## Contents

**Preface**  
Precence Description ................................................. vi  
Conventions Used in this Guide ...................................... vi

1 **Introduction**  
Introducing SCO Authentication ........................................ 1  
Using a Sample Network .............................................. 4

2 **Installing the Extensions to the MS Management Console and Active Directory Components**  
Installing on the Schema Master Domain Controller .................... 8  
Extending the Schema .................................................. 9  
Installing Administrative Components on the Administrator’s Workstation ........ 11  
Enabling UNIX and Linux Groups ...................................... 12  
Enabling UNIX and Linux Accounts ................................... 14  
Synchronizing Time .................................................... 16

3 **Installing UNIX/Linux Client Components**  
Required Information for Installation ................................ 17  
SCO Authentication Client Components ................................ 18  
Hardware Requirements ................................................. 18  
Software Requirements ................................................ 19  
Installing and Configuring Linux Clients ................................ 19  
Installing Linux Clients ................................................. 19  
Synchronizing Time .................................................... 20  
Configuring Linux Clients .............................................. 21  
Using DNS ..................................................................... 21  
Using vastool join Without Using DNS ................................ 22
Installing and Configuring UNIX Clients ........................................ 24
  Installing UnixWare Clients ................................................. 25
  Synchronizing Time on UnixWare Clients .................................. 26
  Configuring UnixWare Clients .............................................. 27
    Using DNS ............................................................... 27
    Using vastool join Without Using DNS .................................. 28
SCO Authentication-Enabled Applications on UnixWare ....................... 29
  Configuring SCO Authentication-Enabled Server Applications .......... 29
Installing SCO OpenServer Clients ............................................. 31
  Synchronizing Time SCO OpenServer Clients ............................... 33
  Configuring SCO OpenServer Clients .................................... 33
    Using DNS ............................................................... 34
    Using vastool join Without Using DNS .................................. 35
SCO Authentication-Enabled Applications on SCO OpenServer ............... 36
  Configuring SCO Authentication-Enabled Server Applications .......... 36
Installing Solaris Clients ...................................................... 38
  Synchronizing Time on Solaris Clients ................................... 39
  Configuring Solaris Clients .............................................. 40
    Using DNS ............................................................... 40
    Using vastool join Without Using DNS .................................. 41

A  Time Synchronization ................................................................ 43
  Configuring the SNTP Service on
    Window 2000/2003 ............................................................. 44
  Synchronizing Time on Client Platforms .................................... 45

B  Error Messages ....................................................................... 49

C  Troubleshooting ....................................................................... 51
Preface

System administrators today must provide heterogeneous platforms and applications for their users’ business needs and requirements. By providing users with the best network accessibility and state-of-the art applications, system administrator are left with an integration and security nightmare.

Critical to the security of any network is the authentication and verification of user identities. By adopting Microsoft Active Directory® some issues with authentication and management are solved but this introduces significant problems for the organization that additionally runs business critical applications on UNIX® and Linux®. If system administrators are required to maintain multiple user authentication systems then users are required to remember multiple passwords. System administrators might be clever enough to devise script-based password synchronization tools but this solution can become hard to support, maintain, and train additional staff to use.

SCO Authentication provides the solution for integrating UNIX, and Linux systems with Active Directory. It supplies the discipline and controls necessary to ensure the security and integrity demanded in today’s business climate.

SCO Authentication allows administrators to provide a secure environment where users have the same username and password for Windows®, UNIX, and Linux logins without having to maintain password synchronizers or perform user administration tasks on multiple systems. SCO Authentication users can log in and authenticate to Active Directory in the same way that Windows XP and Windows 2000/2003 users do. SCO Authentication makes possible the management of all users and network client machines from within the standard Active Directory management environment.
Audience Description

This guide is intended for Windows, UNIX, and Linux system administrators and system integrators who need to perform one or both of the following tasks:

• Migrate user and application authentication data from an existing UNIX systems into Active Directory.

• Have UNIX and Linux machines that need to authenticate against Active Directory.

Conventions Used in this Guide

The following notation conventions are used throughout this guide:

• Modules, directories and filenames are bolded. For example, /etc/pam.conf.

• Daemon names are bolded. For example, vascd.

• Manual titles appear in italics. For example, SCO Authentication Installation and Configuration Guide.

• Commands appear in a monofont. For example,

```
# vastool configure pam
```

Within text, commands are bolded for readability. For example,

Using the vastool command line utility you can create users, delete users, and list user information.

• Variables for which you must supply a value are shown in italic monofont. For example,

```
./vastool -u matt join vasdemo.com mozart.vasdemo.com
```

SCO Authentication Installation and Configuration Guide
Where:

matt is a user with admin privileges.

vasdemo.com is your Active Directory domain.

• Menu items and buttons appear in bold. For example, click Next.

• Selecting a menu item is indicated as follows:

  Programs > Administrative Tools > Active Directory Users and Computers
1 Introduction

Introducing SCO Authentication

SCO Authentication allows UNIX® and Linux® users to log in and authenticate to Active Directory in the same way that Windows XP and Window 2000/2003 users can log in and authenticate to Active Directory.

SCO Authentication gives the Microsoft network administrator total control over UNIX and Linux network clients and their users. It puts user account management into the single Active Directory context. This product uniquely eliminates the need for duplication of systems and control efforts, and above all, it eliminates the need to layer third-party software over the top of the most critical security components of Windows 2000/2003 the authentication subsystems.

All other identity management solutions layer additional software on top of Active Directory or replace it altogether. In either case, solutions that add to the Windows 2000/2003 services add to the level of complexity as well as potential for failure in critical operating system components that directly affect system security and stability.

SCO Authentication provides the following features and benefits:

- Fully integrated with standardized protocols supported by Windows 2000/2003 as well as with UNIX and Linux.
• By implementing Kerberos the need for SSL configuration and key and certificate distribution is eliminated.

SCO Authentication uses a Kerberos implementation that is compatible with Active Directory to secure all LDAP communication. Both LDAP Binds and subsequent LDAP search and modify requests are fully encrypted using Kerberos based security contexts. There is no plain text or “anonymous” LDAP traffic of any kind.

• Minimizes network traffic and search complexity on Windows 2000/2003 Active Directory servers.

SCO Authentication is a scalable product that uses intelligent caching algorithms that are designed to limit the amount of network traffic and reduce the search complexity on Active Directory servers. The design also makes efficient use the UNIX host resources that make it suitable for deployment on “big iron” UNIX systems that handle hundreds of concurrent login processes.

• Provides secure user authentication even when you can’t get to the network or the Active Directory server is down. This is especially useful on UNIX and Linux laptops.

SCO Authentication is a robust product that is designed to work well in disconnected or loosely connected environments. For example, SCO Authentication components are suitable for use on UNIX and Linux laptops and continue to allow user authentication and UID and GID mappings even when completely disconnected from the network!

