and applications relying on claims-based authorization. AD FS also supports web Single-Sign-On (SSO) technologies to improve user experience across multiple protected applications.

Trust relationships are used to project a user's digital identity and access rights to trusted partners and can be deployed in multiple organizations to facilitate business-to-business (B2B) transactions between trusted partner organizations.

Document Purpose

This documentation is intended to provide guidance on how to configure LoadMaster products to provide high availability for an AD FS 3.0 or AD FS 4.0 environment, based on Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019. This documentation is created using a representative sample environment described later in the document. As this documentation is not intended to cover every possible deployment scenario, it may not address unique setup or requirements. The Progress Kemp Support Team is always available to provide solutions for scenarios not explicitly defined.

Intended Audience

It is assumed that the reader is a server/network administrator or a person otherwise familiar with networking and general computer terminology and is familiar with AD FS technology.

2

Template

Progress Kemp has developed a template containing our recommended settings for this workload. You can install this template to help create Virtual Services (VSs) because it automatically populates the settings. You can use the template to easily create the required VSs with the recommended settings. For some workloads, additional manual steps may be required such as assigning a certificate or applying port following. These steps are covered in the document, if needed.

You can remove templates after use and this will not affect deployed services. If needed, you can make changes to any of the VS settings after using the template.

Download released templates from the following page: LoadMaster Templates.

For more information and steps on how to import and use templates, refer to the Virtual Services and Templates, Feature Description.

3

Load Balancing AD FS

The LoadMaster family of products provide high availability to AD FS and AD FS proxy farms (WAP). AD FS proxy servers (Web Application Proxy(WAP)) provide termination of external traffic at the DMZ and provide an additional layer of protection against external threats. AD FS proxy servers also help internal AD FS servers clearly identify which authentication attempts are external. This is achieved by inserting x-ms-proxy claims in AD FS requests.

AD FS administrators can configure advanced claim rules that allow granular control over user authentication restrictions such as requiring users to be a part of a certain group or requiring users to authenticate from certain IP networks. When such claims rules are configured on AD FS servers, it becomes critical to identify if the user is trying to authenticate from an external or internal location.

In deployments where select advanced claim rules such as IP network and trust levels for instance are not in use, LoadMaster devices can be placed in the DMZ and can proxy authentication requests to internal AD FS servers without requiring additional AD FS Proxy (WAP) servers. This can help customers save on hardware, software, and management costs associated with maintaining additional AD FS proxy servers.

Related Links

For details, see the following topics:

- Load Balancing Internal AD FS Servers
- Load Balancing AD FS Proxy (WAP) Servers
- Using LoadMaster to Proxy External Clients to AD FS Servers

