ESX Server Login Using Windows NT 4.0

VMware® ESX Server™ maintains its own database of authorized users. Each authorized user may create and manage virtual machines. This document explains how to use Microsoft® Windows® NT® 4.0 with domain as an authentication source in the ESX Server 2.1 environment. After following the instructions in this paper, administrators should be able to configure ESX Server to allow users to log in to ESX Server using their domain usernames and passwords.

This document applies primarily to Windows NT 4.0. This document does contain a discussion of authenticating against an Active Directory domain with a primary domain controller (PDC) emulator acting as a Windows NT PDC. This document applies only to ESX Server 2.1. For information on NT domain login with ESX Server 1.5 and 2.0 see the VMware white paper, *NT 4 Domain Login*. For information on domain authentication with Active Directory see the VMware Technical Note *ESX Server Login Using Active Directory*.

ESX Server Overview

ESX Server is high-end virtualization software for Intel x86 architecture computers. It allows an enterprise to treat one such computer as a collection of independently managed virtual machines.

The Service Console (sometimes referred to as the console operating system) serves as the administrative interface to the ESX Server system as a whole. The Service Console allows authorized users to

- Create new virtual machines
- Power on, power off, reset and suspend existing virtual machines
- Connect to virtual machines using the VMware remote console
- Delete virtual machines

Each virtual machine has an owner, a user defined in the Service Console. By default, only this owner and the Service Console's privileged user (the root user) may administer the virtual machine.

The username/password database kept by the Service Console is independent of the virtual machines' username/password databases. A user need not be registered with the Service Console in order to use a virtual machine, just as someone can use a physical computer without being authorized to administer it.

By default, the usernames and passwords for users of the Service Console are stored in the Service Console. Some organizations may prefer to use an external password store. The advantage of doing so is that users need not remember an additional password. The disadvantage of doing so is that a new dependency has been introduced: users may be unable to log in to ESX Server if the password store goes down or if network connectivity is lost. This document contains a way to mitigate the risk.

Pluggable Authentication Modules

The ESX Server Service Console is a modified version of Red Hat Linux. Like many Linux and Unix versions, the Service Console supports a technology called Pluggable Authentication Modules (PAM). PAM allows administrators to specify additional services against which users may authenticate themselves, in addition to the traditional local password store — for example, Windows domains, Kerberos servers and RADIUS servers.

Multiple services use PAM for authentication. Example include local logins, logins by FTP and logins by Telnet. The VMware authentication model builds on PAM. Whenever a user wishes to log into the VMware Management Interface or the VMware remote console, PAM is invoked, and it follows the installed rules for a login using a special service called **vmware-authd**.

Allowing Windows Authentication

If you wish to use a Microsoft Windows NT 4.0 domain as your database of usernames and passwords for ESX Server users, follow these steps:

1. Log into the ESX Server command line interface.
2. Create a configuration file identifying the domain and its domain controllers.
3. Make sure that the names of those domain controllers are known to the Service Console.
4. Modify `/etc/pam.d/vmware-authd` to use the PAM module.
5. Tell the Service Console about each authorized Windows user.

The following sections cover each step in detail.

Logging In to the Command Line Interface

To perform this setup, you must work with the Service Console at its command prompt. If the ESX Server machine itself is readily accessible, you can work at its Service Console. To do so, press Alt-F2 on the keyboard. You see a screen that displays your version of ESX Server and offers a `login:` prompt. Enter `root` at the prompt, then at the `Password:` prompt, enter the root user's password.

You may also connect to the Service Console remotely using the secure shell (SSH) protocol. To do so, your local workstation must have an SSH client installed. One popular freeware SSH client for Windows systems is PuTTY, which you can download from

www.chiark.greenend.org.uk/~sgtatham/putty/

A popular commercial SSH client is SecureCRT, a product of Van Dyke Technologies.

www.vandyke.com/

Most Linux distributions contain a command-line version of SSH. You may also download and install OpenSSH for most versions of Unix and Linux from

www.openssh.com/

VMware neither endorses nor supports these products.

Use your SSH client to connect to the ESX Server Service Console, using its DNS hostname (if it has one) or its IP address. Specify that you wish to use password authentication. Enter the username `root` when prompted, then your system's root password.

When you log in, you see a command prompt that ends in #.This is your signal that you have system privileges in the Service Console.