• SCO Authentication is easy to install and deploy.

Product components can be installed and configured quickly and even automatically using the native UNIX and Linux packaging systems and intuitive command line utilities. Migration from legacy systems such as the Network Information System (NIS) or /etc/passwd based authentication is facilitated by a scriptable bulk user import utility within vastool as well as Active Directory based “NIS Map” compatibility functionality for sites that use NIS as a distribution mechanism for more than UNIX and Linux user and group databases.
• Integrates into existing services and Open Source projects.

SCO Authentication is a flexible product that can be customized to fit specialized user authentication requirements. Its PAM and NSS design allows it to be quickly integrated with many existing services and Open Source projects. SCO Authentication includes script-friendly command line utilities that expose its full functionality to UNIX and Linux shell programming and login scripts.

The following illustrates how a user named **JD** with a password of **Hockey** logs in to Active Directory from a UNIX or Linux system in the same way that this user would log in to Active Directory from a Windows workstation.

**Figure 1. SCO Authentication Users Log in to Active Directory**
Using a Sample Network

Throughout most of this document as well as in the *SCO Authentication Administration Guide* we have used an example scenario to assist you in your system setup. The following illustration depicts the sample network:

**Figure 2. SCO Authentication Sample Network**

![Sample Network Diagram]
Computers in example.com include:

### Table 1. Sample System Names and Descriptions (Part 1 of 2)

<table>
<thead>
<tr>
<th></th>
<th>adserv.example.com</th>
<th>linserv1.example.com</th>
<th>linserv2.example.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>192.168.100.10</td>
<td>192.168.100.20</td>
<td>192.168.100.30</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows 2000/2003 Advanced Server</td>
<td>Red Hat Linux 8.0</td>
<td>SuSE 8.1</td>
</tr>
<tr>
<td>Servers/Services</td>
<td>Active Directory, DNS</td>
<td>SSH</td>
<td>Apache, Samba</td>
</tr>
<tr>
<td>Realm</td>
<td>example.com</td>
<td>No Kerberos is configured or running.</td>
<td>No Kerberos is configured or running.</td>
</tr>
<tr>
<td>Description</td>
<td>Serves as the central repository for authentication data.</td>
<td>Remote secure login (SSH) server.</td>
<td>Company intranet web server, Samba server</td>
</tr>
<tr>
<td>User Accounts</td>
<td>matt, wynn, erik</td>
<td>wynn</td>
<td>matt</td>
</tr>
</tbody>
</table>

### Table 2. Sample System Names and Descriptions (Part 2 of 2)

<table>
<thead>
<tr>
<th></th>
<th>linclient1.example.com</th>
<th>linclient2.example.com</th>
<th>solclient.example.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>192.168.100.40</td>
<td>192.168.100.50</td>
<td>192.168.100.60</td>
</tr>
<tr>
<td>Operating System</td>
<td>UnitedLinux 1.0</td>
<td>UnitedLinux 1.0</td>
<td>Solaris 8</td>
</tr>
<tr>
<td>Servers/Services</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Realm</td>
<td>No Kerberos is configured or running.</td>
<td>No Kerberos is configured or running.</td>
<td>No Kerberos is configured or running.</td>
</tr>
<tr>
<td>Description</td>
<td>User Accounts</td>
<td>Description</td>
<td>User Accounts</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------</td>
<td>----------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Linux workstation.</td>
<td>matt</td>
<td>Linux workstation.</td>
<td>wynn</td>
</tr>
<tr>
<td>linclient1. example.com</td>
<td></td>
<td>linclient2. example.com</td>
<td></td>
</tr>
</tbody>
</table>
Installing the Extensions to the MS Management Console and Active Directory Components

The installation of the SCO Authentication software can be completed in a few short steps. The first of these steps extends the Active Directory schema to support UNIX account information and LDAP as a network information service. This extension needs to be applied only once on the schema master for your Active Directory forest. A schema extension utility is provided with SCO Authentication to facilitate this process.

The next step installs the snap-in to the Microsoft Management Console (MMC). The new snap-in provides a means by which user and group UNIX properties in Active Directory can be managed within the MMC. This snap-in can be installed at the same time as the Active Directory schema extension utility or separately on a Windows administrator's workstation.

UNIX and Linux accounts are enabled in the next phase of installation. Before you can actually enable any user’s UNIX and Linux accounts, you need to have at least one Active Directory group that is UNIX enabled. Information on this process is included in the section “Enabling UNIX and Linux Groups” on page 12.
The final section of this chapter provides information on how to synchronize your Windows 2000/2003 time server with a reliable time source. Comparable sections on how to synchronize time on the SCO Authentication clients with time on the Windows 2000/2003 time server are found in Chapter 3, “Installing UNIX/Linux Client Components,” on page 17. Also included in this chapter are instructions on how to install and configure the client components on each of the supported platforms and join them to the Active Directory domain using the `vastool join` command.

The following lists the sections found in this chapter:

- “Installing on the Schema Master Domain Controller” on page 8
- “Installing Administrative Components on the Administrator’s Workstation” on page 11
- “Extending the Schema” on page 9
- “Enabling UNIX and Linux Groups” on page 12
- “Enabling UNIX and Linux Accounts” on page 14
- “Synchronizing Time” on page 16

### Installing on the Schema Master Domain Controller

SCO Authentication provides authentication services to UNIX and Linux by extending the Active Directory schema. To initiate the graphical installation on Windows 2000/2003 servers, complete the following:

1. Insert the product CD into the drive of the Schema Master Domain Controller.
2. Browse to the win32 folder on the CD.
3. Double-click the **Setup** icon to initiate the Setup Wizard.
4. Click **Next** on the Welcome screen.

5. Read the license agreement and click **I Accept** to accept the license agreement then click **Next** to indicate that you agree.

The installation profile screen appears with the following choices.

**Admin Workstation**- Installs the UNIX and Linux users and computers snap-in extension. Select this installation type if the schema has been previously extended or if you only want to install the UNIX and Linux users and computers snap-in extension on an administrator’s workstation.

**Schema Master**- Additionally installs the schema extender. Select this installation profile if you are installing on the Schema Master Active Directory domain controller.

6. Select **Schema Master**.

7. Click **Install**.

8. Click **Finish**.

Your system is now enabled for the schema extension. To actually extend the schema complete the following.

---

**Extending the Schema**

**Note:** The schema needs only to be extended once on the Schema Master domain controller.

In order to extend the schema you must use an Active Directory user account that has Schema Admin privileges. If you don’t have these privileges, contact your Enterprise Admin.

To extend the schema, complete the following:
1. From the Start menu, browse to Program Files > Vintela > VAS.

2. Double-click the Schema Extension Tool icon (schemext) to run it.

   The following appears:

   **Figure 3. Schema Extension Tool**

   ![Schema Extension Tool](image)

   Defaults values for your system are included.

