vmware

Technical Note

Integrating Linux Hosted ACE Management Server with Active Directory

VMware ACE 2.0.1

This technical note outlines how Linux hosted ACE Management Server integrates with Active Directory, describes default installations, and outlines basic troubleshooting.

This document applies to the Linux hosted ACE Management Servers, which use RHEL4 and the debian-based Virtual Appliance from VMware.

Implementation Overview

ACE Management Server uses LDAP to query Active Directory for user and group information. To access LDAP, ACE uses the SASL authentication abstraction layer. In particular, ACE Management Server uses the GSSAPI authentication method when binding to the LDAP server.

To successfully complete a GSSAPI bind, ACE Management Server makes use of the MIT Kerberos5 library. ACE Management Server implements a Kerberos client that authenticates users to the Active Directory Key Distribution Center (KDC). Kerberos5 has been a part of Windows NT since Windows 2000.

The data passed by the LDAP protocol is protected by application layer encryption based on the keys exchanged by the Kerberos authentication protocol.

Ports in Use

ACE Management Server uses the following ports directly when integrated with Active Directory:

- 389 – LDAP traffic
- 88 – Kerberos authentication traffic

Indirectly, ACE Management Server also uses DNS services by default (due to features enabled in the Kerberos library).

Active Directory Integration Details

During the configuration phase of the ACE Management Server, the administrator provides the following information:

- LDAP server host name – The network host name of the machine that is running your LDAP service (your domain controller). For example, ldap.vmware.com.
- Query user UPN – The account that ACE Management Server uses to log onto the LDAP service to query for user and group information. The format of the user name is user@domain, otherwise known as user

principal name. In the LDAP service the attribute for the user object is called userPrincipalName. For example, ams@vmware.com.

- Query user password – The password for the query user account.
- Default domain – The name of the domain to use by default. This default domain is used when users do not enter domain information while logging in. The format of the domain name is dot delimited. For example, vmware.com.
- Admin group DN – The FQDN of the group to which ACE administrators belong. Users who use WSAE to create and modify ACEs and instances must belong to this group. The format of the admin group DN is FQDN. For example, cn=Ace Administrators, cn=Users, dc=vmware, dc=com.

This information is used when ACE authenticates users and verifies group memberships.

ACE Management Server interactions with Active Directory fall into several categories:

- Authentication of administrators in the web configuration UI
- Authentication of administrators or help desk personnel in the Web UI (Helpdesk Web application)
- Authentication of administrators in the Workstation Ace Edition application
- Authentication of end users in the player application
- Enables proxy change of password requests using the player application

Authentication of Users and Accessing the LDAP Service

ACE Management Server uses the MIT Kerberos library for two purposes:

- To authenticate user credentials
- To gain necessary credentials to complete a GSSAPI bind to the LDAP service with the query user specified during configuration

Both of these operations are identical except that when you do an LDAP bind, you store the tickets that are received from the Kerberos server after a successful authentication so that the LDAP library can use them.

For the Kerberos library to perform an authentication, your Linux ACE Management Server host machine must be able to resolve certain DNS queries. For more information, read the Kerberos documentation included with your Linux distribution.

- The KDC host is resolved through DNS. This means that your DNS server must resolve a request for the _kerberos tcp service for the specified domain (either default domain or a domain specified by the user).
- The domain name must resolve to a valid host IP. For example, vmware.com in your network resolves to ldap.vmware.com's IP address.
- Reverse lookups for the KDC must resolve.
- Reverse lookups for the domain name IP must resolve.
- The host name of the ACE Management Server host must resolve in your DNS.
- A reverse lookup entry for your ACE Management Server host IP must resolve in your DNS.

If any of these DNS queries fail, you get a failure from the Kerberos library. Some of these failures are easy to identify (for example, “cannot find KDC host”) and some are more difficult to identify (for example, local errors).

