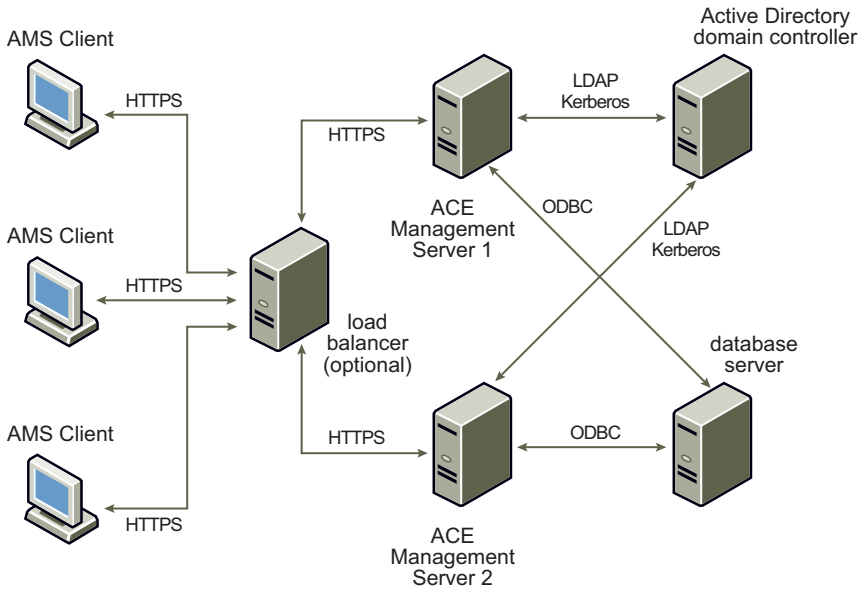
Configuring Multiple ACE Management Servers

VMware ACE 2.0

This technical note describes how to configure multiple VMware ACE Management Servers to work together. VMware® recommends this configuration for scaling ACE Management Server service for thousands of clients. See Figure 1.

Figure 1. Two ACE Management Servers Configured to Work Together



A single ACE Management Server can handle a preset number of clients, but you can add more servers to your ACE Management Server infrastructure by using load balancing. When you add more servers to the load-balancing group, the number of clients that you can serve will scale in a linear fashion. For example, if you can serve 2,000 clients with one server, using two load-balanced servers will allow you to serve 4,000 clients.

This technical note assumes that you are familiar with the installation and configuration of a standalone ACE Management Server with external database support. It also describes how to set up two or more servers and the extra steps that are necessary to use the load balance feature.

This technical note contains the following sections:

Requirements

To use the information in this technical note, you will need the following:

- Two or more machines (or Virtual Machines) to host the ACE Management Server processes
- An external database to host the ACE Management Server data
- A load balancing solution to manage traffic

Installation of Services

Install the ACE Management Server package on two or more machines (or virtual machines). Configure each one separately to access the same external database.

You must use an external database to configure multiple ACE Management Servers. Both ACE Management Server installations must be able to identify the same data store so either installation can field queries for clients and scale the number of clients that can be served.

You can verify that both ACE Management Servers are working properly by starting Workstation ACE Edition and connecting to each ACE Management Server directly (by IP or hostname). You should see the same data in the Instance View window. If you create a test ACE and preview it, you see the preview instance on both servers.

Using the Same SSL Certificate on All Servers

The following procedure describes how to copy the SSL certificate and key from one ACE Management Server to another.

To copy the SSL certificate and key from one ACE Management Server to another

1 Log into ACE Management Server 1.

2 Locate both the SSL certificate and key directory files.

- On Windows machines, the files are located at `C:\Program Files\VMware\VMware ACE Management Server\ssl`.
- On Linux machines, the files are located at `\var\lib\vmware\acesc\ssl.`

The certificate file is `server.crt`. The key file is `server.key`.

3 Use scp (secure copy) to copy the following files if you are using the Virtual Appliance of the ACE Management Server by performing the following steps:

a Enter **scp user@<host>:<file> user@<host>:<file>**.

You can also enable shared folders (if you are using VMware Workstation to run the Virtual Appliance), and copy the files out of the virtual machine through the shared folders feature.

b Open a browser, and load the configuration page for ACE Management Server 2.

c Click the **Custom SSL Certificates** tab.

d Specify the key file in the Server Private Key field.

e Specify the certificate file in the Server Public Certificate field.

f Click **Upload certificates**.

g Click **Apply**.

4 Restart ACE Management Server 2.

Creating New SSL Certificates and Keys for Each Server

If you do not want to use the same SSL certificate and key for each ACE Management Server, you must create new SSL certificates and keys for each server. The following steps guide you through the process of creating new SSL certificates and keys and installing them on your ACE Management Server.

To create new SSL certificates and keys

1 Create as many SSL certificate and key pairs as you need (one for each server in your server farm).

The procedure for doing this varies depending on the tools you use. See the documentation for your platform to determine how to create these certificates and keys. Each certificate must have a unique common name and a unique serial number.

2 If your certificates require a certificate chain to be verified, create a certificate chain file.

The certificate chain file is a text file that contains every certificate (in PEM format) needed in order to verify the leaf certificate (including the root certificate of the chain).

a Download the verification chain from your certificate authority.

b Each certificate must be in PEM format prior to creating the certificate chain file. To convert to PEM format, use the open SSL tools available online.

c Create the certificate chain file by concatenating each PEM-encoded certificate into one file.

You now have a certificate chain file for every new certificate that you have created. For example, if you are using two ACE Management Servers you would have two certificate chain files.