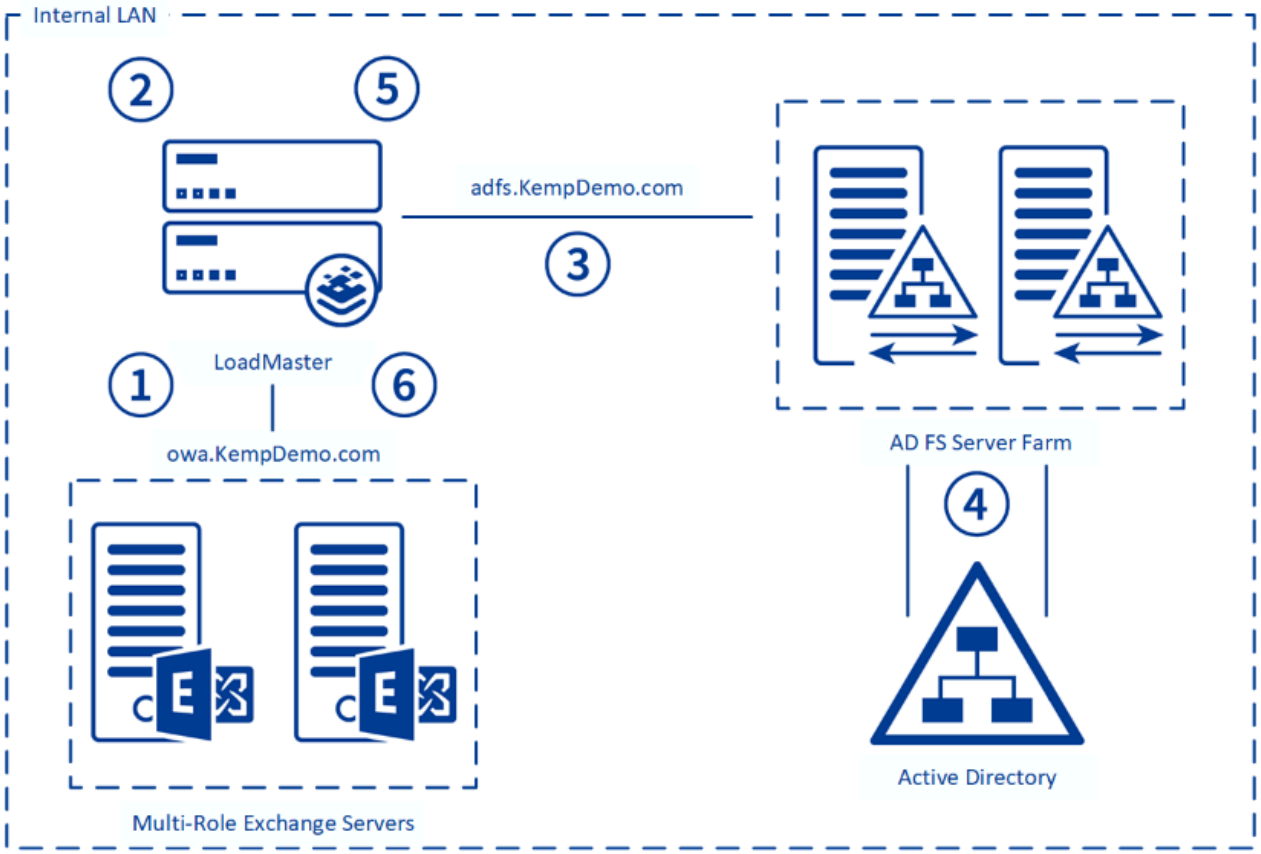
Load Balancing Internal AD FS Servers

An AD FS server is responsible for issuance of claims and user authentication. This server must be able to connect to a Domain Controller. It authenticates users from multiple domains by using Windows Trust.

In our example deployment, “Kemp Demo” has deployed AD FS 3.0 in their environment to facilitate claims-based authentication for their Microsoft Exchange 2013 infrastructure and allow for SSO capabilities across applications. The deployment contains the following:

- Two AD FS 3.0 servers
- Two Microsoft Exchange 2013 Multi-Role servers
- A LoadMaster High Availability (HA) cluster

A name space of **owa.Kempdemo.com** is used for access to the Microsoft Exchange environment. A name space of **adfs.Kempdemo.com** is used for access to the AD FS environment.



1. The client accesses the workload at https://owa.kempdemo.com/owa.
2. The client is directed to the AD FS URL, https://adfs.kempdemo.com, which is a VS on LoadMasters for internal AD FS.
3. The LoadMaster sends traffic to a healthy AD FS server based on scheduling method.
4. The AD FS server authenticates the user against Active Directory.
5. The AD FS server returns a SAML token to the client through the LoadMaster for authentication.