3. Select the text in the *Select schema extensions to apply* box and click **Extend Schema**.

   A Schema Info window appears.

4. Click **Yes** to indicate that you want to extend the schema.

   A dialog appears indicating that the schema was successfully extended.

5. Click **OK**.

   The installation and configuration for this component is complete.
Installing Administrative Components on the Administrator’s Workstation

Note: These instructions are only required if you are installing the server components on a different system from the Active Directory server.

To initiate the graphical installation of the server management components on Windows 2000/2003 or Windows XP, complete the following:

1. Locate the administrator’s workstation.
2. Insert the product CD in to the drive of the administrator’s workstation.
3. Browse to the win32 folder on the CD.
4. Double-click the Setup icon to initiate the Setup Wizard.
5. Click Next on the Welcome screen.
6. Read the license agreement and click I Accept to accept the license agreement then click Next to indicate that you agree.

The installation profile screen appears with the following choices.

Admin Workstation-Installs the UNIX and Linux Users and Computers snap-in extension. Select this installation type if the schema has been previously extended or if you only want to install the UNIX and Linux Users and Computers snap-in extension on an administrator’s workstation.

Schema Master-Additionally installs the SCO Authentication schema extender. Select this installation profile if you are installing on a Schema Master domain controller.

7. Select Admin Workstation.
8. Click **Install > Finish**.

The UNIX and Linux Users and Computers snap-in is now installed on the administrator’s workstation.

---

**Enabling UNIX and Linux Groups**

Before you can enable any users' UNIX and Linux accounts, you need to have at least one Active Directory group that is UNIX and Linux enabled.

To create a group, do the following:

1. From the Start menu click **Programs > Administrative Tools > Active Directory Users and Computers**.
2. Right-click on the Users folder.
3. Select **New > Group**.
4. Enter the Group name.
5. Make sure that Group type is set to **Security** (default) and click **OK**.

To enable a UNIX and Linux Group, do the following:

1. Right-click on an existing Group and then select **Properties** to view the properties associated with that Group.
2. Click the **UNIX Group** tab on the Properties dialog.

   This tab appears as a result of having extended the schema.

   The following appears:
3. Click the **Enable UNIX Group** checkbox and make sure the group has an appropriate GID.

   If there are no other UNIX enabled groups, the first group receives a suggested GID of 1000. This is a default and can be changed. If there are other groups in the current container, a default GID of one greater than the highest current GID in the container is suggested. On most UNIX and Linux operating systems the system groups typically have GIDs between 0 and 100. We recommend that you do not set any UNIX or Linux enabled group's GID below 1000.

4. When you have finished editing the group information, click **OK** to save the changes.
Enabling UNIX and Linux Accounts

To enable UNIX and Linux accounts, complete the following:

1. From the Start menu click **Programs > Administrative Tools > Active Directory Users and Computers**.
2. Open the Users folder.
3. Right-click on a user and then select **Properties** to view the properties associated with that account.
4. Click the **UNIX Account tab** on the Properties dialog.

The following appears:
Figure 5. User Properties

5. Click in the **Enable UNIX Account** checkbox.

6. Modify the suggested defaults as necessary.

To select a different Primary group, click on the group selection button labeled with “...” next to the **Primary Group ID** edit box, and select a group from the presented list.
This enables the user to login into all UNIX and Linux systems where the SCO Authentication client software is running.

The User ID (UID) for a user must be unique within the Active Directory Tree. The first user that has a UNIX or Linux account enabled receives a suggest UID of 1000 by default. This value (1000) is not required, it is just a suggested default that you can change. On most UNIX and Linux operating systems the system accounts typically have UIDs between 0 and 100. We recommend that you do not set any UNIX or Linux enabled users UID below 1000.

**Important:** The default value for Login Shell is `/bin/bash`. If you do not have this shell on the systems the user is logging into, you must change this setting to a valid login shell.

### Synchronizing Time

Kerberos is a time sensitive protocol that requires “rough” synchronization of the Windows 2000/2003 time server with the UNIX and Linux workstation clocks. A difference of more than 2 minutes between the time on the Windows 2000/2003 server and the time on the UNIX and Linux workstations results in an error.

Your Windows 2000/2003 server should be set up to synchronize its time server with a reliable external time source. For instructions on synchronizing time on Windows, UNIX, and Linux systems, see Appendix A, “Time Synchronization,” on page 43.

Time servers are available at one the following locations:

http://www.boulder.nist.gov/timefreq/service/time-servers.html

or

http://tycho.usno.navy.mil

or

http://www.ntp.org
3 Installing UNIX/Linux Client Components

This section tells you how to install SCO Authentication and its components. The following information is included:

- “Required Information for Installation” on page 17
- “SCO Authentication Client Components” on page 18
- “Hardware Requirements” on page 18
- “Software Requirements” on page 19
- “Installing and Configuring Linux Clients” on page 19
- “Installing and Configuring UNIX Clients” on page 24

Required Information for Installation

Before you begin installing the client components, make sure you have the following information:

- Your Active Directory domain (this is the same as your Kerberos realm)
• A user account on your Active Directory server that is not the built in Administrator account but has domain administrator equivalent privileges.

SCO Authentication Client Components

The SCO Authentication client components consist of the following:

• Client daemon (vascd)
• NSS module
• PAM module
• vastool command line configuration tool

Hardware Requirements

If your hardware is suitable to run the supported operating systems then there are no additional considerations for running SCO Authentication.
Software Requirements

SCO Authentication supports the following as clients:

- Linux distributions powered by United Linux 1.0
- Red Hat® Linux® 7.2, 7.3, 8.0, and Advanced Server 2.1
- SuSE® Linux® 8.0 and 8.1
- UnixWare® 7.1.2 and 7.1.3
- SCO OpenServer® 5.0.6 and 5.0.7
- Solaris® 8 and 9 (Sparc)

Installing and Configuring Linux Clients

Instructions in this section detail how to install client components on supported Linux platforms. With the SCO Authentication client components installed, your system can authenticate against Active Directory. This section includes the following:

- “Installing Linux Clients” on page 19
- “Synchronizing Time” on page 20
- “Configuring Linux Clients” on page 21

Installing Linux Clients

To install Linux clients, complete the following:

1. Log in as root.
2. Mount the CD and go to the **linux** directory at the root of the CD.

   On SuSE and UnitedLinux distributions, enter:
   
   ```
   mount /media/cdrom
   cd /media/cdrom/linux
   ```

   On Red Hat, enter:
   
   ```
   mount /mnt/cdrom
   cd /mnt/cdrom/linux
   ```

3. To install the RPM at the command line, enter:

   ```
   rpm -ivh vas-client-2.1-1.i386.rpm
   ```

   The client component is now installed but not configured. For instructions on configuring Linux clients, see “Configuring Linux Clients” on page 21.

