VMware ACE

Custom Authentication

This document explains how to write a simple script to authenticate remote VMware ACE users.

This document contains the following topics:

About Authentication

You set encryption and authentication policies to ensure that data on a virtual machine is protected and that only authorized users can power on the virtual machine. VMware ACE provides several different methods to authenticate users' access to encrypted virtual machines.

The most basic authentication method requires a user to set a password when opening the virtual machine for the first time. The password is required each time the virtual machine runs.

For more dynamic control, you can define access to the virtual machine in your Active Directory server. However, if you are managing virtual machines that are installed on host machines outside your company firewall, using Active Directory is not a good solution because an Active Directory server should be located within the firewall.

This document describes how to write an authentication script that plugs in to the VMware ACE environment. An authentication script runs automatically whenever the virtual machine is powered on or reset and either allows or denies access to the virtual machine depending on whether its validation criteria are met.

The advantage of using a script for authentication is that you can customize the validation criteria for your particular situation. The authentication script that this document describes is very simple — it verifies the name of the user and host machine against a list of authorized users and hosts. But you can write a script with criteria as varied and strict as you need, and you can customize the script to work with other security features you already have in place. For example, you can write a script that works with smart-card or biometric technologies to validate users.

Note: The simple authentication script described in this document is not meant as a production quality solution to authentication. For example, the script does not require a password for validation and the encryption key is stored in an unencrypted text file in plain view on a server. This script is intended to show you how to write an authentication script and it illustrates how the authentication process works when you write and install an authentication plug-in.

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.

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

***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.

Implementing A Solution with VMware ACE

VMware ACE provides a scripting interface that you can use to write plug-in scripts for a number of different policies, including authentication. You create an authentication script to run on the host machine to validate access and decrypt the virtual machine. In VMware ACE Manager you specify a script-based authentication policy and identify the script to run. The script runs whenever a virtual machine powers on or resets.

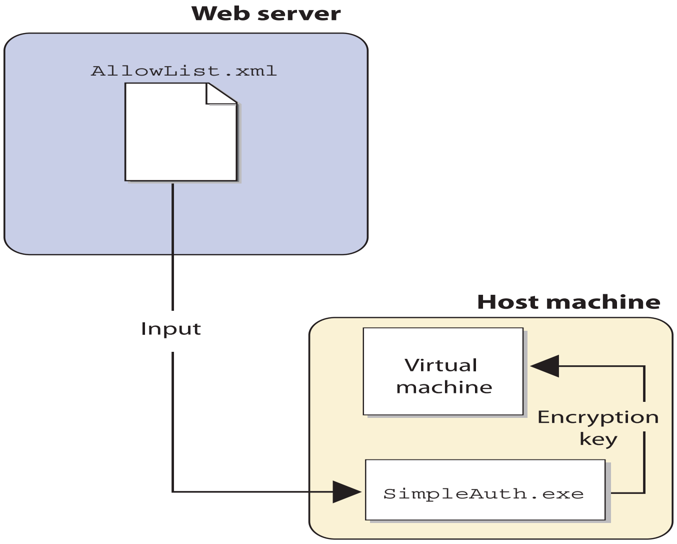
The first time an authentication script runs, the output of the script is hashed to create a key to encrypt the virtual machine. When the script runs subsequently, if the access criteria are met, the script must return the same value to decrypt the virtual machine.

You can specify any access criteria you want for an authentication script. For example, you could integrate the script with a card-reading mechanism and require that users enter a pin and a random number from a smart card. The sample authentication script described in this document is deliberately simple. It is easy to implement and understand, and clearly illustrates the VMware ACE scripting mechanism, but it is not meant as a real-world solution. By understanding this sample, you should be able to write your own, more complex, authentication script.

The sample authentication script, `SimpleAuth`, is written in C. You can write the script in any language that can run on your end users' machines.

How the Sample Script Works

The following figure illustrates how the `SimpleAuth` program authenticates a user who powers on a virtual machine.



You store the list of allowed users on a web server, which makes it easy to add or remove users at any time. The script takes the Web server name and path to the authentication list (`AllowList.xml`) as input. It gets the current user name and host name from the environment and compares them to the list of user/host pairs. If the current user and host are on the list of approved users and host, the user is granted access and the script returns the key to decrypt the virtual machine. If the user is not granted access, the script exits with a non-zero value and prints an error message.

Getting Started

To get started, use VMware ACE Manager to create a project, add a virtual machine and apply policies to the virtual machine. This section provides a high-level view of that process. 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.

What You Need

To complete the procedures in this document, you need the following:

- VMware ACE Manager.
- The sample script and files from VMware, which are contained in the `SimpleAuth` folder. You can download this folder from: *http://www.vmware.com/support/resources/ace_resources.html*. `SimpleAuth` includes source files, the `SimpleAuth` executable and any library files needed to build the executable.
- A C compiler to compile the sample scripts if you plan to modify any of them.
- A Web server.

