

Likewise® Open

Installation and Administration Guide

Version 6.1

Likewise Open Installation and Administration Guide

Abstract

Last updated: June 28, 2011.

This guide describes how to install and manage Likewise Open, an open source version of the Likewise agent that connects Linux, Unix, and Mac OS X computers to Microsoft Active Directory and authenticates users with their domain credentials. The guide covers installing the agent, joining an Active Directory domain, logging on with domain credentials, configuring the agent, and troubleshooting.

This guide is supplemented by the Likewise Open community forum, which you can join at <http://www.likewise.com/community/>.

This Version

Likewise Open **6.0 and 6.1** (in Ubuntu 11.04 or later): http://www.likewise.com/resources/documentation_library/manuals/open/likewise-open-guide.html

Previous Versions

Likewise Open 5.4 (in Ubuntu 10.04): http://www.likewise.com/resources/documentation_library/manuals/open/likewise-open-54-guide.html

Likewise Open 5.2 and 5.3: http://www.likewise.com/resources/documentation_library/manuals/open/likewise-open-53-guide.html

Likewise Open 5.1: http://www.likewise.com/resources/documentation_library/manuals/open/likewise-open-51-guide.html

Likewise Open 5.0: http://www.likewise.com/resources/product_documentation/Likewise-Open-5-Guide.pdf

Likewise Open 4.1: http://www.likewise.com/resources/user_documentation/Likewise-Open-Guide.pdf

Table of Contents

1. Quick Start	1
1.1. Install the Agent on Linux, Join a Domain, and Log On	1
1.2. Set Common Options	4
1.3. Give Your Domain Account Admin Rights	5
1.4. Upgrade to the Latest Version	5
2. The Likewise Agent	6
2.1. About the Likewise Agent	6
2.2. Daemons	6
2.3. The Likewise Registry	10
2.4. Ports and Libraries	10
2.5. Caches and Databases	10
2.6. Time Synchronization	12
2.7. Using a Network Time Protocol Server	12
2.8. Automatic Detection of Offline Domain Controller and Global Catalog	13
2.9. UID-GID Generation in Likewise Open and Likewise Enterprise Cells	13
2.10. Cached Credentials	13
2.11. Trust Support	14
2.12. Integrating with Samba	15
2.13. Supported Platforms	15
3. Configuring Clients Before Agent Installation	16
3.1. Configure nsswitch.conf	16
3.2. Configure resolv.conf	16
3.3. Configure Firewall Ports	16
3.4. Extend Partition Size Before Installing Likewise on IBM AIX	17
3.5. Increase Max Username Length on IBM AIX	17
3.6. Check System Health Before Installing the Agent	17
4. Installing the Agent	22
4.1. Install the Correct Version for Your Operating System	22
4.2. Requirements for the Agent	22
4.3. Install the Agent on Linux or Unix with the Shell Script	25
4.4. Install the Agent on Linux in Unattended Mode	25
4.5. Install the Agent on Unix with the Command Line	26
4.6. Install the Agent on a Mac Computer	26
4.7. Install the Agent on a Mac in Unattended Mode	27
4.8. Installing the Agent in Solaris Zones	28
4.9. Upgrading Your Operating System	29
5. Joining an Active Directory Domain	30
5.1. About Joining a Domain	30
5.2. Join Active Directory with the Command Line	32
5.3. <code>domainjoin-cli</code> Options, Commands, and Arguments	33
5.4. Join Active Directory Without Changing <code>/etc/hosts</code>	39
5.5. Join a Linux Computer to Active Directory with the GUI	40
5.6. Join a Mac Computer to Active Directory with the GUI	41
5.6.1. Turn Off OS X Directory Service Authentication	44
5.7. Use Likewise with a Single OU	44
5.8. Rename a Joined Computer	45
5.9. Files Modified When You Join a Domain	47
5.10. With NetworkManager, Use a Wired Connection to Join a Domain	49
6. Logging On with Domain Credentials	50
6.1. About Logging On	50
6.2. Log On with AD Credentials	50

6.3. Log On with SSH	51
6.4. Solve Logon Problems from Windows	51
6.5. Solve Logon Problems on Linux or Unix	52
7. Troubleshooting Domain-Join Problems	57
7.1. Top 10 Reasons Domain Join Fails	57
7.2. Solve Domain-Join Problems	57
7.3. Ignore Inaccessible Trusts	60
7.4. Dealing with Common Error Messages	61
7.4.1. Configuration of Krb5	61
7.4.2. Chkconfig Failed	61
7.5. Diagnose NTP on Port 123	61
7.6. Turn Off Apache to Join a Domain	63
8. Configuring the Agent	64
8.1. Modify Settings with the Config Tool	64
8.2. Add Domain Accounts to Local Groups with /etc/group	65
8.3. Configure Entries in Your Sudoers Files	65
8.4. Set a Sudoers Search Path	66
8.5. Set Up AIX Audit Classes to Monitor Events	67
9. Troubleshooting the Agent	68
9.1. Likewise Daemons and Services	68
9.1.1. Troubleshoot Likewise Daemons with the Service Manager	68
9.1.2. Check the Status of the Authentication Daemon	69
9.1.3. Check the Status of the DCE/RPC Daemon	69
9.1.4. Check the Status of the Network Logon Daemon	70
9.1.5. Check the Status of the Input-Output Service	70
9.1.6. Restart the Authentication Daemon	71
9.1.7. Restart the DCE/RPC Daemon	71
9.1.8. Restart the Network Logon Daemon	71
9.1.9. Restart the Input-Output Service	71
9.2. Logging	72
9.2.1. Generate a Domain-Join Log	75
9.2.2. Generate an Authentication Agent Debug Log	76
9.2.3. Generate a PAM Debug Log	76
9.2.4. Generate a Directory Service Log on a Mac	77
9.2.5. Log Group Policy Debugging Data	77
9.2.6. Generate a Network Trace	78
9.3. Basics	78
9.3.1. Check the Version and Build Number	78
9.3.2. Determine a Computer's FQDN	79
9.3.3. Make Sure Outbound Ports Are Open	79
9.3.4. Check the File Permissions of nsswitch.conf	80
9.3.5. Configure SSH After Upgrading It	80
9.3.6. Upgrading an Operating System	80
9.4. Accounts	81
9.4.1. Allow Access to Account Attributes	81
9.4.2. A User's Settings Are Not Displayed in ADUC	81
9.4.3. Resolve an AD Alias Conflict with a Local Account	82
9.4.4. Fix the Shell and Home Directory Paths	83
9.4.5. Troubleshooting with the Get Status Command	83
9.4.6. Troubleshoot User Rights with Ldp.exe and Group Policy Modeling	84
9.4.7. Fix Selective Authentication in a Trusted Domain	87
9.5. Cache	88
9.5.1. Clear the Authentication Cache	88
9.5.2. Clear a Corrupted SQLite Cache	89

9.6. Kerberos	90
9.6.1. Fix a Key Table Entry-Ticket Mismatch	91
9.6.2. Fix KRB Error During SSO in a Disjoint Namespace	92
9.6.3. Eliminate Logon Delays When DNS Connectivity Is Poor	92
9.7. PAM	93
9.7.1. Dismiss the Network Credentials Required Message	93
9.8. Red Hat and CentOS	93
9.8.1. Modify PAM to Handle UIDs Less Than 500	93
9.9. SLED	93
9.9.1. A Note About the Home Directory on SLED 11	93
9.9.2. Updating PAM on SLED 11	94
9.10. AIX	94
9.10.1. Increase Max Username Length on AIX	94
9.10.2. Updating AIX	94
9.11. Mac OS X	95
9.11.1. Find the Likewise Service Manager Daemon on a Mac	95
9.12. FreeBSD	95
9.12.1. Keep Usernames to 16 Characters or Less	95
9.13. Solaris	96
9.13.1. Turn On Core Dumps on Solaris 10	96
10. Command-Line Reference	97
10.1. lwsm: Manage Services	97
10.2. lwconfig	98
10.3. lwregshell: The Registry Shell	98
10.4. lw-edit-reg: Export the Registry to Your Editor	98
10.5. lw-set-log-level: Set the Log Level	99
10.6. lw-set-machine-name: Change the Hostname in the Local Provider	99
10.7. Find a User or a Group	99
10.8. Find a User by a SID	100
10.9. List Groups for a User	101
10.10. lw-enum-groups: List Groups	101
10.11. lw-enum-users: List Users	101
10.12. lw-get-status: View the Status of the Authentication Providers	102
10.13. Get the Current Domain	103
10.14. lw-get-dc-list: List Domain Controllers	103
10.15. lw-get-dc-name: Get Domain Controller Information	103
10.16. lw-get-dc-time: Get Domain Controller Time	104
10.17. lw-get-log-info	104
10.18. lw-get-metrics	104
10.19. Get Machine Account Information	105
10.20. Reload Changes to the Configuration File	105
10.21. lw-trace-info: Turn on Trace Markers in Log Messages	105
10.22. lw-update-dns: Dynamically Update DNS	105
10.23. lw-ad-cache: Manage the AD Cache	106
10.24. domainjoin-cli: Join or Leave a Domain	107
10.25. lw-ypcat	107
10.26. lw-ypmatch	107
10.27. lw-adtool: Modify Objects in AD	107
10.28. lwio: Input-Output Commands	113
10.28.1. lwio-copy: Copy Files Across Disparate Operating Systems	114
10.28.2. lwio-refresh: Reload the Input-Output Settings After Changes	114
10.28.3. lwio-set-log-level	114
10.28.4. lwio-get-log-info	114
10.29. Commands to Modify Local Accounts	115

10.29.1. lw-add-user: Add a Local User by Name or UID	115
10.29.2. lw-add-group: Add a Local Group Member by Name or GID	115
10.29.3. lw-del-user: Remove a Local User by Name or UID	115
10.29.4. lw-del-group: Remove a Local Group by Name or GID	116
10.29.5. lw-mod-user: Modify a Local User by Name or UID	116
10.29.6. lw-mod-group: Modify a Local Group's Members	116
10.30. Kerberos Commands	116
10.30.1. kdestroy: Destroy the Kerberos Ticket Cache	116
10.30.2. klist: View Kerberos Tickets	117
10.30.3. kinit: Obtain and Cache a TGT	117
10.30.4. kpasswd: Change a Password	118
10.30.5. ktutil: The Keytab File Maintenance Utility	118
10.30.6. Kvno: Acquire a Service Ticket and Print Key Version Number	118
10.31. Commands and Scripts Not for Customer Use	119
10.31.1. ConfigureLogin	119
10.31.2. dceidl	119
10.31.3. gpccron	119
10.31.4. gpccron.sh	119
10.31.5. gprsrmtnt.sh	119
10.31.6. init-base.sh	119
10.32. Likewise Enterprise Tools Installed on Windows Computers	119
10.32.1. Lwopt.exe	119
11. Monitoring Events with the Event Log	121
11.1. Monitor Events with the Event Log	121
11.2. View the Local Event Log	121
11.3. The Event Type	124
11.4. The Event Source	124
11.5. List of Events by Source ID	124
12. Leaving a Domain and Uninstalling the Agent	127
12.1. Leave a Domain	127
12.2. Uninstall the Domain Join GUI	128
12.3. Uninstall the Agent on a Linux or Unix Computer	128
12.4. Uninstall the Agent on a Mac	129
13. Using Likewise for Single Sign-On	130
13.1. About Single Sign-On	130
13.2. Make Sure PAM Is Enabled for SSH	131
13.3. Configure PuTTY for Windows-Based SSO	132
13.4. Configure Apache for SSO	135
13.4.1. Kerberos Library Mismatch	145
13.5. Configure a Java Application Server for SSO	146
13.6. Examples	151
14. Configuring the Likewise Services with the Registry	152
14.1. About the Registry	152
14.1.1. The Structure of the Registry	152
14.1.2. Data Types	154
14.2. Modify Settings with the lwconfig Tool	155
14.3. Gain Access to the Registry	157
14.4. Change the Value of an Entry with the Shell	158
14.4.1. Set Common Options with the Registry Shell	159
14.5. Change the Value of an Entry from the Command Line	160
14.6. Find a Value Entry	160
14.7. Settings in the lsass Branch	160
14.7.1. Log Level Value Entries	161
14.7.2. Turn On Event Logging	161

14.7.3. Turn Off Network Event Logging	161
14.7.4. Restrict Logon Rights	162
14.7.5. Display an Error to Users Without Access Rights	162
14.7.6. Display an MOTD	163
14.7.7. Change the Domain Separator Character	163
14.7.8. Change the Replacement Character for Spaces	164
14.7.9. Turn Off System Time Synchronization	164
14.7.10. Set the Default Domain	165
14.7.11. Set the Home Directory and Shell for Domain Users	165
14.7.12. Set the Umask for Home Directories	167
14.7.13. Set the Skeleton Directory	167
14.7.14. Force Likewise Enterprise to Work Without Cell Information	168
14.7.15. Refresh User Credentials	169
14.7.16. Turn Off K5Logon File Creation	169
14.7.17. Change the Duration of the Machine Password	170
14.7.18. Sign and Seal LDAP Traffic	171
14.7.19. NTLM Value Entries	171
14.7.20. Additional Subkeys	172
14.7.21. Add Domain Groups To Local Groups	173
14.7.22. Control Trust Enumeration	173
14.7.23. Modify Smart Card Settings	174
14.7.24. Set the Interval for Checking the Status of a Domain	174
14.7.25. Set the Interval for Caching an Unknown Domain	175
14.8. Cache Settings in the lsass Branch	175
14.8.1. Set the Cache Type	175
14.8.2. Cap the Size of the Memory Cache	175
14.8.3. Change the Duration of Cached Credentials	176
14.8.4. Change NSS Membership and NSS Cache Settings	176
14.9. Settings in the eventlog Branch	178
14.9.1. Allow Users and Groups to Delete Events	178
14.9.2. Allow Users and Groups to Read Events	178
14.9.3. Allow Users and Groups to Write Events	179
14.9.4. Set the Maximum Disk Size	179
14.9.5. Set the Maximum Number of Events	179
14.9.6. Set the Maximum Event Timespan	180
14.9.7. Change the Purge Interval	180
14.10. Settings in the netlogon Branch	180
14.10.1. Set the Negative Cache Timeout	181
14.10.2. Set the Ping Again Timeout	181
14.10.3. Set the Writable Rediscovery Timeout	181
14.10.4. Set the Writable Timestamp Minimum Change	182
14.10.5. Set CLdap Options	182
14.11. Settings in the lwio Branch	182
14.11.1. Sign Messages If Supported	183
14.11.2. Enable Security Signatures	183
14.11.3. Require Security Signatures	183
14.11.4. Set Support for SMB2	183
14.12. Settings in the Lwedsplugin Branch for Mac Computers	184
15. Contacting Technical Support	186
15.1. Contact Support	186
15.2. Provide Diagnostic Information to Technical Support	186
16. Legal Disclaimer and Copyright Notice	189

Chapter 1. Quick Start

1.1. Install the Agent on Linux, Join a Domain, and Log On

This section skips system requirements and information about pre-configuring clients to cut to the chase: Installing Likewise Open on a Linux computer, connecting it to an Active Directory domain, and logging on with your domain credentials. (Jump to [install on Unix](#) or [install on Mac OS X](#).)

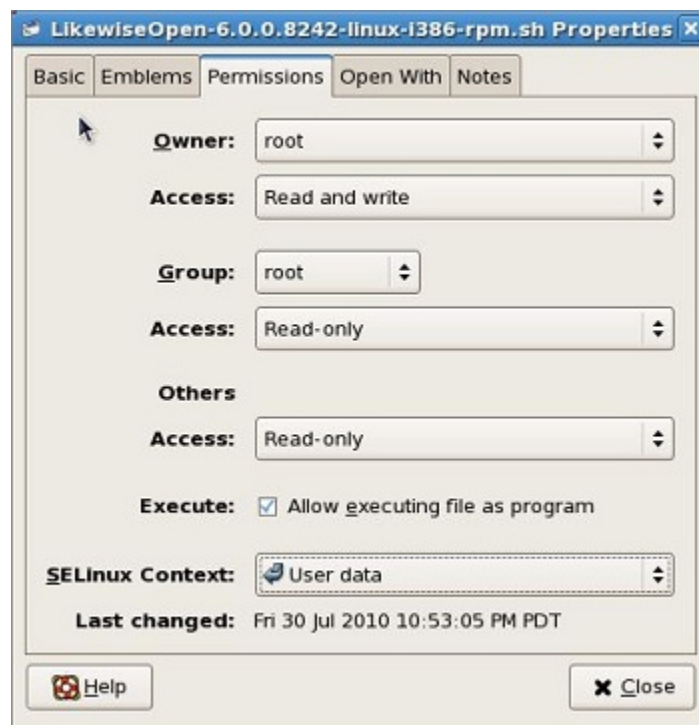
Before you deploy Likewise Open in anything other than a test environment, however, you should read the overview of the agent, the chapter on installing the agent, the chapter on joining a domain, and the chapter on configuring the Likewise services.

Step 1: Download Likewise Open

Go to <http://www.likewise.com/download/>. After you register, right-click the download link for your platform on the Likewise Open Download page and then save the installer to the desktop of your Linux computer.

Step 2: Install Likewise Open on Linux

You install Likewise Open by using a shell script that contains a self-extracting executable -- an SFX installer with a file name that ends in `sh`. Example:
`LikewiseIdentityServiceEnterprise-6.0.0.3499-linux-i386-rpm.sh`.



1. As root, make the installer executable: On the desktop, right-click the installer, click **Properties**, click the **Permissions** tab, and depending on your operating system select either **Allow executing file as program** or **Execute for Owner**, and then click **Close**.

Keep in mind that the dialog box can vary by platform. The point is that you must set the owner to be the root account and you must set the file to be executable as a program by the root account with read and write permissions.

Tip: You can also make the installer executable from the command line by changing directories to the desktop and then running `chmod a+x` as root or with `sudo`:

```
chmod a+x LikewiseIdentityServiceEnterprise-6.0.0.3499-linux-i386-rpm.sh
```

On Ubuntu, execute the `sudo` command before you execute the `chmod` command:

```
sudo chmod a+x LikewiseIdentityServiceEnterprise-6.0.0.3499-linux-i386-rpm.sh
```

2. As root, run the installer:

```
./LikewiseIdentityServiceEnterprise-6.0.0.3499-linux-i386-rpm.sh
```

3. Follow the instructions in the installer.

Note: On SLES and other systems on which the pager is set to `less`, you must exit the end user license agreement, or EULA, by typing the following command: `q`

Step 3: Join Active Directory

After the wizard finishes installing Likewise Open, the user interface for joining a domain appears. If it does not appear, see [Join Active Directory with the Command Line](#).

To join a computer to a domain, you must use the root account and you must have the user name and password of an Active Directory account that has privileges to join computers to the domain.

1. In the **Domain** box, enter the Fully Qualified Domain Name (FQDN) of your Active Directory domain. Example: `CORP.LIKEWISEDEMO.COM`



2. To avoid typing the domain prefix before your user or group name each time you log on, select **Enable default user name prefix** and enter your domain prefix in the box. Example: CORP
3. Under **Organizational Unit**, you can optionally join the computer to an OU by selecting **Specific OU Path** and then typing a path in the box. The OU path is from the top of the Active Directory domain down to the OU that you want. (See Use Likewise with a Single OU.)

Or, to join the computer to the Computers container, select **Default (Computers or previously joined OU)**.

4. Click **Join Domain**.
5. Enter the user name and password of an Active Directory account that has privileges to join computers to the domain and then click **OK**.

After you join a domain for the first time, you must restart the computer before you can log on.

To solve problems, see Troubleshooting Domain-Join Problems or run this command at the command line: `domainjoin-cli --help`

Step 4: Log On with AD Credentials

After you join a domain and restart your Linux computer, you can log on interactively or from the text login prompt with your Active Directory credentials in the following form: `DOMAIN\username`. If you set a default domain, just use your Active Directory username.

1. Log out of the current session.

2. Log on the system console by using the name of your Active Directory user account.

If you did not set a default domain, log on the system console by using an Active Directory user account in the form of DOMAIN\username, where DOMAIN is the Active Directory domain name. Example:

```
likewisedemo.com\kathy
```

Important: When you log on from the command line, for example with ssh, you must use a slash to escape the slash character, making the logon form DOMAIN\\username.

To troubleshoot issues, see [Solve Logon Problems on Linux](#).

1.2. Set Common Options

This section shows you how to quickly modify two common Likewise settings -- the default domain and the shell -- by running the following `lwconfig` command-line tool as root:

/opt/likewise/bin/lwconfig

To view the settings you can change with `lwconfig`, execute the following command:

```
/opt/likewise/bin/lwconfig --list
```

The syntax to change the value of a setting is as follows, where `setting` is replaced by the Likewise option that you want to change and `value` by the new value that you want to set:

```
/opt/likewise/bin/lwconfig setting value
```

Here's an example of how to use `lwconfig` to change the `AssumeDefaultDomain` setting:

```
[root@rhel5d bin]# ./lwconfig ---detail AssumeDefaultDomain ❶
Name: AssumeDefaultDomain
Description: Apply domain name prefix to account name at logon
Type: boolean
Current Value: false
Accepted Values: true, false
Current Value is determined by local policy.
```

```
[root@rhel5d bin]# ./lwconfig AssumeDefaultDomain true ❷
```

```
[root@rhel5d bin]# ./lwconfig ---show AssumeDefaultDomain ❸
boolean
true
local policy
```

- ❶ Use the `--detail` argument to view the setting's current value and to determine the values that it accepts.
- ❷ Set the value to `true`.
- ❸ Use the `--show` argument to confirm that the value was set to `true`.

Here's another example. To set the shell for a domain account, run `lwconfig` as root with the `LoginShellTemplate` setting followed by the path and shell that you want:

```
[root@rhel5d bin]# /opt/likewise/bin/lwconfig LoginShellTemplate -/
bin/ksh
```

For more information, see Set the Home Directory and Shell for Domain Users and the section on `lwconfig`.

1.3. Give Your Domain Account Admin Rights

You can give your Active Directory account local administrative rights to execute commands with superuser privileges and perform tasks as a superuser.

On Ubuntu, you can simply add your domain account to the `admin` group in the `/etc/group` file by entering a line like the following as root:

```
admin:x:115:LIKEWISEDEMO\kathy
```

On other Linux systems, you can add an entry for your Active Directory group to your `sudoers` file -- typically, `/etc/sudoers` -- by editing the file with the `visudo` command as root. Editing the `sudoers` file, however, is recommended only for advanced users, because an improperly configured `sudoers` file could lock out administrators, mess up the privileges of important accounts, or undermine the system's security.

Example entry of an AD user account:

```
% LIKEWISEDEMO\domain^admins ALL=(ALL) ALL
```

Note: The example assumes that you are a member of the Active Directory domain administrators group.

For information about how to format your `sudoers` file, see your computer's man page for `sudo`.

1.4. Upgrade to the Latest Version

With Likewise Open 6.0 or later, you can seamlessly upgrade from Likewise Open 5, preserving your local configuration and maintaining your Active Directory state. Simply install Likewise Open 6.0 or later while Likewise Open 5.3 or earlier is running and the computer is joined to a domain. It is unnecessary to leave the domain and uninstall the old version before you install the latest version. After installation, you will still be connected to your domain.

Likewise Open 6 preserves the changes you made to your local Likewise configuration. When you upgrade, a utility in Likewise Open 6 converts the configuration files from versions 5.0, 5.1, 5.2, and 5.3 into registry files and loads the files into the registry. The registry files that capture the old configuration are stored in `/tmp/lw-upgrade`; the original configuration files in `/etc/likewise` are removed.

Although the latest Ubuntu release makes the `likewise-open` package available through the `apt-get install` command, the Likewise Open 6 installer does not support upgrading from the package. Before you upgrade from the version available through Ubuntu, it is recommended that you leave the domain, uninstall the domain join GUI package (`likewise-open-gui`), and uninstall the `likewise-open` package.

Important: If you plan to upgrade from a 4.x or earlier version of Likewise Open to Likewise Open 6.0 or later, please first contact Likewise Technical Support at support@likewise.com. At this time, it is recommended that you do not attempt to upgrade to a 6.x version from a 4.x version without assistance from Likewise support.

Chapter 2. The Likewise Agent

2.1. About the Likewise Agent


The Likewise agent is installed on a Linux, Unix, or Mac OS X computer to connect it to Microsoft Active Directory and to authenticate users with their domain credentials. The agent integrates with the core operating system to implement the mapping for any application, such as the logon process (`/bin/login`), that uses the name service (NSS) or pluggable authentication module (PAM). As such, the agent acts as a Kerberos 5 client for authentication and as an LDAP client for authorization. In Likewise Enterprise, the agent also retrieves group policy objects to securely update local configurations, such as the sudo file.

The Likewise agent is also known as the Likewise client and the Likewise identity service.

2.2. Daemons

Likewise Open

The Likewise Open agent comprises the following daemons:

Daemon	Description	Dependencies
<code>/opt/likewise/sbin/lsassd</code>	<p>The Likewise authentication daemon. <i>Lsass</i> stands for Likewise Security and Authentication Subsystem. The service handles authentication, authorization, caching, and idmap lookups. You can check its status or restart it.</p> <p> View a diagram of the Lsass architecture.</p>	<code>netlogond lwiod dcerpcd eventlogd</code>
<code>/opt/likewise/sbin/netlogond</code>	Detects the optimal domain controller and global catalog and caches them. You can check its status or restart it.	None
<code>/opt/likewise/sbin/lwiod</code>	<p>The Likewise input-output service.</p> <p>The DCE-RPC client libraries use the Likewise input-output client library, which makes calls to <code>lwiod</code> with Unix domain sockets.</p> <p>You can check its status or restart it.</p> <p>The input-output service also communicates over SMB with</p>	<code>netlogond</code>

	SMB servers. For instructions on how to set up and use the Likewise CIFS/SMB file server, see the Likewise CIFS file server user guide.	
/opt/likewise/sbin/dcerpcd	The Likewise DCE/RPC endpoint mapper. DCE/RPC stands for Distributed Computing Environment/Remote Procedure Calls. The daemon handles communication between Linux, Unix, and Mac computers and Microsoft Active Directory by mapping data to endpoints. You can check its status or restart it.	netlogond lwiod
/opt/likewise/sbin/eventlogd	Collects and processes data for the event log.	netlogond lwiod dcerpcd For AD user account requests (but not for root account requests), eventlogd also depends on lsassd.
/opt/likewise/sbin/lwregd	The daemon for the registry service.	All the Likewise services depend on lwregd.
/opt/likewise/sbin/lwsmd	The Likewise service manager. It manages all the other Likewise daemons and services.	All the Likewise services depend on lwsmd.

Likewise Enterprise

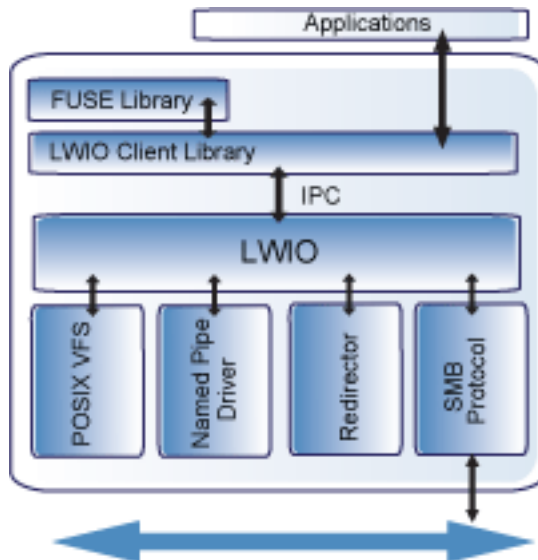
Likewise Enterprise includes all the daemons that are in Likewise Open. The following additional daemons are in Likewise Enterprise to apply group policies, handle smart cards, and monitor security events:

Daemon	Description	Dependencies
/opt/likewise/sbin/gpagentd	<p>The group policy agent. Part of Likewise Enterprise, it runs as a background service to pull group policy objects from Active Directory and apply them to the computer.</p> <p>The daemon uses LDAP to look up information about group policies and uses lwiod and its redirector to retrieve group policy objects.</p> <p>You can check its status or restart it.</p>	netlogond lwiod dcerpcd eventlogd lsassd

/opt/likewise/sbin/eventfwdd	Event forwarding daemon, part of the Likewise Enterprise data collection service.	eventlogd
/opt/likewise/sbin/reapsysld	Part of the Likewise data collection service that is included in Likewise Enterprise.	eventlogd eventfwdd
/opt/likewise/sbin/lwscd	The daemon for the smart card service. See the chapter on using Likewise with a smart card.	lwpkcs11d
/opt/likewise/sbin/lwpkcs11d	A daemon that aids the Likewise smart card service by supporting the PKCS#11 API.	None

The Likewise Input-Output Service


The `lwiod` daemon multiplexes input and output by using SMB1 or SMB2. The daemon's plugin-based architecture includes several drivers, the most significant of which is coded as `rdr` -- the redirector.



The redirector multiplexes CIFS/SMB connections to remote systems. For instance, when two different processes on a local Linux computer need to perform input-output operations on a remote system by using CIFS/SMB, with either the same identity or different identities, the preferred method is to use the APIs in the `lwio` client library, which routes the calls through the redirector. In this example, the redirector maintains a single connection to the remote system and multiplexes the traffic from each client by using multiplex IDs.

The input-output service plays a key role in the Likewise architecture because Likewise makes heavy use of DCE/RPC, short for Distributed Computing Environment/Remote Procedure Calls. DCE/RPC, in turn, uses SMB: Thus, the DCE-RPC client libraries use the Likewise input-output client library, which in turn makes calls to `lwiod` with Unix domain sockets.

When you join a domain, for example, Likewise uses DCE-RPC calls to establish the machine password. The Likewise authentication daemon periodically refreshes the machine password by using DCE-RPC calls. Authentication of users and groups in Active Directory takes place with Kerberos, not

RPC. ( View a data-flow diagram that shows how systems interact when you join a domain.)

In addition, when a joined computer starts up, the Likewise authentication daemon enumerates Active Directory trusts by using DCE-RPC calls that go through the redirector. With one-way trusts, the authentication daemon uses RPC to look up domain users, groups, and security identifiers. With two-way trusts, lookup takes place through LDAP, not RPC.

Because the authentication daemon registers trusts only when it starts up, you should restart `lsassd` with the Likewise Service Manager after you modify a trust relationship.

The Likewise group policy agent also uses the input-output client library and the redirector when it copies files from the `sysvol` share of a domain controller.

To troubleshoot remote procedure calls that go through the input-output service and its redirector, use a Wireshark trace or a TCP dump to capture the network traffic. Wireshark, a free open-source packet analyzer, is recommended.

To troubleshoot connection problems with the redirector, set the log level of `lwiod` to debug:

```
/opt/likewise/bin/lwio-set-log-level debug
```

PAM Options

Likewise uses three standard PAM options – `try_first_pass`, `use_first_pass`, and `use_authtok` -- and adds three non-standard options to the PAM configuration on some systems: `unknown_ok`, `remember_chpass`, and `set_default_repository`. The `unknown_ok` option allows local users to continue down the stack (first line succeeds but second line fails) while blocking domain users who do not meet group membership requirements. On AIX systems, which have both PAM and LAM modules, the `remember_chpass` prevents the AIX computer from trying to change the password twice and prompting the user twice. On Solaris systems, the `set_default_repository` option is used to make sure password changes work as expected.

