



VMware ACE

Integration with Active Directory

This document explains how to set up Active Directory to use with VMware ACE.

This document contains the following topics:

- [About Active Directory on page 1](#)
- [About VMware ACE on page 1](#)
- [Getting Started on page 2](#)
- [Setting Up Active Directory on page 4](#)
- [Viewing Active Directory Data on page 5](#)

About Active Directory

Active Directory is a directory service included with Windows® 2000 server. It stores information about objects in a network and provides a single point of administration for permitted resources anywhere on a network.

You can use Active Directory with VMware ACE in a number of ways:

- To define users and groups who can power on a virtual machine
- To store a dynamic, custom or version-based network quarantine policy
- To define users and groups who can connect devices in a virtual machine

Before you can store VMware ACE objects in Active Directory, you must have at least one Active Directory domain set up and you must initialize a domain by using VMware ACE Manager.

About VMware ACE

VMware ACE extends virtual machine technology to address security issues in a networked computing environment. VMware ACE enables you to apply corporate IT policies to a virtual machine containing an operating system, enterprise applications and data to create a secure, isolated PC environment known as an "assured computing environment".

A primary of advantage of using VMware ACE is that you create a standard, self-policing PC environment for your user. This means:

- Users can run standard PC applications without modification.
- Users can connect to the corporate network with standard networking protocols.



- Users can work whether connected to the corporate network or not; when users are not connected, IT policies, such as authentication and access to devices and networks, are still enforced.

With VMware ACE, you create a virtual machine and apply a set of Virtual Rights Management policies to it. Policies include:

- **Encryption and authentication** — Protect data on the virtual machine through encryption and control access through password and directory service authentication.
- **Life cycle control** — Set an expiration date, after which the virtual machine is disabled. For example, you can limit guest workers to the length of a contract, or reclaim licenses that have expired.
- **Network quarantine** — Restrict the networks that the virtual machine or host can access. For example, you can require that the virtual machine connect to the corporate network through a VPN server only and restrict the host machine from any access to the corporate network.
- **Device access** — Restrict the virtual machine access to some or all of the host's devices, such as CD-ROM/DVD, floppy and USB drives, to create a totally isolated environment.

After you create a virtual machine, set desired policies and install any software on the virtual machine, you create an installable package. You can easily supply the newly created virtual machine to employees, contractors or business partners as needed.

If IT policies change, or if particular users need to change policies, you can easily create a new set of policies and distribute an update package with the new policies to your end users.

Basic Terminology

The following terms are important in the context of this document:

Guest operating system — An operating system that runs inside a virtual machine.

Host computer (or machine) — The physical computer on which the VMware ACE software is installed. It hosts VMware ACE virtual machines. The operating system on a host machine is referred to as the host operating system.

Network quarantine policy — A policy that controls the access of a virtual machine to networks and machines. Network quarantine policies can be either static or dynamic. A static policy is installed with the virtual machine and cannot be updated except by updating the entire virtual machine. A dynamic policy resides on a Web server or on an Active Directory server, and can be updated as necessary without updating the virtual machine.

Virtual Rights Management policies — Policies control the capabilities of a virtual machine. You set policies by using the policy editor in VMware ACE Manager.

Getting Started

This section describes at a high level how to create a project and virtual machine by using VMware ACE Manager. It assumes you are familiar with using VMware ACE Manager and that you have read the technical note, "VMware ACE: Best Practices Setup," available at: http://www.vmware.com/support/resources/ace_resources.html. That document describes in detail the process that this section covers at a high level. After you create a project and virtual machine you can begin to use Active Directory to manage your VMware ACE policies.



What You Need

To complete the procedures in this document requires the following:

- VMware ACE Manager.
- An Active Directory server
- An Active Directory editor, such as ADSI Edit, that you can use to view and edit Active Directory objects. ADSI Edit is included in the Microsoft support tools package, which you can download for free from either of the following sites:
 - **Windows 2000** — <http://www.microsoft.com/windows2000/downloads/servicepacks/SP4/supporttools.asp>.
 - **Windows XP** — <http://www.microsoft.com/downloads/details.aspx?FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38&DisplayLang=en>.

Before starting the step-by-step procedures in this document, make certain you have the *VMware ACE Administrator's Manual* available. You should also photocopy and fill out the two checklists in that manual:

- Checklist: Creating a Project
- Checklist: Adding a Virtual Machine

Creating a Project and Adding a Virtual Machine

A project contains one or more virtual machines and the VMware ACE application to run the virtual machines. In the project you create a package to install a virtual machine and the application on a user's machine.

To create a project, run VMware ACE Manager and click the New Project icon or click **File > New Project** to start the New Project Wizard. Enter a name for the project and a location in which to store project files. When you are finished, select **Open the Add Virtual Machine Wizard** to go directly to the wizard for adding a virtual machine to the project.

