ACE Management Server Deployment Guide

VMware ACE 2.0

This technical note provides guidelines for the deployment of VMware ACE Management Servers, including capacity planning and best practices. The following sections are included:

Deploying ACE Management Server

A typical ACE Management Server deployment has the following components:

- One or more ACE Management Servers

  You can configure multiple servers to work on the same database and increase the capacity of your service. You can also deploy multiple servers for high availability.

- HTTP load balancer (optional)

  Use a load balancer to help you scale the capacity of your ACE Management Server deployment.

- Database server

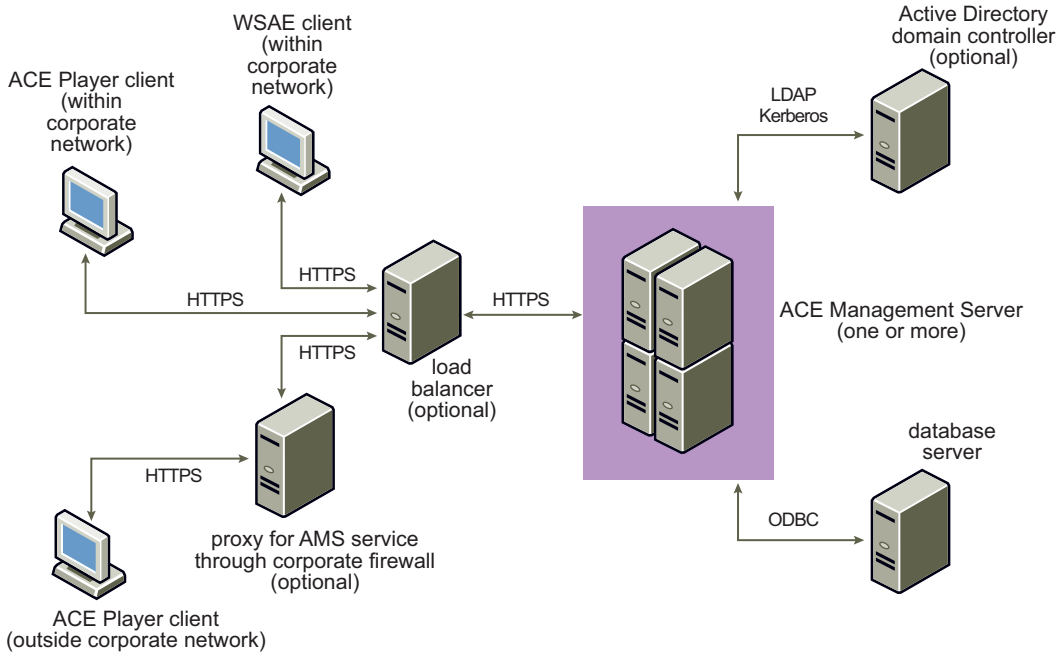
  For production deployments, VMware recommends Oracle or MS-SQL (Windows ACE Management Server), and Postgres (Linux ACE Management Server).

- Active Directory domain controller (optional)

  To enable the ACE Management Server Active Directory integration, you must configure ACE Management Server to communicate with your domain controller.

See Figure 1 for an example of an ACE Management Server deployment.

Figure 1. Comprehensive ACE Management Server Deployment



Performing Capacity Planning

The ACE Management Server enables you to manage ACE instances and policies in real time. It is important to perform capacity planning because it is possible that every ACE instance deployed in your enterprise will need to communicate with your ACE Management Servers.

Deployment Platforms

Choose from the following platforms to deploy the ACE Management Server:

- Windows 2003 Server
- VMware Virtual Appliance
- RHEL 4
- SLES 9

The platforms differ in the libraries they use to connect to active directory and the external databases they support.

Scalability Factors

The number of clients served by a single ACE Management Server installation depends on several key factors, including the following:

- Database throughput and scalability
- LDAP throughput (if you are using Active Directory)
- Network bandwidth available for incoming client requests
- Policy update frequency for your deployed instances
- ACE policy configuration

Clients Supported Per Server

Refer to Table 1 for a listing of the number of clients supported based on the platform you are using. The figures shown reserve some server processing power so that interactive clients receive responses in a timely fashion and increases in demand are satisfied by the server.