6. The client connects to Microsoft Exchange 2016 with a SAML token for authentication and accesses the workload.

Load Balancing AD FS Proxy (WAP) Servers

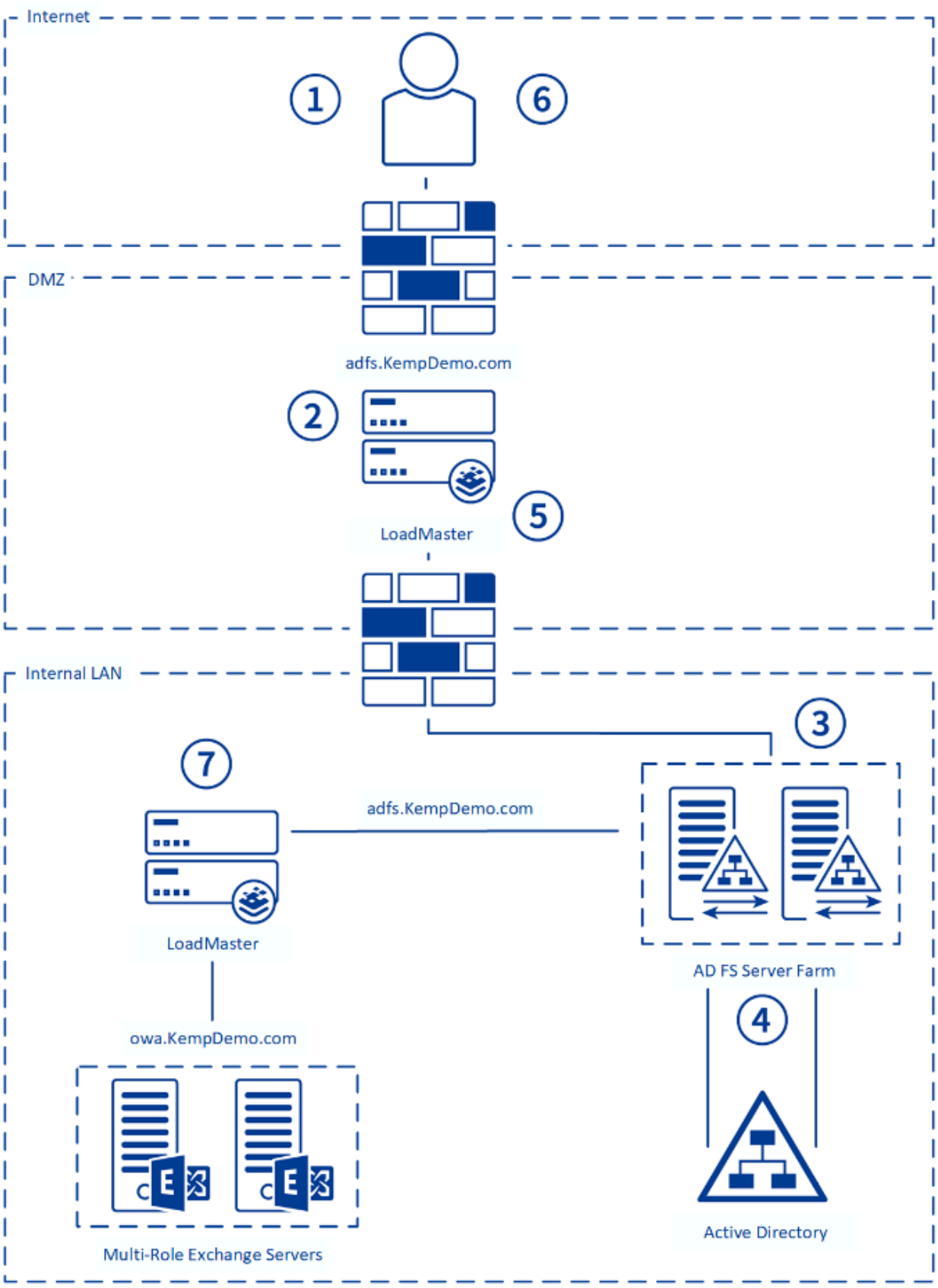
An AD FS proxy server (WAP) protects the AD FS server from internet-based threats. The WAP server also authenticates users from the internet.

Note: Terminating SSL between the WAP and AD FS server is not supported. Terminating SSL breaks the trust between the WAP and AD FS.

