Enabling Active Directory Authentication with ESX Server

This document provides information about how to configure ESX Server to use Active Directory for authentication. ESX Server system includes an authentication service, but users might want to use other authentication providers. Information provided in this document includes:

Authentication Concepts

An identity is authenticated when someone or something proves they are who they claim to be. Anything that can be authenticated, such as users, computers, or services, is called a *principal*. A principal proves its identity by proving knowledge of some secret. For example, a password is a secret that a user keeps, but by proving knowledge of that secret, users prove they are who they claim to be.

Authentication permits principals to use a service, and, at the same time, prevents unauthorized users from masquerading as legitimate users to steal resources. For example, unknown users can be denied access to payroll information. Similarly, unknown services can be prevented from using virtual machines to complete tasks. Authenticated users, however, can use their virtual machines and access their data.

Authentication is one of several security technologies that work together to enable appropriate access to services:

- Access control grants or denies principals access. If any principal can access any service, access control is insufficient. For access control to be useful, principals must be authenticated.
- Authentication verifies that principals are who they claim to be. If any principal can claim an identity or provide credentials for an identity, such as root, there is insufficient authentication. For authentication to be useful, there must be trust in the form of physical security and trust of an authentication authority.
- Trust exists among a set of principals. For example, trust is necessary among authentication servers, principals that use services, and physical computers in a domain or realm. If any service is trusted to authenticate principals, trust is not sufficiently restricted.

This technical note deals with the configuration of authentication interoperability in ESX Server. Authentication is made possible by the implementation of an authentication protocol. Protocols are abstract processes. For example, Kerberos is a protocol for establishing the identities of principals, but it is not an implementation of that process. Active Directory provides an authentication service that implements the Kerberos protocol, so principals can use Kerberos to authenticate to Active Directory.

A variety of authentication providers are available for use. ESX Server includes services that can be used to meet your authentication needs but also supports the use of other authentication providers. This is especially useful in cases where a collection of users has already been established, as in organizations using Active Directory. To facilitate the use of such providers, ESX Server includes an option in the esxcfg tool to configure the use of other authentication providers.

Especially in large, previously established environments with many users, creating trust with an existing authentication authority is easier than recreating all the required users in ESX Server. Furthermore, reducing the number of authentication systems reduces the number of user names and passwords each user must remember. Users are more likely to follow recommended practices for creating strong passwords when they have fewer passwords to remember, and reusing any password, even a strong one, for multiple accounts effectively weakens the security of an authentication system.

Esxcfg-auth Tool

The esxcfg-auth tool enables authentication interoperability with authentication providers such as Windows Active Directory. Active Directory is the collection of services and data that Windows uses to authenticate principals. The esxcfg-auth tool makes authentication with Active Directory possible by configuring a pluggable authentication module (PAM) and modifying the ESX Server system's configuration. Specifically, esxcfg-auth:

- Modifies the `krb5.conf` file. The tool adds the name of the Active Directory Domain and the DNS name or IP address of at least one domain controller, allowing the ESX Server host to find a domain controller.
- Creates the `kdc.conf` file, which contains information that specifies which cryptographic options are used during authentication processes.
- Modifies the `pam.d` file, configuring the ESX Server system to authenticate MUI and remote console users using the Active Directory domain.

Commands

The esxcfg-auth command includes options for configuring interoperability with several authentication providers. This note focuses on the options that are relevant to Active Directory:

esxcfg-auth [[**--enablead** | **--disablead**] [**--addomain=<domain**> | **--removedomain=<domain>**] [**--addc=<dc>** | **--removedc=<dc>**]]

Example

Consider a case in which a Windows domain is named vmtest.com, and in this domain is a domain controller named DC1. That server's fully qualified domain name (FQDN) is DC1.vmtest.com. To establish interoperability with this Windows domain, issue the following command on an ESX Server system as root:

```
# esxcfg-auth --enablead --addomain=vmtest.com --addc=DC1.vmtest.com
```

This enables Active Directory–based user authentication in the vmtest.com domain with the domain controller DC1.vmtest.com. After entering the preceding command, create a user on the ESX Server system with permissions to use the service console. To create a user, use the Linux command `useradd`. For example, to add a user named ConsoleUser, issue the following command on an ESX Server system as root:

```
# useradd ConsoleUser
```

After a service console user account is created, that user can log on to the console locally. For every user that you want to enable access through authentication to Active Directory, you must also create a corresponding user on the ESX Server system using the `useradd` command.

Frequently Asked Questions

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

A. VMware does not recommend this practice. ESX Server users are administrators, not ordinary users. They can create virtual machines and consume resources. Therefore,

letting all the users in the domain log on to ESX Server systems gives everyone unrestricted access to computing resources.

Q. Does the ESX Server system have to be part of the domain?

A. No.

Q. What if my ESX Server computer cannot contact a domain controller? Will my virtual machines shut down?

A. Virtual machines continue to run. ESX Server users who are not defined locally are unable to log on to administer their machines. VMware recommends that you maintain the root locally on the service console, but do not attempt to map this to the Administrator logon in the domain. By preserving root access to the local service console, authorized personnel can always log on as root, even if contact with the domain is lost.

Q. Does maintaining a local root password for the service console work on all versions of the ESX Server system?

A. This solution should work on all versions of the ESX Server system, but it has been tested only on ESX Server 2.1.

Q. What if I want to use my Windows domain to authenticate other kinds of service console logons, such as FTP or SSH logons?

A. A PAM module allows you to do so, although the setup is outside the scope of this document. See "Further Reading" on page 4 for where to find more information on PAM.

Q. Authentication fails or works for some users, but not for others. Why is this?

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 cannot authenticate, even with valid user names and passwords. To avoid this problem, limit user global group membership.

Further Reading

Kerberos is documented here:

```
http://web.mit.edu/kerberos/www/
http://www.ietf.org/rfc/rfc1510.txt
```

Microsoft Active Directory (AD) is documented here:

```
http://www.microsoft.com/windows2000/technologies/directory/ad/default.asp
http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/
                default.mspx
```

Services for UNIX (SFU) is documented here:

http://support.microsoft.com/default.aspx?scid=kb;en-us;321712&sd=tech

Pluggable authentication module (PAM) is documented here:

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