Table 1. Number of Clients Supported

Platform	Recommended Clients
Ghz AMD 2-way Server machine (Opteron 280) (4 GB RAM)	6,000
Ghz Intel 2-way Desktop Machine (4 GB RAM)	4,000

Database Throughput and Scalability

The following are recommendations and requirements for database throughput and scalability:

- For production deployments, VMware recommends that you use Oracle, MS-SQL, or Postgres as your database platform.
- Over 95% of the storage space required by the ACE Management Server is used to log event information, which is an audit trail of all transactions performed through the ACE Management Server. Refer to Table 2 for the recommended database size based on the number of clients that are being served.

  The figures in the table are based on a 90-day database archival period. Store your database records every 90 days and keep event logs for up to 90 days.

Table 2. Database Storage Recommendations

Number of Clients	Recommended Database Size
100	50 Mb
1,000	500 Mb
10,000	5,000 Mb

You can configure your ACE Management Server to purge event logs every 90 days.

It is possible to configure ACE Management Server to log less event information. From the ACE Management Server web configuration page, click the **Logging** tab. The authentication event generates most of the data because an event is generated every time someone attempts to authenticate to the ACE Management Server.

LDAP Throughput

The ACE Management Server will communicate with your Active Directory domain controller to authenticate user credentials. Your domain controller infrastructure handles the LDAP traffic required to support the number of clients that you anticipate.

Integrating with Active Directory through LDAP is implemented differently in the Windows ACE Management Server than in the Linux-based ACE Management Server. The Windows ACE Management Server uses the WinLDAP library bundled with your Windows Operating System. The Linux ACE Management Server uses a third-party Kerberos Library and OpenSSL. Internal testing results indicate that the Windows implementation is superior in both performance and configuration.

When configuring ACE Management Server to use LDAP, follow these guidelines to avoid affecting performance:

- Use a fully qualified hostname for the LDAP host. (for example, `ldap.vmware.com`) instead of an IP address or hostname with no domain postfix.
- The default domain is the domain for which the LDAP host is a domain controller.

- The query user is a user in the default domain.
- The admin user group is a group that exists in the default domain.

Network Bandwidth

The amount of network bandwidth required by the ACE Management Server and ACE instances depends on the frequency of policy updates that you have configured. Table 3 shows the amount of bandwidth that you will need when using a policy update frequency value of 10 minutes.

Table 3. Network Bandwidth Required with a Policy Update Frequency of 10 Minutes

Number of Clients	Bandwidth Required
100	0.125 Mbit/sec
1,000	1.25 Mbit/sec
10,000	12.5 Mbit/sec

VMware recommends that you increase the time between policy updates by clients for large deployments (more than 5,000 clients) because this reduces the amount of required bandwidth.

If you modify your policy update frequency, you can increase or decrease your network bandwidth requirements. For example, if you change the value to 30 minutes it requires one third as much bandwidth for the same number of clients.

Table 4 shows the bandwidth when the policy update frequency value is set to 30 minutes.

Table 4. Network Bandwidth Required with a Policy Update Frequency of 30 Minutes

Number of Clients	Bandwidth Required
100	0.04 Mbit/sec
1,000	0.4 Mbit/sec
10,000	4 Mbit/sec

The amount of network bandwidth required could also be higher if your policy set is very complex.

VMware recommends that you have a separate network link between the ACE Management Server and your database server, so that traffic coming and going from the ACE Management Server to its clients does not interfere with the traffic to and from your database server.

ACE Policy Configuration

Your configuration of ACE policies can affect performance. You can increase the amount of data that is transferred between the ACE Management Server and the ACE Player.

- Use of host policies

  Enabling host policies (such as host network quarantine) requires that a host-side daemon retrieve the host policies from the ACE Management Server.

- Complex network quarantine policies

  If the set of rules that makes up your network quarantine is very large, then the transfer of these rules from the ACE Management Server to the clients can affect the scalability.

  The numbers shown in Table 3 and Table 4 are estimations of required bandwidth given average size rule sets for network quarantine. You can view the size of your policy set by examining the ACE file directory, and counting the size of the .vmpl file. An average policy set is 15K bytes or less.

Deploying Thousands of Clients

The ACE Management Server client/server protocol is built on top of the HTTPS protocol. You can use HTTP load-balancing software and hardware solutions to scale an ACE Management Server deployment beyond the capacity of a single server (or for high-availability deployments).

The ACE Management Server scales in a linear fashion when an enterprise grade HTTPS load balancer is used. For more information on how to configure the ACE Management Server in multiserver deployments, see the *Configuring Multiple ACE Management Servers* technical note.