Note: When you create a project, the New Project Wizard automatically adds the VMware ACE application to the project. End users use this application to run and manage the virtual machine. You can set preferences for this application if you wish, although this document does not show you how to do so.

When the Add Virtual Machine Wizard starts, take the following steps to add a virtual machine to the project:

1. Click **Next** to enter the wizard. The Add New or Existing Virtual Machine panel appears.

Note: This document assumes you have already created a corporate virtual machine image that contains your supported operating system and applications.

Select **Existing virtual machines** and click **Next**.

2. The Select Virtual Machines panel appears.

Click **Browse** and navigate to the configuration (`.vmtx`) file for the virtual machine you want to add to the project, then click **Next**.

3. The Ready to Complete panel appears.

When you are ready to finish the Add Virtual Machine Wizard, do not select **Set policies after the wizard closes** — you are going to set up Active Directory before setting policies.

Click **Finish** to exit the wizard.



Setting Up Active Directory

Before you can store policies in Active Directory you must initialize a domain for use with VMware ACE by using the project settings editor in VMware ACE Manager. Be certain you have access to the Active Directory domain you plan to use from the workstation on which you are running VMware ACE Manager.

Note: To complete the steps in the following procedure, you must have domain administrator's authority for the Active Directory domain you plan to use to store VMware ACE data. VMware ACE Manager cannot be installed on the same machine as the Active Directory domain controller.

To initialize an Active Directory domain, run VMware ACE Manager and complete the following steps:

1. Open a project and click **Project > Settings**.
The Project Settings dialog box opens. Click the **Policies Domain** tab.
2. From the Policies domain drop-down list, select the domain to use with the VMware ACE project.
Enter the user name and password for the domain administrator.
3. Click **OK** to initialize this domain. Click **OK** again to exit the Policy Settings dialog box.

Note: When you store policies on your Active Directory server, you must be sure end users' host computers have been added to the domain where the policies are stored. End users must log on to that domain so VMware ACE has access to the policies. Similarly if you set policies based on users and groups in your Active Directory domain, end users' host computers must log on to a domain where those users and groups are defined.

After you initialize a domain, you can set any of the following policy options that require an Active Directory server:

- Set an authentication policy that uses Active Directory to define the users and groups who can power on a virtual machine.
- Set a network quarantine policy that stores the policy file in Active Directory.
- Set a device policy that uses Active Directory to define the users and groups who can connect or disconnect a device in the virtual machine.

Setting VMware ACE policies that use Active Directory does not require any special tools or knowledge of Active Directory. You can set and manage policies, including Active Directory-backed policies, by using the policy editor in VMware ACE Manager. Likewise, if you need to make changes to a policy that is stored in Active Directory, you do so by using the policy editor in VMware ACE Manager not by using an Active Directory editor.

The one situation in which you might need to edit VMware ACE data directly in Active Directory is if a project is obsolete or contains obsolete data. VMware ACE Manager does not give you the ability to remove data from Active Directory. Therefore, if you are just curious and want to know where Active Directory stores VMware ACE data, or if you want to clean up after an obsolete project, the next section shows you how to locate VMware ACE data in Active Directory.



Viewing Active Directory Data

You can use any Active Directory editor to view and edit VMware ACE data that is stored in Active Directory. Microsoft provides a free editor, ADSI Edit, in the support tools packages for the Windows operating system. You can get the appropriate support tools package at one of the following sites:

- **Windows 2000** — The support tools package for Windows 2000 SP4 is available on the Windows 2000 CD and on the Microsoft Web site at:
<http://www.microsoft.com/windows2000/downloads/servicepacks/SP4/supporttools.asp>.
- **Windows XP** — The support tools package for Windows XP SP2 is available on the Microsoft Web site at:
<http://www.microsoft.com/downloads/details.aspx?FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38&DisplayLang=en>.

With ADSI Edit you can add, delete and move objects within Active Directory. You can also use ADSI Edit to search Active Directory.

To run ADSI Edit, click **Start > Programs > Windows 2000 Support Tools > Tools ADSI Edit**.

Note: ADSI Edit automatically attempts to load the current domain to which the user is logged on. If this is not the domain you use with VMware ACE, you can configure ADSI Edit to connect to a different domain.

To connect to a different domain, run ADSI Edit and complete the following steps:

1. Select ADSI Edit at the root of the console tree and Click **Action > Connect to**.
2. The Connection dialog box opens.
Select the option under **Computer: Select or type a domain or server**.
Enter a domain or Active Directory server name.
3. Click **OK**.

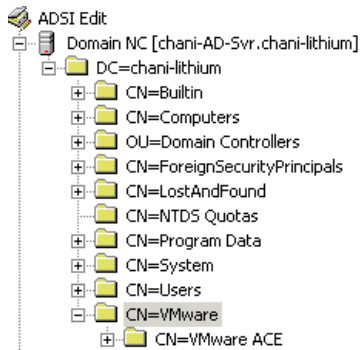
The following section shows the structure that Active Directory creates to store VMware ACE data.