3 Join all of these certificate chain files into one large file. If you can, eliminate the duplicate entries.

4 Convert the server's SSL certificates to PEM format.

5 Add the server's SSL certificates in PEM format to the certificate chain file.

You have three files that need to be uploaded to every ACE Management Server in your farm:

- SSL certificate file
- SSL key file
- Certificate chain file

Complete this procedure for every ACE Management Server in your farm to upload files to each ACE Management Server.

To upload the files to the servers in your server farm

1 Open a browser and load the configuration page for your ACE Management Server.

2 Click the **Custom SSL Certficates** tab.

3 Specify the key file in the Server Private Key field.

4 Specify the certificate file in the Server Public Certificate field.

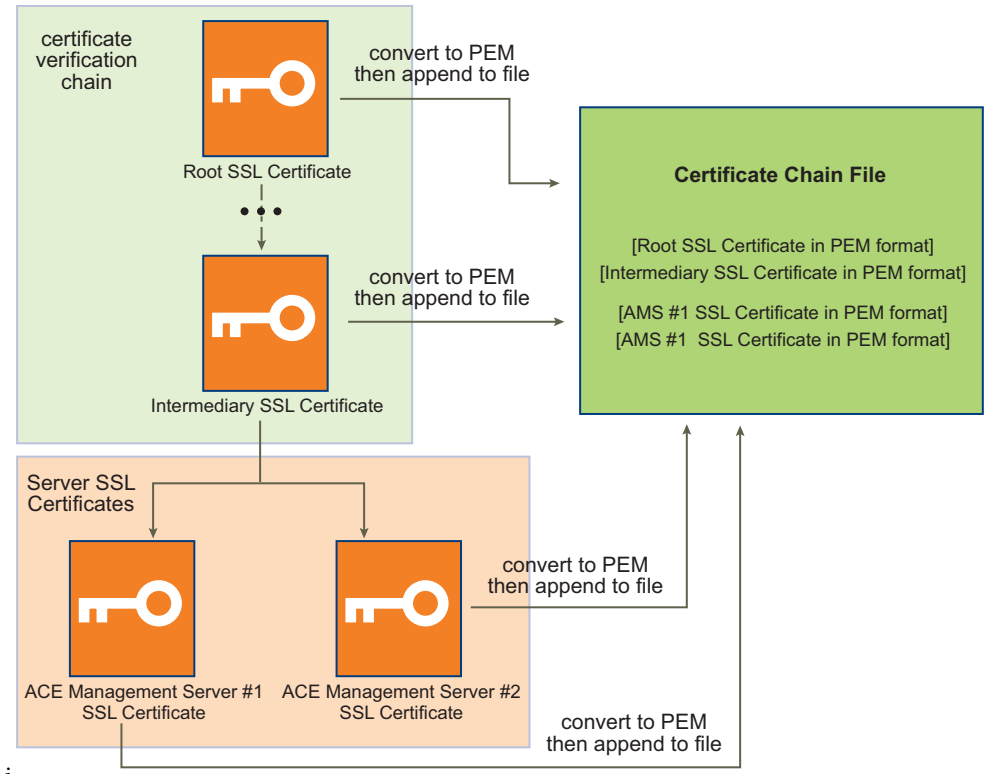
5 Specify the certificate chain file in the Server Public Certificate Authentication Chain field.

6 Click **Upload certificates**.

7 Click **Apply**.

8 Restart the ACE Management Server.

Figure 2. Creating the Certificate Chain File



i

Load Balancing

ACE Management Server uses HTTPS to communicate with its clients. Any load balancing solution that supports HTTPS should work with ACE Management Server.

Install your load balancer and configure port 443 (HTTP over SSL) for load balancing. Do not configure port 8080 or 8000 for load balancing. These two ports are used for configuration. Port 8080 is the virtual appliance configuration port and 8000 is the ACE Management Server configuration port.

Verification

Restart your Workstation ACE Edition client before verification. This is required so that Workstation ACE Edition re-downloads the SSL Certificate when a connection to the ACE Management Server is established.

You should be able to connect to your ACE Management Server using the address of the load-balancer. Create a test ACE instance and preview it. The preview instance should run and regardless of which ACE Management Servers its requests, you can test this in the following way:

To test your ACE instance

1 Create a test ACE template.

2 Open the policy editor.

3 Select **Policy Update Frequency**.

4 Select **Disable Offline Usage**.

5 Click **OK**.

6 Remove the first ACE Management Server from your load balancing configuration (all traffic will go to the second ACE Management Server).

7 Preview the test ACE.

This will create an instance on the ACE Management Server.

8 Close the ACE Player.

9 Remove the second ACE Management Server from the load-balancing configuration and add the first ACE Management Server back into the configuration.

All traffic will go to the first ACE Management Server now.

10 Preview the same ACE template again, when prompted whether to re-instantiate or re-use the instance, select **Use Existing Instance**.

The instance should start successfully. If the instance starts successfully, both servers are using the same SSL certificate.

Final Notes

It is also possible to configure multiple ACE Management Servers using different certificates, (self-signed or with a verification chain).

The steps for this procedure are similar. You must create new certificates and keys (or download them from your Certificate Authority). Upload them to each server.

An extra step is required when using separate certificates. Create a certificate chain file. The certificate chain file is a file that contains multiple certificates concatenated together (in PEM format). If both of your certificates are self-signed, your certificate chain file should be a file that contains both certificates concatenated. If you received your certificates from the same certificate authority, the chain file must contain only the verification chain for these certificates (which should be the same). If the certificates come from different certificate authorities, the chain file must contain both certificate verification chains.

Upload the certificate chain file at the same time that you upload the certificate and key file to the server.

VMware, Inc. 3401 Hillview Ave., Palo Alto, CA 94304 www.vmware.com

Revision 20070919