Managing the Likewise Daemons

The Likewise Service Manager lets you track and troubleshoot all the Likewise services with a single command-line utility. You can, for example, check the status of the services, view their dependencies, and start or stop them. The service manager is the preferred method for restarting a service because it automatically identifies a service's dependencies and restarts them in the right order. In addition, you can use the service manager to set the logging destination and the log level.

To list status of the services, run the following command with superuser privileges at the command line:

```
/opt/likewise/bin/lwsm list
```

Example:

```
[root@rhel5d bin]# -/opt/likewise/bin/lwsm list
lwreg      running (standalone: 1920)
dcerpc     running (standalone: 2544)
eventlog   running (standalone: 2589)
lsass      running (standalone: 2202)
lwio       running (standalone: 2191)
netlogon   running (standalone: 2181)
npfs       running (io: 2191)
rdr        running (io: 2191)
```


After you change a setting in the registry, you must use the service manager to force the service to begin using the new configuration by executing the following command with super-user privileges. This example refreshes the `lsass` service:

```
/opt/likewise/bin/lwsm refresh lsass
```

2.3. The Likewise Registry

Configuration information for the daemons is stored in the Likewise registry, which you can access and modify by using the registry shell or by executing registry commands at the command line. The registry shell is at `/opt/likewise/bin/lwregshell`. For more information, see [Configuring the Likewise Services with the Registry](#).

2.4. Ports and Libraries

The agent includes a number of libraries in `/opt/likewise/lib`.

The agent uses the following ports for outbound traffic.



View a data-flow diagram that shows how systems interact when you join a domain.

Port	Protocol	Use
53	UDP/ TCP	DNS
88	UDP/TCP	Kerberos
123	UDP	NTP
135	TCP	RPC endpoint mapper
137	UDP	NetBIOS Name Service
139	TCP	NetBIOS Session (SMB)
389	UDP/TCP	LDAP
445	TCP	SMB over TCP
464	UDP/TCP	Machine password changes (typically after 30 days)
3268	TCP	Global Catalog search

2.5. Caches and Databases

To maintain the current state and to improve performance, the Likewise authentication service (`lsass`) caches information about users and groups in memory. You can, however, change the cache to store the information in a SQLite database; for more information, see the [chapter on configuring Likewise with the registry](#).

The Likewise site affinity service, `netlogon`, caches information about the optimal domain controller and global catalog in the Likewise registry.

The following files are in `/var/lib/likewise/db`:

File	Description
------	-------------

registry.db	The SQLite 3.0 database in which the Likewise registry service, lwreg, stores data.
sam.db	Repository managed by the local authentication provider to store information about local users and groups.
lwi_events.db	The database in which the event logging service, eventlog, records events.
lsass-adcache.db.fqdn	Cache managed by the Active Directory authentication provider to store user and group information. The file is in <code>/var/lib/likewise/db</code> only when you set the database type to be the non-default SQLite database. In the name of the file, FQDN is replaced by your fully qualified domain name.

Since the default UIDs that Likewise generates are large, the entries made by the operating system in the `lastlog` file when AD users log in make the file appear to increase to a large size. This is normal and should not cause concern. The `lastlog` file (typically `/var/log/lastlog`) is a sparse file that uses the UID and GID of the users as disk addresses to store the last login information. Because it is a sparse file, the actual amount of storage used by it is minimal.

With Likewise Open, you can manage the following settings for your cache by editing the Likewise registry. See [Cache Settings](#) in the [lsass Branch](#).

- The Cache Type
- The Size of the Memory Cache
- The Duration of Cached Credentials
- The NSS Membership and NSS Cache Settings
- The Interval for Caching an Unknown Domain

With Likewise Enterprise, you can manage the settings with group policies; see the [Group Policy Administration Guide](#).

Additional information about a computer's Active Directory domain name, machine account, site affinity, domain controllers, forest, the computer's join state, and so forth is stored in the Likewise registry. Here's an example of the kind of information that is stored under the `Pstore` key and the `netlogon` key:

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory
\DomainJoin\LIKEWISEDEMO.COM\Pstore]
"ClientModifyTimestamp"=dword:4b86d9c6
"CreationTimestamp"=dword:4b86d9c6
"DomainDnsName"="LIKEWISEDEMO.COM"
"DomainName"="LIKEWISEDEMO"
"DomainSID"="S-1-5-21-3190566242-1409930201-3490955248"
"HostDnsDomain"="likewisedemo.com"
"HostName"="RHEL5D"
"MachineAccount"="RHEL5D$"
"SchannelType"=dword:00000002

[HKEY_THIS_MACHINE\Services\netlogon\cachedb\likewisedemo.com-0]
```

```
"DcInfo-ClientSiteName"="Default-First-Site-Name"
"DcInfo-DCSiteName"="Default-First-Site-Name"
"DcInfo-DnsForestName"="likewisedemo.com"
"DcInfo-DomainControllerAddress"="192.168.92.20"
"DcInfo-DomainControllerAddressType"=dword:00000017
"DcInfo-DomainControllerName"="w2k3-r2.likewisedemo.com"
"DcInfo-
DomainGUID"=hex:71,c1,9e,b5,18,35,f3,45,ba,15,05,95,fb,5b,62,e3
"DcInfo-Flags"=dword:000003fd
"DcInfo-FullyQualifiedDomainName"="likewisedemo.com"
"DcInfo-LMToken"=dword:0000ffff
"DcInfo-NetBIOSDomainName"="LIKEWISEDEMO"
"DcInfo-NetBIOSHostName"="W2K3-R2"
"DcInfo-NTToken"=dword:0000ffff
"DcInfo-PingTime"=dword:00000006
"DcInfo-UserName"=" "
"DcInfo-Version"=dword:00000005
"DnsDomainName"="likewisedemo.com"
"IsBackoffToWritableDc"=dword:00000000
"LastDiscovered"=hex:c5,d9,86,4b,00,00,00,00
"LastPinged"=hex:1b,fe,86,4b,00,00,00,00
"QueryType"=dword:00000000
"SiteName"=" "
```

2.6. Time Synchronization

For the Likewise agent to communicate over Kerberos with the domain controller, the clock of the client must be within the domain controller's maximum clock skew, which is 300 seconds, or 5 minutes, by default. (For more information, see <http://web.mit.edu/kerberos/krb5-1.4/krb5-1.4.2/doc/krb5-admin/Clock-Skew.html>.)

The clock skew tolerance is a server-side setting. When a client communicates with a domain controller, it is the domain controller's Kerberos key distribution center that determines the maximum clock skew. Since changing the maximum clock skew in a client's `krb5.conf` file does not affect the clock skew tolerance of the domain controller, the change will not allow a client outside the domain controller's tolerance to communicate with it.

The clock skew value that is set in the `/etc/likewise/krb5.conf` file of Linux, Unix, and Mac OS X computers is useful only when the computer is functioning as a server for other clients. In such cases, you can use a Likewise Enterprise group policy to change the maximum tolerance; for more information, see [Set the Maximum Tolerance for Kerberos Clock Skew in the Likewise Group Policy Administration Guide](#).

The domain controller uses the clock skew tolerance to prevent replay attacks by keeping track of every authentication request within the maximum clock skew. Authentication requests outside the maximum clock skew are discarded. When the server receives an authentication request within the clock skew, it checks the replay cache to make sure the request is not a replay attack.

2.7. Using a Network Time Protocol Server

If you set the system time on your computer with a Network Time Protocol (NTP) server, the time value of the NTP server and the time value of the domain controller could exceed the maximum skew. As a result, you will be unable to log on your computer.

If you use an NTP server with a cron job, there will be two processes trying to synchronize the computer's time -- causing a conflict that will change the computer's clock back and forth between the time of the two sources.

Likewise recommends that you configure your domain controller to get its time from the NTP server and configure the domain controller's clients to get their time from the domain controller.

2.8. Automatic Detection of Offline Domain Controller and Global Catalog

The Likewise authentication daemon -- `lsassd` -- manages site affinity for domain controllers and global catalogs and caches the information with `netlogond`. When a computer is joined to Active Directory, `netlogond` determines the optimum domain controller and caches the information. If the primary domain controller goes down, `lsassd` automatically detects the failure and switches to another domain controller and another global catalog within a minute.

However, if another global catalog is unavailable within the forest, the Likewise agent will be unable to find the Unix and Linux information of users and groups. The Likewise agent must have access to the global catalog to function. Therefore, it is recommended that each forest has redundant domain controllers and redundant global catalogs.

2.9. UID-GID Generation in Likewise Open and Likewise Enterprise Cells

In Likewise Open, a UID and GID are generated by hashing the user or group's security identifier, or SID, from Active Directory. With Likewise Open, you do not need to make any changes to Active Directory. A UID and GID stays the same across host machines. With Likewise Open, you cannot set UIDs and GIDs for Linux and Unix in Active Directory; using AD to set and manage UIDs and GIDs is a feature of Likewise Enterprise or the Likewise UID-GID management tool.

If your Active Directory relative identifiers, or RIDs, are a number greater than 524,287, the Likewise Open algorithm that generates UIDs and GIDs can result in UID-GID collisions among users and groups. In such cases, it is recommended that you use Likewise Enterprise or the Likewise UID-GID management tool.

The Likewise Open algorithm is the same in 4.1 and 5.0, and if you are running 4.1 on one computer and 5.0 or later on another, each user and group should have the same UID and GID on both machines.

Note: If you have UIDs and GIDs defined in Active Directory, Likewise Open will not use those UIDs and GIDs.

In Likewise Enterprise, you can specify the UIDs and GIDs that you want, including setting multiple UID and GID values for a given user based on OU membership by using Likewise cells. (Likewise cells, available only in Likewise Enterprise, provide a method for mapping Active Directory users and groups to UIDs and GIDs.) You can also set Likewise Enterprise to automatically generate UID and GID values sequentially.

2.10. Cached Credentials

Both Likewise Open and Likewise Enterprise cache credentials so users can log on when the computer is disconnected from the network or Active Directory is unavailable.

2.11. Trust Support

The Likewise agent supports the following Active Directory trusts:

Trust Type	Transitivity	Direction	Likewise Default Cell Support	Likewise Non-Default Cell Support (Named Cells)
Parent and child	Transitive	Two-way	Yes	Yes
External	Nontransitive	One-way	No	Yes
External	Nontransitive	Two-way	No	Yes
Forest	Transitive	One-way	No	Yes
Forest	Transitive	Two-way	Yes: Must enable default cell in both forests.	Yes

There is information on the types of trusts at [http://technet.microsoft.com/en-us/library/cc775736\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc775736(WS.10).aspx).

Notes on Trusts

The following list contains general information about working with trusts.

- You must place the user or group that you want to give access to the trust in a cell other than the default cell.
- In a two-way forest or parent-child trust, Likewise merges the default cells. When merged, users in one domain can log on computers in another domain, and vice-versa.
- To put a user in a child domain but not the parent domain, you must put the user in a non-default cell, which is a cell associated with an organizational unit.
- If there is a UID conflict across two domains, one domain will be dropped.
- In a cross-forest transitive one- or two-way trust, the root of the trusted forest must have a default cell.
- In a one-way trust in which Forest A trusts Forest B, a computer in Forest A cannot get group information from Forest B, because Forest B does not trust Forest A. The computer in Forest A can obtain group information if the user logs on with a password for a domain user, but not if the user logs on with Kerberos single sign-on credentials. Only the primary group information, not the secondary group information, is obtained.
- To support a 1-way trust without duplicating user accounts, you must use a cell associated with an OU, not a default cell. If Domain A trusts Domain B (but not the reverse) and if Domain B contains all the account information in cells associated with OUs, then when a user from Domain B logs on a machine joined to Domain A, Domain B will authenticate the user and authorize access to the machine in Domain A.

In such a scenario, you should also add a domain user from the trusted domain to an administrative group in the trusting domain so you can manage the trusting domain with the appropriate level of read access to trusted user and group information. However, before you add the domain user from the trusted domain to the trusting domain, you must first add to the trusting domain a group that includes

the user because Unix and Linux computers require membership in at least one group and Active Directory does not enumerate a user's membership in foreign groups.

- If you have a network topology in which the "front" domain trusts the "back" domain, and you join a machine to the front domain using a back domain administrator, as in the following example, the attempt to join the domain will fail: `domainjoin-cli join front.likewise.com back \\administrator password`. However, the attempt to join the domain will succeed if you use the following nomenclature:

```
domainjoin-cli join front.likewise.com
administrator@BACK.likewise.COM password
```

- With Likewise Enterprise, aliased user names are supported in the default cell and in named cells.

Trusts and Cells in Likewise Enterprise

In Likewise Enterprise, a cell contains Unix settings, such as a UID and a GID, for an Active Directory user. When an AD user logs on a Likewise client, Likewise Enterprise searches Active Directory for the user's cell information -- and must find it to operate properly. Thus, your AD topology and your trust relationships may dictate where to locate a cell in Active Directory so that your Likewise clients can access their Unix settings.

With a default cell, Likewise searches for a user or group's attributes in the default cell of the domain where the user or group resides. In a multi-domain topology, a default cell must exist in the domain where user and group objects reside in addition to the default cell that exists in the domain to which Unix, Linux, and Mac computers are joined. In a multi-domain topology, then, be sure to create a default cell in each domain.

Ideally, Unix information is stored on the user object in default cell schema mode. If the client computer does not have the access rights to read and write the information to the user object, as in an external one-way trust, the Unix information cannot be stored on the user object. It can, however, be stored locally in a named cell, that is, a cell associated with an organizational unit.

Since a named cell can be linked to the default cell, you can store Unix information on the user object in default cell schema mode when possible, and otherwise in a named cell that represents the external user. For information about cells, see the chapter on planning your Likewise Enterprise installation and deployment.

2.12. Integrating with Samba

Likewise includes a tool to install the files necessary to use Samba with Likewise. Located in `/opt/likewise/bin`, the tool is named `samba-interop-install`. The Likewise Samba Guide describes how to use the tool to integrate Samba 3.0.25, 3.2.X, or 3.5.X with Likewise Enterprise 6 or Likewise Open 6.

2.13. Supported Platforms

Likewise Open and Likewise Enterprise run on a broad range of Unix, Mac OS X, and Linux platforms. Likewise frequently adds new vendors and distributions to the list of supported platforms.

Chapter 3. Configuring Clients Before Agent Installation

3.1. Configure nsswitch.conf

Before you attempt to join an Active Directory domain, make sure the `/etc/nsswitch.conf` file contains the following line:

```
hosts: files dns
```

The `hosts` line can contain additional information, but it must include the `dns` entry, and it is recommended that the `dns` entry appear after the `files` entry.

Computers running Solaris, in particular, may not contain this line in `nsswitch.conf` until you add it.

When you use Likewise with Multicast DNS 4 (mDNS4) and have a domain in your environment that ends in `.local`, you must place the `dns` entry before the `mdns4_minimal` entry and before the `mdns4` entry:

```
hosts: files dns mdns4_minimal [NOTFOUND=return] mdns4
```

The default setting for many Linux systems is to list the `mdns4` entries before the `dns` entry -- a configuration that leaves Likewise unable to find the domain.

Important: For Likewise to process changes to your `nsswitch.conf` file, you must restart the Likewise input-output service (`lwiod`) and the authentication service (`lsassd`). Running the following command as root restarts both services:

```
/opt/likewise/bin/lwsm restart lwio
```

For Likewise to work correctly, the `nsswitch.conf` file must be readable by user, group, and world.

For more information on configuring `nsswitch`, see the man page for `nsswitch.conf`.

3.2. Configure resolv.conf

Before you attempt to join an Active Directory domain, make sure that `/etc/resolv.conf` on your Linux, Unix, or Mac client includes a DNS server that can resolve SRV records for your domain.

Example:

```
[root@rhel5d Desktop]# cat -/etc/resolv.conf

search likewisedemo.com
nameserver 192.168.100.132
```

For more information on `resolv.conf`, see your operating system's man page.

3.3. Configure Firewall Ports

The Likewise agent requires several firewall ports to be open for outbound traffic. For a list of the required ports, see [Make Sure Outbound Ports Are Open](#).

3.4. Extend Partition Size Before Installing Likewise on IBM AIX

On AIX 5.2 and 5.3, you may need to extend the size of certain partitions to complete the installation successfully.

To do so, use IBM's `chfs` command to change the partition sizes -- for example:

```
# chfs -a size=+200M /opt
```

This command increases the size of the `opt` partition by 200 megabytes, which should be sufficient for a successful installation.

3.5. Increase Max Username Length on IBM AIX

By default, IBM AIX is not configured to support long user and group names, which might present a conflict when you try to log on with a long Active Directory username. On AIX 5.3 and AIX 6.1, the symptom is that group names, when enumerated through the `groups` command, are truncated.

To increase the max username length on AIX 5.3, use the following syntax:

```
# chdev -l sys0 -a max_logname=MaxUserNameLength+1
```

Example:

```
# chdev -l sys0 -a max_logname=255
```

This command allocates 254 characters for the user and 1 for the terminating null.

The safest value that you can set `max_logname` to is 255.

You must reboot for the changes to take effect:

```
# shutdown -Fr
```

Note: AIX 5.2 does not support increasing the maximum user name length.

3.6. Check System Health Before Installing the Agent

Members of the Likewise support staff might use a shell script to check the health of a Linux or Unix computer on which you plan to install the Likewise agent. The script helps identify potential system configuration issues before you install the agent and attempt to join a Linux or Unix computer to Active Directory.

With Likewise Open, the script is unavailable, but you can manually check your computer against the list in the table below.

The name of the script is `healthchk.sh`. To execute it, copy the script to the Unix or Linux computer that you want to check, and then execute the following command from the shell prompt:

```
likewise-health-check.sh
```

The script outputs the results of its scan to `/tmp/healthchk.out`.

Configuring Clients
Before Agent Installation

The following table lists each item the script checks, describes the item, and suggests action to correct the issue.

Item Checked	Description	Corrective Action
Type of operating system	The operating system must be one of the platforms that Likewise supports. Supported platforms are listed later in this guide.	Install the agent on a computer that is running a supported operating system.
Hostname	Informational.	Not applicable.
Processor type	The processor type must be supported by the Likewise Agent. See the list of supported platforms later in this guide.	Install the agent on a computer with a supported processor.
Disk usage	Checks the disk space available to <code>/opt</code> to ensure that there is enough to install the agent and its accompanying packages.	Increase the amount of disk space available to <code>/opt</code> .
Contents of <code>/etc/*release</code> (for AIX, to determine the <code>oslevel</code>)	Displays the operating system and version number to ensure that they are supported by Likewise. See the list of supported platforms later in this guide.	Install the agent on a computer that is running a supported operating system and version.
Network interface and its status	Displays network interfaces and IP addresses to ensure that the system has network access.	Configure the computer so that it has network access and can communicate with the domain controller.
Contents of the IP routing table	To determine whether a single default gateway is defined for the computer.	<p>If the computer does not use a single default gateway, you must define a route to a single default gateway.</p> <p>For example, you can run the <code>route -n</code> to view the IP routing table and set a static route. For more information, see the man pages for your system.</p> <p>On Solaris, you may need to create or edit <code>/etc/defaultrouter</code>.</p> <p>On Linux, you can set the default gateway by running the network utility for your distribution.</p>
Connectivity to the default gateway	Pings the default gateway to ensure that the computer can connect to it. A connection to the default gateway is required.	Configure the computer and the network so that the computer can connect to the default gateway.

Configuring Clients
Before Agent Installation

Contents of <code>nsswitch.conf</code> (or, for AIX, <code>netsvc.conf</code>)	Displays information about the <code>nsswitch</code> configuration.	<p>The <code>nsswitch.conf</code> file must contain the following line:</p> <pre>hosts: files dns</pre> <p>Computers running Solaris, in particular, may not contain this line in <code>nsswitch.conf</code>.</p>
FQDN	Determines the fully qualified domain name of the computer to ensure that it is set properly.	<p>Make sure the computer's FQDN is correct in <code>/etc/hosts</code>.</p> <p>You can determine the fully qualified domain name of a computer running Linux, Unix, or Mac OS X by executing the following command:</p> <pre>ping -c 1 `hostname`</pre> <p>On HP-UX:</p> <pre>ping `hostname` -n 1</pre> <p>On Solaris:</p> <pre>FQDN=`usr/lib/mail/sh/check-hostname cut -d" " -f7`;echo \$FQDN</pre> <p>This command prompts the computer to look up the primary host entry for its hostname. In most cases, it looks for its hostname in <code>/etc/hosts</code>, returning the first FQDN name on the same line. So, for the hostname <code>qaserver</code>, here's an example of a correct entry in <code>/etc/hosts</code>:</p> <pre>10.100.10.10 qaserver.corpqa.likewise.com qaserver</pre> <p>If, however, the entry in <code>/etc/hosts</code> incorrectly lists the hostname (or anything else) before the FQDN, the computer's FQDN becomes, using the malformed example below, <code>qaserver</code>:</p> <pre>10.100.10.10 qaserver qaserver.corpqa.likewise.com</pre>

Configuring Clients
Before Agent Installation

		If the host entry cannot be found in <code>/etc/hosts</code> , the computer looks for the results in DNS instead. This means that the computer must have a correct A record in DNS. If the DNS information is wrong and you cannot correct it, add an entry to <code>/etc/hosts</code> .
IP address of local NIC	Determines whether the IP address of the local network card matches the IP address returned by DNS for the computer. The IP address of the local NIC must match the IP address for the computer in DNS.	Either update DNS or change the local IP address so that the IP address of the local network card matches the IP address returned by DNS for the computer.
Contents of <code>resolv.conf</code>	<p>Returns the address for the <code>nameserver</code> set in <code>resolv.conf</code>.</p> <p>The address of <code>nameserver</code> must point to a DNS server that can resolve the Active Directory domain name and return the SRV records for the domain controllers.</p> <p>The SRV record is a DNS resource record that is used to identify computers that host specific services. SRV resource records are used to locate domain controllers for Active Directory.</p>	Compare against the results of the items checked next.
DNS query results for system (hostname and IP)	The IP address for the host name from DNS must match the IP address of the computer's local NIC.	Either update DNS or change the local IP address so that the IP address of the local network card matches the IP address returned by DNS for the computer.
DNS name resolution and connectivity to specified domain controller	Pings the domain name to get the IP address.	Correct <code>resolv.conf</code> so that the <code>nameserver</code> points to a DNS server that can resolve the Active Directory domain name -- typically the domain controller running DNS.
SRV records from DNS	Performs a DNS lookup for the SRV records to get the IP addresses for the domain controller.	Correct <code>resolv.conf</code> so that the <code>nameserver</code> points to a DNS server that can resolve the SRV records.
Connectivity to the Internet	Informational. Although connectivity to the Internet is optional, it makes it easier to	Not applicable.

Configuring Clients
Before Agent Installation

	download the installer for the agent installer.	
Location and version information for sudo, openssl, bash, rpm, and ssh	Checks whether required utilities are installed and are in expected locations.	Likewise requires the following utilities: ssh and openssl. The other utilities are optional but may be useful.
Selected firewall settings (Kerberos, NetBIOS, and LDAP)	Tests whether the computer can connect to ports on the domain controller to make sure that a firewall will not block the computer's attempt to join the domain.	Reconfigure the firewall to allow the computer to access the domain controller.
Listing of files in <code>/etc/pam.d</code>	Lists other software that requires PAM.	Not applicable. Save this information for Likewise support staff in case they need to troubleshoot the installation.
Contents of selected pam files (pam.conf, common-auth, system-auth)	May reveal installation of other applications that are incompatible with the installer.	Not applicable. Save this information for Likewise support staff in case they need to troubleshoot the installation.
Contents of <code>/etc/krb5.conf</code>	Shows Kerberos 5 configuration.	Not applicable. Save this information for Likewise support staff in case they need to troubleshoot the installation.
DHCP	Checks whether DHCP is in use. When the Likewise Agent joins the computer to the domain, the agent restarts the computer. DHCP can then change the contents of <code>/etc/resolv.conf</code> , <code>/etc/hosts</code> , and other files, causing the computer to fail to join the domain.	Set the computer to a static IP address or configure DHCP so that it does not update such files as <code>/etc/resolv.conf</code> and <code>/etc/hosts</code> .
ISA type	Returns 32-bit or 64-bit information.	Use the installer for your ISA type.
Read-only filesystems	Checks whether <code>/opt</code> is mounted as readonly.	Make sure that <code>/opt</code> is writable.
AIX TL levels	Determines the AIX TL level.	Not all TL levels are supported. For AIX, check with Likewise support to make sure that Likewise is compatible with the TL level you are using.

Chapter 4. Installing the Agent

4.1. Install the Correct Version for Your Operating System

You must install the Likewise agent -- the identity service that authenticates users -- on each Linux, Unix, or Mac OS X computer that you want to connect to Active Directory. To obtain the installer or to view a list of supported platforms, see www.likewise.com. The Likewise Open installation package can be downloaded for free at http://www.likewise.com/products/likewise_open/. If you are using Likewise Enterprise, make sure you install the Likewise Enterprise version of the agent.

Important: Before you install the agent, it is recommended that you upgrade your system with the latest security patches. Patch requirements for Unix systems are listed below.

The procedure for installing the Likewise Open agent or the Likewise Enterprise agent depends on the operating system of your target computer or virtual machine. Each procedure is documented in a separate section of this chapter.

Operating System	Procedure by Title
Linux platforms running kernel release number 2.6 or later are supported by Likewise 6.1 or later.	Install the Agent on Linux or Unix with the Shell Script
Linux platforms running kernel release number 2.4 or later are supported by Likewise 6.0 or earlier.	
Unix: Sun Solaris, HP-UX, IBM AIX	Install the Agent on Unix with the Command Line
VMware ESX 3.0 and 3.5 (hypervisor)	Install the Agent on Linux or Unix with the Shell Script
Mac OS X 10.4 or later, including 10.5 and 10.6	Install the Agent on a Mac Computer

You also have the option of installing the agent in unattended mode; see [Install the Agent on Linux in Unattended or Text Mode](#) and [Install the Agent on a Mac in Unattended Mode](#).

Checking Your Linux Kernel Release Number

To determine the release number of the kernel on your Linux machine, run the following command:

```
uname -r
```

For the Linux machine to be supported by Likewise, the kernel release number must be 2.6 or later.

Package Management Commands

For an overview of commands such as `rpm` and `dpkg` that can help you manage Likewise on Linux and Unix platforms, see [Package Management Commands](#).

4.2. Requirements for the Agent

This section lists requirements for installing and running the Likewise agent. Requirements for the Likewise Management Console, which is part of Likewise Enterprise, are detailed in the chapter on installing the console. Likewise Open does not include the Likewise Management Console.

Before you install the Likewise agent, make sure that the following environmental variables are not set: `LD_LIBRARY_PATH`, `LIBPATH`, `SHLIB_PATH`, `LD_PRELOAD`. Setting any of these environmental variables violates best practices for managing Unix and Linux computers because it causes Likewise to use non-Likewise libraries for its services. For more information on best practices, see <http://linuxmafia.com/faq/Admin/ld-lib-path.html>. Likewise does not support installations that use these environmental variables. If joining the domain fails with an error message that one of these environmental variables is set, stop all the Likewise daemons, clear the environmental variable, make sure it is not automatically set when the computer restarts, and then try to join the domain again.

If you must set `LD_LIBRARY_PATH`, `LIBPATH`, or `SHLIB_PATH` for another program, put the Likewise library path (`/opt/likewise/lib` or `/opt/likewise/lib64`) before any other path -- but keep in mind that doing so may result in side effects for your other programs, as they will now use Likewise libraries for their services.

Patch Requirements

It is recommended that you apply the latest patches for your operating system before you install Likewise. Known patch requirements are listed below.

Sun Solaris

All Solaris versions require the `md5sum` utility, which can be found on the companion CD.

Sun Solaris 10 requires update 5 or later. The Solaris 10 05/08 (or later) patch bundle is available at <http://sunsolve.sun.com/>. Solaris 10_x86 requires the patch for `nscd`, either patch ID number 138047-02 or the patch that supersedes it, number 138264-02. This patch available for SPARC as patch 138046.

Solaris 8 Sparc should be fully patched according to Sun's recommendations. Likewise depends on the latest patch for `libuuid`. On Sparc systems, the patch for `libuuid` is 115831. Sun patch 110934-28 for Solaris 5.8 is also required for Solaris 8.

Solaris 8 Intel systems also require the latest patch for `libuuid`: 115832-01. Sun patches 110403-06 and 110935-26 are also required. Patch 110403-06 must be installed before you install patch 110935-26.

Solaris 9 requires Sun patch 113713-28 for Solaris 5.9.

OpenSolaris is compatible with Likewise without any patches.

HP-UX

Secure Shell: For all HP-UX platforms, it is recommended that a recent version of HP's Secure Shell be installed. Likewise recommends that you use HP-UX Secure Shell A.05.00.014 or later.

Sudo: By default, the versions of `sudo` available from the HP-UX Porting Center do not include the Pluggable Authentication Module, or PAM, which Likewise requires to allow domain users to execute `sudo` commands with super-user credentials. It is recommended that you download `sudo` from the HP-UX Porting Center and make sure that you use the `with-pam` configuration option when you build it.

HP-UX 11iv1 requires the following patches: PHCO_36229, PHSS_35381, PHKL_34805, PHCO_31923, PHCO_31903, and PHKL_29243. Although these patches may be superseded by subsequent patches, these patches represent the minimum patch level for proper operation.

Kerberos client libraries: For single sign-on with HP-UX 11.11 and 11.23, you must download and install the latest KRB5-Client libraries from the HP Software Depot. (By default, HP-UX 11.31 includes the libraries.)

Other Requirements for the Agent

AIX

On AIX computers, PAM must be enabled. LAM is supported only on AIX 5.x. PAM must be used exclusively on AIX 6.x.

Secure Shell

To properly process logon events with Likewise, your SSH server or client must support the `UsePam yes` option. For single sign-on, both the SSH server and the SSH client must support GSSAPI authentication.

Other Software

Telnet, rsh, rcp, rlogin, and other programs that uses PAM for processing authentication requests are compatible with Likewise.

Networking Requirements

Each Unix, Linux, or Mac computer must have fully routed network connectivity to all the domain controllers that service the computer's Active Directory site. Each computer must be able to resolve A, PTR, and SRV records for the Active Directory domain, including at least the following:

- A `domain.tld`
- SRV `_kerberos._tcp.domain.tld`
- SRV `_ldap._tcp.domain.tld`
- SRV `_kerberos._udp.siteName.Sites._msdcs.domain.tld`
- A `domaincontroller.domain.tld`

In addition, several ports must be open; see [Make Sure Outbound Ports Are Open](#).

Disk Space Requirements

The Likewise agent requires 100 MB of disk space in the `/opt` mount point. The agent also creates configuration files in `/etc/likewise` and offline logon information in `/var/lib/likewise`. In addition, the Likewise Enterprise agent caches group policy objects in `/var/cache/likewise`.

Memory and CPU Requirements

The agent consists of several daemons that typically use between 9 MB and 14 MB of RAM. Memory utilization of the authentication daemon on a 300-user mail server is typically 7 MB; the other daemons require between 500 KB and 2 MB each. CPU utilization on a 2.0 gigahertz single-core processor under heavy load with authentication requests is about 2 percent. For a description of the Likewise daemons, see [About the Likewise Agent](#).

Clock Skew Requirements

For the Likewise agent to communicate over Kerberos with the domain controller's Kerberos key distribution center, the clock of the client must be within the domain controller's maximum clock skew,

which is 300 seconds, or 5 minutes, by default. For more information on time synchronization, see [About the Likewise Agent](#).

4.3. Install the Agent on Linux or Unix with the Shell Script

You install the Likewise Enterprise agent by using a shell script that contains a self-extracting executable. The file name of the SFX installer ends in `sh`. Example: `LikewiseEnterprise-6.1.0.3499-linux-i386-rpm.sh`.

The examples shown are for Linux RPM-based platforms. For other Linux and Unix platforms -- such as Debian, HP-UX, AIX, and Solaris -- simply substitute the right installer. The installer's name includes the product name, version and build numbers, operating system, computer type, and platform type.

Install the Agent on Linux or Unix with the Shell Script

Perform the following procedure with the **root** account. To view information about the installer or to view a list of command-line options, run the following command: `./LikewiseEnterprise-6.1.0.3499-linux-i386-rpm.sh --help`

After the wizard finishes, the user interface for joining a domain appears. To suppress it, you can run the installer with its `--dont-join` argument.

1. Download or copy the shell script to your Linux or Unix computer's desktop.

Important: If you FTP the file to the desktop of the target Linux or Unix computer, you must select binary, or BIN, for the transfer. Most FTP clients default to AUTO or ASCII, but the installer includes some binary code that becomes corrupted in AUTO or ASCII mode.

2. Change directories to the desktop.
3. As root, change the mode of the installer to executable.