Active Directory Container Structure

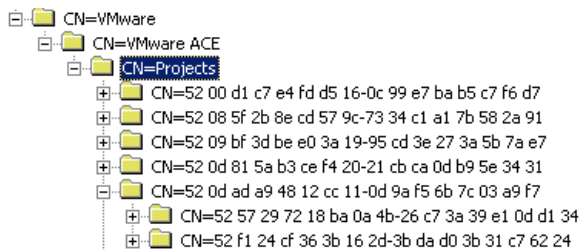
Active Directory uses a hierarchical container, or directory, structure for the objects it manages. When you initialize a domain for use with VMware ACE, Active Directory creates a **VMware** container at the root level of the Active Directory server. The **VMware** container is the root container for any VMware objects that you choose to manage with Active Directory. Underneath the **VMware** container, Active Directory creates containers for each VMware product whose



resources Active Directory manages. For VMware ACE, Active Directory creates a `VMware ACE` container. The following figure shows the hierarchy for VMware and VMware ACE:



When you create a project, Active Directory creates a `Projects` container underneath the `VMware ACE` container to hold individual project containers. Active Directory names project containers with the project ID. Each project container holds containers for all the virtual machines for that project. Virtual machines are named with virtual machine IDs. The following figure shows sample project and virtual machine containers:



You can find the project ID and the virtual machine ID in the virtual machine's policy file, which, by default, is located at:

```
C:\Documents and Settings\

```

In the policy file, the following entries identify the virtual machine and project:

- `support.mvmid` — The virtual machine ID.
- `support.projName` — The name of the project.
- `support.projid` — The project ID.

For example, the following are sample entries from a virtual machine policy file:

```
support.mvmid = "52 f2 5d 4e 21 1f f9 43-d1 68 3e 32 17 28 0e 26"
support.projName = "Fun"
support.projid = "52 d6 12 4a 63 a1 d7 dc-df 09 d4 ad 59 8d 1b fe"
```

VMware ACE Objects

Underneath the virtual machine container, Active Directory creates separate containers for each type of VMware ACE policy you can manage with Active Directory: authentication, network quarantine and device.

Active Directory stores data for a policy in the `url` attribute of a container.

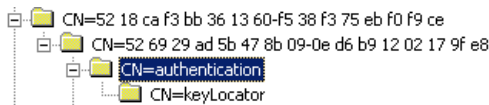
To view attributes in ADSI Edit, complete the following steps:



1. Expand the console tree to view the container that holds the policy. For example, Active Directory stores network quarantine policies in the `configurationBlock` container. Right click the container and click **Properties** from the pop up menu.
2. The Properties dialog box appears
In the Select a property to view drop down box, scroll down and select the **url** attribute.
The Values box contains a string that defines the parameters for the network quarantine policy.
3. Click **Cancel** to exit the Properties dialog box.

Authentication Policies

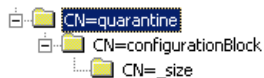
When you set an Authentication policy for a virtual machine, one of the options is to allow access by individuals and groups defined in an Active Directory domain. When you do so, Active Directory creates an `authentication` container as a sub container of the virtual machine container, as shown in the following figure:



The `authentication` container holds a key that can be used to retrieve the encryption key for the virtual machine. When you specify Active Directory users and groups in VMware ACE Manager, Active Directory creates an access control list. Only those users and groups who have access to this container can access the encryption key and power on the virtual machine.

Network Quarantine Policies

When you set network quarantine policies — other than static policies— you have the option of storing the network quarantine policy file in Active Directory. When you do so, Active Directory creates a `configurationBlock` container and `_size` container as shown in the following figure:



The `configurationBlock` container holds a string that contains the configuration parameters from the network quarantine policy file.

The `_size` container stores the size of `configurationBlock`.

Anyone can read the data in the `quarantine` container and in its sub containers. In this way, an end user's host machine can read the `configurationBlock` in Active Directory to check for the policy to apply to a virtual machine running on the host.

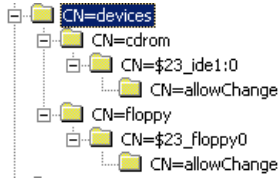
Only a domain administrator can write to the `quarantine` containers.

Device Policies

When you set device connection policies for a virtual machine, you can specify Active Directory users and groups who are allowed to connect or disconnect each device. When you do so, Active



Directory creates a `devices` container to hold individual devices, such as a CD-ROM and floppy drive, as shown in the following figure:



The `<device_name>` container (`$23_ide1:0` in the figure) holds a Boolean value, set to TRUE. This value indicates that users who have access to this container, are allowed to connect or disconnect the device. When you specify Active Directory users and groups in VMware ACE Manager, Active Directory creates an access control list for the container.