The following sections assume that you are logged in to the Service Console as root.

Configuring the pam_smb Module

The `pam_smb` module is a software package that contains the PAM module needed to connect to an NT4 domain. This module is installed by default when you install ESX Server 2.1.

The `pam_smb` module needs three pieces of information from you:

- The name of your Windows NT 4.0 domain
- The NetBIOS name of your primary domain controller
- The NetBIOS name of your backup domain controller (BDC)

You must place these pieces of information into a configuration file called `/etc/pam_smb.conf`

The format of the file is simple: a text file with one item of data per line, three lines total. Suppose you have a domain called TEXAS, with a PDC named AMARILLO and a BDC named HOUSTON. Your `/etc/pam_smb.conf` file looks like this:

```
TEXAS
AMARILLO
HOUSTON
```

The names in this file are not case sensitive.

Use the text editor of your choice to edit the **/etc/pam_smb.conf** file. ESX Server includes the **vi** and Nano editors. If you are not familiar with **vi**, use the easier Nano editor. If you use Nano, make sure to run it with the "**-w**" flag to disable line wrap. For example:

```
nano -w /etc/pam_smb.conf
```

Type in one word per line, pressing the **Enter** key after each word. When you are done, save the file and exit. Make sure you check your work. You can display the file to the screen with the following command:

```
cat /etc/pam_smb.conf
```

Making the Domain Controllers' Names Known

The Service Console must be able to translate the NetBIOS names of the domain controllers to the correct IP addresses. To make this translation possible, you must add entries for these names to the `/etc/hosts` file. Each line in this file contains either a comment (if it begins with a # character) or an IP address, followed by one or more names for that IP address.

After you have performed the basic setup of your ESX Server system, its `/etc/hosts` file looks like this:

```
# Do not remove the following line, or various
# programs that require network functionality
# will fail.
127.0.0.1 localhost.localdomain localhost
192.168.14.2 myesxserver.texas.org myesxserver
```

Your Service Console's IP address appears in place of 192.168.14.2, and the name of your server appears in place of **myesxserver**. Notice that the name appears twice: once with the local DNS domain appended and once without.

You must add entries for your PDC and your BDC to this file. To do so, edit `/etc/hosts` with the text editor of your choice. Remember that if you use Nano, you must use it with the `-w` flag.

At the end of the file, on a new line, enter the IP address of a domain controller, followed by its NetBIOS name. Use spaces or tabs to separate the IP address from the name. You may list the PDC's IP address and name first or that of the BDC, but in all cases the IP address must be the first item on the line. When you have finished, save and exit the file.

It is not necessary to include the DNS domain in the name. If you do so, be sure you also include the name without the domain on the same line.

When you are finished editing, check your work. Use the following command to display the file to the screen:

```
cat /etc/hosts
```

The file should look something like this:

```
# Do not remove the following line, or various
# programs that require network functionality
# will fail.
127.0.0.1 localhost.localdomain localhost
192.168.14.2 myesxserver.texas.org myesxserver
192.168.14.250 AMARILLO.texas.org AMARILLO
192.168.14.251 HOUSTON.texas.org HOUSTON
```

The NetBIOS names you enter in this file are not case sensitive.

Modifying vmware-authd Rules

You must now modify the list of rules PAM uses when attempting to validate a login to the VMware Management Interface or remote console.

Each service which uses PAM for authentication has a file in the Service Console's directory `/etc/pam.d`. For example, here is the file `/etc/pam.d/vmware-authd` as it ships on the base ESX as it ships on the base ESX Server install:

```
#%PAM-1.0
auth required /lib/security/pam_unix_auth.so shadow nullok
account required /lib/security/pam_unix_acct.so
```

The first line of this file is a comment, identifying the current version of PAM. The second line says that users must authenticate themselves using a username and password as stored on the local system. The third line says that users must also have an account on the local system.

The effect of this file is to limit users of all VMware-related services to local users known to the Service Console.

You must modify this file so that users may log in using local usernames and passwords, but in the event that their password is not known locally, it must be known to the Windows domain. Use your text editor to edit this file.

Starting at the first letter of the word `required` on the first `auth` line, change the word `required` to read `sufficient`.