```
chmod a+x LikewiseEnterprise-6.1.0.3499-linux-i386-rpm.sh
```

On Ubuntu, execute the `sudo` command before you execute the `chmod` command:

```
sudo chmod a+x LikewiseEnterprise-6.1.0.3499-linux-i386-rpm.sh
```

4. As root, run the installer:

```
./LikewiseEnterprise-6.1.0.3499-linux-i386-rpm.sh
```

5. Follow the instructions in the installer.

Note: On SLES and other systems on which the pager is set to less, you must exit the end user license agreement, or EULA, by typing the following command: `q`

4.4. Install the Agent on Linux in Unattended Mode

You can install the agent in unattended mode by using the `install` command:


```
./LikewiseEnterprise-6.1.0.67-linux-i386-rpm.sh install
```

4.5. Install the Agent on Unix with the Command Line

You install the Likewise Open agent or the Likewise Enterprise agent on Sun Solaris, HP-UX, and IBM AIX by using a shell script that contains a self-extracting executable -- an SFX installer with a file name that ends in `.sh`. Example: `LikewiseEnterprise-6.1.0.70-solaris-sparc-pkg.sh`.

The examples shown below are for Solaris Sparc systems. For other Unix platforms, simply substitute the right installer. The installer's name includes the product name, version and build numbers, operating system, computer type, and platform type.

Note: The name of a Unix installer for Likewise Enterprise on installation media might be truncated to an eight-character file name with an extension. For example, `l3499sus.sh` is the truncated version of `LikewiseEnterprise-6.1.0.3499-solaris-sparc-pkg.sh`.

Perform the following procedure with the root account.

1. Download or copy the installer to the Unix computer's desktop.
2. Change directories to the desktop.
3. As root, change the mode of the installer to executable:

```
chmod a+x LikewiseEnterprise-6.1.0.70-solaris-sparc-pkg.sh
```

Tip: To view a list of command-line options, run the following command:

```
./LikewiseEnterprise-6.1.0.70-solaris-sparc-pkg.sh --help
```

4. As root, run the installer:

```
./LikewiseEnterprise-6.1.0.70-solaris-sparc-pkg.sh
```

5. Follow the instructions in the installer.

4.6. Install the Agent on a Mac Computer

To install the Likewise agent on a computer running Mac OS X, you must have administrative privileges on the Mac. Likewise supports Mac OS X 10.4 or later.

1. Obtain the Likewise agent installation package for your Mac from Likewise Software and place it on your desktop.

Important: On an Intel-based Mac, install the **i386** version of the `.dmg` package. On a Mac that does not have an Intel chip, install the **powerpc** version of the `.dmg` package. On Mac OS X 10.6 (Snow Leopard), you must use the 10.6 universal installation package.

2. Log on the Mac with a local account.

3. On the **Apple** menu , click **System Preferences**.

4. Under **Internet & Network**, click **Sharing**, and then select the **Remote Login** check box. Turning on Remote Login lets you access the Mac with SSH after you install Likewise.
5. On the Mac computer, go to the Desktop and double-click the Likewise .dmg file.
6. In the Finder window that appears, double-click the Likewise .mpkg file.
7. Follow the instructions in the installation wizard.

When the wizard finishes installing the package, you are ready to join the Mac computer to an Active Directory domain.

4.7. Install the Agent on a Mac in Unattended Mode

The Likewise command-line tools can remotely deploy the shell version of the Likewise agent to multiple Mac OS X computers, and you can automate the installation of the agent by using the installation command in unattended mode.

The commands in this procedure require administrative privileges.

Important: For Intel-based Macs, use the **i386** version of the .dmg installer; for example: `LikewiseEnterprise-6.1.0.3628-i386.dmg`. For Macs that do not have Intel chips, use the **powerpc** version of the .dmg installer; for example: `LikewiseEnterprise-6.1.0.3628-powerpc.dmg`

The procedure below assumes you are installing the agent on an i386 Mac; if you are installing on a powerpc, replace the i386 installer with the powerpc installer.

1. Use SSH to connect to the target Mac OS X computer and then use SCP to copy the .dmg installation file to the desktop of the Mac or to a location that can be accessed remotely. The rest of this procedure assumes that you copied the installation file to the desktop.
2. On the target Mac, open Terminal and then use the `hdiutil mount` command to mount the .dmg file under Volumes:

```
/usr/bin/hdiutil mount Desktop/LikewiseEnterprise-6.1.0.3628-i386.dmg
```

3. Execute the following command to open the .mpkg volume:

```
/usr/bin/open Volumes/LikewiseEnterprise-6.1.0.3628-i386
```

4. Execute the following command to install the agent:

```
sudo installer -pkg /Volumes/LikewiseEnterprise-6.1.0.3628-i386/LikewiseEnterprise-6.1.0.3628-i386.mpkg -target LocalSystem
```

Note: For more information about the installer command, in Terminal execute the following command:

```
man installer
```

5. To join the domain, execute the following command in the Terminal, replacing `domainName` with the FQDN of the domain that you want to join and `joinAccount` with the user name of an account that has privileges to join computers to the domain:

```
sudo /opt/likewise/bin/domainjoin-cli join domainName joinAccount
```

Example: `sudo /opt/likewise/bin/domainjoin-cli join likewisedemo.com Administrator`

Terminal prompts you for two passwords: The first is for a user account on the Mac that has admin privileges; the second is for the user account in Active Directory that you specified in the join command.

Note: You can also add the password for joining the domain to the command, but Likewise recommends against this approach because another user could view and intercept the full command that you are running, including the password:

```
sudo /opt/likewise/bin/domainjoin-cli join domainName joinAccount joinPassword
```

Example: `sudo /opt/likewise/bin/domainjoin-cli join likewisedemo.com Administrator YourPasswordHere`

4.8. Installing the Agent in Solaris Zones

Solaris Zones are a virtualization technology created by Sun Microsystems to consolidate servers. Primarily used to isolate an application, Solaris Zones act as isolated virtual servers running on a single operating system, making each application in a collection of applications seem as though it is running on its own server. A Solaris Container combines system resource controls with the virtual isolation provided by zones.

Every zone server contains a global zone that retains visibility and control in any installed non-global zones. By default, the non-global zones share certain directories, including `/usr`, which are mounted read-only. The shared directories are writable only for the global zone.

By default, installing Likewise in the global zone results in it being installed in all the non-global zones. You can, however, control the target of the installation by using the following options of the SFX installer:

```
./LikewiseEnterprise-6.1.0.97-solaris-i386-pkg.sh --help
...
--all-zones           (Solaris) Install to all zones (default)
--current-zone        (Solaris) Install only to current zone
```

After a new child zone is installed, booted, and configured, you must run the following command as root to complete the installation:

`/opt/likewise/bin/postinstall.sh`

You cannot join zones to Active Directory as a group. Each zone, including the global zone, must be joined to the domain independently of the other zones.

Caveats

There are some caveats when using Likewise with Solaris Zones:

1. When you join a non-global zone to AD, you will receive an error as Likewise attempts to synchronize the Solaris clock with AD. The error occurs because the root user of the non-global zone

does not have root access to the underlying global system and thus cannot set the system clock. If the clocks are within the 5-minute clock skew permitted by Kerberos, the error will not be an issue. Otherwise, you can resolve the issue by manually setting the clock in the global zone to match AD or by joining the global zone to AD before joining the non-global zone.

2. Some group policies may log PAM errors in the non-global zones even though they function as expected. The cron group policy is one example:

```
Wed Nov 7 16:26:02 PST 2009 Running Cronjob 1 (sh)
Nov 7 16:26:01 zone01 last message repeated 1 time
Nov 7 16:27:00 zone01 cron[19781]: pam_lsass(cron): request failed
```

Depending on the group policy, these errors may result from file access permissions, attempts to write to read-only directories, or both.

3. By default, Solaris displays `auth.notice` syslog messages on the system console. Some versions of Likewise generate significant authentication traffic on this facility-priority level, which may lead to an undesirable amount of chatter on the console or clutter on the screen.

To redirect the traffic to a file instead of displaying it on the console, edit your `/etc/syslog.conf` file as follows:

Change this:

```
*.err;kern.notice;auth.notice /dev/sysmsg
```

To this:

```
*.err;kern.notice /dev/sysmsg
```

```
auth.notice /var/adm/authlog
```

Important: Make sure that you use **tabs**, not spaces, to separate the facility.priority information (on the left) from the action field (on the right). Using spaces will cue syslog to ignore the entire line.

4.9. Upgrading Your Operating System

Before you upgrade your operating system, you must leave the domain, uninstall the domain join GUI, and uninstall the agent. Then, make sure you are using the correct agent for the new version of your operating system, install it, and rejoin the domain.

If, for example, you plan to upgrade your operating system from Mac OS X 10.5 (Leopard) to Mac OS X 10.6 (Snow Leopard), you must first leave the domain and uninstall the current agent. Then, after upgrading your operating system, install the correct agent for the new version of the operating system and join the domain again. See [Uninstall the Agent on a Mac](#).

Chapter 5. Joining an Active Directory Domain

5.1. About Joining a Domain

When Likewise joins a computer to an Active Directory domain, it uses the hostname of the computer to create the name of the computer object in Active Directory. From the hostname, the Likewise domain join tool attempts to derive a fully qualified domain name. By default, the Likewise domain join tool creates the Linux and Unix machine accounts in the default Computers container in Active Directory.

You can, however, choose to pre-create machine accounts in Active Directory before you join your computers to the domain. When you join a computer to a domain, Likewise associates the computer with the pre-existing machine account when Likewise can find it. To locate the machine account, Likewise first looks for a machine account with a DNS hostname that matches the hostname of the computer. If the DNS hostname is not set, Likewise then looks for the name of a machine account that matches the computer's hostname, but only when the computer's hostname is 15 characters or less. Therefore, when the hostname of your computer is more than 15 characters, you should set the DNS hostname for the machine account to ensure that the correct machine account is found. If no match is found, Likewise creates a machine account.

The location of the domain join command-line utility is as follows:

/opt/likewise/bin/domainjoin-cli

After you join a domain for the first time, you must restart the computer before you can log on. If you cannot restart the computer, you must restart each service or daemon that looks up users or groups through the standard nsswitch interface, which includes most services that authenticate users, groups, or computers. You must, for instance, restart the services that use Kerberos, such as `sshd`.

For Linux computers, there is an optional graphical version of the Likewise domain join tool. It is installed on Linux platforms that are running GTK+ version 2.6 or later. For more information, see *Join a Linux Computer to Active Directory with the GUI*.

Important: On Linux computers running NetworkManager -- which is often used for wireless connections -- you must make sure before you join a domain that the computer has a non-wireless network connection and that the non-wireless connection is configured to start when the networking cable is plugged in. You must continue to use the non-wireless network connection during the post-join process of restarting your computer and logging on for the first time with your Active Directory domain credentials. For more information, see *With NetworkManager, Use a Wired Connection to Join a Domain*.

Privileges and Permissions

To join a computer to a domain, you must have the user name and password of an Active Directory account that has privileges to join computers to the domain and the full name of the domain that you want to join. Instructions on how to delegate rights to join a computer to a domain are at <http://support.microsoft.com/kb/932455>. The level of privileges that you need is set by Microsoft Active Directory and is typically the same as performing the corresponding action on a Windows computer. For more information on Active Directory privileges, permissions, and security groups, see the following references on the Microsoft Technet web site: Active Directory Privileges, Active Directory Object Permissions, Active Directory Users, Computers, and Groups, Securing Active Directory Administrative Groups and Accounts.

Removing a Computer from a Domain

You can remove a computer from the domain either by removing the computer's account from Active Directory Users and Computers or by running the domain join tool on the Unix, Linux, or Mac OS X computer that you want to remove; see [Leave a Domain](#).

Creation of Local Accounts

After you join a domain, Likewise creates two local user accounts in the following form: machine-name\Administrator and machine-name\Guest. The administrator account is disabled until you enable it by running the `lw-mod-user` command with the root account. You will be prompted to reset the password the first time you use the account.

You can view information about these accounts by executing the following command:

```
/opt/likewise/bin/lw-enum-users
```

Example output:

```
User info (Level-2):
=====
Name:                NISHI-01\Administrator
UPN:                 Administrator@NISHI-01
Generated UPN:       YES
Uid:                 1500
Gid:                 1544
Gecos:               <null>
Shell:               -/bin/sh
Home dir:            -/
LMHash length:       0
NTHash length:       0
Local User:          YES
Account disabled:    TRUE
Account Expired:     FALSE
Account Locked:      FALSE
Password never expires: FALSE
Password Expired:    TRUE
Prompt for password change: YES
User can change password: NO
Days till password expires: --149314
```

```
User info (Level-2):
=====
Name:                NISHI-01\Guest
UPN:                 Guest@NISHI-01
Generated UPN:       YES
Uid:                 1501
Gid:                 1546
Gecos:               <null>
Shell:               -/bin/sh
Home dir:            -/tmp
LMHash length:       0
NTHash length:       0
```

```
Local User: YES
Account disabled: TRUE
Account Expired: FALSE
Account Locked: TRUE
Password never expires: FALSE
Password Expired: FALSE
Prompt for password change: YES
User can change password: NO
Days till password expires: --149314
```

5.2. Join Active Directory with the Command Line

On Linux, Unix, and Mac OS X computers, the location of the domain join command-line utility is as follows:

```
/opt/likewise/bin/domainjoin-cli
```

Important: To run the command-line utility, you must use a **root** account. To join a computer to a domain, you must have the user name and password of an Active Directory account that has privileges to join computers to the domain and the full name of the domain that you want to join. Instructions on how to delegate rights to join a computer to a domain are at <http://support.microsoft.com/kb/932455>. After you join a domain for the first time, you must restart the computer before you can log on with your domain account.

When you join a domain by using the command-line utility, Likewise uses the hostname of the computer to derive a fully qualified domain name (FQDN) and then automatically sets the FQDN in the `/etc/hosts` file. You can also join a domain without changing the `/etc/hosts` file; see Join Active Directory Without Changing `/etc/hosts`.

Before Joining a Domain

To join a domain, the computer's name server must be able to find the domain and the computer must be able to reach the domain controller. You can make sure the name server can find the domain by running this command:

```
nslookup domainName
```

You can verify that your computer can reach the domain controller by pinging it:

```
ping domainName
```

If either of these tests fails, see Check System Health Before Installing the Agent and Solve Domain-Join Problems.

Join a Linux or Unix Computer to Active Directory

Execute the following command as root, replacing `domainName` with the FQDN of the domain that you want to join and `joinAccount` with the user name of an account that has privileges to join computers to the domain:

```
/opt/likewise/bin/domainjoin-cli join domainName joinAccount
```

Example: `/opt/likewise/bin/domainjoin-cli join likewisedemo.com Administrator`

Tip: On Ubuntu, execute the `sudo su -` command before you run the `domainjoin-cli` command.

Join a Mac Computer to Active Directory

Using `sudo`, execute the following command in Terminal, replacing `domainName` with the FQDN of the domain that you want to join and `joinAccount` with the user name of an account that has privileges to join computers to the domain:

`sudo /opt/likewise/bin/domainjoin-cli join domainName joinAccount`

Example: `sudo /opt/likewise/bin/domainjoin-cli join likewisedemo.com Administrator`

The terminal prompts you for two passwords: The first is for a user account on the Mac that has administrative privileges; the second is for the account in Active Directory that you specified in the join command.

Join a Linux or Unix Computer to an Organizational Unit

Execute the following command as root, replacing `organizationalUnitName` with the path and name of the organizational unit that you want to join, `domainName` with the FQDN of the domain, and `joinAccount` with the user name of an account that has privileges to join computers to the domain:

`/opt/likewise/bin/domainjoin-cli join ---ou organizationalUnitName domainName joinAccount`

Example: `/opt/likewise/bin/domainjoin-cli join --ou Engineering likewisedemo.com Administrator`

Join a Linux or Unix Computer to a Nested Organizational Unit

Execute the following command as root, replacing `path` with the AD path to the OU from the top down, with each node separated by a forward slash (/). In addition, replace `organizationalUnitName` with the name of the organizational unit that you want to join. Replace `domainName` with the FQDN of the domain and `joinAccount` with the user name of an AD account that has privileges to join computers to the target OU:

`/opt/likewise/bin/domainjoin-cli join --ou path/organizationalUnitName domainName joinAccount`

Here's an example of how to join a deeply nested OU:

`domainjoin-cli join --ou topLevelOU/middleLevelOU/LowerLevelOU/TargetOU likewisedemo.com Administrator`

5.3. Domainjoin-cli Options, Commands, and Arguments

The `domainjoin-cli` command-line interface includes the following options:

Option	Description	Example
<code>--help</code>	Displays the command-line options and commands.	<code>domainjoin-cli --help</code>
<code>--help-internal</code>	Displays a list of the internal debugging and configuration commands.	<code>domainjoin-cli --help-internal</code>
<code>--logfile {. path}</code>	Generates a log file or prints the log to the console.	<pre>domainjoin-cli --logfile /var/log/domainjoin.log join likewisedemo.com Administrator</pre> <pre>domainjoin-cli --logfile . join likewisedemo.com Administrator</pre>

Basic Commands

The domain join command-line interface includes the following basic commands:

Command	Description	Example
<code>query</code>	Displays the hostname, current domain, and distinguished name, which includes the OU to which the computer belongs. If the computer is not joined to a domain, it displays only the hostname.	<code>domainjoin-cli query</code>
<code>setname computerName</code>	Renames the computer and modifies the <code>/etc/hosts</code> file with the name that you specify.	<code>domainjoin-cli setname RHEL44ID</code>
<code>fixfqdn</code>	Fixes a computer's fully qualified domain name.	<code>domainjoin-cli fixfqdn</code>
<code>join [--ou organizationalUnit] domainName userName</code>	Joins the computer to the domain that you specify by using the account that you specify. You can use the <code>--ou</code> option to join the computer to an OU within the domain by specifying the path to the OU and the OU's name. When you use this option, you must use an account that has membership in the Domain Administrators security group. The path to the OU is top down.	<code>domainjoin-cli join --ou Engineering likewisedemo.com Administrator</code>
<code>join -- notimesync</code>	Joins the computer to the domain without synchronizing the computer's time with the domain	<code>domainjoin-cli join -- notimesync</code>

	controller's. When you use this option, the <code>sync-system-time</code> value for <code>lsassd</code> is set to <code>no</code> .	<code>likewisedemo.com Administrator</code>
<code>leave [userName]</code>	Removes the computer from the Active Directory domain. If the <code>userName</code> is provided, the computer account is disabled in Active Directory.	<code>domainjoin-cli leave</code> <code>domainjoin-cli leave smithy@likewisedemo.com</code>

Advanced Commands

The command-line interface includes advanced commands that you can use to preview the stages of joining or leaving a domain, find out which configurations are required for your system, view information about a module that will be changed, configure a module such as `nsswitch`, and enable or disable a module. The advanced commands provide a potent tool for troubleshooting issues while configuring a Linux or Unix computer to interoperate with Active Directory.



View a data-flow diagram that shows how systems interact when you join a domain.

Preview the Stages of the Domain Join for Your Computer

To preview the domain, DNS name, and configuration stages that will be used to join a computer to a domain, execute the following command at the command line:

```
domainjoin-cli join --preview domainName
```

Example: `domainjoin-cli join --preview likewisedemo.com`

Here's an example of the results, which can vary by computer:

```
[root@rhel4d bin]# domainjoin-cli join ---preview likewisedemo.com
Joining to AD Domain:    likewisedemo.com
With Computer DNS Name: rhel4d.likewisedemo.com
```

The following stages are currently configured to be run during the domain join:

```
join          -- join computer to AD
krb5          -- configure krb5.conf
nsswitch      -- enable/disable Likewise nsswitch module
start         -- start daemons
pam           -- configure pam.d/pam.conf
ssh           -- configure ssh and sshd
```

Check Required Configurations

To see a full listing of the modules that apply to your operating system, including those modules that will not be run, execute either the following join or leave command:

```
domainjoin-cli join --advanced --preview domainName
```

```
domainjoin-cli leave --advanced --preview domainName
```

Example: `domainjoin-cli join --advanced --preview likewisedemo.com`

The result varies by computer:

```
[root@rhel4d bin]# domainjoin-cli join ---advanced ---preview
likewisedemo.com
Joining to AD Domain:    likewisedemo.com
With Computer DNS Name: rhel4d.likewisedemo.com
    [F] stop                -- stop daemons
    [F] hostname            -- set computer hostname
    [F] firewall            -- open ports to DC
    [F] keytab              -- initialize kerberos keytab
[X] [N] join               -- join computer to AD
[X] [N] krb5               -- configure krb5.conf
[X] [N] nsswitch           -- enable/disable Likewise nsswitch module
[X] [N] start              -- start daemons
    [F] gdm                 -- fix gdm presession script for spaces in
usernames
[X] [N] pam                -- configure pam.d/pam.conf
[X] [S] ssh                -- configure ssh and sshd
```

```
Key to flags
[F]ully configured          -- the system is already configured for
this step
[S]ufficiently configured  -- the system meets the minimum
configuration
                             requirements for this step
[N]ecessary                -- this step must be run or manually
performed.
[X]                         -- this step is enabled and will make
changes
[ -]                       -- this step is disabled and will not
make changes
```

View Details about a Module

The Likewise domain join tool includes the following modules -- the components and services that the tool must configure before it can join a computer to a domain:

Module	Description
join	Joins the computer to Active Directory
leave	Deletes the machine account in Active Directory
dsplugin	Enables the Likewise directory services plugin on a Mac computer
stop	Stops daemons so that the system can be configured
start	Starts daemons after configuration
firewall	Opens ports to the domain controller
hostname	sets the computer hostname

krb5	Configures krb5.conf
pam-mode	Switches authentication from LAM to PAM
nsswitch	Enables or disables Likewise nsswitch module
pam	Configures pam.d and pam.conf
lam-auth	Configures LAM for Active Directory authentication
ssh	Configures ssh and sshd
bash	Fixes the bash prompt for backslashes in usernames
gdm	Fixes gdm presession script for spaces in usernames

As the previous section illustrated, you can see the modules that must be configured on your computer by executing the following command:

```
domainjoin-cli join --advanced --preview domainName
```

You can further bore down into the details of the changes that a module will make by using either the following join or leave command:

```
domainjoin-cli join --details module domainName joinAccount
```

```
domainjoin-cli leave --details module domainName joinAccount
```

Example: domainjoin-cli join --details nsswitch likewisedemo.com Administrator

The result varies depending on your system's configuration:

```
domainjoin-cli join ---details nsswitch likewisedemo.com Administrator
[X] [N] nsswitch          -- enable/disable Likewise nsswitch module
```

Key to flags

```
[F]ully configured          -- the system is already configured for
this step
```

```
[S]ufficiently configured -- the system meets the minimum
configuration
```

```
                                requirements for this step
```

```
[N]ecessary                -- this step must be run or manually
performed.
```

```
[X]                        -- this step is enabled and will make
changes
```

```
[ -]                        -- this step is disabled and will not
make changes
```

Details for '-enable/disable Likewise nsswitch module':

The following steps are required and can be performed automatically:

- * Edit nsswitch apparmor profile to allow libraries in the /opt/likewise/lib

- and /opt/likewise/lib64 directories

- * List lwhidentity module in /usr/lib/security/methods.cfg (AIX only)

```
* Add luidentity to passwd and group/groups line -/etc/  
nsswitch.conf or  
-/etc/netsvc.conf
```

If any changes are performed, then the following services must be restarted:

- * GDM
- * XDM
- * Cron
- * Dbus
- * Nscd

Turn On or Turn Off Domain Join Modules

You can explicitly enable or disable a module when you join or leave a domain. Disabling a module can be useful in cases where a module has been manually configured or in cases where you must ensure that certain system files will not be modified.

Note: If you disable a necessary module and you have not manually configured it, the domain join utility will not join your computer to the domain.

The following command, with either join or leave, can be used to disable a module:

```
domainjoin-cli join ---disable module domainName accountName  
domainjoin-cli leave ---disable module domainName accountName
```

Example: domainjoin-cli join --disable pam likewisedemo.com
Administrator

To enable a module, execute the following command at the command line:

```
domainjoin-cli join ---enable module domainName accountName
```

Example: domainjoin-cli join --enable pam likewisedemo.com Administrator

Configuration and Debugging Commands

The domainjoin-cli tool includes commands for debugging the domain-join process and for configuring or preconfiguring a module. You can, for example, run the configure command to preconfigure a system before you join a domain -- a useful strategy when you are deploying Likewise in a virtual environment and you need to preconfigure the nsswitch, ssh, or PAM module of the target computers to avoid having to restart them after they are added to the domain. Here's an example with nsswitch:

domainjoin-cli configure --enable nsswitch

The following commands, viewable by running domainjoin-cli --help-internal, are available:

```
fixfqdn  
configure { ---enable -| ---disable -} pam [--testprefix <dir>]  
configure { ---enable -| ---disable -} nsswitch [--testprefix  
<dir>]  
configure { ---enable -| ---disable -} ssh [--testprefix <dir>]
```

```
configure { ---enable -| ---disable -} [--testprefix <dir>]
           [--long <longdomain>] [--short <shortdomain>] krb5
configure { ---enable -| ---disable -} firewall [--testprefix
<dir>]
configure { ---enable -| ---disable -} eventfwdd
configure { ---enable -| ---disable -} reapsysld
get_os_type
get_arch
get_distro
get_distro_version
raise_error <error code -| error name -| 0xhex error code>
```

5.4. Join Active Directory Without Changing /etc/hosts

When you join a computer to a domain by using the Likewise domain join tool, Likewise uses the hostname of the computer to derive a fully qualified domain name (FQDN) and automatically sets the computer's FQDN in the `/etc/hosts` file.

To join a Linux computer to the domain without changing the `/etc/hosts` file, execute the following command as **root**, replacing `domainName` with the FQDN of the domain that you want to join and `joinAccount` with the user name of an account that has privileges to join computers to the domain:

```
/opt/likewise/bin/domainjoin-cli join --disable hostname domainName  
joinAccount
```

Example: `/opt/likewise/bin/domainjoin-cli join --disable hostname
likewisedemo.com Administrator`

After you join a domain for the first time, you must restart the computer before you can log on.

If the Computer Fails to Join the Domain

Make sure the computer's FQDN is correct in `/etc/hosts`. For the computer to process tickets in compliance with the Kerberos protocol and to function properly when it uses cached credentials in offline mode or when its DNS server is offline, there must be a correct FQDN in `/etc/hosts`. For more information on GSS-API requirements, see RFC 2743.

You can determine the fully qualified domain name of a computer running Linux, Unix, or Mac OS X by executing the following command:

```
ping -c 1 `hostname`
```

When you execute this command, the computer looks up the primary host entry for its hostname. In most cases, this means that it looks for its hostname in `/etc/hosts`, returning the first FQDN name on the same line. So, for the hostname `qaserver`, here's an example of a correct entry in `/etc/hosts`:

```
10.100.10.10 qaserver.corpqa.likewise.com qaserver
```

If, however, the entry in `/etc/hosts` incorrectly lists the hostname (or anything else) before the FQDN, the computer's FQDN becomes, using the malformed example below, `qaserver`:

```
10.100.10.10 qaserver qaserver.corpqa.likewise.com
```

If the host entry cannot be found in `/etc/hosts`, the computer looks for the results in DNS instead. This means that the computer must have a correct A record in DNS. If the DNS information is wrong and you cannot correct it, add an entry to `/etc/hosts`.

5.5. Join a Linux Computer to Active Directory with the GUI

A graphical user interface for joining a domain is included when you install the Likewise agent.

Important: To join a computer to a domain, you must have the user name and password of a user who has privileges to join computers to a domain and the full name of the domain that you want to join.

1. With **root** privileges, run the following command at the shell prompt of a Linux computer:

```
/opt/likewise/bin/domainjoin-gui
```

2. Still as root, in the **Domain** box, enter the Fully Qualified Domain Name (FQDN) of your Active Directory domain. Example: `CORP.LIKEWISEDEMO.COM`



Note: The domain join tool automatically sets the computer's FQDN by modifying the `/etc/hosts` file. For example, if your computer's name is `qaserver` and the domain is `corpqa.likewise.com`, the domain join tool adds the following entry to the `/etc/hosts` file: `qaserver.corpqa.likewise.com`. To manually set the computer's FQDN, see [Join Active Directory Without Changing /etc/hosts](#).

3. To avoid typing the domain prefix before your user or group name each time you log on -- that is, to force the computer to assume the default domain -- select **Enable default user name prefix** and enter your domain prefix in the box. Example: CORP
4. Under **Organizational Unit**, you can optionally join the computer to an OU by selecting **Specific OU Path** and then typing a path in the box. The OU path is from the top of the Active Directory domain down to the OU that you want.

Or, to join the computer to the Computers container, select **Default (Computers or previously-joined OU)**.

5. Click **Join Domain**.
6. Enter the user name and password of an Active Directory account that has privileges to join computers to the domain and then click **OK**.


Note: If you do not use an Active Directory Domain Administrator account, you might not have sufficient privileges to change a machine object in Active Directory.

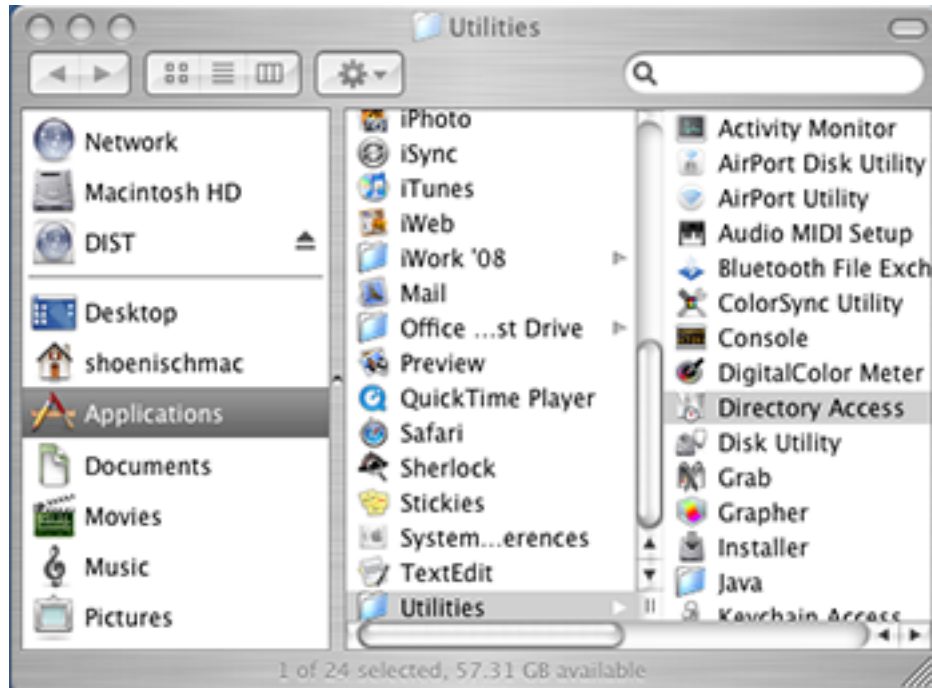
After you join a domain for the first time, you must restart the computer before you can log on.

5.6. Join a Mac Computer to Active Directory with the GUI


To join a computer running Mac OS X 10.4 or later to an Active Directory domain, you must have administrative privileges on the Mac and privileges on the Active Directory domain that allow you to join a computer.

1. In Finder, click **Applications**. In the list of applications, double-click **Utilities**, and then double-click **Directory Access** in OS X 10.4 or **Directory Utility** in OS X 10.5. In Mac OS X 10.6 (Snow

Leopard), you gain access to Directory Utility by using the **Apple** menu  to view the system preferences for accounts; for instructions, see your Mac OS X 10.6 documentation.



2. On Mac OS X 10.5, click **Show Advanced Settings**.

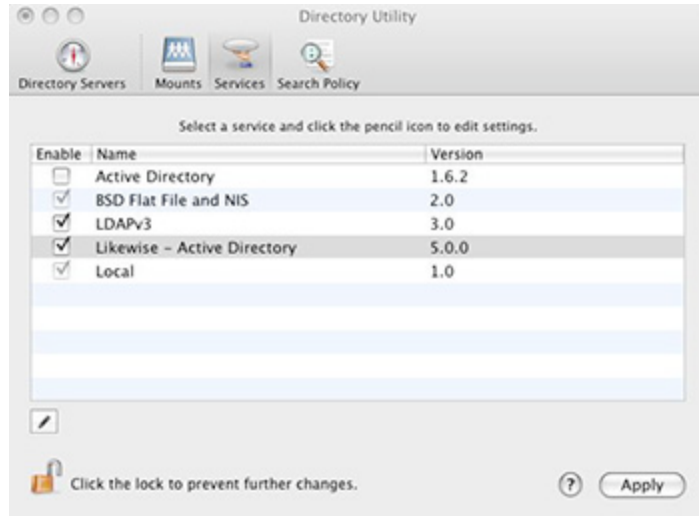
3. On the **Services** tab, click the lock  and enter an administrator name and password to unlock it.

4. In the list, make sure that the check box for **Active Directory** is not selected.


Important: Active Directory, Apple's built-in service for interoperating with AD, must be disabled for Likewise to work properly.

5. In the list, click **Likewise - Active Directory**, make sure the **Enable** check box for **Likewise - Active Directory** is selected, and then click **Configure** in OS X 10.4 or double-click **Likewise - Active Directory** in OS X 10.5 and later.

Note: On Mac OS X 10.6, if **Likewise - Active Directory** does not appear in the list, restart your computer.





6. Enter a name and password of a local machine account with administrative privileges.
7. On the menu bar at the top of the screen, click the **Likewise Domain Join** menu, and then click **Join or Leave Domain**.
8. In the **Computer name** box, type the local hostname of the Mac without the `.local` extension. Because of a limitation with Active Directory, the local hostname cannot be more than 15 characters. Also: `localhost` is not a valid name.

Tip: To find the local hostname of a Mac, on the **Apple** menu , click **System Preferences**, and then click **Sharing**. Under the **Computer Name** box, click **Edit**. Your Mac's local hostname is displayed.

9. In the **Domain to join** box, type the fully qualified domain name of the Active Directory domain that you want to join.
10. Under **Organizational Unit**, you can join the computer to an OU in the domain by selecting **OU Path** and then typing a path in the **OU Path** box.

Note: To join the computer to an OU, you must be a member of the Domain Administrator security group.

Or, to join the computer to the Computers container, select **Default to "Computers" container**.

11. Click **Join**.
12. After you are joined to the domain, you can set the display login window preference on the Mac: On the **Apple** menu , click **System Preferences**, and then under **System**, click **Accounts**.
13. Click the lock  and enter an administrator's name and password to unlock it.
14. Click **Login Options**, and then under **Display login window as**, select **Name and password**.

With Likewise Enterprise, the domain join utility includes a tool to migrate a Mac user's profile from a local user account to the home directory specified for the user in Active Directory; see *Migrate a User Profile on a Mac*.

5.6.1. Turn Off OS X Directory Service Authentication

If you are migrating from Open Directory or Active Directory and you had set authentication from the command line with `dsconfigad` or `dsconfigldap`, you must run the following commands to stop the computer from trying to use the built-in directory service even if the Mac is not bound to it:

```
dscl -. --delete -/Computers
dscl -/Search --delete -/ CSPSearchPath -/LDAPv3/
FQDNforYourDomainController
dscl -/Search --delete -/ CSPSearchPath -/Active\ Directory\All\
Domains
dscl -/Search/Contacts --delete -/ CSPSearchPath -/Active\ Directory/
All\ Domains
dscl -/Search/Contacts --delete -/ CSPSearchPath -/LDAPv3/
FQDNforYourDomainController
```

5.7. Use Likewise with a Single OU

If you have write privileges only for an organizational unit in Active Directory, you can still use Likewise. Your AD rights to create objects in an OU allow you to join Linux and Unix computers to the OU even though you do not have Active Directory Domain Administrator or Enterprise Administrator privileges. (See Delegate Control to Create Container Objects.)

There are additional limitations to this approach:

- You must join the computer to a specific OU, and you must know the path to that OU.
- You cannot use Likewise Enterprise in schema mode unless you have Enterprise Administrator privileges, which are required to upgrade the schema.

Join a Linux Computer to an Organizational Unit

To join a computer to a domain, you must have the user name and password of an account that has privileges to join computers to the OU and the full name of the domain that you want to join. The OU path is from the top OU down to the OU that you want.

As root, execute the following command, replacing `organizationalUnitName` with the path and name of the organizational unit that you want to join, `domainName` with the FQDN of the domain, and `joinAccount` with the user name of an account that has privileges to join computers to the domain:

```
/opt/likewise/bin/domainjoin-cli join --- ou organizationalUnitName
domainName joinAccount
```

Example: `/opt/likewise/bin/domainjoin-cli join -- ou Engineering
likewisedemo.com Administrator`

Example of how to join a nested OU:

```
domainjoin-cli join --ou topLevelOU/middleLevelOU/LowerLevelOU/
TargetOU likewisedemo.com Administrator
```

After you join a domain for the first time, you must restart the computer before you can log on.

5.8. Rename a Joined Computer

To rename a computer that has been joined to Active Directory, you must first leave the domain. You can then rename the computer by using the domain join command-line interface. After you rename the computer, you must rejoin it to the domain. Renaming a joined computer requires the user name and password of a user with privileges to join a computer to a domain.

Important: Do not change the name of a Linux, Unix, or Mac computer by using the `hostname` command because some distributions do not permanently apply the changes.

Rename a Computer by Using the Command-Line Tool

The following procedure removes a Unix or Linux computer from the domain, renames the computer, and then rejoins it to the domain.

1. With root privileges, at the shell prompt of a Unix computer, execute the following command:

```
/opt/likewise/bin/domainjoin-cli leave
```

2. To rename the computer in `/etc/hosts`, execute the following command, replacing `computerName` with the new name of the computer:

```
/opt/likewise/bin/domainjoin-cli setname computerName
```

Example: `/opt/likewise/bin/domainjoin-cli setname RHEL44ID`

3. To rejoin the renamed computer to the domain, execute the following command at the shell prompt, replacing `DomainName` with the name of the domain that you want to join and `UserName` with the user name of a user who has privileges to join a domain:

```
/opt/likewise/bin/domainjoin-cli join DomainName UserName
```

Example: `/opt/likewise/bin/domainjoin-cli join likewisedemo.com Administrator`

It may take a few moments before the computer is joined to the domain.

4. After you change the hostname of a computer, you must also change the name in the Likewise local provider database so that the local Likewise accounts use the correct prefix. To do so, execute the following command as root, replacing `hostName` with the name that you want:

```
/opt/likewise/bin/lw-set-machine-name hostName
```

Rename a Computer by Using the Domain Join Tool GUI

1. From the desktop with root privileges, double-click the Likewise Domain Join Tool, or at the shell prompt of a Linux computer, type the following command:

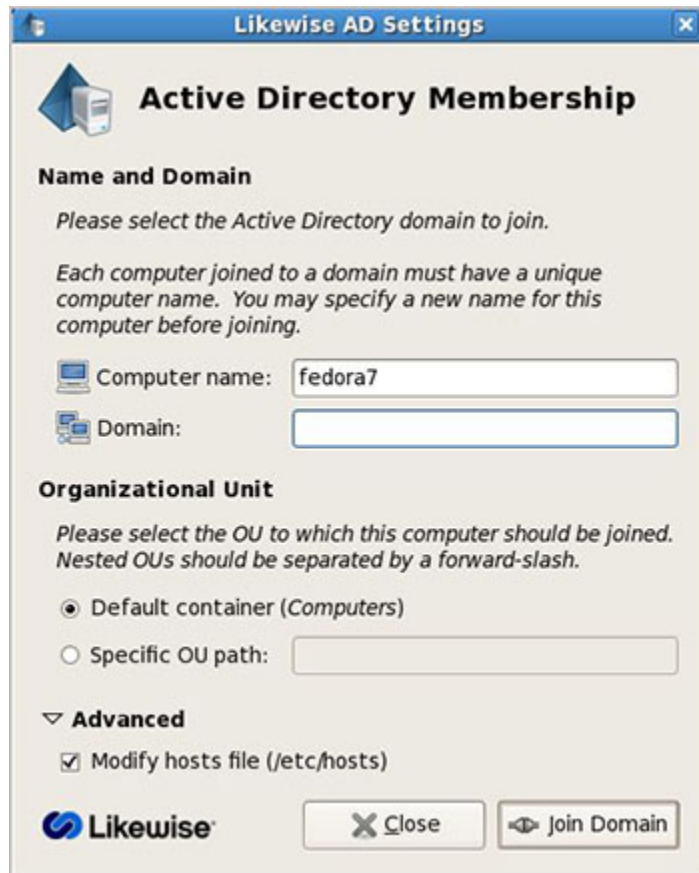
```
/opt/likewise/bin/domainjoin-gui
```

2. Click **Leave**, and then click **OK**.

3. Start the domain join tool again by double-clicking the Likewise Domain Join Tool on the desktop, or by typing the following command at the shell prompt of a Linux computer:

```
/opt/likewise/bin/domainjoin-gui
```

4. Click **Next**.
5. In the **Computer Name** box, rename the computer by typing a new name.



6. In the **Domain to join** box, enter the Fully Qualified Domain Name (FQDN) of the Active Directory domain.
7. Under **Organizational Unit**, you can join the computer to an OU in the domain by selecting **OU Path** and then typing a path in the **OU Path** box.

Or, to join the computer to the Computers container, select **Default to "Computers" container**.

8. Click **Next**.
9. Enter the user name and password of an Active Directory user with authority to join a machine to the Active Directory domain, and then click **OK**.

The computer's name in `/etc/hosts` has been changed to the name that you specified and the computer has been joined to the Active Directory domain with the new name.

10. After you change the hostname of a computer, you must also change the name in the Likewise local provider database so that the local Likewise accounts use the correct prefix. To do so, execute the following command as root, replacing `hostName` with the name that you want:

```
/opt/likewise/bin/lw-set-machine-name hostName
```

5.9. Files Modified When You Join a Domain

When Likewise adds a computer to a domain, it modifies some system files. The files that are modified depend on the platform, the distribution, and the system's configuration. The following files might be modified.

To see a listing of the changes that joining a domain will make to your operating system, execute the following join command:

domainjoin-cli join --advanced --preview domainName

Note: Not all the following files are present on all computers.

- /etc/nsswitch.conf (On AIX, the file is /etc/netsvcs.conf.)
- /etc/pam.conf on AIX, HP-UX, and Solaris
- /etc/pam.d/* on Linux
- /etc/ssh/{ssh_config,sshd_config} (or wherever sshd configuration is located)
- /etc/hosts (To join a domain without modifying /etc/hosts, see [Join Active Directory Without Changing /etc/hosts.](#))
- /etc/apparmor.d/abstractions/nameservice
- /etc/X11/gdm/PreSession/Default
- /etc/vmware/firewall/services.xml
- /usr/lib/security/methods.cfg
- /etc/security/user
- /etc/security/login.cfg
- /etc/netsvc.conf
- /etc/krb5.conf
- /etc/krb5/krb5.conf
- /etc/rc.config.d/netconf
- /etc/nodename
- /etc/{hostname,HOSTNAME,hostname.*}
- /etc/sysconfig/network/config
- /etc/sysconfig/network/dhcp
- /etc/sysconfig/network/ifcfg-*
- /etc/sysconfig/network-scripts/ifcfg-*
- /etc/init.d or /sbin/init.d
- /etc/rcX.d/ (new files and links created)

- /etc/inet/ipnodes

As an example, the following table lists the files that are modified for the *default configuration* of the operating system of a few selected platforms.

Modified files	Solaris 9	Solaris 10	AIX 5.3	AIX 6.1	Red Hat Enterprise Linux 5
/etc/nsswitch.conf (On AIX, the file is /etc/netsvcs.conf.)	Modified	Modified			Modified
/etc/pam.conf on AIX, HP-UX, and Solaris	Modified	Modified	Modified	Modified	
/etc/pam.d/* on Linux					Modified
/etc/ssh/{ssh_config,sshd_config} (or wherever sshd configuration is located)		Modified	Modified		Modified
/etc/hosts	Modified	Modified	Modified	Modified	Modified
/etc/apparmor.d/abstractions/nameservice					
/etc/X11/gdm/PreSession/Default					
/etc/vmware/firewall/services.xml					
/usr/lib/security/methods.cfg			Modified	Modified	
/etc/security/user			Modified	Modified	
/etc/security/login.cfg			Modified		
/etc/netsvc.conf			Modified	Modified	
/etc/krb5.conf			Modified	Modified	Modified
/etc/krb5/krb5.conf	Modified	Modified			
/etc/rc.config.d/netconf					

/etc/nodename	Modified	Modified			
/etc/{hostname, HOSTNAME, hostname.*}	Modified				
/etc/sysconfig/ network/config					
/etc/sysconfig/ network/dhcp					
/etc/sysconfig/ network/ifcfg-*					
/etc/sysconfig/ network-scripts/ ifcfg-*					
/etc/init.d or / sbin/init.d					
/etc/rcX.d/ (new files and links created)				Modified	
/etc/inet/ ipnodes	Modified	Modified			

5.10. With NetworkManager, Use a Wired Connection to Join a Domain

On Linux computers running NetworkManager -- which is often used for wireless connections -- you must make sure before you join a domain that the computer has a non-wireless network connection and that the non-wireless connection is configured to start when the networking cable is plugged in. You must continue to use the non-wireless network connection during the post-join process of restarting your computer and logging on with your Active Directory domain credentials.

After you have joined the domain and logged on for the first time with your AD domain credentials by using a non-wireless connection, you can then revert to using your wireless connection because your AD logon credentials are cached. (You will not, however, be notified when your AD password is set to expire until you either run a sudo command or log on by using a non-wireless connection.)

If, instead, you attempt to use a wireless connection when you join the domain, you will be unable to log on your computer with AD domain credentials after your computer restarts.

Here's why: NetworkManager is composed of a daemon that runs at startup and a user-mode application that runs only after you log on. NetworkManager is typically configured to auto-start wired network connections when they are plugged in and wireless connections when they are detected. The problem is that the wireless network is not detected until the user-mode application starts -- which occurs only after you have logged on.

Information about NetworkManager is available at <http://projects.gnome.org/NetworkManager/>.

Chapter 6. Logging On with Domain Credentials

6.1. About Logging On

Likewise includes the following logon options:

- Full domain credentials -- example: `likewisedemo.com\\hoenstiv`
- Single domain user name -- example: `likewisedemo\\hoenstiv`
- Alias -- example: `stiv`

(For Likewise Enterprise, see [Set a User Alias](#) and [Set a Group Alias](#).)

- Cached credentials

Important: When you log on from the command line, you must use a slash to escape the slash character, making the logon form `DOMAIN\\username`.

To use UPN names, you must raise your Active Directory forest functional level to Windows Server 2003, but raising the forest functional level to Windows Server 2003 will exclude Windows 2000 domain controllers from the domain. For more information, see [About Schema Mode and Non-Schema Mode](#).

When you log on a Linux, Unix, or Mac OS X computer by using your domain credentials, Likewise uses the Kerberos protocol to connect to Active Directory's key distribution center, or KDC, to establish a key and to request a Kerberos ticket granting ticket (TGT). The TGT lets you log on to other computers joined to Active Directory or applications provisioned with a service principal name and be automatically authenticated with Kerberos and authorized for access through Active Directory.

After logon, Likewise stores the password in memory and securely backs it up on disk. You can, however, configure Likewise to store logon information in a SQLite database, but it is not the default method. The password is used to refresh the user's Kerberos TGT and to provide NTLM-based single sign-on through the Likewise GSSAPI library. In addition, the NTLM verifier hash -- a hash of the NTLM hash -- is stored to disk to handle offline logons by comparing the password with the cached credentials.

Likewise stores an NTLM hash and LM hash only for accounts in Likewise's local provider. The hashes are used to authenticate users over CIFS. Since Likewise does not support offline logons for domain users over CIFS, it does not store the LM hash for domain users.

See Also

[About Single Sign-On](#)

[Configure Putty for Windows-Based SSO](#)

[Log On and Verify Your Kerberos Tickets](#)

6.2. Log On with AD Credentials

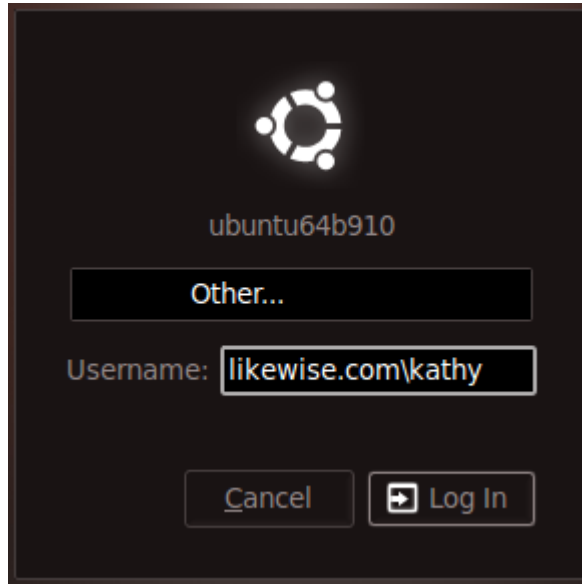
After the Likewise agent has been installed and the Linux or Unix computer has been joined to a domain, you can log on with your Active Directory credentials, either from the command line or

interactively through the system console. After you join a domain for the first time, you must reboot your computer before you can log on interactively through the console.

- Log on from the command line, but make sure you use a slash character to escape the slash, making the logon form DOMAIN\\username.

Example with ssh: `ssh likewisedemo.com\\hoenstiv@localhost`

- Log on the system console or the text login prompt by using an Active Directory user account in the form of DOMAIN\\username, where DOMAIN is the Active Directory short name. Example on Ubuntu:



6.3. Log On with SSH

You can log on with SSH by executing the `ssh` command at the shell prompt in the following format:

```
ssh DOMAIN\\username@localhost
```

Example: `ssh likewisedemo.com\\hoenstiv@localhost`

6.4. Solve Logon Problems from Windows

To troubleshoot a problem with a user who cannot log on a to Linux or Unix computer, perform the following series of diagnostic tests sequentially.

1. On a Windows computer, log off and then log on again with the problem user's AD credentials to verify that the password is correct and that the account is not locked or disabled.
2. Try to SSH to the target Linux or Unix computer again with the user's full NT4-style credentials and password, not just the user's alias. In your SSH command, make sure to use a slash character to escape the slash.
3. If you are using Likewise Enterprise, make sure that the user's computer is in the correct Likewise cell.

4. Make sure that the user is enabled to log on the computer, either by being enabled in the cell (with Likewise Enterprise) or by being in a group allowed to access the computer. Then try to log on the target computer again.
5. Ensure that the Likewise client can communicate with the Active Directory domain controller.
6. Make sure that the shell specified for the user account in Active Directory is available on the target computer. Specifying a shell that is unavailable will block the user account from logging on.
7. Verify that the home directory is set and can be created. A home directory that cannot be created because the path is incorrect or the permissions are insufficient can block an attempt to log on.
8. Make sure there are no logon restrictions in place -- for example, the group policy that restricts logon to certain users or groups -- that prevent the user account from logging on the computer.
9. Log on the computer with a different user account -- one that is enabled for access to the computer.

6.5. Solve Logon Problems on Linux or Unix

To troubleshoot problems logging on a Linux computer with Active Directory credentials after you joined the computer to a domain, perform the following series of diagnostic tests sequentially with a root account. The tests can also be used to troubleshoot logon problems on a Unix or Mac OS X computer; however, the syntax of the commands on Unix and Mac might be slightly different.

Make Sure You Are Joined to the Domain

Execute the following command:

```
/opt/likewise/bin/domainjoin-cli query
```

If you are not joined, see [Join Active Directory with the Command Line](#).

Check Whether You Are Using a Valid Logon Form

When troubleshooting a logon problem, use your full domain credentials: DOMAIN\username.
Example: likewisedemo.com\hoenstiv.

When logging on from the command line, you must escape the slash character with a slash character, making the logon form DOMAIN\\username. Example: likewisedemo.com\\hoenstiv.

To view a list of logon options, see [About Logging On](#).

Clear the Cache

You might need to clear the cache to ensure that the client computer recognizes the user's ID. See [Clear the Authentication Cache](#).

Destroy the Kerberos Cache

Clear the Likewise Kerberos cache to make sure there is not an issue with a user's Kerberos tickets. Execute the following command with the user account that you are troubleshooting:

```
/opt/likewise/bin/kdestroy
```

Check the Status of the Likewise Authentication Daemon

Check the status of the authentication daemon on a Unix or Linux computer running the Likewise Agent by executing the following command as the root user:

```
/opt/likewise/bin/lwsm status lsass
```

If	Do This
The result looks like this: lsassd is stopped	Restart the daemon.
The result looks like this: lsassd (pid 1783) is running...	Proceed to the next test.

Check Communication between the Likewise Daemon and AD

Verify that the Likewise daemon can exchange data with AD by executing this command:

```
/opt/likewise/bin/lw-get-dc-name FullDomainName
```

Example: `/opt/likewise/bin/lw-get-dc-name likewisedemo.com`

If	Do This
The result does not show the name and IP address of your domain controller	<ol style="list-style-type: none"> 1. Make sure the domain controller is online and operational. 2. Check network connectivity between the client and the domain controller. 3. Join the domain again. 4. View log files.
The result shows the correct domain controller name and IP address	Proceed to the next test.

Verify that Likewise Can Find a User in AD

Verify that the Likewise agent can find your user by executing the following command, substituting the name of a valid AD domain for `domainName` and a valid user for `ADUserName`:

```
/opt/likewise/bin/lw-find-user-by-name domainName\\ADUserName
```

Example: `/opt/likewise/bin/lw-find-user-by-name likewisedemo\\hab`

If	Do This
The command fails to find the user	<ol style="list-style-type: none"> 1. Check whether the computer is joined to the domain by executing the following command as root:

	<pre>domainjoin-cli query</pre> <p>Displays the hostname, current domain, and distinguished name, which includes the OU to which the computer belongs. Make sure the OU is correct. If the computer is not joined to a domain, it displays only the hostname.</p> <ol style="list-style-type: none"> 2. Check Active Directory to make sure the user has an account. If you are using Likewise Enterprise, also ensure that the user is associated with the correct cell. 3. Check whether the same user is in the <code>/etc/passwd</code> file. If necessary, migrate the user to Active Directory. 4. Make sure the AD authentication provider is running by proceeding to the next test.
The user is found	Proceed to the PAM test later in this topic.

Make Sure the AD Authentication Provider Is Running

Likewise includes two authentication providers:

1. The local provider
2. The Active Directory provider

If the AD provider is not online, users are unable to log on with their AD credentials. To check the status of the authentication providers, execute the following command as root:

```
/opt/likewise/bin/lw-get-status
```

A healthy result should look like this:

```
LSA Server Status:
Agent version: 5.0.0
Uptime:          2 days 21 hours 16 minutes 29 seconds
[Authentication provider: lsa-local-provider]
    Status:    Online
    Mode:      Local system
[Authentication provider: lsa-activedirectory-provider]
    Status:    Online
    Mode:      Un-provisioned
    Domain:    likewisedemo.com
    Forest:    likewisedemo.com
    Site:      Default-First-Site-Name
```

An unhealthy result will not include the AD authentication provider or will indicate that it is offline. If the AD authentication provider is not listed in the results, restart the authentication daemon.

If the result looks like the line below, check the status of the Likewise daemons to make sure they are running.

Failed to query status from LSA service.
The LSASS server is not responding.

Run the `id` Command to Check the User

Run the following `id` command to check whether `nsswitch` is properly configured to handle AD user account information:

```
id DOMAIN\\username
```

Example: `id likewisedemo\\kathy`

If the command does not show information for the user, check whether the `/etc/nsswitch.conf` file is properly configured for `passwd` and `group`: Both entries should include the `lsass` parameter.

If `/etc/nsswitch.conf` is properly configured, the Likewise name service libraries might be missing or misplaced. It is also possible that the `LD_PRELOAD` or `LD_LIBRARY_PATH` variables are defined without including the Likewise libraries.

Switch User to Check PAM

Verify that a user's password can be validated through PAM by using the `switch user` service. Either switch from a non-root user to a domain user or from root to a domain user. If you switch from root to a domain user, run the command below twice so that you are prompted for the domain user's password:

```
su DOMAIN\\username
```

Example: `su likewisedemo\\hoenstiv`

If	Do This
The <code>switch user</code> command fails to validate the user	<p>Generate a PAM debug log.</p> <p>Also, check the following log files for error messages (the location of the log files varies by operating system):</p> <pre>/var/log/messages</pre> <pre>/var/log/secure</pre>

Test SSH

Check whether you can log on with SSH by executing the following command:

```
ssh DOMAIN\\username@localhost
```

Example: `ssh likewisedemo.com\\hoenstiv@localhost`

If you believe the issue might be specific to SSH, see troubleshooting SSH SSO.

Run the Authentication Daemon in Debug Mode

To troubleshoot the lookup of a user or group ID, you can set the Likewise authentication daemon to run in debug mode and show the log in the console by executing this command:

`/opt/likewise/sbin/lsassd --loglevel debug`

Check Nsswitch.Conf

Make sure `/etc/nsswitch.conf` is configured correctly to work with Likewise. For more information, see [Configuring Clients Before Agent Installation](#).

On HP-UX, Escape Special Characters at the Console

When you log on to the console on some versions of HP-UX, such as 11.23, you might need to escape special characters, such as `@` and `#`, by preceding them with a slash (`\`). For more information, see your HP-UX documentation.

Additional Diagnostic Tools

There are additional command-line utilities that you can use to troubleshoot logon problems in the following directory:

`/opt/likewise/bin`

See Also

[Resolve an AD Alias Conflict with a Local Account](#)

Chapter 7. Troubleshooting Domain-Join Problems

7.1. Top 10 Reasons Domain Join Fails

Here are the top 10 reasons that an attempt to join a domain fails:

1. Root was not used to run the domain-join command (or to run the domain-join graphical user interface).
2. The user name or password of the account used to join the domain is incorrect.
3. The name of the domain is mistyped.
4. The name of the OU is mistyped.
5. The local hostname is invalid.
6. The domain controller is unreachable from the client because of a firewall or because the NTP service is not running on the domain controller. (See [Make Sure Outbound Ports Are Open and Diagnose NTP on Port 123.](#))
7. The client is running RHEL 2.1 and has an old version of SSH.
8. On SUSE, GDM (dbus) must be restarted. This daemon cannot be automatically restarted if the user logged on with the graphical user interface.
9. On HP-UX and Solaris, dtlogin must be restarted. This daemon cannot be automatically restarted if the user logged on with the HP-UX or Solaris graphical user interface. To restart dtlogin, run the following command: `/sbin/init.d/dtlogin.rc start`
10. SELinux is turned on by being set to either enforcing or permissive -- which is especially likely on Fedora and some versions of Red Hat. SELinux must be set to disabled before the computer can be joined to the domain.

To turn off SELinux, edit the following file, which is the primary configuration file for enabling and disabling SELinux:

`/etc/sysconfig/selinux`

or

`/etc/selinux/config`

For instructions on how to edit the file to disable SELinux, see the SELinux man page.

See Also

[Generate a Domain-Join Log](#)

7.2. Solve Domain-Join Problems

To troubleshoot problems with joining a Linux computer to a domain, perform the following series of diagnostic tests sequentially on the Linux computer with a root account. The tests can also be used

to troubleshoot domain-join problems on a Unix or Mac OS X computer; however, the syntax of the commands on Unix and Mac might be slightly different.

The procedures in this topic assume that you have already checked whether the problem falls under the Top 10 Reasons Domain Join Fails. It is also recommended that you generate a domain-join log.

Verify that the Name Server Can Find the Domain

Run the following command as root:

```
nslookup YourADrootDomain.com
```

Make Sure the Client Can Reach the Domain Controller

You can verify that your computer can reach the domain controller by pinging it:

```
ping YourDomainName
```

Verify that Outbound Ports Are Open

Run the following command as root:

```
domainjoin-cli join --details firewall likewisedemo.com
```

The results of the command show whether you must open any ports.

For a list of ports that must be open on the client, see [Make Sure Outbound Ports Are Open](#).

Check DNS Connectivity

The computer might be using the wrong DNS server or none at all. Make sure the nameserver entry in `/etc/resolv.conf` contains the IP address of a DNS server that can resolve the name of the domain you are trying to join. The IP address is likely to be that of one of your domain controllers.

Make Sure `nsswitch.conf` Is Configured to Check DNS for Host Names

The `/etc/nsswitch.conf` file must contain the following line. (On AIX, the file is `/etc/netsvc.conf`.)

```
hosts: files dns
```

Computers running Solaris, in particular, may not contain this line in `nsswitch.conf` until you add it.

Generate a Domain-Join Log

To log information about your attempt to join a domain, you can use the command-line utility's `log` option with the `join` command. The `log` option captures information about the attempt to join the domain on the screen or in a file.

- To display the information in the terminal, execute the following command; the dot after the `logfile` option denotes that the information is to be shown in the console:

```
domainjoin-cli --logfile . join domainName userName
```

- To save the information in a log file, execute the following command:

```
domainjoin-cli --logfile path join domainName userName
```

Example:

```
domainjoin-cli --logfile /var/log/domainjoin.log join  
likewisedemo.com Administrator
```

After you generate a log, review it for information that might help solve the problem.

Ensure that DNS Queries Are Not Using the Wrong Network Interface Card

If the computer is multi-homed, the DNS queries might be going out the wrong network interface card. Temporarily disable all the NICs except for the card on the same subnet as your domain controller or DNS server and then test DNS lookups to the AD domain. If this works, re-enable all the NICs and edit the local or network routing tables so that the AD domain controllers are accessible from the host.

Determine Whether the DNS Server Is Configured to Return SRV Records

Your DNS server must be set to return SRV records so the domain controller can be located. It is common for non-Windows (bind) DNS servers to not be configured to return SRV records.

Diagnose it by executing the following command:

```
nslookup -q=srv _ldap._tcp.ADdomainToJoin.com
```

Make Sure that the Global Catalog Is Accessible

The global catalog for Active Directory must be accessible. A global catalog in a different zone might not show up in DNS. Diagnose it by executing the following command:

```
nslookup -q=srv _ldap._tcp.gc._msdcs.ADrootDomain.com
```

From the list of IP addresses in the results, choose one or more addresses and test whether they are accessible on Port 3268 by using telnet.