In our example deployment, “Kemp Demo” has deployed AD FS 3.0 in their environment to facilitate claims-based authentication for their Microsoft Exchange 2013 infrastructure and allow for SSO capabilities across applications. A pair of AD FS Proxy (WAP) servers are added in the DMZ to provide additional protection and security for clients accessing the application from the internet. External clients connect to the AD FS Proxy (WAP) servers and the AD FS Proxy (WAP) server proxy that connection through the internal LoadMaster to a healthy AD FS server. The deployment contains the following:

- Two AD FS 3.0 servers
- Two AD FS 3.0 Proxy servers (WAP)
- Two Microsoft Exchange 2013 Multi-Role servers
- LoadMaster HA cluster on the internal LAN
- LoadMaster HA cluster in the DMZ

A name space of **owa.Kempdemo.com** is used for access to the Microsoft Exchange environment. A name space of **adfs.Kempdemo.com** is used for access to the AD FS and the AD FS Proxy (WAP) farms. Split Domain Name System (DNS) is implemented, which allows these name spaces to be used both internally and externally in the environment.


Internet
1
6
DMZ
adfs.KempDemo.com
2
LoadMaster
5
Internal LAN
3
7
adfs.KempDemo.com
LoadMaster
AD FS Server Farm
4
owa.KempDemo.com
Active Directory
Multi-Role Exchange Servers

1. The client accesses the workload at https://owa.kempdemo.com/owa.
2. The client is directed to the AD FS URL, https://adfs.kempdemo.com, which is a Virtual Service on the DMZ LoadMasters for AD FS Proxies (WAP).
3. The LoadMaster sends traffic to a healthy AD FS Proxy (WAP) server based on the scheduling method.
4. The AD FS Proxy (WAP) server proxies the connection to the AD FS servers published through the internal LoadMasters.
5. The LoadMaster sends traffic to the healthy AD FS server based on the scheduling method.
6. The AD FS server authenticates the user against Active Directory.
7. The AD FS server returns a SAML token to the AD FS Proxy (WAP).
8. The AD FS Proxy (WAP) returns a SAML token to the client for authentication.
9. The client connects to Microsoft Exchange 2013 with a SAML token for authentication and accesses the workload.