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 (`.vmx`) file for the virtual machine you want to add to the project.

3. The Ready to Complete panel appears.

   When you are ready to finish the Add Virtual Machine Wizard, select **Set policies after the wizard closes** to go directly to the policy settings editor after the wizard creates the virtual machine.

   Click **Finish** to exit the wizard.

Creating Policies for the Virtual Machine

Policies are at the heart of managing a virtual machine. You set policies using the policy editor in VMware ACE Manager. The current document explains how to set a script-based authentication policy. At a minimum, you should also set the following policies:

- **Copy protection** ensures that the virtual machine can be run only from the location in which you install it.
- **Device policies** restrict access for the virtual machine to the host's devices such as DVD/CD-ROM, floppy and so on. This prevents data on the virtual machine from being exposed when the host machine is outside the corporate network.
- **Network quarantine** gives you fine-grained control over the network access you provide to users of your virtual machines. Network quarantine has a number of specific uses, which

are described in the following VMware ACE white papers, available at *http://www.vmware.com/support/resources/ace_resources.html*:

- VMware ACE: Managing Remote Access, explains how to use network quarantine and other policies to manage remote access through VPN to a corporate network.
- VMware ACE: Managing Guest Workers explains how to use network quarantine and other policies to manage workers who at different times access the corporate network remotely and from within the network.
- VMware ACE: Enforcing Patch Management explains how to use version-based network quarantine policies to enforce patch management strategies.
- VMware ACE: Enforcing Patch Management Using Custom Quarantine explains how to write a custom script to apply network quarantine policies that enforce patch management strategies.

You can set other policies as well, such as an expiration date when the virtual machine can no longer be used. But the policies just described ensure that the virtual machine is secure and isolated from the host on which it runs.

For detailed information about why and how to set these policies, see the technical paper "VMware ACE: Best Practices Setup," available at: *http://www.vmware.com/support/resources/ace_resources.html*.

Installing SimpleAuth

All the files required to compile and run `SimpleAuth` are contained in the `SimpleAuth` folder, which you can download from *http://www.vmware.com/support/resources/ace_resources.html*. The `SimpleAuth` folder contains the following items:

- `Helpers` — A folder that contains the `objectlist` folder, which hold C libraries for use by `SimpleAuth`. You only need the helper files if you modify and recompile the source for the application.
- `SimpleAuth` — A folder that contains the `SimpleAuth` source and executable.
- `AllowList.xml` — An XML file that contains a list of allowed user/host pairs.

You must place a copy of `SimpleAuth.exe` in the `Project Resources` directory of the main project directory so VMware ACE can execute the script. The default path to the `Project Resources` directory is:

```
C:\Documents and Settings\<user>\My Documents\VMware ACE
Projects\<project_name>\Project Resources
```

You must also put a copy of `AllowList.xml` on a Web server that is accessible to users' host machines.

Setting Up Authentication

This section explains in detail how the `SimpleAuth` program works and provides some tips on how you can create a more robust authentication script for your environment.

`SimpleAuth` is a C program, included in the `SimpleAuth` folder, that runs on the host machine and determines whether to grant access and decrypt the virtual machine. The program takes an XML file, `AllowList.xml`, as input. The XML file contains a list of allowed user/host name pairs. See About the Authentication List on page 7.

`SimpleAuth` does the following:

- Downloads the XML file with the list of approved users and hosts from the Web server. You pass the server name and path of the file to `SimpleAuth` on the command line.

  The custom function, `GetAllowList`, that downloads the file, uses the WinInet support library from Microsoft®. This function does not support SSL or proxies. A more complete example of how to use Microsoft WinInet library can be found at the Microsoft developer's site (MSDN): *http://msdn.microsoft.com/archive/*.

- Parses the XML file.

  The `ParseXMLConfigFile` function creates a linked object list with an object for each entry in the XML file. Each object represents an allowed user and contains a user name, host name, and encryption key for the virtual machine.

- Retrieves the current user name and host name from the host machine environment.

  The `GetCurrentUserObject` function uses the Windows® API to get the user name and host name.

- Compares the current user name and host name to the list of valid users from the XML file.

  The `UserObjectCompare` function looks for a match between the current user and the objects in the list of valid users. If there is a match, the function returns 0; otherwise, it returns a non-zero value. Note that this function looks for a user name first. If successful, it looks for a host name. If the XML file does not have a host name, the function skips this validation and returns 0. In this way, the authentication script allows you to be flexible in your implementation of authentication criteria in the XML file.

- Prints the encryption key if validation is successful.

  If validation fails, or if the script encounters errors, it exits with a value of 1. All output to StdErr is written to the VMware ACE log file. For example, the script writes to StdErr a list of any required products or patches that are missing.