4. To install your license key, change to `/opt/vas/bin` and enter the following:

   ```
   # ./vastool license serial_number key
   ```

   Where:

   - `serial number` is your key serial number.
   - `key` is your license key.

   You need both your license key and your license serial number.

### Synchronizing Time

In order to communicate with Active Directory, the SCO Authentication client must be synchronized within 2 minutes of the time on the Active Directory domain. The recommended method for synchronizing time is to configure and use the NTP client available
on all UNIX and Linux platforms. Refer to your system documentation for instruction on using NTP client.

You can also use `vastool timesync`, however, this is only a quick fix and will not provide the accuracy required.

To synchronize time with Active Directory, enter the following:

```
/opt/vas/bin/vastool timesync <adserver>
```

Where `adserver` is the hostname of the Active Directory server or the server offering NTP time services. Do not enter the brackets.

For additional information on synchronizing time, see Appendix A, “Time Synchronization,” on page 43.

### Configuring Linux Clients

In order for your client to communicate with Active Directory you must configure the operating system’s PAM and NSS subsystems to use the SCO Authentication components (for more information on PAM and NSS, see the *SCO Authentication Administration Guide*), set the realm that the client uses to log in to the Active Directory domain, and add a computer object for your system in Active Directory. This can all be done using the command line configuration tool, `vastool join`.

### Using DNS

By default, SCO Authentication searches your DNS server for the Active Directory service locator (SRV) records when it tries to locate an appropriate Active Directory server. Your DNS server must be set up to allow dynamic updates.

If your DNS server is set up to handle dynamic updates from Active Directory, complete the following instructions to configure your Linux clients:

1. As `root`, change directory to `/opt/vas/bin`.
2. Set the realm that the Linux system will use to log in to the Active Directory domain by issuing the following command:

```
./vastool -u matt join example.com
```

Where:

- `-u` specifies the name of the user with domain administrator equivalent privileges.
- `matt` is a user in the sample network with Active Directory Domain Admin privileges.

**Note:** For Linux systems to join the domain you must use an Active Directory user that has the equivalent privileges of the Domain Admins group. Do not use the built-in Administrator account. This account cannot be used by `vastool`.

`example.com` is the name of the Active Directory domain in the sample network.

A prompt appears requesting the password for the user you entered.

3. Enter the user’s (`matt`) account password.

The results of the `vastool join` command appear. Using this command results in changes made to the configuration files, `/etc/opt/vas/vas.conf`, `/etc/nsswitch.conf`, and in the `/etc/pam.d` directory and starts the `vascd` daemon automatically.

To view this Linux system in Active Directory use the Active Directory Users and Computers snapin.

4. For these changes to take effect reboot your system or enter the following:

```
init 1
init 5
```

**Using vastool join Without Using DNS**

If you are not using DNS or if your DNS server does not contain the Active Directory SRV records, use the following instructions to configure your Linux clients. The fol-
lowing command allows you to pass the name of the Active Directory server to vastool on the vastool join command line.

To configure Linux clients without using DNS, complete the following:

1. As root, change directory to /opt/vas/bin.
2. Set the realm that the Linux system will use to log in to the Active Directory domain by issuing the following command:

   ```bash
   ./vastool -u matt join example.com adserv
   ```

   Where:

   - `u` specifies the name of the user with domain administrator equivalent privileges.
   - `matt` is a user with Active Directory Domain Admin privileges.

   **Note:** For Linux systems to join the domain you must use an Active Directory user that has the equivalent privileges of the Domain Admins group. Do not use the built-in Administrator account. This account cannot be used by vastool.

   - `example.com` is the name of the Active Directory domain in the sample network.
   - `adserv` is the machine name of the Active Directory server in the sample network.

   A prompt appears requesting the password for the user you entered.
3. Enter the user’s (matt) account password.

   The results of the join command appear. Using this command results in changes made to the configuration files, /etc/opt/vas/vas.conf, /etc/nsswitch.conf, and in the /etc/pam.d directory. The vascd daemon starts automatically.

   To view this Linux system in Active Directory use the Active Directory Users and Computers snapin.
4. For these changes to take effect reboot your system or enter the following:

    init 1

    init 5

Installing and Configuring UNIX Clients

Instructions follow for installing and configuring UNIX clients. This section includes the following:

- “Installing UnixWare Clients” on page 25
- “Synchronizing Time on UnixWare Clients” on page 26
- “Configuring UnixWare Clients” on page 27
- “SCO Authentication-Enabled Applications on UnixWare” on page 29
- “Installing SCO OpenServer Clients” on page 31
- “Synchronizing Time SCO OpenServer Clients” on page 33
- “Configuring SCO OpenServer Clients” on page 33
- “SCO Authentication-Enabled Applications on SCO OpenServer” on page 36
- “Installing Solaris Clients” on page 38
- “Synchronizing Time on Solaris Clients” on page 39
- “Configuring Solaris Clients” on page 40
Installing UnixWare Clients

To install UnixWare clients, complete the following:

1. Log in as root.

2. Mount the SCO Authentication CD as follows:

   ```
   mount -F cdfs -o ro /dev/cdrom/cdrom1 /mnt/cd
   ```

   Where:

   `/dev/cdrom/cdrom1` is the special device name for your CDROM drive.

   `/mnt/cd` is the directory to which the CD will be mounted.

3. Enter the following to install the SCO Authentication client components from the `uw7/` subdirectory in the CD mount directory:

   ```
   pkgadd -d /mnt/cd/uw7/vasclient_UnixWare_5_x86at-1.2.pkg
   ```

4. Press Enter when prompted to specify the packages you want to install.

   **Note:** In certain situations the system requests information on `pkgadd`. Respond appropriately for your system setup.

5. Add the following lines to `/etc/syslog.conf` to enable the logging of SCO Authentication notices and error messages:

   ```
   daemon.notice                  /usr/adm/syslog
   daemon.emerg                   *
   ```

   **Important:** You must use tabs for the whitespace between the two columns of text, not spaces.

6. Re-start syslogd in order for your changes to take affect:

   ```
   kill -HUP `cat /etc/syslog.pid`
   ```

   **Installing and Configuring UNIX Clients  25**
**Important:** Use the left-single quotes around `cat /etc/syslog.pid`.

7. To install your license key, change to `/opt/vas/bin` and enter the following:

```
# ./vastool license serial_number key
```

Where:

- `serial_number` is your key serial number.
- `key` is your license key.

You need both your license key and your license serial number.

**Synchronizing Time on UnixWare Clients**

In order to communicate with Active Directory, the SCO Authentication client must be synchronized within 2 minutes of the time on the Active Directory domain. The recommended method for synchronizing time is to configure and use the NTP client available on all UNIX and Linux platforms. Refer to your system documentation for instruction on using NTP client.

You can also use `vastool timesync`, however, this is only a quick fix and will not provide the accuracy required.

