



ESX Server 2.1

Login Authentication Using Active Directory

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 a Microsoft® Windows® 2000 Active Directory domain as an authentication source, so that users may log into ESX Server using their domain user names and passwords. This document does not cover Windows NT® 4.0 issues. For specific coverage of Windows NT 4.0 domain login issues, see the technical note *Login Authentication Using Windows NT 4.0*. 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, *Active Directory Login*.

- [ESX Server Overview](#)
- [Pluggable Authentication Modules](#)
- [Active Directory and Kerberos](#)
- [Special Note for Mixed Mode Domains](#)
- [Allowing Windows Authentication](#)
- [Questions and Answers](#)
- [Further Reading](#)

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 user name and password database kept by the Service Console is independent of the virtual machines' user name and 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 user names 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. Examples 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`.

Active Directory and Kerberos

The Microsoft Active Directory system is a replacement for the domain system used to manage administrative data in Windows NT 4.0. Active Directory is built on top of the Domain Name System.

Among the items stored in an Active Directory domain are user names and passwords. To authenticate users, Active Directory builds on top of an authentication technology called Kerberos 5. Kerberos uses encrypted communication to avoid transmitting passwords in the clear.

For our purposes, the same software that allows systems to authenticate using PAM against a Kerberos 5 server suffices to allow our ESX Server users to authenticate against Active Directory.

Special Note for Mixed Mode Domains

One of the server roles in any Active Directory domain is the Primary Domain Controller (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 your ESX Server users. See the VMware technical note *VMware ESX Server NT 4 Domain Login* for more information. Follow the instructions contained in that document, using the short compatibility name of your domain wherever a domain name is requested, and the NetBIOS name of your PDC emulator wherever a PDC is requested. Supply no Backup Domain Controller.



Continue with 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.

Allowing Windows Authentication

If you wish to use a Microsoft Windows Active Directory domain as your database of user names and passwords for ESX Server users, take the following steps:

1. Log in to the ESX Server command line interface.
2. Create configuration files identifying and locating the Active Directory domain and its controller.
3. Modify `/etc/pam.d/vmware-authd` to use the PAM module.
4. 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 procedure, 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 user name `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_krb5` Module

The `pam_krb5` module needs two pieces of information from you:

- The name of your Windows Active Directory domain
- The DNS name or IP address of at least one Active Directory controller

You must place these pieces of information into a configuration file called `/etc/krb5.conf`.

Suppose you have an Active Directory domain called TEXAS.ORG, with a domain controller named AD.TEXAS.ORG. Your `/etc/krb5.conf` file would look like this:



```

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
ticket_lifetime = 24000
default_realm = TEXAS.ORG
dns_lookup_realm = false
dns_lookup_kdc = false

[realms]
TEXAS.ORG = {
kdc = AD.TEXAS.ORG:88
admin_server = AD.TEXAS.ORG:464
default_domain = texas.org
}

[domain_realm]
.texas.org = TEXAS.ORG
texas.org = TEXAS.ORG

[kdc]
profile = /var/kerberos/krb5kdc/kdc.conf

[pam]
debug = false
ticket_lifetime = 36000
renew_lifetime = 36000
forwardable = true
krb4_convert = false

```

Use the text editor of your choice to create the `/etc/krb5.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/krb5.conf
```

Type in the data file as shown above. Substitute your own Active Directory domain name in place of `TEXAS.ORG`. Substitute the name of a domain controller for the domain in place of `AD.TEXAS.ORG`. Follow the uppercase/lowercase pattern shown in the sample above.

When you are satisfied with your work, save your file and exit. Make sure you check your work. You can display the file to the screen with the following command:

```
more /etc/krb5.conf
```

This displays the file, one screen at a time. Press the space bar to advance to the next screen, or press `q` to stop displaying the file before you reach the end.

Ensure that the hostname you gave for your Active Directory controller is correct. If your controller had as its hostname `AD.TEXAS.ORG`, you should be able to ping it from the ESX Server computer with the following command:

```
ping AD.TEXAS.ORG
```

You must also create a file called `kdc.conf`. Cryptographic keys are at the heart of Kerberos' operation, and this configuration file describes how your ESX Server computer interacts with the Key Distribution Center that Active Directory provides.



First, you must create the directory in which this file resides. Enter the following command:

```
mkdir -p /var/kerberos/krb5kdc
```

Now change to that directory:

```
cd /var/kerberos/krb5kdc
```

Edit the `kdc.conf` file.

Enter the following text:

```
acl_file = /var/kerberos/krb5kdc/kadm5.acl
dict_file = /usr/share/dict/words
admin_keytab = /var/kerberos/krb5kdc/kadm5.keytab
v4_mode = nopreauth

[realms]
TEXAS.ORG = {
    master_key_type = des-cbc-crc
    supported_encetypes = des3-cbc-raw:normal des3-cbc-raw:norealm
                        des3-cbc-raw:onlyrealm des3-cbc-shal:normal
                        des3-cbc-shal:norealm des3-cbc-shal:onlyrealm
                        des-cbc-crc:v4 des-cbc-crc:afs3
                        des-cbc-crc:normal des-cbc-crc:norealm
                        des-cbc-crc:onlyrealm des-cbc-md4:v4
                        des-cbc-md4:afs3 des-cbc-md4:normal
                        des-cbc-md4:norealm des-cbc-md4:onlyrealm
                        des-cbc-md5:v4 des-cbc-md5:afs3
                        des-cbc-md5:normal des-cbc-md5:norealm
                        des-cbc-md5:onlyrealm des-cbc-raw:v4
                        des-cbc-raw:afs3 des-cbc-raw:normal
                        des-cbc-raw:norealm des-cbc-raw:onlyrealm
                        des-cbc-shal:v4 des-cbc-shal:afs3
                        des-cbc-shal:normal des-cbc-shal:norealm
                        des-cbc-shal:onlyrealm
}
```

Substitute the name of your Active Directory domain for TEXAS.ORG.

To avoid the tiresome chore of typing in the above file, you can copy the text above from this document, within Acrobat, using the **Select Text** option in the **Basic Tool Bar**. (If you are reading a hard copy of this document you can find an online copy using the **Search** feature on www.vmware.com). Edit the file if necessary, confirming that it looks like the above. Do not forget to include the name of your Active Directory domain.

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 the remote console.

Each service that 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 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 user name 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 user names and passwords, but in the event that their password is not known locally, it must be known to the Windows Active Directory domain.

Edit the file `/etc/pam.d/vmware-authd`.

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_krb5.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_krb5.so use_first_pass
```

Your ESX Server system is now ready to authenticate MUI and Remote Console users against an Active Directory domain. No reboot or service restart is necessary.

Telling the Service Console about Each Authorized User

Now you are ready to authorize specific user names 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
```

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 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 only. You can find information for ESX Server 1.5 and 2.0 in the VMware Technical Note *Active Directory 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. Authentication fails or works for some users, but not for others.

A. Due to a bug in the version of Kerberos shipped with ESX Server 2.1, users who are members of more than 15 global groups will fail to authenticate, even if the users supply the correct password. There is currently no workaround or fix for ESX 2.1.

Further Reading

The Pluggable Authentication Module system is documented here:

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

Kerberos is documented here:

web.mit.edu/kerberos/www/

Microsoft Active Directory is documented here:

www.microsoft.com/windows2000/technologies/directory/ad/default.asp