```
telnet 192.168.100.20 3268
```

```
Trying 192.168.100.20... Connected to sales-dc.likewisedemo.com  
(192.168.100.20). Escape character is '^]'. Press the Enter key to close the  
connection: Connection closed by foreign host.
```

Verify that the Client Can Connect to the Domain on Port 123

The following test checks whether the client can connect to the domain controller on Port 123 and whether the Network Time Protocol (NTP) service is running on the domain controller. For the client to join the domain, NTP -- the Windows time service -- must be running on the domain controller.

On a Linux computer, run the following command as root:

```
ntpdate -d -u DC_hostname
```

Example: `ntpdate -d -u sales-dc`

For more information, see [Diagnose NTP on Port 123](#).

In addition, check the logs on the domain controller for errors from the source named `w32tm`, which is the Windows time service.

7.3. Ignore Inaccessible Trusts

An inaccessible trust can block you from successfully joining a domain. If you know that there are inaccessible trusts in your Active Directory network, you can set Likewise to ignore all the trusts before you try to join a domain. To do so, use the `lwconfig` tool to modify the values of the `DomainManagerIgnoreAllTrusts` setting.

First, list the available trust settings:

```
/opt/likewise/bin/lwconfig --list | grep -i trust
```

The results will look something like this. The setting at issue is `DomainManagerIgnoreAllTrusts`.

```
DomainManagerIgnoreAllTrusts
DomainManagerIncludeTrustsList
DomainManagerExcludeTrustsList
```

Second, list the details of the `DomainManagerIgnoreAllTrusts` setting to see the values it accepts:

```
[root@rhel5d bin]# ./lwconfig ---details DomainManagerIgnoreAllTrusts
Name: DomainManagerIgnoreAllTrusts
Description: When true, ignore all trusts during domain enumeration.
Type: boolean
Current Value: false
Accepted Values: true, false
Current Value is determined by local policy.
```

Third, change the setting to `true` so that Likewise will ignore trusts when you try to join a domain.

```
[root@rhel5d bin]# ./lwconfig DomainManagerIgnoreAllTrusts true
```

Finally, check to make sure the change took effect:

```
[root@rhel5d bin]# ./lwconfig ---show DomainManagerIgnoreAllTrusts
boolean
true
local policy
```

Now try to join the domain again. If successful, keep in mind that only users and groups who are in the local domain will be able to log on the computer.

In the example output above that shows the setting's current values, `local policy` is listed -- meaning that the policy is managed locally through `lwconfig` because a Likewise Enterprise

group policy is not managing the setting. Typically, with Likewise Enterprise, you would manage the `DomainManagerIgnoreAllTrusts` policy by using the corresponding group policy, but you cannot apply group policies to the computer until after it is added to the domain. The corresponding Likewise group policy is named `Lsass: Ignore all trusts during domain enumeration`. For more information on the domain manager group policies to set whitelists and blacklists for trusts, see the Group Policy Administration Guide.

For information on the arguments of `lwconfig`, run the following command:

```
/opt/likewise/bin/lwconfig --help
```

7.4. Dealing with Common Error Messages

This section lists solutions to common errors that can occur when you try to join a domain.

7.4.1. Configuration of Krb5

Error Message:

```
Warning: A resumable error occurred while processing a module.  
Even though the configuration of -'krb5' was executed, the  
configuration did not  
fully complete. Please contact Likewise support.
```

Solution:

Delete `/etc/krb5.conf` and try to join the domain again.

7.4.2. Chkconfig Failed

This error can occur when you try to join a domain or you try to execute the domain-join command with an option but the `netlogond` daemon is not already running.

Error Message:

```
Error: chkconfig failed [code 0x00080019]
```

Description: An error occurred while using `chkconfig` to process the `netlogond` daemon, which must be added to the list of processes to start when the computer is rebooted. The problem may be caused by startup scripts in the `/etc/rc.d/` tree that are not LSB-compliant.

Verification: Running the following command as root can provide information about the error:

```
chkconfig --add netlogond
```

Solution: Remove startup scripts that are not LSB-compliant from the `/etc/rc.d/` tree.

7.5. Diagnose NTP on Port 123

When you use the Likewise domain-join utility to join a Linux or Unix client to a domain, the utility might be unable to contact the domain controller on Port 123 with UDP. The Likewise agent requires that Port 123 be open on the client so that it can receive NTP data from the domain controller. In addition, the time service must be running on the domain controller.

You can diagnose NTP connectivity by executing the following command as root at the shell prompt of your Linux machine:

```
ntpdate -d -u DC_hostname
```

Example: `ntpdate -d -u sales-dc`

If all is well, the result should look like this:

```
[root@rhel44id ~]# ntpdate --d --u sales-dc
2 May 14:19:20 ntpdate[20232]: ntpdate 4.2.0a@1.1190-r Thu Apr 20
11:28:37 EDT 2006 (1)
Looking for host sales-dc and service ntp
host found -: sales-dc.likewisedemo.com
transmit(192.168.100.20)
receive(192.168.100.20)
transmit(192.168.100.20)
receive(192.168.100.20)
transmit(192.168.100.20)
receive(192.168.100.20)
transmit(192.168.100.20)
receive(192.168.100.20)
transmit(192.168.100.20)
server 192.168.100.20, port 123
stratum 1, precision --6, leap 00, trust 000
refid [LOCL], delay 0.04173, dispersion 0.00182
transmitted 4, in filter 4
reference time:      cbc5d3b8.b7439581  Fri, May  2 2008 10:54:00.715
originate timestamp: cbc603d8.df333333  Fri, May  2 2008 14:19:20.871
transmit timestamp:  cbc603d8.dda43782  Fri, May  2 2008 14:19:20.865
filter delay:  0.04207  0.04173  0.04335  0.04178
                0.00000  0.00000  0.00000  0.00000
filter offset:  0.009522 0.008734 0.007347 0.005818
                0.000000 0.000000 0.000000 0.000000
delay 0.04173, dispersion 0.00182
offset 0.008734
2 May 14:19:20 ntpdate[20232]: adjust time server 192.168.100.20
offset 0.008734 sec
```

Output When There Is No NTP Service

If the domain controller is not running NTP on Port 123, the command returns a response such as no server suitable for synchronization found, as in the following output:

```
5 May 16:00:41 ntpdate[8557]: ntpdate 4.2.0a@1.1190-r Thu Apr 20
11:28:37 EDT 2006 (1)
Looking for host RHEL44ID and service ntp
host found -: rhel44id.likewisedemo.com
transmit(127.0.0.1)
transmit(127.0.0.1)
transmit(127.0.0.1)
transmit(127.0.0.1)
transmit(127.0.0.1)
127.0.0.1: Server dropped: no data
```

```
server 127.0.0.1, port 123
stratum 0, precision 0, leap 00, trust 000
refid [127.0.0.1], delay 0.00000, dispersion 64.00000
transmitted 4, in filter 4
reference time:      00000000.00000000  Wed, Feb  6 2036 22:28:16.000
originate timestamp: 00000000.00000000  Wed, Feb  6 2036 22:28:16.000
transmit timestamp:  cbca101c.914a2b9d  Mon, May  5 2008 16:00:44.567
filter delay:  0.00000  0.00000  0.00000  0.00000
               0.00000  0.00000  0.00000  0.00000
filter offset: 0.000000 0.000000 0.000000 0.000000
               0.000000 0.000000 0.000000 0.000000
delay 0.00000, dispersion 64.00000
offset 0.000000
5 May 16:00:45 ntpdate[8557]: no server suitable for synchronization
found
```

7.6. Turn Off Apache to Join a Domain

The Apache web server locks the keytab file, which can block an attempt to join a domain. If the computer is running Apache, stop Apache, join the domain, and then restart Apache.

Chapter 8. Configuring the Agent

8.1. Modify Settings with the Config Tool

To quickly change an end-user setting for the Likewise agent, you can run the `lwconfig` command-line tool as root:

`/opt/likewise/bin/lwconfig`

The syntax to change the value of a setting is as follows, where `setting` is replaced by the registry entry that you want to change and `value` by the new value that you want to set:

```
/opt/likewise/bin/lwconfig setting value
```

Here's an example of how to use `lwconfig` to change the `AssumeDefaultDomain` setting:

```
[root@rhel5d bin]# ./lwconfig --detail AssumeDefaultDomain ❶
Name: AssumeDefaultDomain
Description: Apply domain name prefix to account name at logon
Type: boolean
Current Value: false
Accepted Values: true, false
Current Value is determined by local policy.
```

```
[root@rhel5d bin]# ./lwconfig AssumeDefaultDomain true ❷
```

```
[root@rhel5d bin]# ./lwconfig --show AssumeDefaultDomain ❸
boolean
true
local policy
```

- ❶ Use the `--detail` option to view the setting's current value and to determine the values that it accepts.
- ❷ Set the value to `true`.
- ❸ Use the `--show` option to confirm that the value was set to `true`.

To view the settings that you can change with `lwconfig`, execute the following command:

```
/opt/likewise/bin/lwconfig --list
```

You can also import and apply a number of settings with a single command by using the `--file` option combined with a text file that contains the settings that you want to change followed by the values that you want to set. Each setting-value pair must be on a single line. For example, the contents of my flat file, named `newRegistryValuesFile` and saved to the desktop of my Red Hat computer, looks like this:

```
AssumeDefaultDomain true
RequireMembershipOf -"likewisedemo\\support" -"likewisedemo\
\domain^admins"
HomeDirPrefix -/home/ludwig
LoginShellTemplate -/bash/sh
```

To import the file and automatically change the settings listed in the file to the new values, I would execute the following command as root:

```
/opt/likewise/bin/lwconfig --file /root/Desktop/newRegistryValuesFile
```

8.2. Add Domain Accounts to Local Groups with `/etc/group`

You can add domain users to your local groups on a Linux, Unix, and Mac OS X computer by placing an entry for the user or group in the `/etc/group` file. Adding an entry for an Active Directory user to your local groups can give the user local administrative rights. The entries must adhere to the following rules:

- Use the correct case; entries are case sensitive.
- Use a user or group's alias if the user or group has one in Active Directory.
- If the user or group does not have an alias, you must set the user or group in the Likewise canonical name format of `NetBIOSdomainName\SAMaccountName`.

Note: For users or groups with an alias, the Likewise canonical name format is the alias, which you must use; you cannot use the format of `NetBIOS domain name\SAM account name`.

So, for users and groups without an alias, the form of an entry is as follows:

```
root:x:0:LIKEWISEDEMO\kristeva
```

For users and groups with an alias, the form of an entry is as follows:

```
root:x:0:kris
```

In `/etc/group`, the slash character separating the domain name from the account name does not typically need to be escaped.

Tip: On Ubuntu, you can give a domain user administrative privileges by adding the user to the `admin` group as follows:

```
admin:x:119:LIKEWISEDEMO\bakhtin
```

On a Mac OS X computer, you can add users to a local group with Apple's directory service command-line utility: `dscl`. In `dscl`, go to the `/Local/Default/Groups` directory and then add users to a group by using the `append` command.

8.3. Configure Entries in Your Sudoers Files

When you add Active Directory entries to your sudoers file -- typically, `/etc/sudoers` -- you must adhere to at least the following rules:

- ALL must be in uppercase letters.
- Use a slash character to escape the slash that separates the Active Directory domain from the user or group name.
- Use the correct case; entries are case sensitive.
- Use a user or group's alias if the user or group has one in Active Directory.

- If the user or group does not have an alias, you must set the user or group in the Likewise canonical name format of NetBIOSdomainName\SAMaccountName (and escape the slash character).

Note: For users or groups with an alias, the Likewise canonical name format is the alias, which you must use; you cannot use the format of NetBIOS domain name\SAM account name.

So, for users and groups without an alias, the form of an entry in the sudoers file is as follows:

```
DOMAIN\\username
```

```
DOMAIN\\groupname
```

Example entry of a group:

```
% LIKEWISEDEMO\\LinuxFullAdmins ALL=(ALL) ALL
```

Example entry of a user with an alias:

```
kyle ALL=(ALL) ALL
```

For more information about how to format your sudoers file, see your computer's man page for sudo.

Check a User's Canonical Name on Linux

To determine the canonical name of a Likewise user on Linux, execute the following command, replacing the domain and user in the example with your domain and user:

```
getent passwd likewisedemo.com\\hab
```

```
LIKEWISEDEMO\\hab:x:593495196:593494529: Jurgen Habermas:/home/local/
LIKEWISEDEMO/ hab:/bin/ sh
```

In the results, the user's Likewise canonical name is the first field.

8.4. Set a Sudoers Search Path

Although Likewise searches a number of common locations for your sudoers file, on some platforms Likewise might not find it. In such cases, you can specify the location of your sudoers file by adding the following line to the Sudo GP Extension section of `/etc/likewise/grouppolicy.conf`:

```
SudoersSearchPath = /your/search/path
```

Example: `SudoersSearchPath = "/opt/sfw/etc";`

Here's an example in the context of the `/etc/likewise/grouppolicy.conf` file:

```
[{20D139DE-D892-419f-96E5-0C3A997CB9C4}]
Name = -"Likewise Enterprise Sudo GP Extension";
DllName = -"liblwisudo.so";
EnableAsynchronousProcessing = 0;
NoBackgroundPolicy = 0;
NoGPOListChanges = 1;
NoMachinePolicy = 0;
NoSlowLink = 1;
NoUserPolicy = 1;
```

```
PerUserLocalSettings = 0;
ProcessGroupPolicy = -"ProcessSudoGroupPolicy";
ResetGroupPolicy = -"ResetSudoGroupPolicy";
RequireSuccessfulRegistry = 1;
SudoersSearchPath = -"/opt/sfw/etc";
```

8.5. Set Up AIX Audit Classes to Monitor Events

On AIX, you can set up audit classes to monitor the activities of users who log on with their Active Directory credentials. The file named `/etc/likewise/auditclasses.sample` is a template that you can use to set up audit classes for AD users.

To set up an audit class, make a copy of the file, name it `/etc/likewise/auditclasses`, and then edit the file to specify the audit classes that you want.

After you set up audit classes for a user, the auditing will take place the next time the user logs in.

The sample Likewise `auditclasses` file looks like this:











```
#
# Sample auditclasses file.
#
# A line with no label specifies the default audit classes for
# users that are not explicitly listed:
#
general, files
#
# A line starting with a username specifies the audit classes for
# that AD user. The username must be specified as the -"canonical"
# name for the user: either -"DOMAIN\username" or just -"username"
# if -"--assumeDefaultDomain yes" was passed to domainjoin-cli
# with -"--userDomainPrefix DOMAIN". In Likewise Enterprise, if
# the user has an alias specified in the cell the alias name must
# be used here.
#
DOMAIN\user1: general, files, tcpip
user2: general, cron
#
# A line starting with an @ specifies the audit classes for members
# of an AD group. These classes are added to the audit classes
# for the user (or the default, if the user is not listed here).
# Whether to specify -"DOMAIN\groupname" or just -"groupname" follows
# the same rules as for users.
#
@DOMAIN\mail_users: mail
group2: cron
```

For information on AIX audit classes, see the IBM documentation for your version of AIX.

Chapter 9. Troubleshooting the Agent

This chapter contains information on how to troubleshoot the Likewise agent, including the authentication service, the input-output service, and the network logon daemon.

Additional troubleshooting information is in the following chapters:

-  Troubleshooting Domain Join Problems
-  Solve Logon Problems on Linux, Unix, or Mac
-  Solve Logon Problems from Windows
-  Troubleshooting SSH SSO Problems
-  Troubleshooting the Group Policy Agent
-  Monitoring Events with the Event Log
-  Troubleshooting the Likewise Database
-  Troubleshooting Samba Integration
-  Likewise Tips and Tricks
-  Command-Line Reference

For an overview of commands such as `rpm` and `dpkg` that can help troubleshoot Likewise packages on Linux and Unix platforms, see [Package Management Commands](#).

9.1. Likewise Daemons and Services

9.1.1. Troubleshoot Likewise Daemons with the Service Manager

The Likewise Service Manager lets you troubleshoot all the Likewise services from a single command-line utility. You can, for example, check the status of the services and start or stop them. The service manager is the preferred method for restarting a service because it automatically identifies a service's dependencies and restarts them in the right order.

To list the status of the services, run the following command with superuser privileges at the command line:

`/opt/likewise/bin/lwsm list`

Here's an example:

```
[root@rhel5d bin]# -/opt/likewise/bin/lwsm list
lwreg          running (standalone: 1920)
dcerpc         running (standalone: 2544)
eventlog       running (standalone: 2589)
lsass          running (standalone: 2202)
```

```
lwio          running (standalone: 2191)
netlogon      running (standalone: 2181)
npfs          running (io: 2191)
pvfs          stopped
rdr           running (io: 2191)
srv           stopped
srvsvc        stopped
```

To restart the `lsass` service, run the following command with superuser privileges:

```
/opt/likewise/bin/lwsm restart lsass
```

To view all the service manager's commands and arguments, execute the following command:

```
/opt/likewise/bin/lwsm --help
```

9.1.2. Check the Status of the Authentication Daemon

On Linux and Unix

You can check the status of the authentication daemon on a Unix or Linux computer running the Likewise agent by executing the following command at the shell prompt as the root user:

```
/opt/likewise/bin/lwsm status lsass
```

If the service is not running, execute the following command:

```
/opt/likewise/bin/lwsm start lsass
```

9.1.3. Check the Status of the DCE/RPC Daemon

The Likewise DCE/RPC daemon handles communication between Likewise clients and Microsoft Active Directory.

On Linux and Unix

You can check the status of `dcerpcd` on a Unix or Linux computer running the Likewise agent by executing the following command as the root user:

```
/opt/likewise/bin/lwsm status dcerpc
```

If the service is not running, execute the following command:

```
/opt/likewise/bin/lwsm start dcerpc
```

On Mac OS X

On a Mac OS X computer, you cannot use the `status` command, but you can monitor the daemon by using Activity Monitor:

1. In Finder, click **Applications**, click **Utilities**, and then click **Activity Monitor**.
2. In the list under **Process Name**, make sure `dcerpcd` appears. If the process does not appear in the list, you might need to start it.
3. To monitor the status of the process, in the list under **Process Name**, click the process, and then click **Inspect**.

9.1.4. Check the Status of the Network Logon Daemon

The `netlogond` daemon detects the optimal domain controller and global catalog and caches the data.

On Linux and Unix

You can check the status of `netlogond` on a Unix or Linux computer running the Likewise agent by executing the following command as the root user:

```
/opt/likewise/bin/lwsm status netlogon
```

If the service is not running, execute the following command:

```
/opt/likewise/bin/lwsm start netlogon
```

On Mac OS X

On a Mac OS X computer, you cannot use the `status` command, but you can monitor the daemon by using Activity Monitor:

1. In Finder, click **Applications**, click **Utilities**, and then click **Activity Monitor**.
2. In the list under **Process Name**, make sure `netlogond` appears. If the process does not appear in the list, you might need to start it.
3. To monitor the status of the process, in the list under **Process Name**, click the process, and then click **Inspect**.

9.1.5. Check the Status of the Input-Output Service

The Likewise input-output service -- `lwiod` -- communicates over SMB with external SMB servers and internal processes.

On Linux and Unix

You can check the status of `lwiod` on a Unix or Linux computer running the Likewise agent by executing the following command as the root user:

```
/opt/likewise/bin/lwsm status lwio
```

If the service is not running, execute the following command:

```
/opt/likewise/bin/lwsm start lwio
```

On Mac OS X

On a Mac OS X computer, you cannot use the `status` command, but you can monitor the daemon by using Activity Monitor:

1. In Finder, click **Applications**, click **Utilities**, and then click **Activity Monitor**.
2. In the list under **Process Name**, make sure `lwiod` appears. If the process does not appear in the list, you might need to start it.
3. To monitor the status of the process, in the list under **Process Name**, click the process, and then click **Inspect**.

9.1.6. Restart the Authentication Daemon

The authentication daemon handles authentication, authorization, caching, and idmap lookups. For more information, see [About the Likewise Agent](#).

You can restart the Likewise authentication daemon by executing the following command at the shell prompt:

```
/opt/likewise/bin/lwsm restart lsass
```

To stop the daemon, type this command:

```
/opt/likewise/bin/lwsm stop lsass
```

To start the daemon, type this command:

```
/opt/likewise/bin/lwsm start lsass
```

9.1.7. Restart the DCE/RPC Daemon

The Likewise DCE/RPC daemon helps route remote procedure calls between computers on a network by serving as an end-point mapper. For more information, see [About the Likewise Agent](#).

You can restart the Likewise DCE/RPC daemon by executing the following command at the shell prompt:

```
/opt/likewise/bin/lwsm restart dcerpc
```

To stop the daemon, type this command:

```
/opt/likewise/bin/lwsm stop dcerpc
```

To start the daemon, type this command:

```
/opt/likewise/bin/lwsm start dcerpc
```

9.1.8. Restart the Network Logon Daemon

The `netlogond` daemon determines the optimal domain controller and global catalog and caches the data. For more information and a list of start-order dependencies, see [About the Likewise Agent](#).

You can restart the Likewise network logon daemon by executing the following command at the shell prompt:

```
/opt/likewise/bin/lwsm restart netlogon
```

To stop the daemon, type this command:

```
/opt/likewise/bin/lwsm stop netlogon
```

To start the daemon, type this command:

```
/opt/likewise/bin/lwsm start netlogon
```

9.1.9. Restart the Input-Output Service

The Likewise input-output service -- `lwiod` -- communicates over SMB with SMB servers; authentication is with Kerberos 5.

You can restart the input-output service by executing the following command at the shell prompt:

```
/opt/likewise/bin/lwsm restart lwio
```

To stop the daemon, type this command:

```
/opt/likewise/bin/lwsm stop lwio
```

To start the daemon, type this command:

```
/opt/likewise/bin/lwsm start lwio
```

9.2. Logging

Logging can help identify and solve problems. There are debug logs for the following services in Likewise Open and Likewise Enterprise:

- **lsass**, the authentication service. Generate a debug log for lsass when you need to troubleshoot authentication errors or failures.
- **PAM**, the pluggable authentication modules used by Likewise. Create a debug log for PAM when you need to troubleshoot logon or authentication problems.
- **netlogon**: Generate a debug log for netlogon, the site affinity service that detects the optimal domain controller and global catalog, when you need to troubleshoot problems with sending requests to domain controllers or getting information from the global catalog.
- **lwio**: The input-output service that manages interprocess communication.
- **eventlog**, the event collection service. Generate a debug log for eventlog to troubleshoot the collection and processing of security events.
- **lwreg**, the Likewise registry service. Generate a debug log for lwreg to troubleshoot ill-fated configuration changes to the registry.
- **lwsm**, the service manager.
- The Mac OS X directory service plug-in

In addition, the following services are part of Likewise Enterprise only -- they are not relevant to troubleshooting problems with Likewise Open:

- **gpagent**, the group policy agent. Generate a debug log for gpagent to troubleshoot the application or processing of group policy objects.
- **eventfwd**, the event forwarding daemon. Generate a debug log to verify the service is properly receiving events and forwarding them to a collector server.
- **reapsysl**, part of the data collection service. Capture a debug log for reapsysl to investigate the collection and processing of events.
- **lwsc**, the smart card service. Gather logging information for the smart card service when card-insertion or card-removal behavior is other than expected.
- **lwpcsl1d**, a daemon that aids in logging on and logging off with a smart card. Gather logging information about it when there is a problem logging on or logging off with a smart card.

The log messages are processed by syslog, typically through the daemon facility. Although the path and file name of the log vary by platform, they typically appear in a subdirectory of `/var/log`. Remember

that when you change the log level of a Likewise service to debug, you must also add the following line to `/etc/syslog.conf`, save it, and then restart the syslog service by running `service syslog restart` at the command line:

***.debug /tmp/debug.log**

Alternatively, you can use the `logfile` option to specify a location and name for the log file, as the procedure to generate an authentication debug log illustrates.

Log levels can be changed both temporarily and permanently. The following log levels are available for most Likewise services: `debug`, `error`, `warning`, `info`, `verbose`, and `trace`. The default is `error`. To troubleshoot, it is recommended that you change the level to `debug`. To conserve disk space, it is recommended that you set the log level back to `error` when you finish troubleshooting.

To temporarily change the log level, you can execute a command for the command line or you can stop the service and then start it up again, specifying the log level you want in the start command. To permanently change the log level, you must modify the service's entry in the Likewise registry.

Instantly Change the Authentication Service's Log Level from the Command Line

You can quickly set the Likewise log level for the Likewise authentication daemon by executing the following command and replacing `level` with one of the available logging levels: `error`, `warning`, `info`, `verbose`, `debug`, `trace`.

Changing the log level on the fly is useful to isolate and capture information when a command or operation fails. If, for example, you run a command and it fails, you can change the log level and then run the command again to get information about the failure.

/opt/likewise/bin/lw-set-log-level newLevel

Example: `/opt/likewise/bin/lw-set-log-level debug`

When you change the log level with the `lw-set-log-level` command, the log level is changed only until the service or the computer restarts. You can use the following command to view the current log level of the authentication service:

/opt/likewise/bin/lw-set-log-level

Syslog messages are logged through the daemon facility. The default setting is `error`.

Instantly Change the Log Level for Other Services

In `/opt/likewise/bin`, there are commands to change the log level of several other services:

Service	Logging Commands in /opt/likewise/bin
netlogon	<code>lwnet-get-log-info</code>
	<code>lwnet-set-log-level</code>
	Example: <code>lwnet-set-log-level debug</code>
Input-output	<code>lwio-get-log-info</code>
	<code>lwio-set-log-level</code>

	Example: <code>lwio-set-log-level debug</code>
Event forwarding	<code>evtfwd-get-log-info</code> <code>evtfwd-set-log-level</code> Example: <code>evtfwd-set-log-level debug</code>
Group policy	<code>gp-set-log-level</code> Example: <code>gp-set-log-level debug</code>
System log reaper for the reporting services	<code>rsys-get-log-info</code> <code>rsys-set-log-level</code> Example: <code>rsys-set-log-level debug</code>

Change the Log Level to Debug Until the Service Restarts

The following example demonstrates how to change the log level to debug to help troubleshoot a Likewise service. The change is temporary: The service returns to the level specified in the registry when the service restarts. Although this example changes the log level for the site affinity service (netlogon), which detects the optimal domain controller and global catalog, you can use this method to change the log level for the following Likewise daemons: eventlogd, lsassd, lwiod, netlogond, gpagentd, reapsysld, eventfwdd. (See the topics on how to change the log level for the authentication service (lsass) or the group policy agent (gpagentd).)

1. As root, stop the site affinity service with the Likewise service manager:

```
/opt/likewise/bin/lwsm stop netlogon
```

2. As root, restart the site affinity daemon and specify the log level and the target log file:

```
/opt/likewise/sbin/netlogond --loglevel debug --logfile /tmp/
netlogond.log --start-as-daemon
```

3. After you finish troubleshooting, use the kill command to stop the daemon and then start it again with the service manager to return the log level to its default:

```
/opt/likewise/bin/lwsm start netlogon
```

Note: Leaving the log level at `info`, `debug` or `verbose` might result in disk space issues.

Permanently Change the Log Level by Editing the Registry

The following example demonstrates how to change the log level to debug by modifying a daemon's arguments in the Likewise registry. You can modify the log level in the registry if you want to permanently change a daemon's log level or log file destination: The log level that you set persists after you restart the service or the computer.

Although the example permanently changes the log level for the authentication service, you can use this method to change the log level and log file location for the following Likewise daemons: eventlogd, lsassd, lwiod, netlogond, gpagentd, reapsysld, eventfwdd.

In the registry, the default setting for lsass looks like this, viewed here by using the registry shell's `ls` command combined with the path to the lsass key:

```
/opt/likewise/bin/lwregshell ls -'[HKEY_THIS_MACHINE\Services\lsass]'
[HKEY_THIS_MACHINE\Services\lsass]
"Arguments"="/opt/likewise/sbin/lsassd ---syslog"
"Autostart"=dword:00000001
"Dependencies"="netlogon lwio lwreg rdr npfs"
"Description"="Likewise Security and Authentication Subsystem"
"Environment"=""
"FdLimit"=dword:00000400
"Path"="/opt/likewise/sbin/lsassd"
"Type"=dword:00000001
```

Notice that the default logging target is syslog. You can change the value by executing the registry shell's `set_value` command from the command line, like this:

```
/opt/likewise/bin/lwregshell set_value '[HKEY_THIS_MACHINE\Services\lsass]' Arguments "/opt/likewise/sbin/lsassd --logfile /tmp/lsasslog.txt --loglevel debug"
```

The value of Arguments has been updated to the specified value:

```
/opt/likewise/bin/lwregshell ls -'[HKEY_THIS_MACHINE\Services\lsass]'
[HKEY_THIS_MACHINE\Services\lsass]
-"Arguments"      REG_SZ      -"/opt/likewise/sbin/lsassd ---logfile -/tmp/lsasslog.txt ---loglevel debug"
-"Autostart"      REG_DWORD    0x00000001 (1)
-"Dependencies"   REG_SZ      -"netlogon lwio lwreg rdr npfs"
-"Description"    REG_SZ      -"Likewise Security and Authentication Subsystem"
-"Environment"    REG_SZ      -""
-"FdLimit"        REG_DWORD    0x00000400 (1024)
-"Path"           REG_SZ      -"/opt/likewise/sbin/lsassd"
-"Type"           REG_DWORD    0x00000001 (1)
```

After you modify a registry setting for a Likewise service, you must refresh the corresponding service with the Likewise Service Manager for the changes to take effect.

Note: Permanently changing the log level to info, debug or verbose will likely result in issues with disk space over time.

9.2.1. Generate a Domain-Join Log

To help troubleshoot problems with joining a domain, you can use the command-line utility's `logfile` option with the `join` command. The `logfile` option captures information about the attempt to join the domain on the screen or in a file. When an attempt to join a domain fails, a log is generated by default at `/var/log/likewise-join.log`.

- To display the information in the terminal, execute the following command; the dot after the `logfile` option denotes that the information is to be shown in the console:

```
domainjoin-cli --logfile . join domainName userName
```

- To save the information in a log file, execute the following command:

```
domainjoin-cli --logfile path join domainName userName
```

Example:

```
domainjoin-cli --logfile /var/log/domainjoin.log join
likewisedemo.com Administrator
```

9.2.2. Generate an Authentication Agent Debug Log

You can specify the level of logging for the Likewise authentication daemon's interaction with PAM. Running the authentication daemon in debug mode can help troubleshoot the lookup of a user or group ID as well as help solve other authentication problems.

The following log levels are available: `debug`, `error`, `warning`, `info`, `verbose`, and `trace`. The default is `error`. To troubleshoot, it is recommended that you change the level to `debug`.

The log messages are processed by `syslog`. Although the path and file name of the log vary by platform, they typically appear in a subdirectory of `/var/log`. Alternatively, you can use the `logfile` option to specify a location and name for the log file, as the following procedure demonstrates:

1. As root, stop the authentication service.
2. As root, restart the authentication service and specify the log level and the target log file:

```
/opt/likewise/sbin/lsassd --loglevel debug --logfile /tmp/lsassd.log
--start-as-daemon
```

3. After you finish troubleshooting, use the `kill` command to stop the daemon and then start it again with the service manager to return the log level to its default.

Note: Leaving the log level at `info`, `debug` or `verbose` might result in disk space issues over time.

9.2.3. Generate a PAM Debug Log

You can set the level of reporting in the PAM debug log for the Likewise authentication daemon on a Linux or Unix computer. PAM stands for pluggable authentication modules.

The log levels are `disabled`, `error`, `warning`, `info`, and `verbose`. The logged data is sent to your system's `syslog` message repository for security and authentication. The location of the repository varies by operating system. Here are the typical locations for a few platforms:

- Ubuntu: `/var/log/auth.log`
- Red Hat: `/var/log/secure`
- Solaris: `/var/log/authlog`
- Mac OS X: `/var/log/secure.log`

The following procedure demonstrates how to change the value of the PAM key's `LogLevel` entry with the `lwconfig` command-line utility.

First, use the `details` option to list the values that the `DomainManagerIgnoreAllTrusts` setting accepts:

```
/opt/likewise/bin/lwconfig ---details PAMLogLevel
Name: PAMLogLevel
```

```
Description: Configure PAM lsass logging detail level
Type: string
Current Value: -"disabled"
Acceptable Value: -"disabled"
Acceptable Value: -"error"
Acceptable Value: -"warning"
Acceptable Value: -"info"
Acceptable Value: -"verbose"
Current Value is determined by local policy.
```

Now, as root change the setting to error so that Likewise will log PAM errors:

```
/opt/likewise/bin/lwconfig PAMLogLevel error
```

Finally, confirm that the change took effect:

```
/opt/likewise/bin/lwconfig ---show PAMLogLevel
string
error
local policy
```

For more information on the arguments of lwconfig, run the following command:

```
/opt/likewise/bin/lwconfig --help
```

9.2.4. Generate a Directory Service Log on a Mac

To troubleshoot logon failures on a Mac OS X computer, you can generate a debug-level directory service log. For information on turning on debug-level logs, see [Enabling Directory Service Debug Logging](#) on the Apple support web site.

Using the `killall -USR1` command that Apple suggests, however, puts the directory service into debug logging mode for only about 5 minutes. Instead, try using the following commands:

```
sudo touch -/Library/Preferences/DirectoryService/.DSLogDebugAtStart
sudo killall DirectoryService
```

Reproduce the error and then scan the logs named `DirectoryService.debug.log` in `/Library/Logs/DirectoryService`. Look for messages containing the string `LWEDS`, which indicates that they are produced by the Likewise directory service plug-in.

Examine the logs from the time the user entered a password. If the logs suggest that there may be a networking issue, obtain a `tcpdump` from the time the password is entered until you notice the logon failure:

```
tcpdump --s0 --wnetwork.pcap
```

When you are done troubleshooting, turn off debug logging and restart the directory service by issuing the following commands:

```
sudo rm -/Library/Preferences/DirectoryService/.DSLogDebugAtStart
sudo killall DirectoryService
```

9.2.5. Log Group Policy Debugging Data

You can generate a group policy agent debug log for Likewise Enterprise by running these commands in this order as root:

```
/opt/likewise/bin/lwsm stop gpagent
/opt/likewise/sbin/gpagentd ---loglevel debug ---logfile -/tmp/
gpagentd.log ---start-as-daemon
```

When you are done logging the information, use the `kill` command to stop the service and return the log level to its default setting. Then start the group policy daemon with the Likewise service manager:

```
/opt/likewise/bin/lwsm start gpagent
```

9.2.6. Generate a Network Trace

Execute the following command in a separate session to dump network traffic as the root user and interrupt the trace with CTRL-C:

```
tcpdump -s 0 -i eth0 -w trace.pcap
```

The result should look something like this:

```
tcpdump: listening on eth0
28 packets received by filter
0 packets dropped by kernel
```

9.3. Basics

9.3.1. Check the Version and Build Number

Check the Version and Build Number of the Agent on Linux, Unix, or Mac

To check the version number of the Likewise agent, execute the following command:

```
cat /opt/likewise/data/VERSION
```

Another option is to execute the following command:

```
/opt/likewise/bin/lw-get-status
```

Check the Version and Build Number of the Agent with ADUC

You can check the version and build number of the Likewise agent from a Windows administration workstation that is connected to your domain controller:

1. In Active Directory Users and Computers, right-click the Linux, Unix, or Mac computer that you want, and then click **Properties**.
2. Click the **Operating System** tab. The build number is shown in the **Service pack** box.

Check the Build Number of the Agent

On Linux distributions that support RPM -- for example, Red Hat Enterprise Linux, Fedora, SUSE Linux Enterprise, OpenSUSE, and CentOS -- you can determine the version and build number of the agent (5.0.0.xxxx in the examples below) by executing the following command at the shell prompt:

```
rpm -qa | grep likewise
```

The result shows the build version after the version number:

```
likewise-sqlite-5.0.0-1.26353.3513
likewise-libxml2-5.0.0-1.26353.3513
likewise-netlogon-5.0.0-1.26353.3513
likewise-openldap-5.0.0-1.26353.3513
likewise-pstore-5.0.0-1.26353.3513
likewise-passwd-5.0.0-1.26353.3513
likewise-domainjoin-5.0.0-1.26353.3513
likewise-lsass-5.0.0-1.26353.3513
likewise-krb5-5.0.0-1.26353.3513
likewise-base-5.0.0-1.26353.3513
likewise-rpc-5.0.0-1.26353.3513
```

On Unix computers and Linux distributions that do not support RPM, the command to check the build number varies by platform:

Platform	Command
Debian and Ubuntu	<code>dpkg -S /opt/likewise/</code>
Solaris	<code>pkginfo grep -i likewise</code>
AIX	<code>lspp -l grep likewise</code>
HP-UX	<code>swlist grep -i likewise</code>

9.3.2. Determine a Computer's FQDN

You can determine the fully qualified domain name of a computer running Linux, Unix, or Mac OS X by executing the following command at the shell prompt:

```
ping -c 1 `hostname`
```

On HP-UX

The command is different on HP-UX:

```
ping `hostname` -n 1
```

On Solaris

On Sun Solaris, you can find the FQDN by executing the following command (the computer's configuration can affect the results):

```
FQDN=`/usr/lib/mail/sh/check-hostname|cut -d" " -f7`;echo $FQDN
```

See Also

Join Active Directory Without Changing /etc/hosts

9.3.3. Make Sure Outbound Ports Are Open

If you are using local firewall settings, such as `iptables`, on a computer running the Likewise agent, make sure the following ports are open for outbound traffic.

Note: The Likewise agent is a client only; it does not listen on any ports.

Port	Protocol	Use
53	UDP/ TCP	DNS
88	UDP/TCP	Kerberos 5
123	UDP	NTP
137	UDP	NetBIOS Name Service
139	TCP	NetBIOS Session (SMB)
389	UDP/TCP	LDAP
445	TCP	SMB over TCP
464	UDP/TCP	Machine password changes (typically after 30 days)
3268	TCP	Global Catalog search

Tip: To view the firewall rules on a Linux computer using `iptables`, execute the following command:

```
iptables -nL
```

9.3.4. Check the File Permissions of `nsswitch.conf`

For Likewise to work correctly, the `/etc/nsswitch.conf` file must be readable by user, group, and world. The following symptoms indicate that you should check the permissions of `nsswitch.conf`:

- Running the `id` command with an AD account as the argument (example: `id likewisedemo.com\kathy`) works when it is executed as root, but when the same command is executed by the AD user, it returns only a UID and GID without a name.
- Getting an "I have no name!" or "intruder alert" error message for non-root users.
- On HP-UX, running the `whoami` command with an AD user account returns "Intruder alert."

9.3.5. Configure SSH After Upgrading It

After SSH is upgraded, run the following command as root to make sure that the `sshd_config` file is set up properly to work with Likewise:

```
domainjoin-cli configure --enable ssh
```

9.3.6. Upgrading an Operating System

After upgrading an operating system or installing a kernel patch, you should rerun the `domain-join` command to make sure that the files related to the operating system, such as PAM and `nsswitch`, are configured properly to work with Likewise. Re-executing the `domain-join` command also updates the `operatingSystemVersion` value and the `operatingSystemServicePack` value in Active Directory so the Likewise reporting tool reflects the correct version numbers.

Another suggestion, nearly universal in scope, is to apply updates to test systems before you apply updates to production systems, giving you the opportunity to identify and resolve potential issues before they can affect production machines.

9.4. Accounts

9.4.1. Allow Access to Account Attributes

Likewise Enterprise is compatible with Small Business Server 2003. However, because the server locks down several user account values by default, you must create a group in Active Directory for your Unix computers, add each Likewise client computer to it, and configure the group to read all user information.

On other versions of Windows Server, the user account values are available by default. If, however, you use an AD security setting to lock them down, they will be unavailable to the Likewise agent.

To find Unix account information, the Likewise agent requires that the AD computer account for the machine running Likewise can access the attributes in the following table.

Attribute	Requirement
uid	Required when you use Likewise Enterprise in schema mode.
uidNumber	Required when you use Likewise Enterprise in schema mode.
gidNumber	Required when you use Likewise Enterprise in schema mode.
userAccountControl	Required for schema mode and non-schema mode. It is also required for unprovisioned mode, which means that you have not created a Likewise cell in Active Directory, as will be the case if you are using Likewise Open .

Allow Access to Account Attributes

1. In Active Directory Users and Computers, create a group named `Unix Computers`.
2. Add each Likewise client computer to the group.
3. In the console tree, right-click the domain, choose **Delegate Control**, click **Next**, click **Add**, and then enter the group named `Unix Computers`.
4. Click **Next**, select **Delegate the following common tasks**, and then in the list select **Read all user information**.
5. Click **Next**, and then click **Finish**.
6. On the target Unix, Linux, or Mac computer, restart the Likewise agent to reinitialize the computer account's logon to Active Directory and to get the new information about group membership.
7. Run `/opt/likewise/lw-enum-users` to verify that you can read user information.

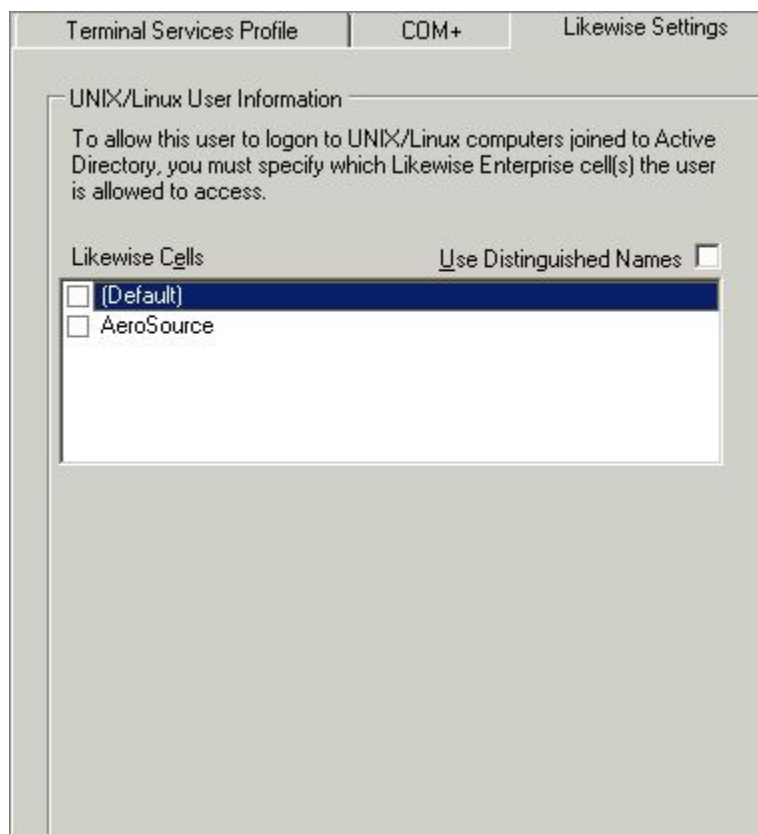
See Also

About Schema Mode and Non-Schema Mode

9.4.2. A User's Settings Are Not Displayed in ADUC

If there is no group in a cell that can serve as the user's primary GID -- for instance, because the default primary group, domain users, has been removed from the cell -- the Likewise Settings tab for a user in

ADUC will not display the user or group settings, as shown in the screen shot below. To display the settings, enable a group that the user is a member of.



9.4.3. Resolve an AD Alias Conflict with a Local Account

When you use Likewise to set an Active Directory alias for a user, the user can have a file-ownership conflict under the following conditions if the user logs on with the AD account:

- The AD alias is the same alias as the original local account name.
- The home directory assigned to the user in Active Directory is the same as the local user's home directory.
- The owner UID-GID of the AD account is different from that of the local account.

To avoid such conflicts, by default Likewise includes the short AD domain name in each user's home directory. If the conflict nevertheless occurs, there are two options to resolve it:

1. Make sure that the UID assigned to the user's AD alias is the same as that of the user's local account. See Specify a User's ID and Unix or Linux Settings.
2. Log on as root and use the `chown` command to recursively change the ownership of the local account's resources to the AD user alias.

Change Ownership

Log on the computer as root and execute the following commands:

```
cd <users home directory root>
```

```
chown -R <AD user UID>:<AD primary group ID> *.*
```

```
Or: chown -R <short domain name>\\<account name>:<short domain name>\
\\<AD group name> *.*
```

See Also

Show Duplicate UIDs, GIDs, Login Names, and Group Aliases

9.4.4. Fix the Shell and Home Directory Paths

Symptom: A local directory is in the home directory path and the home directory path does not match the path specified in Active Directory or in `/etc/passwd`.

Example: `/home/local/DOMAIN/USER` instead of `/home/DOMAIN/USER`

The shell might also be different from what is set in Active Directory -- for example, `/bin/ksh` instead of `/bin/bash`.

Problem: The computer is not in a Likewise cell in Active Directory.

Solution: Make sure the computer is in a Likewise cell. For more information, see Associate a Cell with an OU or a Domain, or create a default cell.

A default cell handles mapping for computers that are not in an OU with an associated cell. The default cell can contain the mapping information for all your Linux and Unix computers. For instance, a Linux or Unix computer can be a member of an OU that does not have a cell associated with it. In such a case, the home directory and shell settings are obtained from the nearest parent cell or the default cell. If there is no parent cell and no default cell, the computer will not receive its shell and home directory paths from Active Directory.

See Also

Set the Default Home Directory and Login Shell

9.4.5. Troubleshooting with the Get Status Command

The `/opt/likewise/bin/lw-get-status` command shows whether the domain or the Likewise AD provider is offline. The results of the command include information useful for general troubleshooting.

`/opt/likewise/bin/lw-get-status`

Here's an example of the information the command returns:

```
[root@rhel5d bin]# -/opt/likewise/bin/lw-get-status
LSA Server Status:
Compiled daemon version: 6.1.272.54796
Packaged product version: 6.1.272.54796
Uptime:                15 days 21 hours 24 minutes 1 seconds

[Authentication provider: lsa-activedirectory-provider]

Status:                Online
Mode:                  Un-provisioned
Domain:                LIKEWISEDEMO.COM
Forest:                likewisedemo.com
Site:                  Default-First-Site-Name
```

```

Online check interval:  300 seconds
[Trusted Domains: 1]

[Domain: LIKEWISEDEMO]

      DNS Domain:          likewisedemo.com
      Netbios name:        LIKEWISEDEMO
      Forest name:         likewisedemo.com
      Trustee DNS name:
      Client site name: Default-First-Site-Name
      Domain SID:
S-1-5-21-3190566242-1409930201-3490955248
      Domain GUID:         71c19eb5-1835-f345-ba15-0595fb5b62e3
      Trust Flags:         [0x000d]
                           [0x0001 -- In forest]
                           [0x0004 -- Tree root]
                           [0x0008 -- Primary]
      Trust type:          Up Level
      Trust Attributes:    [0x0000]
      Trust Direction:     Primary Domain
      Trust Mode:          In my forest Trust (MFT)
      Domain flags:        [0x0001]
                           [0x0001 -- Primary]

[Domain Controller (DC) Information]

      DC Name:             w2k3-r2.likewisedemo.com
      DC Address:          192.168.92.20
      DC Site:             Default-First-Site-Name
      DC Flags:            [0x000003fd]
      DC Is PDC:           yes
      DC is time server:   yes
      DC has writeable DS: yes
      DC is Global Catalog: yes
      DC is running KDC:   yes

[Authentication provider: lsa-local-provider]

      Status:              Online
      Mode:                 Local system
      Domain:               RHEL5D
  
```

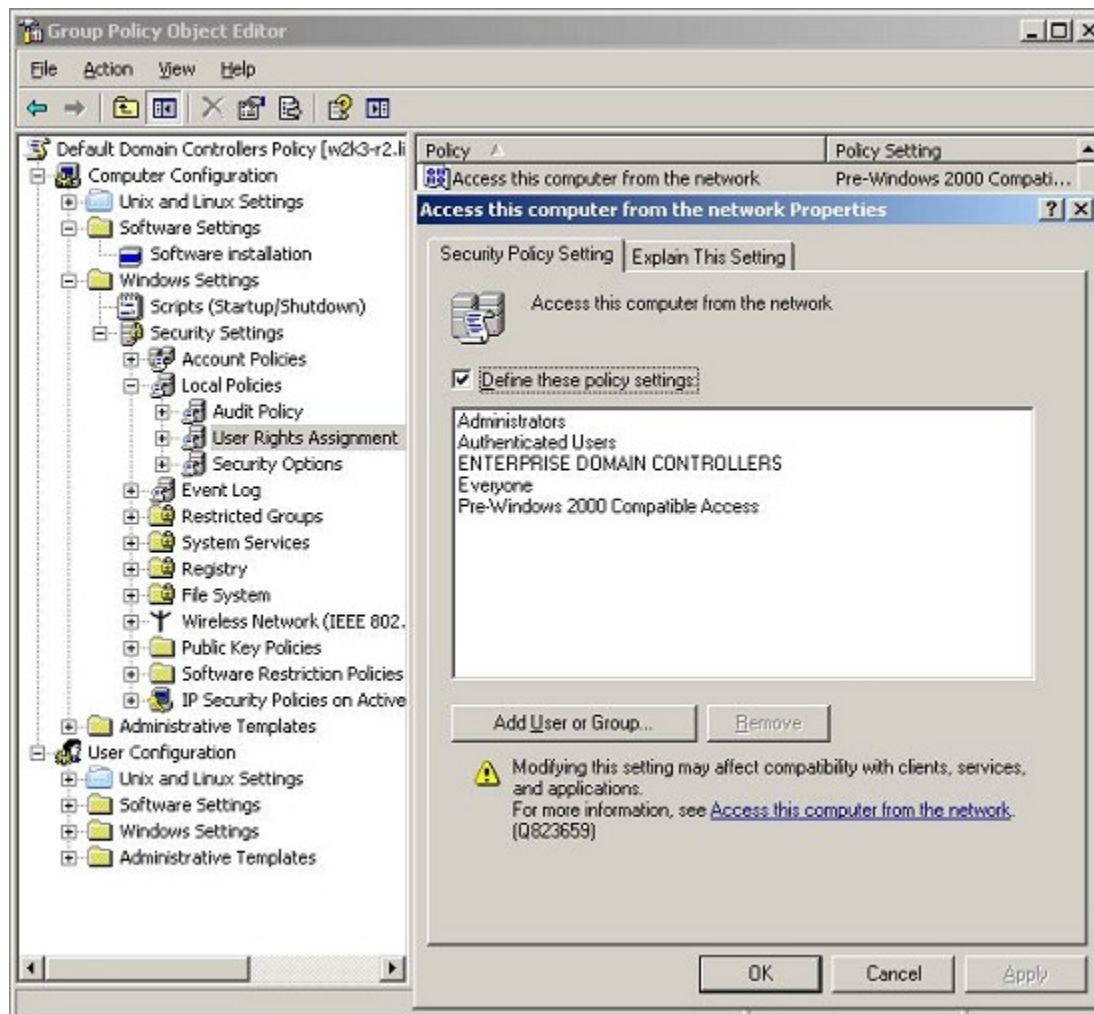
9.4.6. Troubleshoot User Rights with Ldp.exe and Group Policy Modeling

The following Microsoft default domain policies and default domain controller policies can cause a Likewise client to fail to join a domain or to fail to enumerate trusts:

- Access this computer from the network. Users and computers that interact with remote domain controllers require the access-this-computer-from-network user right. Users, computers, and service accounts can lose the user right by being removed from a security group that has been granted the right. Removing the administrators group or the authenticated users group from the policy can cause domain join to fail. Microsoft says, "There is no valid reason for removing Enterprise Domain

Controllers group from this user right." For more information, see <http://support.microsoft.com/kb/823659>.

- Deny access to this computer from the network. Including the domain computers group in the policy, for instance, causes domain-join to fail.



The symptoms of a user-right problem can include the following:

- An attempt to join the domain is unsuccessful.
- The Likewise authentication service, lsass, does not start.
- The `/opt/likewise/bin/lw-get-status` command shows the domain or the AD provider as offline.

You can pin down the issue by using the `ldp.exe` tool to check whether you can access AD by using the machine account and machine password. `Ldp.exe` is typically included in the support tools (`suptools.msi`) for Windows and located on the Windows installation CD (Support folder, Tools subfolder). You might also be able to download the support tools that contain `ldp.exe` from the Microsoft web site.

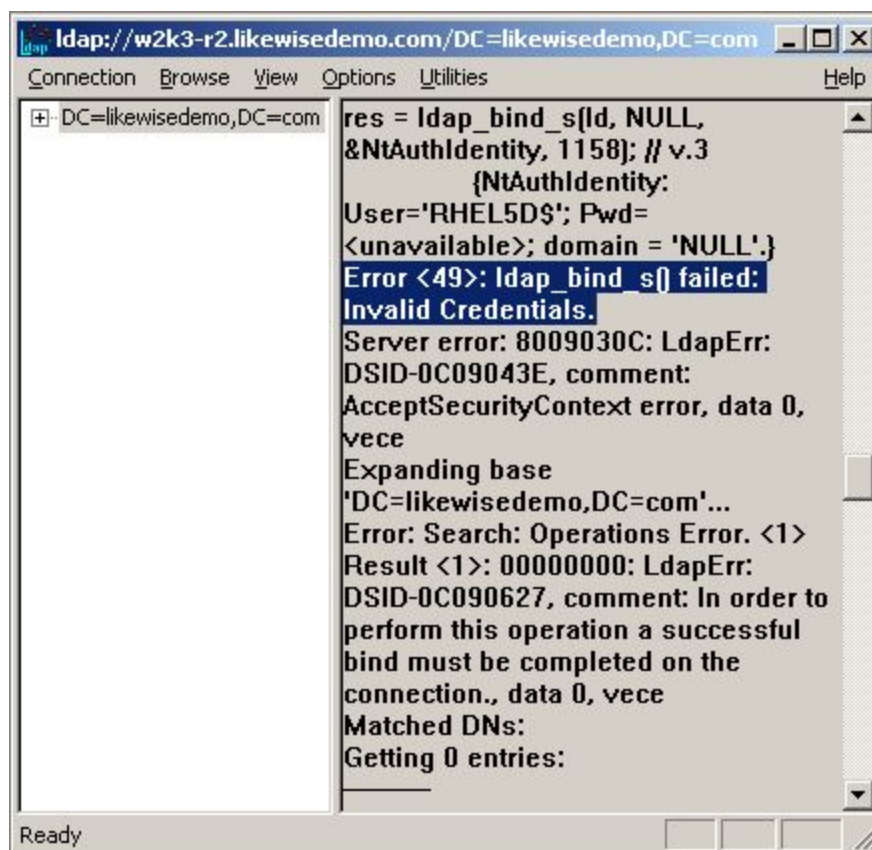
To resolve a user-right issue, you can use group policy modeling in the GPMC to find the offending policy and then modify it with the GPOE.

1. On the Likewise client, run the `/opt/likewise/bin/lw-lsa ad-get-machine password` command as root to get the machine password stored in Active Directory:

```
/opt/likewise/bin/lw-lsa ad-get-machine password
Machine Password Info:
  DNS Domain Name: LIKEWISEDEMO.COM
  NetBIOS Domain Name: LIKEWISEDEMO
  Domain SID: S-1-5-21-3190566242-1409930201-3490955248
  SAM Account Name: RHEL5D$
  FQDN: rhel5d.likewisedemo.com
  Join Type: 1
  Key Version: 0
  Last Change Time: 129401233790000000
  Password: i(2H2e41F7tHN275
```

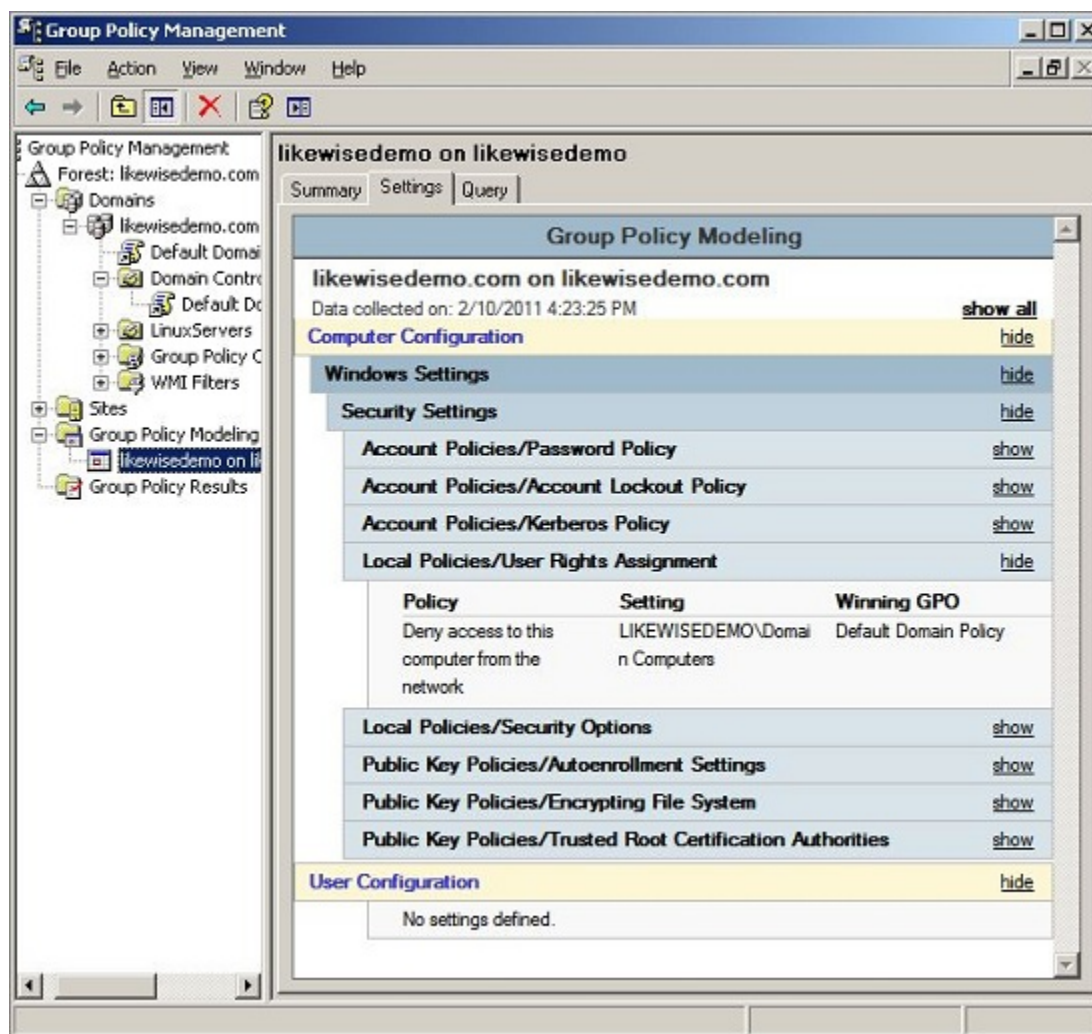
2. On a Windows administrative workstation that can connect to AD, start `ldp.exe` and connect to the domain. (See the LDP UI article for more information.)
3. In LDP, on the **Connection** menu, click **Bind**, and then use the Likewise client's SAM account name and machine password from the output of the `lw-lsa ad-get-machine password` command to bind to the directory.

If the attempt to bind with the machine account and the machine password fails because of invalid credentials, as shown in the LDP output below, go to the Group Policy Management Console and use group policy modeling to try to identify the policy causing the problem.



4. In the GPMC, run the group policy modeling tool to pinpoint the offending policy and then modify the policy to grant the correct level of user right to the computer or user. For more information, see Group Policy Modeling.

In the following screen shot, for example, the cause of the problem is that the deny-access-to-this-computer-from-the-network default domain policy contains the domain computers group.



9.4.7. Fix Selective Authentication in a Trusted Domain

When you turn on selective authentication for a trusted domain, Likewise can fail to look up users in the trusted domain because the machine account is not allowed to authenticate with the domain controllers in the trusted domain. Here's how to grant the machine account access to the trusted domain:

1. In the domain the computer is joined to, create a global group and add the computer's machine account to the group.
2. In the trusted domain, in Active Directory Users and Computers, select the **Domain Controllers** container and open **Properties**.
3. On the **Security** tab, click **Advanced**, click **Add**, enter the global group, and then click **OK**.

4. In the **Permission Entry** box, under **Apply onto**, select **Computer objects**. Under **Permissions**, find **Allowed to Authenticate** and enable it. Click **OK** and then click **Apply** in the **Advanced Security Settings** box.
5. If you have already joined the Likewise client computer to the domain, restart the Likewise authentication service:

```
/opt/likewise/bin/lwsm restart lsass
```

9.5. Cache

9.5.1. Clear the Authentication Cache

There are certain conditions under which you might need to clear the cache so that a user's ID is recognized on a target computer.

By default, the user's ID is cached for 4 hours. If you change a user's UID for a Likewise cell with Likewise Enterprise, during the 4 hours after you change the UID you must clear the cache on a target computer in the cell before the user can log on. If you do not clear the cache after changing the UID, the computer will find the old UID until the cache expires.

There are three Likewise Enterprise group policies that can affect the cache time:

- The Cache Expiration Time, which stores UID-SID mappings, user/group enumeration lists, `getgrnam()` and `getpwnam()`, and so forth. Its default expiration time is 4 hours.
- The ID Mapping Cache Expiration Time, which caches the mapping tables for SIDs, UIDs, and GIDs. Its default is 1 hour. This policy applies only to Likewise Enterprise 4.1 or earlier.
- The ID Mapping Negative Cache Expiration Time, which stores failed SID-UID-GID lookups to prevent an overload of resolution requests. Its default is 5 minutes. This policy applies only to Likewise Enterprise 4.1 or earlier.

Tip: While you are deploying and testing Likewise, set the cache expiration time of the Likewise agent's cache to a short period of time, such as 1 minute.

Clear the Cache on a Unix or Linux Computer

To delete all the users and groups from the Likewise AD provider cache on a Linux or Unix computer, execute the following command with superuser privileges:

```
/opt/likewise/bin/lw-ad-cache --delete-all
```

You can also use the command to enumerate users in the cache, which may be helpful in troubleshooting. Here's an example:

```
[root@rhel5d bin]# ./lw-ad-cache ---enum-users
TotalNumUsersFound:      0
[root@rhel5d bin]# ssh likewisedemo.com\hab@localhost
Password:
Last login: Tue Aug 11 15:30:05 2009 from rhel5d.likewisedemo.com
[LIKEWISEDEMO\hab@rhel5d ~]$ exit
logout
```

```

Connection to localhost closed.
[root@rhel5d bin]# ./lw-ad-cache ---enum-users
User info (Level-0):
=====
Name:      LIKEWISEDEMO\hab
Uid:       593495196
Gid:       593494529
Gecos:     <null>
Shell:     -/bin/bash
Home dir:  -/home/LIKEWISEDEMO/hab
TotalNumUsersFound:      1
[root@rhel5d bin]#

```

To view the command's syntax and arguments, execute the following command:

```
/opt/likewise/bin/lw-ad-cache --help
```

Clear the Cache on a Mac OS X Computer

On a Mac OS X computer, clear the cache by running the following command with superuser privileges in Terminal:

```
dscacheutil -flushcache
```

9.5.2. Clear a Corrupted SQLite Cache

To clear the cache when Likewise is caching credentials in its SQLite database and the entries in the cache are corrupted, use the following procedure for your type of operating system.

Clear the Cache on a Linux Computer

1. Stop the Likewise authentication daemon by executing the following command as root:

```
/opt/likewise/bin/lwsm lsass stop
```

2. Clear the AD-provider cache and the local-provider cache by removing the following two files:

```
rm -f /var/lib/likewise/db/lsass-adcache.db
```

```
rm -f /var/lib/likewise/db/lsass-local.db
```

Important: Do not delete the other .db files in the /var/lib/likewise/db directory.

3. Start the Likewise authentication daemon:

```
/opt/likewise/bin/lwsm lsass start
```

Clear the Cache on a Mac

1. In Terminal, stop the Likewise authentication daemon by executing the following command as sudo:

```
/opt/likewise/bin/lwsm lsass stop
```


2. Clear the AD-provider cache and the local-provider cache by removing the following two files:

```
sudo rm -f /var/lib/likewise/db/lsass-adcache.db
```

```
sudo rm -f /var/lib/likewise/db/lsass-local.db
```

Important: Do not delete the other .db files in the /var/lib/likewise/db directory.

3. Restart the Likewise authentication daemon:

```
/opt/likewise/bin/lwsm lsass start
```

Clear the Cache on a Unix Computer

1. Stop the Likewise authentication daemon by executing the following command as root:

```
/opt/likewise/bin/lwsm stop lsass
```

2. Clear the AD-provider cache and the local-provider cache by removing the following two files:

```
rm -f /var/lib/likewise/db/lsass-adcache.db
```

```
rm -f /var/lib/likewise/db/lsass-local.db
```

Important: Do not delete the other .db files in the /var/lib/likewise/db directory.

3. Start the Likewise authentication daemon:

```
/opt/likewise/bin/lwsm start lsass
```

9.6. Kerberos

The following resources can help troubleshoot time synchronization and other Kerberos issues:

- Kerberos Authentication Tools and Settings:

<http://technet2.microsoft.com/windowsserver/en/library/b36b8071-3cc5-46fa-be13-280aa43f2fd21033.mspx>

- Authentication Errors Caused by Unsynchronized Clocks:

<http://technet2.microsoft.com/windowsserver/en/library/6ee8470e-a0e8-40b2-a84f-dbec6bcbd8621033.mspx>

- Kerberos Technical Supplement for Windows:

<http://msdn2.microsoft.com/en-us/library/aa480609.aspx>

- The Kerberos Network Authentication Service (V5) RFC:

<http://www.ietf.org/rfc/rfc4120.txt>

- Troubleshooting Kerberos Errors:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/tkerberr.mspx>

- Kerberos and LDAP Troubleshooting Tips:

<http://www.microsoft.com/technet/solutionaccelerators/cits/interopmigration/unix/usecdirw/17wsdsu.mspx>

9.6.1. Fix a Key Table Entry-Ticket Mismatch

Problem

When an AD machine account password changes two or more times during the lifetime of a domain user's credentials, the computer's entry that matches the Kerberos service ticket is dropped from the Kerberos key table. Even though the service ticket has not expired, an action that depends on the entry, such as reading the event log or using single sign-on, will fail.

To avoid issues with Kerberos key tables, keytabs, and single sign-on, the machine password expiration time must be at least twice the maximum lifetime for user tickets, plus a little more time to account for the permitted clock skew.

The expiration time for a user ticket is set by using an Active Directory group policy called Maximum lifetime for user ticket. The default user ticket lifetime is 10 hours; the default Likewise machine password lifetime is 30 days.

Causes

The machine account password can change more frequently than the user's AD credentials under the following conditions:

1. Joining a domain two or more times.
2. Setting the expiration time of the machine account password group policy to be less than twice the maximum lifetime of user tickets. For more information, see [Set the Machine Account Password Expiration Time](#).
3. Setting the local `machine-password-lifespan` for the `lsass` service in the Likewise registry to be less than twice the maximum lifetime for user tickets.

Solution

If a computer's entry is dropped from the Kerberos key table, you must remove the unexpired service tickets from the user's credentials cache by reinitializing the cache. Here's how:

On Linux and Unix, reinitialize the credentials cache by executing the following command with the account of the user who is having the problem:

```
/opt/likewise/bin/kinit
```

On Mac, you must run both the native `kinit` command and the Likewise `kinit` command with the account of the user who is having the problem. You must run both commands because the native `ssh` client uses the native credentials cache while the Likewise processes, such as those that access the event log, use the MIT credentials cache:

```
/opt/likewise/bin/kinit
kinit
```

9.6.2. Fix KRB Error During SSO in a Disjoint Namespace

When you are working in a network with a disjoint namespace in which the Active Directory domain name is different from the DNS domain suffix for computers, you may need to modify the `domain_realm` section of `/etc/krb5.conf` on your target computer even though your DNS A and PTR records are correct for both DNS domains and can be found both ways.

The following error, in particular, indicates that you might have to modify your `krb5.conf` file before single sign-on (with SSH, for example) will work:

```
KRB ERROR BAD OPTION
```

Assume your computer's Active Directory domain is `bluesky.likewisedemo.com` and your computer's FQDN is `somehostname.green.likewisedemo.com` and you have already created the following entries in DNS:

```
_kerberos._tcp.green.likewisedemo.com 0 100 389
ad2.bluesky.likewisedemo.com
_kerberos._udp.green.likewisedemo.com 0 100 389
ad2.bluesky.likewisedemo.com
```

Meantime, on the target computer, the `[domain_realm]` entry of your `/etc/krb5.conf` file looks like this:

```
[domain_realm]
.bluesky.likewisedemo.com = BLUESKY.LIKEWISEDEMO.COM
bluesky.likewisedemo.com = BLUESKY.LIKEWISEDEMO.COM
```

To resolve the error, add the following two lines to the `[domain_realm]` entry of your `/etc/krb5.conf` file:

```
.green.likewisedemo.com = BLUESKY.LIKEWISEDEMO.COM
green.likewisedemo.com = BLUESKY.LIKEWISEDEMO.COM
```

After adding the two lines above, the complete `[domain_realm]` entry now looks like this:

```
[domain_realm]
.bluesky.likewisedemo.com = BLUESKY.LIKEWISEDEMO.COM
bluesky.likewisedemo.com = BLUESKY.LIKEWISEDEMO.COM
.green.likewisedemo.com = BLUESKY.LIKEWISEDEMO.COM
green.likewisedemo.com = BLUESKY.LIKEWISEDEMO.COM
```

Finally, make sure that you have a correct `.k5login` file and then try to log on again.

9.6.3. Eliminate Logon Delays When DNS Connectivity Is Poor

If connectivity to your DNS servers is tenuous or becomes unavailable, name resolution can time out, delaying the logon process. Because Active Directory is heavily dependent on a well-functioning DNS system, you should work to resolve your DNS issues.

If you cannot fix your DNS system, however, you can as a last resort set up a caching-forwarding name server on the Likewise client to eliminate the logon delay. For instance, you can set up a BIND server on each Linux or Unix computer on which you are running Likewise. Then you can configure BIND

as a local caching resolver and add your nameserver addresses to the forwarder list, leaving `/etc/resolv.conf` with only the local loopback address:

```
search likewisedemo.com
nameserver 127.0.0.1
```

For instructions on how to set up BIND, see the BIND documentation.

9.7. PAM

For instructions on how to generate a PAM debug log, see the section on Logging.

9.7.1. Dismiss the Network Credentials Required Message

After leaving the screen saver on a Gnome desktop that is running the Gnome Display Manager, or GDM, you might see a pop-up notification saying that network authentication is required or that network credentials are required. You can ignore the notification. The GDM process that tracks the expiration time of a Kerberos TGT might not recognize the updated expiration time of a Kerberos TGT after it is refreshed by Likewise.

9.8. Red Hat and CentOS

9.8.1. Modify PAM to Handle UIDs Less Than 500

By default, the configuration file for PAM system authentication – `/etc/pam.d/system-auth` – on Red Hat Enterprise Linux 5 and CentOS 5 contains the following line, which blocks a user with a UID value less than or equal to 500 from logging on to a computer running the Likewise agent. The symptom is a login failure with a never-ending password prompt.

```
auth requisite pam_succeed_if.so uid >= 500 quiet
```

Solution: Either delete the line from `/etc/pam.d/system-auth` or modify it to allow users with UIDs lower than 500:

```
auth requisite pam_succeed_if.so uid >= 50 quiet
```

For more information on the PAM test of account characteristics, see http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/sag-pam_succeed_if.html.

9.9. SLED

9.9.1. A Note About the Home Directory on SLED 11

SUSE Linux Enterprise Desktop 11 includes Likewise Enterprise. When a user gains access to SLED 11 through Nomad -- a remote desktop using RDP protocol with session management -- the default home directory specified in `/lib/security/pam_lsass.so` is ignored. To correct the issue, change `/etc/pam.d/xrdp-sesman` to include the following line:

```
session sufficient /lib/security/pam_lsass.so
```

9.9.2. Updating PAM on SLED 11

SUSE Linux Enterprise Desktop 11 includes Likewise Enterprise. Novell has issued a PAM update (pam-config-0.68-1.22) for SLED 11 that modifies the common-session-pc file to include the following entry:

```
session optional pam_gnome_keyring.so auto_start_if=gdm
```

Because the PAM update makes a backup of the file and replaces it with the modified version, the changes that Likewise had made to the file are no longer present, which blocks new AD users from logging on. The following error messages may appear:

```
Could not update ICEauthority file -/home/john/.ICEauthority
There is a problem with the configuration server.
(/user/lib/gconf/2/gconf-sanity-check-2 exited with status 256)
```

Solution: After you update PAM, run the following command as root:

```
/opt/likewise/bin/domainjoin-cli configure --enable pam
```

Or, you can make the changes manually: Open the backed up version of the common-session-pc file, add the following line to it, and then use it to overwrite the new version of the common-session-pc file:

```
session optional          pam_gnome_keyring.so      auto_start_if=gdm
```

9.10. AIX

9.10.1. Increase Max Username Length on AIX

By default, AIX is not configured to support long user and group names, which might present a conflict when you try to log on with a long Active Directory username. On AIX 5.3 and AIX 6.1, the symptom is that group names, when enumerated through the `groups` command, are truncated.

To increase the max username length on AIX 5.3, use the following syntax:

```
# chdev -l sys0 -a max_logname=MaxUserNameLength+1
```

Example:

```
# chdev -l sys0 -a max_logname=255
```

This command allocates 254 characters for the user and 1 for the terminating null.

The safest value to which you can set `max_logname` is 255.

You must reboot for the changes to take effect:

```
# shutdown -Fr
```

Note: AIX 5.2 does not support increasing the maximum user name length.

9.10.2. Updating AIX

When you update AIX, the authentication of users, groups, and computers might fail because the AIX upgrade process overwrites changes that Likewise makes to system files. Specifically, upgrading AIX to

version 6.1tl3 overwrites `/lib/security/methods.cfg`, so you must manually add the following code to the last lines of the file after you finish upgrading:

```
LSASS:
    program = -/usr/lib/security/LSASS
```

9.11. Mac OS X

9.11.1. Find the Likewise Service Manager Daemon on a Mac

To locate the Likewise service manager process on a Mac OS X computer, execute the following command in Terminal:

```
sudo launchctl list | grep likewise
```

On a Mac computer, the name of the daemon for the service manager is as follows:

```
com.likewiseoftware.lwsmd
```

9.12. FreeBSD

9.12.1. Keep Usernames to 16 Characters or Less

On FreeBSD, user names that are longer than 16 characters, including the domain name, exceed the FreeBSD username length limit. Attempts to connect by ssh, for example, to a FreeBSD computer with a user name that exceeds the limit can result in the following notification:

```
bvt-fbs72-64# ssh testuser1@localhost
Password:
Connection to localhost closed by remote host.
Connection to localhost closed.
```

The log for sshd, meanwhile, might show an error that looks something like this:

```
Oct  7 18:22:57 vermont02 sshd[66387]: setlogin(LIKEWISEDEMO
\adm.kathy):
Invalid argument
Oct  7 18:25:02 vermont02 sshd[66521]: setlogin(LIKEWISEDEMO
\adm.kathy):
Invalid argument
```

Although `testuser1` is less than 16 characters, when you use the `id` command to check the account, something longer than 16 characters is returned:

```
[root@bvt-fbs72-64 ~/home/testuser]# id testuser1
uid=1100(BVT-FBS72-64\testuser1) gid=1801(BVT-FBS72-64\testgrp)
groups=1801(BVT-FBS72-64\testgrp)
```

The result of the `id` command exceeds the FreeBSD username length limit.

There are several solutions: set the default domain, change the user name to 16 characters or less, or with Likewise Enterprise use aliases. Keep in mind, though, that aliases will not solve the problem in relation to the Likewise local provider.

9.13. Solaris

9.13.1. Turn On Core Dumps on Solaris 10

If you are investigating a process that is crashing on Solaris 10 or Solaris Sparc 10, but a core dump is not being generated, it's probably because per-process core dumps are turned off. You can use the `coreadm` command to manage the core dumps. The settings are saved in the `/etc/coreadm.conf` file.

A configuration for core dumps with the per-process option turned off looks like this:

```
# coreadm
  global core file pattern:
  global core file content: default
    init core file pattern: core
    init core file content: default
      global core dumps: disabled
    per-process core dumps: disabled
  global setid core dumps: disabled
per-process setid core dumps: disabled
  global core dump logging: disabled
```

You'll need per-process core dumps, though, to troubleshoot a process that is terminating unexpectedly. To turn on core dumps for a process, execute the following command as root:

`coreadm -e process`

For more information, see Core Dump Management on the Solaris OS and the man page for `coreadm`.

Chapter 10. Command-Line Reference

This chapter presents an overview of the commands in `/opt/likewise/bin`. Most of the commands are intended to be run as root. Additional troubleshooting information, some of which involves command-line utilities, is in *Troubleshooting the Agent*.

The group policy commands for Likewise Enterprise are not included in this chapter; they are in *Troubleshooting the Group Policy Agent*. The commands for managing the event log are in *Monitoring Events with the Event Log*.

For an overview of commands such as `rpm` and `dpkg` that can help you manage Likewise on Linux and Unix platforms, see *Package Management Commands*.

10.1. lwsm: Manage Services

The Likewise Service Manager lets you track and troubleshoot all the Likewise services with a single command-line utility. You can, for instance, check the status of the services and start or stop them. The service manager is the preferred method for restarting a service because it automatically identifies a service's dependencies and restarts them in the right order. In addition, you can use the service manager to set the logging destination and the log level.

To list the status of the services, run the following command with superuser privileges at the command line:

`/opt/likewise/bin/lwsm list`

Example:

```
[root@rhel5d bin]# -/opt/likewise/bin/lwsm list
lwreg      running (standalone: 1920)
dcerpc     running (standalone: 2544)
eventlog   running (standalone: 2589)
lsass      running (standalone: 2202)
lwio       running (standalone: 2191)
netlogon   running (standalone: 2181)
npfs       running (io: 2191)
pvfs       stopped
rdr        running (io: 2191)
srv        stopped
srvsvc     stopped
```

To restart the `lsass` service, run the following command with superuser privileges:

`/opt/likewise/bin/lwsm restart lsass`

After you change a setting in the registry, you must use the service manager to force the service to begin using the new configuration by executing the following command with super-user privileges. This example refreshes the `lsass` service:

`/opt/likewise/bin/lwsm refresh lsass`

To view information about the `lsass` service, including its dependencies, run the following command:

`/opt/likewise/bin/lwsm info lsass`

Example:

```
[root@rhel5d bin]# -/opt/likewise/bin/lwsm info lsass
Service: lsass
Description: Likewise Security and Authentication Subsystem
Type: executable
Autostart: no
Path: -/opt/likewise/sbin/lsassd
Arguments: -'/opt/likewise/sbin/lsassd' -'--syslog'
Dependencies: netlogon lwio lwreg rdr npfs
```

To view all the service manager's commands and arguments, run the following command:

```
/opt/likewise/bin/lwsm --help
```

10.2. lwconfig

To quickly change an end-user setting in the registry for the Likewise agent, you can run the `lwconfig` command-line tool as root:

```
/opt/likewise/bin/lwconfig
```

For more information, see [Modify Settings with the lwconfig Tool](#).

10.3. lwregshell: The Registry Shell

You can access and modify the Likewise registry by using the registry shell -- `lwregshell`. The shell works in a way that is similar to BASH. You can view a list of the commands that you can execute in the shell by entering `help`:

```
/opt/likewise/bin/lwregshell
\> help
```

You can also manage the registry by executing the registry's commands from the command line. For more information, see [Configuring the Likewise Services with the Registry](#).

10.4. lw-edit-reg: Export the Registry to Your Editor

Executing the following command exports the contents of the Likewise registry to the editor specified by your `EDITOR` environment variable. You can use the `lw-edit-reg` command to quickly view the contents of the registry and make changes to the settings. Then, you can launch the registry shell and import the modified file so that your changes take effect.

```
/opt/likewise/bin/lw-edit-reg
```

If you have not set a default editor, the script searches for an available editor in the following order: `gedit`, `vi`, `friends`, `emacs`. On platforms without `gedit`, an error may occur. You can correct the error by setting the `EDITOR` environment variable to an available editor, such as `vi`:

```
export EDITOR=vi
```

10.5. lw-set-log-level: Set the Log Level

You can set the Likewise log level for the Likewise authentication daemon by executing the following command and replacing `level` with one of the available logging levels: error, warning, info, verbose, debug, trace.

```
/opt/likewise/bin/lw-set-log-level level
```

Example: `/opt/likewise/bin/lw-set-log-level debug`

The log level is changed only until the authentication service (lsass) or the computer restarts. Syslog messages are logged through the daemon facility. The default setting is error.

10.6. lw-set-machine-name: Change the Hostname in the Local Provider

After you change the hostname of a computer, you must also change the name in the Likewise local provider database so that the local Likewise accounts use the correct prefix. To do so, execute the following command as root, replacing `hostName` with the name that you want:

```
/opt/likewise/bin/lw-set-machine-name hostName
```

10.7. Find a User or a Group

On a Unix or Linux computer that is joined to an Active Directory domain, you can check a domain user's or group's information by either name or ID. These commands can verify that the client can locate the user or group in Active Directory.

Find a User by Name

Execute the following command, replacing `domain\\username` with the full domain user name or the single domain user name of the user that you want to check:

```
/opt/likewise/bin/lw-find-user-by-name domain\\username
```

Example: `/opt/likewise/bin/lw-find-user-by-name likewisedemo\\hab`

You can optionally specify the level of detail of information that is returned. Example:

```
/opt/likewise/bin/lw-find-user-by-name ---level 2 likewisedemo\\hab
User info (Level-2):
=====
Name:                LIKWISEDEMO\\hab
UPN:                 hab@likewisedemo.com
Uid:                 593495196
Gid:                 593494529
Gecos:               Jurgen Habermas
Shell:               -/bin/sh
Home dir:             -/home/LIKWISEDEMO/hab
LMHash length:       0
NTHash length:       0
Local User:          NO
```

```
Account disabled:      FALSE
Account Expired:      FALSE
Account Locked:        FALSE
Password never expires: TRUE
Password Expired:      FALSE
Prompt for password change: YES
```

For more information, execute the following command:

```
/opt/likewise/bin/lw-find-user-by-name --help
```

Find a User by UID

To find a user by UID, execute the following command, replacing UID with the user's ID:

```
/opt/likewise/bin/lw-find-user-by-id UID
```

Example:

```
/opt/likewise/bin/lw-find-user-by-id 593495196
```

Find a Group by Name

```
/opt/likewise/bin/lw-find-group-by-name domain\username
```

Example:

```
/opt/likewise/bin/lw-find-group-by-name likewisedemo.com\dnsadmins
```

Find a Group by ID

```
/opt/likewise/bin/lw-find-group-by-id GID
```

Example:

```
[root@rhel4d bin]# -/opt/likewise/bin/lw-find-group-by-id 593494534
Group info (Level-0):
=====
Name:      LIKEWISEDEMO\schema^admins
Gid:       593494534
SID:       S-1-5-21-382349973-3885793314-468868962-518
```

Tip: To view this command's options, type the following command:

```
/opt/likewise/bin/lw-find-group-by-id --help
```

10.8. Find a User by a SID

On a Linux, Unix, or Mac OS X computer that is joined to a domain, you can find a user in Active Directory by his or her security identifier (SID). To find a user by SID, execute the following command as root, replacing SID with the user's security identifier:

```
/opt/likewise/bin/lw-find-by-sid SID
```

Example:

```
[root@rhel4d bin]# /opt/likewise/bin/lw-find-by-sid
S-1-5-21-382349973-3885793314-468868962-1180
User info (Level-0):
=====
Name:      LIKEWISEDEMO\hab
SID:       S-1-5-21-382349973-3885793314-468868962-1180
Uid:       593495196
Gid:       593494529
Gecos:     Jurgen Habermas
Shell:     -/bin/ sh
Home dir:  -/home/ LIKEWISEDEMO/ hab
```

Tip: To view the command's options, type the following command:

```
/opt/likewise/bin/lw-find-by-sid --help
```

10.9. List Groups for a User

To find the groups that a user is a member of, execute the following command followed by either the user's name or UID:

```
/opt/likewise/bin/lw-list-groups-for-user
```

Example: `/opt/likewise/bin/lw-list-groups-for-user 593495196`

Here's the command and its result for the user `likewisedemo\hab`:

```
[root@rhel5d bin]# ./lw-list-groups-for-user likewisedemo\hab
Number of groups found for user -'likewisedemo\hab' -: 2
Group[1 of 2] name = LIKEWISEDEMO\enterprise^admins (gid = 593494535)
Group[2 of 2] name = LIKEWISEDEMO\domain^users (gid = 593494529)
```

Tip: To view this command's options, type the following command:

```
/opt/likewise/bin/lw-list-groups-for-user --help
```

10.10. lw-enum-groups: List Groups

On a Linux, Unix, or Mac OS X computer that is joined to a domain, you can enumerate the groups in Active Directory and view their members, GIDs, and SIDs:

```
/opt/likewise/bin/lw-enum-groups --level 1
```

The Likewise agent enumerates groups in the primary domain. Groups in trusted domains and linked cells are not enumerated. NSS membership settings in the registry do not affect the result of the command.

Tip: To view the command's options, type the following command:

```
/opt/likewise/bin/lw-enum-groups --help
```

10.11. lw-enum-users: List Users

On a Linux, Unix, or Mac OS X computer that is joined to a domain, you can enumerate the users in Active Directory and view their members, GIDs, and SIDs:

/opt/likewise/bin/lw-enum-users

The Likewise agent enumerates users in the primary domain. Users in trusted domains and linked cells are not enumerated. NSS membership settings in the registry do not affect the result of the command.

Tip: To view the command's options, type the following command:

```
/opt/likewise/bin/lw-enum-users --help
```

To view full information about the users, include the `level` option when you execute the command:

```
/opt/likewise/bin/lw-enum-users --level 2
```

Example result for a one-user batch:

```
User info (Level-2):
=====
Name:                LIKWISEDEMO\sduval
UPN:                 SDUVAL@LIKWISEDEMO.COM
Generated UPN:       NO
Uid:                 593495151
Gid:                 593494529
Gecos:               Shelley Duval
Shell:               -/bin/sh
Home dir:            -/home/LIKWISEDEMO/sduval
LMHash length:       0
NTHash length:       0
Local User:          NO
Account disabled:    FALSE
Account Expired:     FALSE
Account Locked:      FALSE
Password never expires: FALSE
Password Expired:    FALSE
Prompt for password change: NO
```

10.12. lw-get-status: View the Status of the Authentication Providers

Likewise includes two authentication providers:

1. A local provider
2. An Active Directory provider

If the AD provider is offline, you will be unable to log on with your AD credentials. To check the status of the authentication providers, execute the following command as root:

```
/opt/likewise/bin/lw-get-status
```

A healthy result should look like this:

```
LSA Server Status:
Agent version: 5.4.0
Uptime:        22 days 21 hours 16 minutes 29 seconds
[Authentication provider: lsa-local-provider]
```

```

        Status:    Online
        Mode:      Local system
[Authentication provider: lsa-activedirectory-provider]
        Status:    Online
        Mode:      Un-provisioned
        Domain:    likewisedemo.com
        Forest:    likewisedemo.com
        Site:      Default-First-Site-Name

```

An unhealthy result will not include the AD authentication provider or will indicate that it is offline. If the AD authentication provider is not listed in the results, restart the authentication daemon.

If the result looks like the line below, check the status of the Likewise daemons to make sure they are running.

```
Failed to query status from LSA service. The LSASS server is not responding.
```

To check the status of the daemons, run the following command as root:

```
/opt/likewise/bin/lwsm list
```

10.13. Get the Current Domain

This command retrieves the Active Directory domain to which the computer is connected. The command's location is as follows:

```
/opt/likewise/bin/lw-lsa ad-get-machine account
```

10.14. lw-get-dc-list: List Domain Controllers

This command lists the domain controllers for a target domain. You can delimit the list in several ways, including by site. The command's location is as follows:

```
/opt/likewise/bin/lw-get-dc-list
```

Example usage:

```

[root@rhel5d bin]# ./lw-get-dc-list likewisedemo.com
Got 1 DCs:
=====
DC 1: Name = -'steveh-dc.likewisedemo.com', Address
= -'192.168.100.132'

```

To view the command's syntax and arguments, execute the following command:

```
/opt/likewise/bin/lw-get-dc-list --help
```

10.15. lw-get-dc-name: Get Domain Controller Information

This command displays the name of the current domain controller for the domain you specify. The command can help you select a domain controller. The command's location is as follows:

/opt/likewise/bin/lw-get-dc-name DomainName

To select a domain controller, run the following command as root until the domain controller you want is displayed. Replace DomainName with the name of your domain:

```
/opt/likewise/bin/lw-get-dc-name DomainName --force
```

10.16. lw-get-dc-time: Get Domain Controller Time

This command displays the time of the current domain controller for the domain that you specify. The command can help you determine whether there is a Kerberos time-skew error between a Likewise client and a domain controller. The command's location is as follows:

/opt/likewise/bin/lw-get-dc-time

Example:

```
[root@rhel5d bin]# ./lw-get-dc-time likewisedemo.com
DC TIME: 2009-09-08 14:54:18 PDT
```

10.17. lw-get-log-info

This command displays the logging status of the Likewise authentication service. The location of the command is as follows:

/opt/likewise/bin/lw-get-log-info

Example output:

```
[root@rhel5d bin]# ./lw-get-log-info
Current log settings:
=====
LSA Server is logging to syslog
Maximum allowed log level: error
```

10.18. lw-get-metrics

This command displays local security events from the Likewise event log. For information about using the log, see Monitoring Events. The location of the command is as follows:

/opt/likewise/bin/lw-get-metrics

Example output:

```
[root@rhel5d bin]# ./lw-get-metrics
Failed authentications:      3
Failed user lookups by name: 34
Failed user lookups by id:   0
Failed group lookups by name: 0
Failed group lookups by id:  0
Failed session opens:       32
Failed session closures:    33
Failed password changes:    0
```

```
Unauthorized access attempts: 0
```

To view the command's options, execute the following command:

```
/opt/likewise/bin/lw-get-metrics --help
```

10.19. Get Machine Account Information

You can print out the machine account name, machine account password, SID, and other information by running the following command as root.

```
/opt/likewise/bin/lw-lsa ad-get-machine account domainDNSName
```

Example: `/opt/likewise/bin/lw-lsa ad-get-machine account
likewisedemo.com`

10.20. Reload Changes to the Configuration File

After you change a setting in the registry for the Likewise agent, you must force the agent to load the change by executing the following command with super-user privileges:

```
/opt/likewise/bin/lw-refresh-configuration
```

10.21. lw-trace-info: Turn on Trace Markers in Log Messages

This command turns on trace markers in the messages logged by the `lwiod` and `lsassd` daemons. You can use the command to obtain more debugging information than that provided by the log level for debugging.

```
/opt/likewise/bin/lw-lsa trace-info
```

Example usage:

```
/opt/likewise/bin/lw-lsa trace-info --set user-group-  
queries:0,authentication:1 --get user-group-administration
```

To view this command's options, type the following command:

```
/opt/likewise/bin/lw-lsa trace-info --help
```

10.22. lw-update-dns: Dynamically Update DNS

This command registers an IP address for the computer in DNS. The command is useful when you want to register A and PTR records for your computer and the DHCP server is not registering them.

```
/opt/likewise/bin/lw-update-dns
```

Here's an example of how to use it to register an IP address:

```
/opt/likewise/bin/lw-update-dns --ipaddress 192.168.100.4 --fqdn  
corp.likewisedemo.com
```


If your system has multiple NICs and you are trying to register all their IP addresses in DNS, run the command once with multiple instances of the `ipaddress` option:

```
/opt/likewise/bin/lw-update-dns --fqdn corp.likewisedemo.com --
ipaddress 192.168.100.4 --ipaddress 192.168.100.7 --ipaddress
192.168.100.9
```

To troubleshoot, you can add the `loglevel` option with the `debug` parameter to the command:

```
/opt/likewise/bin/lw-update-dns --loglevel debug --fqdn
corp.likewisedemo.com --ipaddress 192.168.100.4 --ipaddress
192.168.100.7
```

For more information on the command's syntax and arguments, execute the following command:

```
/opt/likewise/bin/lw-update-dns --help
```

10.23. `lw-ad-cache`: Manage the AD Cache

This command manages the Likewise cache for Active Directory users and groups on Linux and Unix computers. The command's location is as follows:

```
/opt/likewise/bin/lw-ad-cache
```

You can use the command to clear the cache. The command's arguments can delete from the cache a user, a group, or all users and groups. The following example demonstrates how to delete all the users and groups from the cache:

```
/opt/likewise/bin/lw-ad-cache --delete-all
```

Tip: To reclaim disk space from SQLite after you clear the cache when you are using the non-default SQLite caching option, execute the following command as root, replacing `fqdn` with your fully qualified domain name:

```
/opt/likewise/bin/sqlite3 /var/lib/likewise/db/lsass-adcache.db.fqdn
vacuum
```

You can also use the `lw-ad-cache` command to enumerate users in the cache, which may be helpful in troubleshooting. Example:

```
[root@rhel5d bin]# ./lw-ad-cache ---enum-users
TotalNumUsersFound:      0
[root@rhel5d bin]# ssh likewisedemo.com\hab@localhost
Password:
Last login: Tue Aug 11 15:30:05 2009 from rhel5d.likewisedemo.com
[LIKEWISEDEMO\hab@rhel5d ~]$ exit
logout
Connection to localhost closed.
[root@rhel5d bin]# ./lw-ad-cache ---enum-users
User info (Level-0):
=====
Name:      LIKEWISEDEMO\hab
Uid:       593495196
Gid:       593494529
Gecos:     <null>
Shell:     -/bin/bash
Home dir:  -/home/LIKEWISEDEMO/hab
```

```
TotalNumUsersFound:      1
[root@rhel5d bin]#
```

To view all the command's syntax and arguments, execute the following command:

```
/opt/likewise/bin/lw-ad-cache --help
```

Clear the Cache on a Mac OS X Computer

On a Mac OS X computer, clear the cache by running the following command with superuser privileges in Terminal:

```
dscacheutil -flushcache
```

10.24. domainjoin-cli: Join or Leave a Domain

`domainjoin-cli` is the command-line utility for joining or leaving a domain. For instructions on how to use it, see [Join Active Directory with the Command Line](#).

10.25. lw-ypcat

This command is the Likewise NIS ypcat function for group passwd and netgroup maps.