Using LoadMaster to Proxy External Clients to AD FS Servers

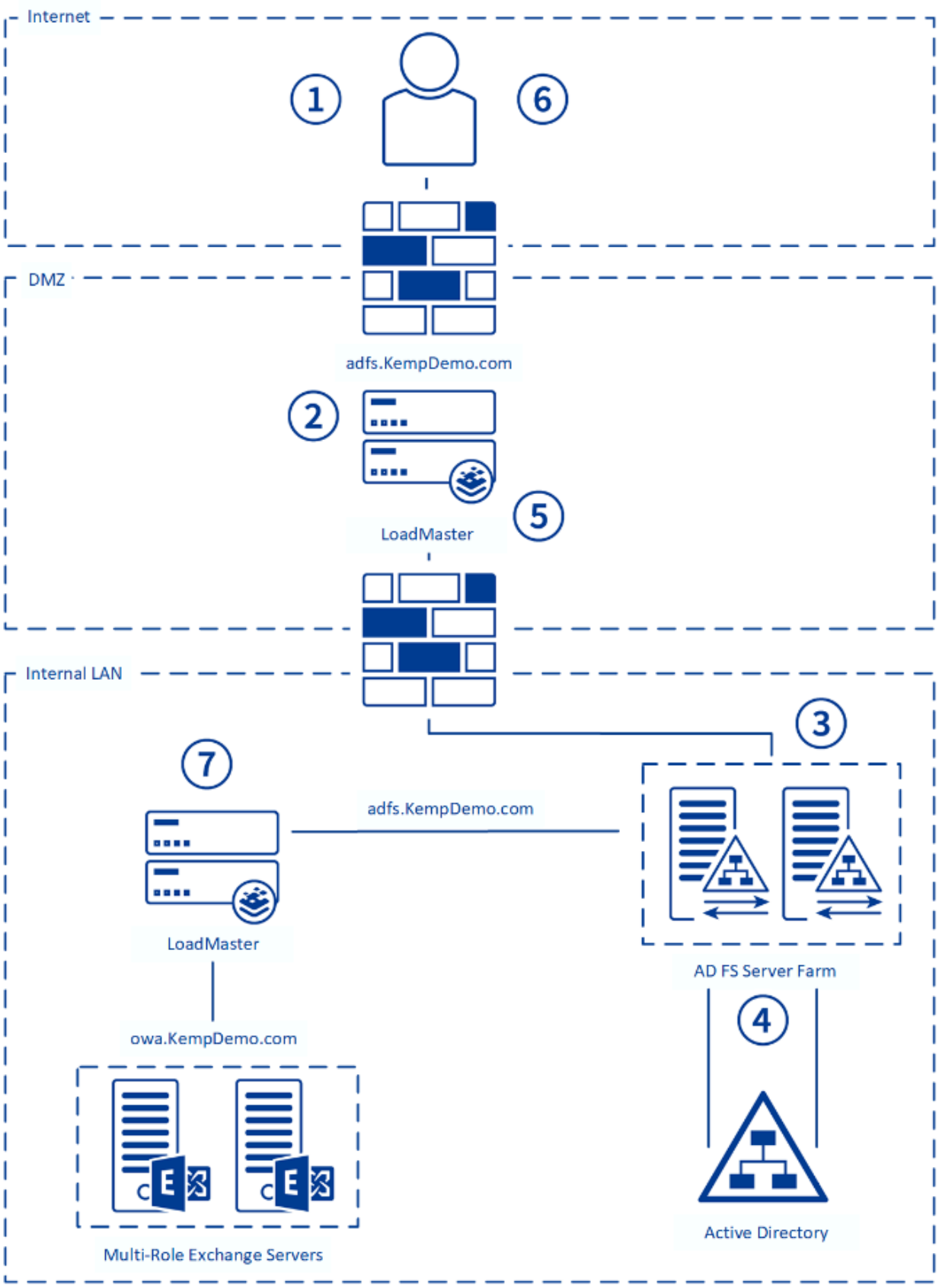
In deployments where select advanced claim rules such as IP network and trust levels for instance are not in use, LoadMaster devices can be placed in the DMZ and can proxy authentication requests to internal AD FS servers without requiring additional AD FS proxy (WAP) servers. This can help customers save on hardware, software, and management costs associated with maintaining additional AD FS proxy servers.

Note: If you are using advanced claims with the AD FS infrastructure, the LoadMaster can be used alongside the AD FS Proxy Farm but cannot be used as a replacement.

In our example deployment, “Kemp Demo” has deployed AD FS 3.0 in their environment to facilitate claims-based authentication for their Microsoft Exchange 2013 infrastructure and allow for SSO capabilities across applications. A pair of LoadMasters are added in the DMZ to provide additional protection and security for clients accessing the application from the internet. External clients will connect to the LoadMasters and the LoadMasters will proxy that connection directly to a healthy AD FS server. The deployment contains the following:

- Two AD FS 3.0 servers
- Two Exchange 2013 Multi-Role servers
- LoadMaster HA cluster “acting” as the AD FS Proxy (WAP)
- LoadMaster HA cluster for internal traffic (optional)

A name space of **owa.Kempdemo.com** is used for access to the Microsoft Exchange environment. A name space of **adfs.Kempdemo.com** is used for access to the AD FS environment. Split DNS is implemented, which allows these name spaces to be used both internally and externally in the environment.