To synchronize time with Active Directory, enter the following:

```
/opt/vas/bin/vastool timesync <adserver>
```

Where `adserver` is the hostname of the Active Directory server or the server offering NTP time services. Do not enter the brackets.

For additional information on synchronizing time, see Appendix A, “Time Synchronization,” on page 43.
Configuring UnixWare Clients

In order for your client to communicate with Active Directory you must configure the operating system’s PAM and NSS subsystems to use the SCO Authentication components (for more information on PAM and NSS, see the SCO Authentication Administration Guide), set the realm that the client uses to log in to the Active Directory domain, and add a computer object for your system in Active Directory. This can all be accomplished using the command line configuration tool, vastool join.

Using DNS

By default, SCO Authentication searches your DNS server for the Active Directory service locator (SRV) records when it tries to locate an appropriate Active Directory server. Your DNS server must be set up to allow dynamic updates from Active Directory.

If your DNS server is set up to handle auto detection of your Active Directory server, complete the following instructions to configure your UnixWare clients:

1. As root, change directory to /opt/vas/bin.

2. Set the realm that the UnixWare system will use to log in to the Active Directory domain by issuing the following command:

   ./vastool -u matt join example.com

   Where:

   -u specifies the name of the user with domain administrator equivalent privileges.

   matt is a user in the sample network with Active Directory Domain Admin privileges.

   Note: For UnixWare systems to join the domain you must use an Active Directory user that has the equivalent privileges of the Domain Admins group. Do not use the built-in Administrator account. This account cannot be used by vastool.

   example.com is the name of the Active Directory domain in the sample network.
A prompt appears requesting the password for the user you entered.

3. Enter the user’s (matt) account password.

The results of the `vastool join` command appear. Using this command results in changes made to the configuration files, `/etc/opt/vas/vas.conf`, `/etc/nsswitch.conf`, and in the `/etc/pam.conf` directory and re-starts the `vascd` daemon automatically.

4. For these changes to take effect reboot your system or enter the following:
   ```
   init 1
   init 3
   ```

**Using `vastool join` Without Using DNS**

If you are not using DNS or if your DNS server does not contain the Active Directory SRV records, use the following instructions to configure your UnixWare clients. The following command allows you to pass the name of the Active Directory server to `vastool` on the `vastool join` command line.

To configure UnixWare clients without using DNS, complete the following:

1. As `root`, change directory to `/opt/vas/bin`.

2. Set the realm that the UnixWare system will use to log in to the Active Directory domain by issuing the following command:
   ```
   ./vastool -u matt join example.com adserv
   ```
   Where:
   - `u` specifies the name of the user with domain administrator equivalent privileges.
   - `matt` is a user in the sample network with Active Directory Domain Admin privileges.
Note: For UnixWare systems to join the domain you must use an Active Directory user that has the equivalent privileges of the Domain Admins group. Do not use the built-in Administrator account. This account cannot be used by vastool.

example.com is the name of the Active Directory domain in the sample network.

adserv is the machine name of the Active Directory server in the sample network.

A prompt appears requesting the password for the user you entered.

3. Enter the user’s (matt) account password.

The results of the join command appear. Using this command results in changes made to the configuration files, /etc/opt/vas/vas.conf, /etc/nsswitch.conf, and /etc/pam.conf directory. The vascd daemon starts automatically.

You can view this UnixWare system by using the Active Directory Users and Computers snapin.

4. For these changes to take effect reboot your system or enter the following:

   init 1
   init 3

SCO Authentication-Enabled Applications on UnixWare

Many server services and client applications use the Pluggable Authentication Module (PAM) to integrate with SCO Authentication. UnixWare does not ship with PAM. In order to enable these applications and services you must complete the configuration instructions that follow.

Configuring SCO Authentication-Enabled Server Applications

All of the SCO Authentication-enabled server applications must be installed on your
UnixWare system before the installation can be considered complete. Trying to interact with SCO Authentication components without having these applications installed can leave your system unstable and hence is highly discouraged.

**Configuring the Telnet Server**

To set up a Telnet server on your UnixWare system, complete the following:

1. Open `/etc/inetd.conf` and locate the following lines. Make sure both are commented out (add a “#” to the beginning of each line if one isn't already there):

   ```
telnet stream tcp nowait root /usr/sbin/in.tcpd in.telnetd

telnet stream tcp nowait root /usr/sbin/in.telnetd in.telnetd
   ```

2. Below those lines, add the following line for the SCO Authentication-enabled replacement Telnet server:

   ```
telnet stream tcp nowait root /opt/vas/sbin/in.telnetd
in.telnetd -a none
   ```

3. Restart the inetd server by running:

   ```
   kill -HUP `cat /etc/saf/inetd/_pid`
   ```

**Configuring the FTP Server**

To set up an FTP server on your UnixWare system, complete the following:

1. In `/etc/inetd.conf`, locate the following lines and make sure both are commented out (add a “#” to the beginning of each line if one isn't already there):

   ```
ftp stream tcp nowait root /usr/sbin/in.tcpd in.ftpd

ftp stream tcp nowait root /usr/sbin/in.ftpd in.ftpd
   ```
2. Below those lines, add the following line for the SCO Authentication-enabled replacement FTP server:

```
ftp stream tcp nowait root /opt/vas/sbin/in.ftpd
in.ftpd -a none
```

3. Restart the inetd server by running:

```
kill -HUP `cat /etc/saf/inetd/_pid`
```

### Installing SCO OpenServer Clients

To install SCO OpenServer clients, complete the following:

1. Log in as root.

2. If you are installing SCO Authentication to an OpenServer 5.0.6 system, install Release Supplement rs506a. You must install this supplement before continuing.

   The Release Supplement and instructions on how to install are available at the following URL:


   **Note:** Versions of SCO OpenServer newer than 5.0.6 do not need this Release Supplement.

3. Mount the SCO Authentication CD:

   ```
   mount -o ro -f ISO9660 /dev/cd0 /mnt/cd
   ```

   Where:

   `/dev/cd0` is the special device for your CDROM drive.

   `/mnt/cd` is the directory to which the CD is mounted.
4. Enter the following to install the SCO Authentication client components from the osr5/ subdirectory in the CD mount directory:

```bash
pkgadd -d /mnt/cd/osr5/vasclient_SCO_SV_3.2-2.1.pkg
```

5. Press **Enter** when prompted to specify the packages you want to install.

**Note:** In certain situations the system requests information on `pkgadd`. Respond appropriately for your system setup.

6. Add the following lines to `/etc/syslog.conf` to enable the logging of SCO Authentication notices and error messages:

```bash
daemon.notice /usr/adm/syslog
```

```bash
daemon.emerg *
```

**Important:** You must use tabs for the whitespace between the two columns of text, not spaces.

7. Re-start syslogd in order for your changes to take affect:

```bash
kill -HUP `cat /etc/syslog.pid`
```

**Important:** Use the left-single quotes around `cat /etc/syslog.pid`.

8. To install your license key, change to `/opt/vas/bin` and enter the following:

```bash
# ./vastool license serial_number key
```

Where:

- `serial number` is your key serial number.
- `key` is your license key.