Security

The ACE Management Server has several security features. Following is an overview of these features and recommendations on how to configure the ACE Management Server to avoid security problems.

- Traffic to and from clients is protected by HTTPS.

  By default, ACE Management Server creates a self-signed certificate when you install it to use for HTTPS traffic. These certificates are secure, but you can also configure ACE Management Server to use your own certificate and key pairs.

- Traffic from ACE Management Server to Active Directory is encrypted.

  LDAP traffic is encrypted at the application layer. Credentials are protected by using the Kerberos protocol to authenticate credentials.

- Sensitive Configuration Options are encrypted.

  Passwords stored in the configuration file are encrypted.

- Database Security.

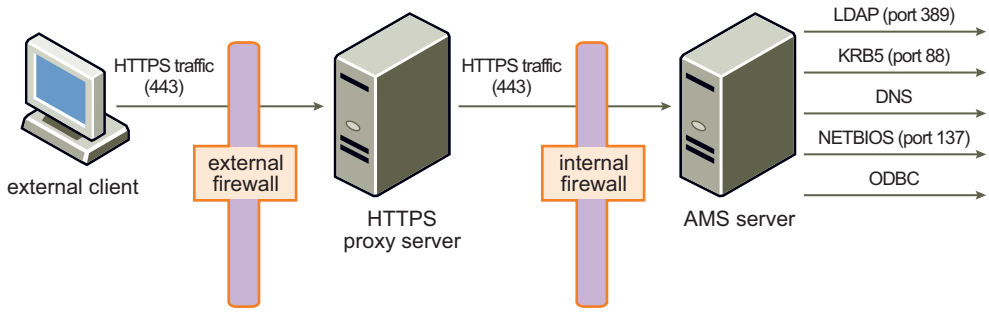
  The database store contains sensitive data such as cryptographic keys. Configure your database security so that it is protected from intrusion and protected in case of data loss. (Consult your database documentation for information on what features are available to protect your data.)

Access from Outside the Corporate Firewall

All client requests to the ACE Management Server are HTTPS traffic on port 443. This means that any solution using a proxy to secure HTTPS traffic into your corporate servers can be used to proxy ACE Management Server traffic.

VMware recommends the use of an HTTPS proxy in the DMZ, which relays ACE Management Server traffic to the actual ACE Management Server inside the corporate network. VMware recommends this deployment strategy because of the number of data connections that the ACE Management Server will need to make on the back end (LDAP, DNS, ODBC, KERBEROS).

Figure 2. Recommended Deployment for External Access to ACE Management Server



The following is a list of data connections that the ACE Management Server will make use of

- LDAP – Port 389, LDAP queries are encrypted.
- Kerberos – Port 88.
- DNS
- ODBC – Refer to the ODBC documentation on your server platform for information on how to secure ODBC traffic.
- NETBIOS – Port 137.

We have verified that the ACE Management Server can be deployed with the following HTTPS proxy solutions:

- Apache Proxy – Using mod_proxy
- Zeus Technology Load Balancer – A commercially available load balancer and traffic management solution.

There are a few notable pitfalls to avoid when using a proxy for traffic into the ACE Management Server:

- SSL Termination – If your HTTPS proxy terminates the SSL connection, then you must use the same SSL key/certificate on the HTTPS proxy server and the ACE Management Server. (Or you need to make use of the ACE Management Server's certificate chain to embed the HTTPS proxy certificate verification chain in the ACE package).

  An example of a proxy server that terminates SSL connections is Apache Proxy. The Zeus load balancing products support SSL passthrough, which means that the SSL connection is terminated at the ACE Management Server.
- Multiple ACE Management Server SSL certificates – If you are deploying multiple ACE Management Servers behind a load-balancing solution, all ACE Management Servers must use the same SSL key/certificate pair. (Alternatively you can use the ACE Management Server certificate chain feature to embed every SSL certificate verification chain into the ACE package).
- DNS resolution – When you create an ACE Master, you must specify a hostname for the Ace Management Server. This hostname must resolve to the appropriate IP address for both internal and external clients. Internally, it can resolve to the ACE Management Server itself. Externally, it can resolve to the HTTPS proxy server.

Final Note

Because the traffic coming into the ACE Management Server is plain HTTPS traffic and the server is stateless, many other configurations can be deployed to provide external access to the ACE Management Server. VMware recommends that you think of the ACE Management Server as a regular web server with secure traffic when designing your deployment.

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

Revision 20070919