Internet
1
6
DMZ
adfs.KempDemo.com
2
LoadMaster
5
Internal LAN
3
7
adfs.KempDemo.com
LoadMaster
AD FS Server Farm
4
owa.KempDemo.com
Multi-Role Exchange Servers
Active Directory

1. The external client accesses the workloadat https://owa.kempdemo.com/owa.
2. The client is directed to the AD FS url, https://adfs.kempdemo.com, which is a VS on the DMZ LoadMasters “acting” as the AD FS Proxy (WAP).
3. The LoadMaster sends traffic to the healthy AD FS server based on the scheduling method.
4. The AD FS server authenticates the user against Active Directory.
5. The AD FS server returns a SAML token to the LoadMaster “acting” as the AD FS Proxy (WAP).
6. The LoadMaster returns a SAML token to the client for authentication.
7. The client connects to Microsoft Exchange 2013 with a SAML token for authentication and accesses the workload.

4

Prerequisites

There are some prerequisites to be aware of before deploying the LoadMaster with AD FS.

It is assumed that the AD FS 3.0 or AD FS 4.0 environment is already set up and the LoadMaster is installed. We recommend reviewing the LoadMaster Web User Interface (WUI), Configuration Guide.

At a minimum, the following actions should be completed:

- Implemented Active Directory, AD FS, DNS, WAP, and other Microsoft requirements
- Configured the application servers to support claims-based authentication
- Established access to the LoadMaster WUI

Related Links

For details, see the following topics:

- DNS
- AD FS SSL Certificate Import on LoadMaster

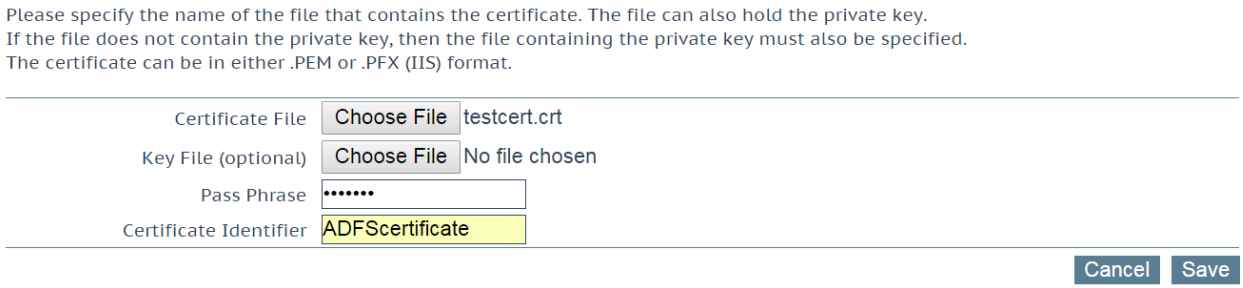
DNS

Access to the DNS used in the environment must be available. This is needed to set up name resolution of the AD FS services to the VS IP addresses that will be configured on the LoadMaster.

AD FS SSL Certificate Import on LoadMaster

The AD FS SSL certificate has to be imported into the LoadMaster before deployment if using Progress Kemp as a proxy. To import the certificate, follow the steps below:

1. Log in to the relevant Virtual Load Master (VLM).
2. In the main menu, click **Certificates & Security** and select **SSL Certificates**.
3. Click the **Import Certificate** button.



4. Click **Choose File** next to the **Certificate File** field.
5. Browse to and select the certificate file.
6. Click **Open**.
7. Browse to and select the **Key File** if needed.
8. Enter the **Pass Phrase** of the certificate.
9. Enter a name for the certificate in the **Certificate Identifier** field.
10. Click **Save**.
11. If it works, a success message is displayed. Click **OK**.

Note: Despite the fact that clients establish a single TCP connection with the AD FS server to request and receive a security token, certain applications can suffer from multiple login redirections if persistence is not enabled on the load balancer. For this reason, a Layer 7 service is used, along with SSL reencryption, to allow for the more intelligent forms of persistence that are not available at Layer 4 or when SSL traffic is not terminated at the LoadMaster.

5

Enable Subnet Originating Requests Globally

It is best practice to enable the **Subnet Originating Requests** option globally.