You need both your license key and your license serial number.

---

32 SCO Authentication Installation and Configuration Guide
Synchronizing Time SCO OpenServer Clients

In order to communicate with Active Directory, the SCO Authentication client must be synchronized within 2 minutes of the time on the Active Directory domain. The recommended method for synchronizing time is to configure and use the NTP client available on all UNIX and Linux platforms. Refer to your system documentation for instruction on using NTP client.

You can also use `vastool timesync`, however, this is only a quick fix and will not provide the accuracy required.

To synchronize time with Active Directory, enter the following:

```
/opt/vas/bin/vastool timesync <adserver>
```

Where `adserver` is the hostname of the Active Directory server or the server offering NTP time services. Do not enter the brackets.

For additional information on synchronizing time, see Appendix A, “Time Synchronization,” on page 43.

Configuring SCO OpenServer Clients

In order for your client to communicate with Active Directory you must configure the operating system’s PAM and NSS subsystems to use the SCO Authentication components (for more information on PAM and NSS, see the *SCO Authentication Administration Guide*), set the realm that the client uses to log in to the Active Directory domain, and add a computer object for your system in Active Directory. This can all be accomplished using the command line configuration tool, `vastool join`. 
Using DNS

By default, SCO Authentication searches your DNS server for the Active Directory service locator (SRV) records when it tries to locate an appropriate Active Directory server. Your DNS server must be set up to allow dynamic updates from Active Directory.

If your DNS server is set up to handle auto detection of your Active Directory server, complete the following instructions to configure your SCO OpenServer clients:

1. As root, change directory to /opt/vas/bin.

2. Set the realm that the SCO OpenServer client system will use to log in to the Active Directory domain by issuing the following command:

   ```bash
   ./vastool -u matt join example.com
   ```

   Where:

   -u specifies the name of the user with domain administrator equivalent privileges.

   matt is a user in the sample network with Active Directory Domain Admin privileges.

   **Note:** For SCO OpenServer systems to join the domain you must use an Active Directory user that has the equivalent privileges of the Domain Admins group. Do not use the built-in Administrator account. This account cannot be used by vastool.

   example.com is the name of the Active Directory domain in the sample network.

   A prompt appears requesting the password for the user you entered.

3. Enter the user’s (matt) account password.

   The results of the vastool join command appear. Using this command results in changes made to the configuration files, /etc/opt/vas/vas.conf, /etc/nsswitch.conf, and in the /etc/pam.conf directory and re-starts the vascd daemon automatically.
4. For these changes to take effect reboot your system or enter the following:

   init 1

   init 3

Using vastool join Without Using DNS

If you are not using DNS or if your DNS server does not contain the Active Directory SRV records, use the following instructions to configure your SCO OpenServer clients. The following command allows you to pass the name of the Active Directory server to vastool on the vastool join command line.

To configure SCO OpenServer clients without using DNS, complete the following:

1. As root, change directory to /opt/vas/bin.

2. Set the realm that the SCO OpenServer system will use to log in to the Active Directory domain by issuing the following command:

   ./vastool -u matt join example.com adserv

   Where:

   -u specifies the name of the user with domain administrator equivalent privileges.

   matt is a user in the sample network with Active Directory Domain Admin privileges.

   example.com is the name of the Active Directory domain in the sample network.

   adserv is the machine name of the Active Directory server in the sample network.

   A prompt appears requesting the password for the user you entered.

   Note: For SCO OpenServer systems to join the domain you must use an Active Directory user that has the equivalent privileges of the Domain Admins group. Do not use the built-in Administrator account. This account cannot be used by vastool.
3. Enter the user’s (matt) account password.

   The results of the join command appear. Using this command results in changes made to the configuration files, /etc/opt/vas/vas.conf, /etc/nsswitch.conf, and /etc/pam.conf directory. The vascd daemon starts automatically.

   You can view this SCO OpenServer system by using the Active Directory Users and Computers snapin.

4. For these changes to take effect reboot your system or enter the following:

   init 1

   init 3

SCO Authentication-Enabled Applications on SCO OpenServer

Many server services and client applications use the Pluggable Authentication Modules system (PAM) to integrate with SCO Authentication. SCO OpenServer does not ship with PAM. In order to enable these applications and services you must complete the configuration instructions that follow.

Configuring SCO Authentication-Enabled Server Applications

All of the SCO Authentication-enabled server applications must be installed on SCO OpenServer systems before the installation can be considered complete. Trying to interact with SCO Authentication components without having these applications installed can leave your system unstable and hence is highly discouraged.

Configuring the Telnet Server

To set up a Telnet server on your SCO OpenServer system, complete the following:

1. Open /etc/inetd.conf and locate the following line. Make sure it is commented out
Installing and Configuring UNIX Clients

SCO Authentication Installation and Configuration Guide
July 18, 2003

Configuring the Telnet Server

To set up a Telnet server on your SCO OpenServer system, complete the following:

1. In /etc/inetd.conf, locate the following line and make sure it is commented out (add a “#” to the beginning of the line if one isn't already there):

   telnet stream tcp nowait NOLUID /etc/telnetd telnetd

2. Below that line, add the following line for the SCO Authentication-enabled replacement Telnet server:

   telnet stream tcp nowait root /opt/vas/sbin /in.telnetd in.telnetd -a none

3. Restart the inetd server by running:

   kill -HUP `cat /etc/saf/inetd/_pid`

Configuring the FTP Server

To set up an FTP server on your SCO OpenServer system, complete the following:

1. In /etc/inetd.conf, locate the following line and make sure it is commented out (add a “#” to the beginning of the line if one isn't already there):

   ftp stream tcp nowait root /etc/ftpd/ftpd

2. Below those lines, add the following line for the SCO Authentication-enabled replacement FTP server:

   ftp stream tcp nowait root /opt/vas/sbin/in.ftpd in.ftpd -a none

3. Restart the inetd server by running:

   kill -HUP `cat /etc/saf/inetd/_pid`
Installing Solaris Clients

**Important:** Before you begin the installation of the client components on Solaris systems you should install the latest patches (including 110934-05 and 110380-04 on Solaris 8) from the Sun web site. The patches are available at:

http://www.sun.com/bigadmin/patches

To install Solaris clients, complete the following:

1. Log in as **root**.

2. Insert the SCO Authentication CD and go to the **solaris** directory at the root of the CD.

   The CD mounts automatically. A file browser appears containing the contents of the CD. If you are running in non-graphic mode, the CD is accessible from the **/cdrom** directory.