About the Authentication List

The authentication list for `SimpleAuth` is stored in an XML file called `AllowList.xml`. `AllowList.xml` is included in the distribution of the `SimpleAuth` sample code.

`AllowList.xml` uses the following schema to store user names, host names and encryption keys:

```
<AUTHENTICATION_LIST>
   <USER>
      <NAME>Bob</NAME>
      <HOSTNAME>bob-xpwork</HOSTNAME>
      <USEKEY>8E9887...ABC53E1<USEKEY>
   </USER>
   ...
</AUTHENTICATION_LIST>
```

The user key is the encryption key that `SimpleAuth` returns to encrypt and decrypt a virtual machine. To ensure best security, for a value that includes only printable characters, create a value that is at least 32 bytes long.

The `SimpleAuth` sample program looks for the authentication file on a server. This is a good practice in a production environment as well because it allows you to easily update the authentication list as you distribute virtual machines to new users over time.

Obviously, leaving the encryption key in the open allows anyone to break your encryption scheme for virtual machines. In a production environment you need to provide a more secure method of storing and retrieving the encryption key. For example, a simple approach, such as encrypting the authentication file and embedding its decryption key in the authentication script is a start toward a more secure solution.

Setting the Authentication Policy

You set the authentication policy by using the policy editor in VMware ACE Manager. In the policy editor you identify the script to use and the arguments to pass to it. You can also specify a timeout interval.

Note: Before you start this procedure be certain that you have copied `SimpleAuth.exe` to the `Project Resources` directory.

To set the authentication policy, complete the following steps in VMware ACE Manager:

1. Start the policy editor (click **Project > Policies**; or from the project summary page, select the **Edit virtual machine policies** icon).

   Click the + sign beside the name of the virtual machine. The list of policy categories appears below the virtual machine name.

2. Select **Encryption and authentication**.

   In the Encryption panel, select **Encrypt data and configuration files when this virtual machine is installed**.

   Also select **Enable virtual machine recovery** so you are able to use a hot fix to reset the end user's password. If you enable recovery, be sure to create a recovery key. For more information about setting encryption and recovery policies see the technical note: "VMware ACE: Best Practices for Setting Up VMware ACE" available at *http://www.vmware.com/support/resources/ace_resources.html*.

3. In the Authentication panel, select **Determine using script**.

   Click **Set** to open the Set Custom Script dialog box.

   In **Script file**, browse to the `Project Resources` folder and select the name of your script. The default location for this folder is:

   ```
   C:\Documents and Settings\<user>\My Documents\VMware ACE
   Projects\<project_name>\Project Resources
   ```

   In **Command line**, enter the command line for the script. For `SimpleAuth.exe`, the command line includes the name of the executable file (`SimpleAuth.exe`) and two arguments:

   - The server on which the authentication file resides
   - The path to the authentication file (`AllowList.xml`)

   For example:

   ```
   SimpleAuth.exe MyTestHost C:\PlugIns\SimpleAuth\XML\AllowList.xml
   ```

   Set a timeout interval for the script in case it does not run to completion.

4. Click **OK** to exit the Set Custom Script dialog box. Click **OK** again to set the encryption and authentication policies you have set and exit the policy editor.

Testing the Script

To verify that the script is working properly, you can start the virtual machine from VMware ACE Manager. Click **Run in VMWare ACE**, which runs the virtual machine in preview mode.

Note: If you power on the virtual machine by clicking **Start this virtual machine**, the authentication policy is not set because policies are only enforced in preview mode or when a user powers on an installed virtual machine.

Check the log file on the host machine for errors and messages. By default, the log file is in the following directory:

```
C:\Documents and Settings\<username>\My Documents\My Virtual
Machines\<machine_name>\vmware.log
```

Deploying the Virtual Machine Package

For security reasons, you must deploy plug-ins as part of a package to be installed by the package installer. You cannot deploy plug-ins separately to end users' computers and end users cannot modify them.

When you are satisfied with your authentication script and with other aspects of the project you can use the package creation wizard in VMware ACE Manager to create a package. Be certain that the correct version of the script is in the `Project Resources` directory so the package creation wizard can find it and include it in the package.

For details on creating packages, see the *VMware ACE Administrator's Manual* or the technical note "Best Practices for Setting Up VMware ACE," available at: *http://www.vmware.com/support/resources/ace_resources.html*.

VMware, Inc. 3145 Porter Drive Palo Alto, CA 94304 www.vmware.com

Copyright © 1998-2005 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156 and 6,795,966; patents pending. VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation. Linux is a registered trademark of Linus Torvalds. All other marks and names mentioned herein may be trademarks of their respective companies. Revision: 20050602 Item: ACE-ENG-Q105-63