Open a new line at the bottom of the file and type in the following:

```
auth required /lib/security/pam_smb_auth.so use_first_pass
```

Use spaces or tabs to separate words. It is not necessary to align columns.

When you have typed in the above line, save and exit the file.

When you are done, your `/etc/pam.d/vmware-authd` file should look like this:

```
#%PAM-1.0
auth sufficient /lib/security/pam_unix_auth.so shadow nullok
account required /lib/security/pam_unix_acct.so
auth required /lib/security/pam_smb_auth.so use_first_pass
```

Your ESX Server system is now ready to authenticate management interface and remote console users against a Windows NT 4.0 domain. You do not need to reboot the computer or restart any services.

Telling the Service Console about Each Authorized User

Now you are ready to authorize specific usernames from the Windows domain to log in to ESX Server.

Suppose your `TEXAS` domain contains three users whom you wish to authorize: hank, peggy and bobby.

To authorize each user, use the useradd command at the **#** prompt:

```
useradd hank
useradd peggy
useradd bobby
```

Now each of these users can log in to the management interface or the remote console using the appropriate Windows NT 4.0 domain password.

Suppose that, later, user hank leaves the company or changes jobs. You wish to withdraw his permission to log in to ESX Server. To do so, use the `userdel` command at the `#` prompt:

```
userdel hank
```

Use with Active Directory

One of the server roles in any Windows 2000 Active Directory domain is the PDC emulator. Active Directory domains can operate in either native or mixed mode. When a domain is in mixed mode (the default), its PDC emulator is capable of responding to Windows NT 4.0-style queries from clients.

If your Active Directory domain is in mixed mode, and you have no plans to migrate it to native mode, you can simplify your administration by using Windows NT 4.0 authentication for ESX Server, as described in this document. Use the short compatibility name of your domain wherever a domain name is called for: for example, the short name of a Windows 2000 Active Directory domain called TEXAS.ORG would probably be TEXAS. Use the NetBIOS name of your PDC emulator wherever a PDC is called for. Supply no BDC.

You should not use this document if your Active Directory domain is in native mode, or if you plan to migrate your mixed mode domain to native mode in the future. Obtain the VMware Technical Note *ESX Server Login Using Active Directory*.

vmware®

Questions and Answers

Q. What if I want all the users in the domain to be able to log in to ESX Server?

A. VMware does not recommend this practice. Remember that ESX Server users are administrators, not ordinary users. If a user can log in to ESX Server, he or she can create virtual machines and consume resources. Therefore, letting all the users in the domain log in to ESX Server is equivalent to giving them all access to the server room and giving them all a budget to purchase hardware.

Q. Must the ESX Server computer join the domain?

A. No.

Q. What if I don't have a backup domain controller?

A. Simply omit its name from the file.

Q. What if I promote my BDC to PDC status?

A. Authentications will continue uninterrupted. Be sure, however, to remove a server's NetBIOS name from `/etc/pam_smb.conf` when it is no longer functioning as a domain controller.

Q. What if my ESX Server computer loses network access to all the domain controllers? Will virtual machines shut down?

A. Virtual machines will continue to run. ESX Server users who are not defined locally will not be able to log in to administer their machines. VMware recommends that, at a minimum, the root password be maintained locally on the Service Console; do not attempt to map this to the Administrator login in the domain. This way, authorized personnel will always be able to log in as root even if contact with the domain is lost.

Q. Does this technique work on all versions of ESX Server?

A. This information has been tested on ESX Server 2.1. You can find information for ESX Server 1.5 and 2.0 in the VMware Technical Note *NT 4.0 Domain Login*.

Q. What if I want to use my Windows domain to authenticate other kinds of Service Console logins, such as FTP or SSH logins?

A. PAM allows you to do so, although the setup is outside the scope of this document. See the Further Reading section below for pointers to more information on PAM.

Q. What if I want to authenticate users against my Windows 2000 Active Directory system?

A. This is the topic of a separate VMware Technical Note, *ESX Server Login Using Active Directory*.

Further Reading

The Pluggable Authentication Module system is documented here:

www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam.html

The pam_smb module is documented here:

www.mindspring.com/~aegreene/linux/PDC-Authentication-HOWTO.html

VMware, Inc. 3145 Porter Drive Palo Alto, CA 94304 www.vmware.com
 Revision: 20040413 Item: ESX-ENG-Q104-069