3. Enter:

   ```
   pkgadd -d vasclient_SunOS_5.8_sparc-2.1.pkg
   ```

   The following message appears:

   ```
   The following packages are available VAS client component (sparc) x.x.x.
   
   Select Packages you want to process.
   ```

4. Type **All**.

   **Note:** In certain situations the system requests information on pkgadd. Respond appropriately for your system setup.

   A message follows indicating that the installation was successful.

   The client component is now installed but not configured. For instructions on configuring clients, see “Configuring Solaris Clients” on page 40.
5. To install your license key, change to /opt/vas/bin and enter the following:

```bash
# ./vastool license serial_number key
```

Where:

- **serial number** is your key serial number.
- **key** is your license key.

You need both your license key and your license serial number.

### Synchronizing Time on Solaris Clients

In order to communicate with Active Directory, the SCO Authentication client must be synchronized within 2 minutes of the time on the Active Directory domain. The recommended method for synchronizing time is to configure and use the NTP client available on all UNIX and Linux platforms. Refer to your system documentation for instruction on using NTP client.

You can also use `vastool timesync`, however, this is only a quick fix and will not provide the accuracy required.

To synchronize time with Active Directory, enter the following:

```bash
/opt/vas/bin/vastool timesync <adserv>
```

Where `adserv` is the hostname of the Active Directory server in the sample network or it can be the name of the server offering NTP time services. Do not enter the brackets.

For additional information on synchronizing time, see Appendix A, “Time Synchronization,” on page 43.
Configuring Solaris Clients

In order for your client to communicate with Active Directory you must configure the operating system’s PAM and NSS subsystems to use the SCO Authentication components (for more information on PAM and NSS, see the *SCO Authentication Administration Guide*), set the realm that the client uses to log in to the Active Directory domain, and add a computer object for your system in Active Directory. This can all be accomplished using the command line configuration tool, `vastool join`.

Using DNS

By default, SCO Authentication searches your DNS server for the Active Directory service locator (SRV) records when it tries to locate an appropriate Active Directory server. Your DNS server must be set up to allow dynamic updates from Active Directory.

If your DNS server is set up to handle auto detection of your Active Directory server, complete the following instructions to configure your Solaris clients:

1. As `root`, change directory to `/opt/vas/bin`.

2. Set the realm that the Solaris system will use to log in to the Active Directory domain by issuing the following command:

   ```
   ./vastool -u matt join example.com
   ```

   Where:

   - `-u` specifies the name of the user with domain administrator equivalent privileges.

   - `matt` is a user in the sample network with Active Directory Domain Admin privileges.

   **Note:** For Solaris systems to join the domain you must use an Active Directory user that has the equivalent privileges of the Domain Admins group. Do not use the built-in Administrator account. This account cannot be used by `vastool`.

   - `example.com` is the name of the Active Directory domain in the sample network.
A prompt appears requesting the password for the user you entered.

3. Enter the user’s (*matt*) account password.

The results of the `vastool join` command appear. Using this command results in changes made to the configuration files, `/etc/opt/vas/vas.conf`, `/etc/nsswitch.conf`, and in the `/etc/pam.conf` directory and re-starts the `vascd` daemon automatically.

4. For these changes to take effect reboot your system or enter the following:

```
init 1
init 3
```

## Using vastool join Without Using DNS

If you are not using DNS or if your DNS server does not contain the Active Directory SRV records, use the following instructions to configure your Solaris clients. The following command allows you to pass the name of the Active Directory server to `vastool` on the `vastool join` command line.

To configure Solaris clients without using DNS, complete the following:

1. As **root**, change directory to `/opt/vas/bin`.

2. Set the realm that the Solaris system will use to log in to the Active Directory domain by issuing the following command:

```
./vastool -u matt join example.com adserv
```

Where:

- `-u` specifies the name of the user with domain administrator equivalent privileges.

- `matt` is a user in the sample network with Active Directory Domain Admin privileges.

**Note**: For Solaris systems to join the domain you must use an Active Directory user that has the equivalent privileges of the Domain Admins group. Do not use
the built-in Administrator account. This account cannot be used by vastool.

example.com is the name of the Active Directory domain in the sample network.

adserv is the machine name of the Active Directory server in the sample network.

A prompt appears requesting the password for the user you entered.

3. Enter the user’s (matt) account password.

The results of the join command appear. Using this command results in changes made to the configuration files, /etc/opt/vas/vas.conf, /etc/nsswitch.conf, and /etc/pam.conf directory. The vascd daemon starts automatically.

You can view this Solaris system by using the Active Directory Users and Computers snapin.

4. For these changes to take effect reboot your system or enter the following:

   init 1

   init 3
Time Synchronization

Kerberos is a time sensitive protocol that requires “rough” synchronization of the UNIX and Linux workstation clocks with the Windows 2000/2003 time server. A difference of more than 2 minutes between the time on the Windows 2000/2003 server and the time on the UNIX and Linux workstations results in a “clock skew” situation. If the following error message is returned by vastool, the administration should suspect a time problem:

Could not initialize VAS library, error = Clock skew too great.

Windows uses a slightly different protocol for time synchronization than UNIX and Linux. Windows uses Simple Network Time Protocol (SNTP). UNIX and Linux use Network Time Protocol (NTP) which is more secure and accurate than SNTP. The result is that it is not possible for UNIX and Linux clients to be configured to synchronize their time directly with the Windows 200/2003 SNTP server. The reason is that the Windows 200/2003 SNTP server can not handle the NTP time synchronization requests that are generated by UNIX and Linux.

Fortunately, NTP was designed to be backward compatible with the less accurate SNTP. In other words, an NTP server accepts both NTP and SNTP time synchronization requests. This being the case, the best solution for time synchronization is to have the Window 2000 Server and the UNIX and Linux workstations synchronize against a master NTP server. Figure 6 on page 44 depicts using a time server with SCO Authentication.
Configuring the SNTP Service on Window 2000/2003

To configure SNTP on Windows 2000/2003, complete the following:

1. Log in as administrator.
2. Open an MS-DOS command window.
3. At the command prompt, enter:
   
   ```
   c:/> net time /setsntp:tictoc
   ```

   Where: `tictoc` is the name or address of a master time server. If your organization does
not already have an internal NTP time server you can use one of the government National Institute of Standards and Technology (NIST) Internet Time Servers. A list of available time servers can be found at:

http://www.boulder.nist.gov/timefreq/service/time-servers.html

In order for changes to the time source configuration to take affect, the Windows 2000/2003 time service must be restarted as follows:

```
c:\> net stop w32time

c:\> net start w32time
```

Synchronizing Time on Client Platforms

SCO Authentication uses the Kerberos protocol for all authentication. Kerberos is a time sensitive protocol. This means that the system clocks on all computers involved in a Kerberos authentication exchange must be within a set amount of time between each other. By default, Active Directory allows a clock skew of two minutes.