In a one-armed setup (where the Virtual Service and Real Servers are on the same network/subnet) **Subnet Originating Requests** is usually not needed. However, enabling **Subnet Originating Requests** should not affect the routing in a one-armed setup.

In a two-armed setup where the Virtual Service is on network/subnet A, for example, and the Real Servers are on network B, **Subnet Originating Requests** should be enabled on LoadMasters with firmware version 7.1-16 and above.



When **Subnet Originating Requests** is enabled, the Real Server sees traffic originating from 10.20.20.21 (LoadMaster eth1 address) and responds correctly in most scenarios.

With **Subnet Originating Requests** disabled, the Real Server sees traffic originating from 10.0.0.15 (LoadMaster Virtual Service address on **eth0**) and responds to **eth0** which could cause asymmetric routing.

When **Subnet Originating Requests** is enabled globally, it is automatically enabled on all Virtual Services. If

the **Subnet Originating Requests** option is disabled globally, you can choose whether to enable **Subnet Originating Requests** on a per-Virtual Service basis.

To enable **Subnet Originating Requests** globally, follow the steps below:

1. In the main menu of the LoadMaster User Interface (UI), go to **System Configuration > Miscellaneous Options > Network Options**.
2. Select the **Subnet Originating Requests** check box.

6

VS Configuration

This step-by-step set up of VS leverages the Progress Kemp application template for Microsoft AD FS.

The table in each section outlines the settings configured by the application template. You can use this information to manually configure VS or using the LoadMaster API and automation tools.

Related Links

For details, see the following topics:

- Create a VS using a Template

Create a VS using a Template

To configure a VS using the application template, perform the following steps:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.
2. Type a valid **Virtual Address**.
3. Select the appropriate template in the **Use Template** drop-down list.
4. Click **Add this Virtual Service**.
5. **Required only for Progress Kemp as Proxy:** Expand the **SSL Properties** section.
6. **Required only for TLS/SSL Offload and Reencrypt:** Select the certificate to use from **Available Certificates** and click the arrow (>) to move it to **Assigned Certificates**.

Note: Do not enable **SSL Acceleration** on the AD FS Internal VS when using the WAP role. The proxy

server needs to present a certificate of trust to the AD FS server.

7. Expand the **Real Servers** section.
8. Click **Add New**.
9. Type the **Real Server Address**.
10. Confirm that the correct port is entered.
11. Click **Add This Real Server**.

AD FS Internal Farm VS Recommended API Settings (optional)

This table outlines the API parameters and values set using the Progress Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	443
prot	tcp
VStype	http
SubnetOriginating	1
Schedule	lc
CheckType	http
CheckPort	80
CheckUrl	/adfs/probe
CheckUseGet	1

AD FS Proxy Farm VS Recommended API Settings (optional)

This table outlines the API parameters and values set using the Progress Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	443
prot	tcp
VStype	http
SubnetOriginating	1
Persist	src
PersistTimeout	3600
Schedule	lc
CheckType	https
CheckPort	443
CheckUse1.1	1
CheckUrl	/FederationMetadata/2007-06/FederationMetadata.xml
CheckHost	adfs.example.com

API Parameter	API Value
CheckUseGet	1

AD FS Progress Kemp as Proxy VS Recommended API Settings (optional)

This table outlines the API parameters and values set using the Progress Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	443
prot	tcp
VStype	http
SubnetOriginating	1
Schedule	lc
SSLAcceleration	1
SSLReencrypt	1
TLSType	3
CipherSet	BestPractices
ReverseSNIHostname	adfs.example.com

API Parameter	API Value
ExtraHdrKey	x-ms-proxy
ExtraHdrValue	KEMP
CheckType	http
CheckPort	80
CheckUrl	/adfs/probe
CheckUseGet	1

7

References

Unless otherwise specified, the following documents can be found at https://docs.progress.com/.

ESP, Feature Description

LoadMaster Web User Interface (WUI), Configuration Guide