Troubleshooting Guide

If your ACE Management Server host is having trouble integrating with your AD configuration, follow these steps to determine the problem, and how to correct it.

1 Verify your configuration inputs:

- LDAP host name

  Can you ping your LDAP host from the ACE Management Server host?

  Can you do a forward lookup of the host name from your ACE Management Server host? Enter the `nslookup <host name>` command to verify.

  Can you do a reverse lookup of the IP for the LDAP server? Enter the `nslookup <ip–address>` command. The result should be the same host name that you have entered into the configuration.

  Can you connect to port 389 on the LDAP host from the ACE Management Server host? Verify that no firewalls are blocking the connection. To connect to the port, enter the `telnet host name 389` command.

- Query user information

  Verify that the user name is correct.

  Verify that password is correct and not expired.

- Default Domain

  Verify that default domain resolves to a valid IP on DNS. Enter the `nslookup <domain name>` command. For the best results, default domain should be the domain for which the LDAP server host is a domain controller.

2 Verify that your ACE Management Server host clock is accurate:

- If the clock on the ACE Management Server host is off by more than 5 minutes you receive an error message: Clock skew too great.
- Use NTP to keep your clock accurate.

3 Verify your local network configuration (ACE Management Server host):

- Your host name should resolve on DNS. Enter the `nslookup <host name>` command.
- Your IP should have a revert lookup entry that matches the forward lookup entry. Enter the `nslookup <ip address>` command.

If any of these entries fail to resolve, or resolve with inaccurate information, you must correct the problem before continuing to run ACE Management Server.

Resolve these DNS resolution problems by modifying the entries in your DNS server or by adding entries to your `/etc/hosts` file.

After fixing DNS issues, flush the DNS cache on the ACE Management Server host by stopping and starting the NSCD service:

```
/etc/init.d/nscd restart
```

Using the krb5.conf file

If ACE Management Server still will not verify your LDAP configuration options due to an LDAP connection problem, you can direct ACE Management Server not to use DNS while using the Kerberos library. Instead, it can provide all the network topology information to ACE Management Server through a krb5.conf file.

The krb5.conf file is a MIT Kerberos library configuration file. ACE Management Server installs a default krb5.conf at the following location:

```
/var/lib/vmware/acesc/conf/krb5.conf
```

This file contains three configuration settings:

```
[libdefaults]
    dns_lookup_realm = true
    dns_lookup_kdc = true
    clockskew = 3600
```

The first two settings instruct the Kerberos library to use DNS to resolve the KDC host name and the REALM.

If you are having trouble integrating ACE Management Server with Active Directory, this file enables you to bypass all the DNS lookups, and instead provide specific information about your network so that Kerberos will operate. If you turn off DNS lookups for realm and KDC, you must specify the KDC for your realm (domain). Following is an example of a krb5.conf file that turns off DNS lookups and defines the vmware.com realm:

```
[libdefaults]
    dns_lookup_realm = false
    dns_lookup_kdc = false
    clockskew = 3600
[realms]
    VMWARE.COM = {
    kdc = ldap.vmware.com
    }
```

This file tells Kerberos not to perform DNS lookups for realms and KDCs. The file also defines the KDC server for the vmware.com realm as ldap.vmware.com. Because we omitted the port number for the KDC, the default port numberf 88 is used.

For more information on krb5.conf, read the documentation that comes with your Linux distribution.

If you still have problems after modifying your krb5.conf file, modify the /etc/hosts file on your ACE Management Server host so that all hosts involved in the Active Directory configuration are included. For example, your /etc/hosts file for the vmware.com ACE Management Server might have the following entries:

- 10.20.30.40 ldap.vmware.com ldap
- 10.20.30.40 vmware.com
- 10.20.30.41 ams.vmware.com ams

In this example, 10.20.30.40 is the IP for the domain controller (and LDAP server) and 10.20.30.41 is the IP address for the ACE Management Server host.

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

Revision 20070807