There are two approaches for synchronizing a SCO Authentication client's system clock with Active Directory:

- Configuring the NTP client
- Using the built in SCO Authentication SNTP client

The first, and recommended, approach is to use the NTP client that comes with your UNIX or Linux system to synchronize your time with an external NTP server. This is what is shown in Figure 6 on page 44. The NTP client provides sophisticated time synchronization along with a number of other benefits over using an SNTP client.

Configuring the UNIX/Linux NTP client is beyond the scope of this document. Refer to your system administration guide for more information on configuring your system's NTP client.
The second approach for synchronizing a SCO Authentication client's system clock with Active Directory is to use the SNTP client functionality built into SCO Authentication. This SNTP client functionality was written to allow you to synchronize the system clock directly against an Active Directory server. If no NTP client is running on your system, `vascd` synchronized the system time every 12 hours by default. This interval can be modified, and also disabled in `/etc/opt/vas/vas.conf`. For information on modifying the `vascd` timesync behavior, see the `vascd` man page.

Since `vascd` acts only as an SNTP client, it does not provide the features of NTP. However, it does allow you to provide time synchronization without having to deal with the complexities of NTP.

In some cases you will need to quickly synchronize your system clock. There are two utilities you can use to do this. The first is `ntpdate`, which allows you to set your clock against any NTP server. The other is the `vastool timesync` command which allows you to set your clock against any Active Directory or SNTP server. Note that these utilities do not provide a true time synchronization solution since they do not handle clock drift.

To synchronize time with Active Directory using `ntpdate`, complete the following:

Log in as `root` and enter the following:

```bash
# ntpdate -b tictoc
```

```
21 Jan 13:35:52 ntpdate [16320]: step time server
216.250.131.1 offset -0.025796 sec
```

Where `tictoc` is the name or address of a master time server (in this case, the same master time server that is used on the Windows 2000/2003 system).
Refer to your system documentation for your NTP client for more information on `ntpd`.

To synchronize time with Active Directory using `vastool timesync`, enter the following:

```
/opt/vas/bin/vastool timesync <adserver>
```

Where `adserver` is the hostname of the Active Directory server or the server offering NTP time services. Do not enter the brackets. Refer to the `vastool` man page for more information on `vastool timesync`. 
B Error Messages

Error messages and explanations follow.

• Client not found in Kerberos database.

  Explanation: The client was not correctly configured, for information on configuring clients, see Appendix B, “Error Messages,” on page 49.

  This error message might also appear when starting vascd or when running the vastool.

• Clock skew too great.


• Could not authenticate, error = Cannot contact any KDC for requested realm.

  Explanation: The Active Directory server can not be found. Make sure that the name of the Active Directory server is resolvable via DNS. Note that if your Active Directory domain name and your Internet domain name differ, you need to be able to resolve machine names using both the Internet domain name and the Active Directory domain name.

  Example: If your Internet domain name is “nosuchname.com” and your Active Directory domain name is “example.com”, each machine that uses the Active Directory domain should be resolvable in DNS with both a “nosuchname.com” name and an “example.com” name.
Another symptom that can cause this error is if the Active Directory server is no longer accessible from the network. This could be as simple as the Active Directory machine being turned off, or its network cable being unplugged, or its networking being turned off within Windows 2000/2003. Network routing issues could also cause this to happen. Solving network routing issues transcends the scope of this document.

• Could not authenticate, error = Preauthentication failed.

An incorrect password was entered during the authentication phase of a vastool-invoked process (such as vastool -u user join...). Try again using the correct password.

• Could not authenticate, error = Client not found in Kerberos database.

The user name passed to vastool (for example, vastool -u user join...) does not exist in Active Directory. Create the user account in Active Directory if necessary and try again.

• Adding host/machine@REALM.COM to the Domain.....Failed, error = [text deleted] problem 4003 (INSUFF_ACCESS_RIGHTS), data 0

The user account that was passed to vastool with the -u parameter is not a member of the Domain Admins group. Unless the user running vastool is a member of that group, the computer running vastool can not be added to Active Directory. Either choose a different account that is a member of the Domain Admins group or assign your user account to the Domain Admins group.
Troubleshooting

Use the following information to help you work through issues you might confront.

Changes to Active Directory Data are Not Seen

There might be a situation where you change something like a user or group object in Active Directory, but no matter what you try you can not get SCO Authentication to display the changes. Possible causes for this include an out of sync cache and the presence of `nscd`.

As a troubleshooting tool, it is possible to determine if the cache is out of date by comparing the differences between the output of `vastool list users` and `vastool list -l users`. If the cache is out of date, the output from those two commands will be different. The `-l` parameter to `vastool` bypasses the cache and reads information directly from Active Directory.

```
$ vastool list -l users
matt:x:1000:1000:Matt Peterson:/home/matt:/bin/bash
wynn:x:1001:2000:Wynn Wilkes:/home/wynn:/bin/bash
$ vastool list users
matt:x:1000:1000:Matt Peterson:/usr/home/matt:/bin/bash
wynn:x:1001:2000:Wynn Wilkes:/usr/home/wynn:/bin/bash
```

In this situation you would simply re-start `vascd`. If the changes still don’t appear, run `vastool flush` to clear the cache. With the cache clear, `vastool` updates the cache with current data the next time user data is requested by SCO Authentication. It is worth noting that the same `vastool` commands listed above for user data can be used to query group data. Either classification of data will suffice.
The **nscd** issue can be a bit more difficult to deal with because occasionally Linux vendors install and enable **nscd** when the operating system is updated. If **nscd** is installed on your system and is running, check the `/etc/nscd.conf` file to be sure the passwd and group entries are commented out. If not, comment them (put a “#” at the beginning of each line).

One other possible culprit is the SCO Authentication blackout period. In some situations, **vascd** waits up to 10 minutes by default before caching Active Directory authentication data. In order to change the length of **vascd** we recommend that you change a setting in `/etc/opt/vas/vas.conf`. In the [vascd] section, add a parameter for “update-interval” as follows:

```plaintext
[vascd]
  update-interval = 300
```

This specifies the length of the blackout period in seconds. The default is 600 seconds. For more information on the blackout period, see the **vascd** man page.

**Debugging PAM Problems**

If you experience problems using the **pam_vas** module for system authentication, you can enable verbose debugging for **pam_vas** by appending “debug” to each **pam_vas** line in the respective PAM configuration file. The debug output goes through the “authentication system” log via syslog.

On Red Hat Linux, these log messages are saved to `/var/log/secure` by default. On SuSE and UnitedLinux based Linux distributions, these messages are saved to `/var/log/messages` by default.

On some systems such as Solaris, there is no default log configured to receive these messages. To configure syslog to save these messages to a log file, add the following lines to `/etc/syslog.conf` and restart syslog:

```plaintext
auth.alert /dev/console
auth.crit root
auth.info;auth.debug /var/log/auth
```

Be sure to use **TAB** characters between the left and right columns, not spaces.