```
/opt/likewise/bin/lw-ypcat
```

Example usage:

```
/opt/likewise/bin/lw-ypcat -d likewisedemo.com -k map-name
```

To view the command's syntax and arguments, execute the following command:

```
/opt/likewise/bin/lw-ypcat --help
```

10.26. lw-ypmatch

This command is the Likewise NIS ypmatch function for group passwd and netgroup maps.

```
/opt/likewise/bin/lw-ypmatch
```

Example usage:

```
/opt/likewise/bin/lw-ypmatch -d likewisedemo.com -k key-name map-name
```

To view the command's syntax and arguments, execute the following command:

```
/opt/likewise/bin/lw-ypmatch --help
```

10.27. lw-adtool: Modify Objects in AD

Likewise Enterprise includes a tool to modify objects in Active Directory from the command line of a Linux, Unix, or Mac OS X computer. Located at `/opt/likewise/bin/lw-adtool`, the tool has two interrelated functions:

- Query and modify objects in Active Directory.
- Find and manage objects in Likewise cells.

You can view a list of these two categories by executing the following command:

/opt/likewise/bin/lw-adtool --help -a

Here's what the output of the command looks like:

```
[root@rhel5d bin]# ./lw-adtool ---help --a

List of Actions

Generic Active Directory actions:
-----

add-to-group -- add a domain user/group to a security group.
delete-object -- delete an object.
disable-user -- disable a user account in Active Directory.
enable-user -- enable a user account in Active Directory.
lookup-object -- retrieve object attributes.
move-object -- move/rename an object.
new-computer -- create a new computer object.
new-group -- create a new global security group.
new-ou -- create a new organizational unit.
new-user -- create a new user account.
remove-from-group -- remove a user/group from a security group.
reset-user-password -- reset user's password.
search-computer -- search for computer objects, print DNs.
search-group -- search for group objects, print DNs.
search-object -- search for any type of objects using LDAP filter.
search-ou -- search for organizational units, print DNs
search-user -- search for users, print DNs.

Likewise cell management actions:
-----

add-to-cell -- add user/group to a Likewise cell.
delete-cell -- delete a Likewise cell.
edit-cell -- modify Likewise cell properties.
edit-cell-group -- modify properties of a cell's group.
edit-cell-user -- modify properties of a cell's user.
link-cell -- link Likewise cells.
lookup-cell -- retrieve Likewise cell properties.
lookup-cell-group -- retrieve properties of cell's group.
lookup-cell-user -- retrieve properties of cell's user.
new-cell -- create a new Likewise cell.
remove-from-cell -- remove user/group from a Likewise cell.
search-cells -- search for Likewise cells.
unlink-cell -- unlink Likewise cells.
```

To get information about the options for each action, use the following syntax:

/opt/likewise/bin/lw-adtool --help -a <ACTION>

Here's an example with the information that is returned:

```
/opt/likewise/bin/lw-adtool ---help --a new-user
```

Usage: `lw-adtool [OPTIONS] (-a -|--action) new-user <ARGUMENTS>`

`new-user --` create a new user account.

Acceptable arguments ([X] -- required):

<code>---dn=STRING</code>	DN/RDN of the parent container/ OU containing the
<code>---cn=STRING</code>	user. (use '-' for stdin input) Common name (CN) of the new
<code>---logon-name=STRING</code>	stdin input) Logon name of the new user.
<code>---pre-win-2000-name=STRING</code>	input) [X] Pre Windows-2000 logon name.
<code>---first-name=STRING</code>	First name of the new user.
<code>---last-name=STRING</code>	Last name of the new user.
<code>---description=STRING</code>	Description of the user.
<code>---password=STRING</code>	User's password. (use '-' for stdin input)
<code>---no-password-expires</code>	The password never expires. If omitted -- user
<code>logon.</code>	must change password on next
<code>---account-enabled</code>	User account will be enabled.
By default it is	disabled on creation

Notes on Using the Tool

Privileges: When you run the tool, you must use an Active Directory account with privileges that allow you to perform the command's action. The level of privileges that you need is set by Microsoft Active Directory and is typically the same as performing the corresponding action in Microsoft Active Directory Users and Computers. For example, to add a user to a security group, you must be a member of a security group, such as the enterprise administrators security group, that has privileges to perform the action.

For more information on Active Directory privileges, permissions, and security groups, see the following references on the Microsoft Technet web site: Active Directory Privileges, Active Directory object permissions, Active Directory Users, Computers, and Groups, Securing Active Directory Administrative Groups and Accounts.

Options There are short and long options. You separate arguments from options with either space or equal sign. If you are not sure about the results of an action you want to execute, run it in read-only mode first (-r). Also it can be useful to set log level to TRACE (-l 5) to see all the execution steps the tool is taking. Authentication SSO by default if the machine is domain-joined. Otherwise, KRB5 via a cached ticket, keytab file, or name/password (unless secure authentication is turned-off (--no-sec)) Name resolution In most cases you can reference objects by FQDN, RDN, UPN, or just names that make sense for a specific action. Use "-" if you want the tool to read values from stdin. This allows you to combine commands via pipes, e.g. search and lookup actions. Multi-forest support You can reference object from a name context (forest) different from the one you are currently connected to, provided that there is a proper trust relation between them. In this way, for instance, you can add a user that lives in one forest to a cell defined in another forest.

Creating a New Cell: When you create a new cell, the tool adds the default primary group (domain users) to the cell. If you are adding a user to the cell and the user has a primary group different from the default group, which is an atypical case, you must add the primary group to the cell, too. The tool does not do it automatically.

Adding Users or Groups Across Domains: If you are adding a user or group to a cell, and the user or group is in a domain different from the one hosting the cell, you must use an account that has write permissions in the cell domain and at least read permissions in the domain hosting the user or group. If, for example, you want to add a user such as CORP\kathy, whose primary group is, say, domain users, to a cell in a domain named CORPQA, two conditions must be met: First, you must be authenticated to the CORPQA domain as a user with administrative rights in the CORPQA domain; second, your user account must exist in the CORP domain with at least read permissions for the CORP domain. Further: Since in this example the primary group of CORP\kathy is CORP\domain users, you must add CORP\domain users to the cell in the CORPQA domain, too.

Automating Commands with a Service Account: To run the tool under a service account, such as a cron job, avoid using krb5 tickets for authentication, especially those cached by the Likewise authentication service in the /tmp directory. The tickets may expire and the tool will not renew them. Instead, it is recommended that you create an entry for the service account in a keytab file and use the keytab file for authentication.

Working with a Default Cell: The tool uses the default cell only when the value of the dn parameter is the root naming context, such as when you use an expression like --dn DC=corp,DC=likewise,DC=com to represent corp.likewise.com.

Options

To view the tool's options and to see examples of how to use them, execute the following command:

```
/opt/likewise/bin/lw-adtool --help
```

```
[root@rhel5d bin]# ./lw-adtool ---help
```

```
Usage: lw-adtool [OPTIONS] <ACTION> [ACTION_ARGUMENTS]
```

HELP OPTIONS

--u, ---usage	Display brief usage message
--?, ---help	Show this message, help on all
actions (-a), or help	on a specific action (-a <ACTION>).
--v, ---version	Print program version and exit.

COMMON OPTIONS

--l, ---log-level=LOG_LEVEL	Acceptable values: 1 (error),
2(warning), 3(info),	4(verbose) 5 (trace) (Default:
warning).	
--q, ---quiet	Suppress printing to stdout. Just
set the return code.	
--t, ---print-dn	print-dn option makes an exception.
looked up, modified or	Print DNs of the objects to be
	searched for.
--r, ---read-only	Do not actually modify directory
objects when	

executing actions.

CONNECTION OPTIONS

<code>--s, ---server=STRING</code>	Active Directory server to connect to.
<code>--d, ---domain=STRING</code>	Domain to connect to.
<code>--p, ---port=INT</code>	TCP port number
<code>--m, ---non-schema</code>	Turn off schema mode

AUTHENTICATION OPTIONS

<code>--n, ---logon-as=STRING</code>	User name or UPN.
<code>--x, ---passwd=STRING</code> (use '-' for stdin input)	Password for authentication.
<code>--k, ---keytab=STRING</code> etc/krb5.keytab	Full path of keytab file, e.g. -/etc/krb5.keytab
<code>--c, ---krb5cc=STRING</code> file, e.g.	Full path of krb5 ticket cache

`-/tmp/krb5cc_foo@likewisedemo.com`
Turns off secure authentication.

`--z, ---no-sec`
Simple bind will be

used. Use with caution!

ACTION

<code>--a, ---action[=<ACTION>]</code> a' for a list of	Action to execute. Type <code>--help --a</code> for a list of
for information on a	actions, or <code>--help --a <ACTION></code>
	specific action.

Try `--help --a` for a list of actions.

Examples

Here's an example that shows how to use two authentication options `--logon-as` and `passwd` to search Active Directory even though the computer on which the command was executed was not connected to the domain. The account specified in the `logon-as` option is an Active Directory administrative account.

```
root@ubuntu:/opt/likewise/bin# ./lw-adtool -a search-cells --search-
base dc=connecticut,dc=com --logon-as=Administrator --passwd=-
```

In this case, the successful result looked like this:

```
Enter password:
CN=$LikewiseIdentityCell,DC=connecticut,DC=com
CN=$LikewiseIdentityCell,OU=mySecureOU,DC=connecticut,DC=com
Total cells: 2
```

Here are a variety of examples. In some of them, the command is broken into two lines and the line break is marked by a back slash (\). In such cases, the back slash is not part of the command.

```
Create OU in a root naming context:
lw-adtool --a new-ou ---dn OU=TestOu
```

Create OU in DC=department,DC=company,DC=com:
lw-adtool --a new-ou ---dn OU=TestOu,DC=department,DC=company,DC=com

Create Likewise cell in OU TestOU setting the default login shell property to /bin/ksh:
lw-adtool --a new-ou ---dn OU=TestOu ---default-login-shell=/bin/ksh

Create a new account for user TestUser in OU=Users,OU=TestOu:
lw-adtool --a new-user ---dn OU=Users,OU=TestOu ---cn=TestUserCN ---logon-name=TestUser ---password=\$PASSWD

Enable the user account:
lw-adtool --a enable-user ---name=TestUser

Reset user's password reading the password from TestUser.pwd file:
cat TestUser.pwd -| lw-adtool --a reset-user-password ---name=TestUser ---password=- ---no-password-expires

Create a new group in OU=Groups,OU=TestOu:
lw-adtool --a new-group ---dn OU=Groups,OU=TestOu ---pre-win-2000-name=TestGrooup ---name=TestGroup

Look up -"description" attribute of an OU specified by name with a wildcard:
lw-adtool --a search-ou ---name='*RootOu' --t -| lw-adtool --a lookup-object ---dn=- ---attr=description

Look up -"unixHomeDirectory" attribute of a user with samAccountName TestUser:
lw-adtool --a search-user ---name TestUser --t -| lw-adtool --a lookup-object ---dn=- ---attr=unixHomeDirectory

Look up -"userAccountControl" attribute of a user with CN TestUserCN:
lw-adtool --a search-user ---name CN=TestUserCN --t -| lw-adtool --a lookup-object ---dn=- ---attr=userAccountControl

Look up all attributes of an AD object using filter-based search:
lw-adtool --a search-object ---filter -'(&(objectClass=person)(displayName=TestUser))' --t -| lw-adtool --a lookup-object

Add user TestUser to group TestGroup:
lw-adtool --a add-to-group ---user TestUser ---to-group=TestGroup

Add group TestGroup2 to group TestGroup:
lw-adtool --a add-to-group ---group TestGroup2 ---to-group=TestGroup

Remove user TestUser from group TestGroup:
lw-adtool --a remove-from-group ---user TestUser ---from-group=TestGroup

Rename AD object OU=OldName and move it to a new location:
lw-adtool --a move-object ---from
OU=OldName,DC=department,DC=company,DC=com \

```
--to OU=NewName,OU=TestOU,DC=department,DC=company,DC=com

Add group TestGroup to Likewise cell in TestOU:
lw-adtool --a add-to-cell ---dn
OU=TestOU,DC=department,DC=company,DC=com ---group=TestGroup

Remove user TestUser from Likewise cell in TestOU:
lw-adtool --a remove-from-cell ---dn
OU=TestOU,DC=department,DC=company,DC=com ---user=TestUser

Search for cells in a specific location:
lw-adtool --a search-cells ---search-base
OU=department,DC=country,DC=company,DC=com

Link cell in OU=TestOU1 to the default cell in DC=country:
lw-adtool --a link-cell ---source-dn
OU=TestOU1,DC=department,DC=company,DC=com \
--target-dn DC=country,DC=company,DC=com

Unlink cell in OU=TestOU1 from the default cell in DC=country:
lw-adtool --a unlink-cell ---source-dn
OU=TestOU1,DC=department,DC=company,DC=com \
--target-dn DC=country,DC=company,DC=com

Change the default login shell property of Likewise cell in TestOU:
lw-adtool --a edit-cell ---dn OU=TestOU ---default-login-shell=/bin/
csh

Find cells linked to Likewise cell in
OU=TestOU,DC=department,DC=company,DC=com:
lw-adtool --a lookup-cell ---dn OU=TestOU ---linked-cells

Look up login shell property of user TestUser in cell created in
TestOU:
lw-adtool --a lookup-cell-user ---dn OU=TestOU ---user TestUser ---
login-shell

Change login shell property of user TestUser in cell created in
TestOU:
lw-adtool --a edit-cell-user ---dn OU=TestOU ---user TestUser ---
login-shell=/usr/bin/ksh

Delete a cell object and all its children if any (--force):
lw-adtool --a delete-object ---dn OU=TestOU ---force

Search for Likewise cells in root naming context containing user
TestUser:
lw-adtool --a search-cells ---user TestUser
```

10.28. lwio: Input-Output Commands

The commands prefaced with `lwio` are included as part of the Likewise-CIFS technology preview. These commands are not covered under your support contract.

10.28.1. **lwio-copy: Copy Files Across Disparate Operating Systems**

The `lwio-copy` command-line utility lets you copy files across computers running different operating systems. You can, for example, copy files from a Linux computer to a Windows computer.

There two prerequisites to use `lwio-copy`: The `lwiod` daemon must be running, and the `rdr` driver `-- /opt/likewise/lib/librdr.sys.so --` must be available as specified by the registry. By default, the `rdr` driver is available.

The location of the tool is as follows:

`/opt/likewise/bin/lwio-copy`

To view the tool's arguments, execute the following command on your Unix, Linux, or Mac computer:

`/opt/likewise/bin/lwio-copy --help`

10.28.2. **lwio-refresh: Reload the Input-Output Settings After Changes**

The `lwio-refresh` command reloads the configuration for the `lwio` daemon, `lwiod`. When you modify the daemon's configuration, the changes take effect only after you run the `lwio-refresh` command or after you reboot the computer.

The location of the tool is as follows:

`/opt/likewise/bin/lwio-refresh`

Example usage:

`/opt/likewise/bin/lwio-refresh`

10.28.3. **lwio-set-log-level**

This command sets the logging status of the Likewise SMB file server to one of six levels: error, warning, info, verbose, debug, or trace.

To troubleshoot connection problems with `lwiod` and its redirector, set the log level of `lwiod` to debug.

The location of the tool is as follows:

`/opt/likewise/bin/lwio-set-log-level`

Example usage:

`/opt/likewise/bin/lwio-set-log-level debug`

10.28.4. **lwio-get-log-info**

This command displays the logging status of the Likewise SMB file server. The location of the tool is as follows:

`/opt/likewise/bin/lwio-get-log-info`

Example output:

```
[root@rhel5d bin]# ./lwio-get-log-info
Current log settings:
=====
SMB Server is logging to syslog
Maximum allowed log level: error
```

10.29. Commands to Modify Local Accounts

The Likewise local authentication provider for local users and groups includes a full local authentication database. With functionality similar to the local SAM authentication database on every Windows computer, the local authentication provider lets you create, modify, and delete local users and groups on Linux, Unix, and Mac OS X computers by using the following commands.

To execute the commands that modify local accounts, you must use either the root account or an account that has membership in the local administrators group. The account can be an Active Directory account if you manually add it to the local administrators group. For example, you could add the Domain Administrators security group from Active Directory to the local administrators group, and then use an account with membership in the Domain Administrators security group to execute the commands.

10.29.1. **lw-add-user:** Add a Local User by Name or UID

This command adds a user to the local authentication database. The command's location is as follows:

/opt/likewise/bin/lw-add-user

To view the command's syntax and arguments, execute the following command:

```
/opt/likewise/bin/lw-add-user --help
```

10.29.2. **lw-add-group:** Add a Local Group Member by Name or GID

This command adds a group member to the local authentication database. The command's location is as follows:

/opt/likewise/bin/lw-add-group

To view the command's syntax and arguments, execute the following command:

```
/opt/likewise/bin/lw-add-group --help
```

10.29.3. **lw-del-user:** Remove a Local User by Name or UID

This command deletes a user from the local authentication database. The command's location is as follows:

/opt/likewise/bin/lw-del-user

To view the command's syntax and arguments, execute the following command:

```
/opt/likewise/bin/lw-del-user --help
```

10.29.4. **lw-del-group: Remove a Local Group by Name or GID**

This command deletes a group from the local authentication database. The command's location is as follows:

/opt/likewise/bin/lw-del-group

To view the command's syntax and arguments, execute the following command:

```
/opt/likewise/bin/lw-del-group --help
```

10.29.5. **lw-mod-user: Modify a Local User by Name or UID**

This command modifies a user's account settings in the local authentication database, including an account's expiration date and password. You can also enable a user, disable a user, unlock an account, or remove a user from a group. The command's location is as follows:

/opt/likewise/bin/lw-mod-user

To view the command's syntax and arguments, execute the following command:

```
/opt/likewise/bin/lw-mod-user --help
```

10.29.6. **lw-mod-group: Modify a Local Group's Members**

This command adds members to or removes members from a group in the local authentication database. The command's location is as follows:

/opt/likewise/bin/lw-mod-group

Here's an example that demonstrates how to add domain accounts to a local group:

```
/opt/likewise/bin/lw-mod-group --add-members DOMAIN\\Administrator  
BUILTIN\\Administrators
```

To view the command's syntax and arguments, execute the following command:

```
/opt/likewise/bin/lw-mod-group --help
```

10.30. **Kerberos Commands**

Likewise includes several command-line utilities for working with Kerberos. It is recommended that you use these Kerberos utilities, located in `/opt/likewise/bin`, to manage those aspects of Kerberos authentication that are associated with Likewise. For complete instructions on how to use the Kerberos commands, see the man page for the command.

10.30.1. **kdestroy: Destroy the Kerberos Ticket Cache**

The `kdestroy` utility destroys the user's active Kerberos authorization tickets obtained through Likewise. Destroying the user's tickets can help solve logon problems.

Note: This command destroys only the tickets in the Likewise Kerberos cache of the user account that is used to execute the `kdestroy` command; tickets in other Kerberos caches, including root, are not destroyed. To destroy another user's cache, use the command with its `-c` option.

To destroy a user's Likewise Kerberos tickets, execute the following command with the user's account:

```
/opt/likewise/bin/kdestroy
```

Tip: To view this command's options, type the following command:

```
/opt/likewise/bin/kdestroy -
```

10.30.2. klist: View Kerberos Tickets

On a target Linux or Unix computer, you can see a list of Kerberos tickets by executing the following command:

```
/opt/likewise/bin/klist
```

The command lists the location of the credentials cache, the expiration time of each ticket, and the flags that apply to the tickets. For more information, see the man page for `klist`.

Because Likewise includes its own Kerberos 5 libraries (in `/opt/likewise/lib`), you must use the Likewise `klist` command by either changing directories to `/opt/likewise/bin` or including the path in the command.

Example:

```
-sh-3.00$ -/opt/likewise/bin/klist
Ticket cache: FILE:/tmp/krb5cc_593495191
Default principal: hoenstiv@LIKEWISEDEMO.COM
Valid starting    Expires    Service principal
07/22/08 16:07:23  07/23/08 02:06:39  krbtgt/
LIKEWISEDEMO.COM@LIKEWISEDEMO.COM
        renew until 07/23/08 04:07:23
07/22/08 16:06:39  07/23/08 02:06:39  host/rhel4d.LIKEWISEDEMO.COM@
        renew until 07/23/08 04:07:23
07/22/08 16:06:39  07/23/08 02:06:39  host/
rhel4d.LIKEWISEDEMO.COM@LIKEWISEDEMO.COM
        renew until 07/23/08 04:07:23
07/22/08 16:06:40  07/23/08 02:06:39  RHEL4D$@LIKEWISEDEMO.COM
        renew until 07/23/08 04:07:23
```

Note: To address Kerberos issues, see Troubleshooting Kerberos Errors at <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/tkerberr.msp>.

10.30.3. kinit: Obtain and Cache a TGT

This command obtains and caches an initial ticket-granting ticket for a principal. The command's location is as follows:

```
/opt/likewise/bin/kinit
```

To view the command's options and arguments, execute the following command:

```
man kinit
```

10.30.4. kpasswd: Change a Password

The `kpasswd` command changes a Kerberos principal's password on a Linux or Unix computer. (On a Mac computer, use the Mac OS X graphical user interface to change a Kerberos principal's password.) The command's location is as follows:

/opt/likewise/bin/kpasswd

To view the command's options and arguments, execute the following command:

```
man kpasswd
```

10.30.5. ktutil: The Keytab File Maintenance Utility

This command invokes a shell from which you can read, write, or edit entries in a Kerberos keytab. The command's location is as follows:

/opt/likewise/bin/ktutil

To view the command's options and arguments, execute the following command:

```
man ktutil
```

You can use `ktutil` to add a keytab file to a non-default location. When you join a domain, Likewise initializes a Kerberos keytab by adding the `default_keytab_name` setting to `krb5.conf` and setting it to `/etc/krb5.keytab`. If the keytab file referenced in `krb5.conf` does not exist, the Likewise domain-join utility changes the setting to `/etc/krb5.conf`.

You can set the keytab file to be in a location that is different from the default. To do so, you must pre-create the keytab file in the location you want and set a symlink to it in `/etc/krb5.keytab`. Then, you must set the `default_keytab_name` in `/etc/krb5.conf` to point to either the symlink or the real file. The result is that the keytab file will already exist and the Likewise domain-join utility will not modify its location setting.

The keytab's format does not let you create a keytab file without a keytab, but you can use `ktutil` to manually create one with a place-holder entry. When Likewise adds your computer to the domain, a correct entry will be added to the file.

```
/opt/likewise/bin/ktutil
ktutil: addent --password --p nonexistent@nonexistent --k 1 --e RC4-
HMAC
Password for nonexistent@nonexistent:
ktutil: wkt -/var/OtherPlace/etc/krb5.keytab
ktutil: quit
```

10.30.6. Kvno: Acquire a Service Ticket and Print Key Version Number

This command acquires a service ticket for the specified Kerberos principals and prints out the key version numbers of each. The command's location is as follows:

/opt/likewise/bin/kvno

To view the command's options and arguments, execute the following command:

`man kvno`

10.31. Commands and Scripts Not for Customer Use

The commands and scripts listed in this section are not for end users. It is recommended that you do not use them.

10.31.1. ConfigureLogin

`ConfigureLogin` is used by `domainjoin-cli`. It is recommended that you do not execute the `ConfigureLogin` command manually.

10.31.2. dceidl

`dceidl` is used by `dcerpcd`; the command is not for end users.

10.31.3. gpccron

`gpccron` is used by the application. It is recommended that you do not execute it manually.

10.31.4. gpccron.sh

`gpccron.sh` is used by the application. It is recommended that you do not execute it manually.

10.31.5. gprsrmtmnt.sh

The group policy agent -- `gpagentd` -- uses this script to restart the automount service after applying automount policy settings. The script applies different commands to restart the automount service on different operating systems, such as AIX, HP-UX, and Linux.

10.31.6. init-base.sh

`init-base.sh` is included by the initiation scripts. It is recommended that you do not execute it manually.

10.32. Likewise Enterprise Tools Installed on Windows Computers

This section covers the command-line tools that are on a Windows computer running Likewise Enterprise. The commands are in `C:\Program Files\Likewise\Enterprise`. The command-line tools for the Likewise Enterprise database are discussed in the chapter on setting up the database.

10.32.1. Lwopt.exe

`Lwopt.exe` lets you manage options for Likewise Enterprise from the command-line of a Windows administrative workstation connected to Active Directory. You can, for example, set an option to use sequential IDs instead of hashed IDs. In addition, after you set the option to use sequential IDs, you

can set the initial UID number for a cell. Setting UIDs below 1,000 is ill-advised, as they can result in a security vulnerability.

C:\Program Files\Likewise\Enterprise>lwopt

lwopt -- configures local Windows options for Likewise

Usage: lwopt OPTIONS

OPTIONS:

---status Show current configuration status
 ---narrowsearch Only search the default cell on the local domain

---widesearch Search the default cell across all domains and two-way forest trusts

---sequential Use sequential IDs instead of hashed IDs

---hashed Use hashed IDs

---foreignaliases Allow the use of aliases for users and groups from other domains.

---noforeignaliases Disallow the use of aliases for users and groups

from other domains.

---usegc Use the Global Catalog to speed up searches (default)

---ignoregc Do not use the Global Catalog to speed up searches

---startUID=# Sets the initial UID number for a cell (if ---sequential)

---startGID=# Sets the initial GID number for a cell (if ---sequential)

---minID=# Sets minimum UID and GID number configurable through

the UI
 ---cell=LDAPPATH Identifies the cell whose initial IDs (if ---sequential)

Example: LDAP://somedc/ou=anou,dc=somecom,dc=com

---enableloginnames Sets the default login names to all the users enabled

in all the cells.

---disableloginnames Disable the enable default login names option to all

users enabled in all the cells.

---help Displays this usage information

If the ---startUID or ---startGID options are set, the ---cell option must also be set.

Chapter 11. Monitoring Events with the Event Log

11.1. Monitor Events with the Event Log

The Likewise Event Log records and categorizes information about authentication transactions, authorization requests, network events, and other security events on Linux, Unix, and Mac OS X computers. Monitoring events such as failed logon attempts and failed sudo attempts can help prevent unauthorized access to commands, applications, and sensitive resources.

The events are stored in a SQLite database, which is included when you install the Likewise agent. The database is at `/var/lib/likewise/db/lwi_events.db` and its libraries are at `/opt/likewise/lib/`. For viewing and modifying the database, Likewise includes a command-line utility at `/opt/likewise/bin/sqlite3`. For information about SQLite and instructions on how to use the command-line utility, see <http://www.sqlite.org/>.

The event log records the following events: daemon initializations, successful logins, failed logins, denied sudo attempts, the application of new group policy objects, offline-online transitions and other network connectivity events, and a periodic heartbeat that identifies whether the computer is active.

Likewise includes methods by which you can specify which user and group accounts have read or write access permissions to the event log. The typical methods for setting permissions are the local Likewise configuration registry and Likewise Enterprise group policy objects administered from Active Directory. You can filter events in the event log and you can decide which event categories to log.

Event logging is turned off by default. You can turn on event logging by editing the registry or by using a group policy. Then, you can configure the options for the log in the registry or manage them with the corresponding group policies. Keep in mind that group policies are available only with Likewise Enterprise; Likewise Open does not apply group policies.

After you modify the settings in the registry, you must restart the event log daemon with the root account for the changes to take effect:

```
/opt/likewise/bin/lwsm refresh eventlogd
```

For information about managing the event log with the registry, see the chapter on configuring the Likewise agent with the registry. For information about managing the event log with group policies, see the chapter on Likewise group policies.

11.2. View the Local Event Log

On a Linux, Unix, or Mac OS X computer, you view the local Likewise Event Log by using the `eventlog` command-line utility with the root account:

```
/opt/likewise/bin/lw-eventlog-cli
```

To view the command's arguments, execute the following command:

```
/opt/likewise/bin/lw-eventlog-cli -h
```


You can gain access to the event log by using either `localhost` or the virtual loopback interface of the computer, which is typically assigned to the address `127.0.0.1`.

To view a summary of events, execute the following command with the root account:

```
/opt/likewise/bin/lw-eventlog-cli -s - localhost
```

Example output:

```
=====
Event Record: (392/396) (392 total)
=====
Event Record ID..... 392
Event Table Category.... System
Event Type..... Information
Event Date..... 2010-02-16
Event Time..... 07:37:58 AM
Event Source..... Likewise LSASS
Event Category..... Service
Event Source ID..... 1004
Event User..... SYSTEM
Event Computer..... glennnc-mbp
Event Description..... Likewise authentication service provider
configuration settings have been reloaded.

Authentication provider:          lsa-activedirectory-provider
Current settings are...
Cache reaper timeout (secs):      2592000
Cache entry expiry (secs):        14400
Space replacement character:      -'^'
Domain separator character:       -'\ '
Enable event log:                  true
Logon membership requirements:
    CORP\GLENNC-MBP_Users
    CORP\EnterpriseTeam
Log network connection events:    false
Create K5Login file:              true
Create home directory:            true
Sign and seal LDAP traffic:       false
Assume default domain:            false
Sync system time:                 true
Refresh user credentials:         true
Machine password sync lifetime:   2592000
Default Shell:                    -/bin/sh
Default home directory prefix:    -/Users
Home directory template:          %H/local/%D/%U
Umask:                            18
Skeleton directory:               System/Library/User Template/
Non_localized, -/System/Library/User Template/English.lproj
Cell support:                      Invalid
Trim user membership:             true
NSS group members from cache only: false
NSS user members from cache only: false
NSS enumeration enabled:          true
Domain Manager check domain online (secs): 300
```

```
Domain Manager unknown domain cache timeout (secs): 3600
```

```
=====
```

Or, with the following command, you can view the event log in table format:

```
/opt/likewise/bin/lw-eventlog-cli -t - localhost
```

Example:

```
[root@rhel5d bin]# su likewisedemo\\hab
[LIKEWISEDEMO\hab@rhel5d bin]$ sudo blah
Password:
Sorry, try again.
Password:
Sorry, try again.
Password:
sudo: 2 incorrect password attempts
[LIKEWISEDEMO\hab@rhel5d bin]$ exit
[root@rhel5d bin]# -/opt/likewise/bin/lw-eventlog-cli --t -- localhost
Id:| Type           -| Time           -| Source         -|
Category      -| Event -| User
83 -| Information    -| 02:11:29 PM -| Likewise LSASS -|
Service       -| 1004   -| SYSTEM
84 -| Success Audit -| 02:13:07 PM -| Likewise LSASS -| Login/
Logoff -| 1201   -| LIKEWISEDEMO\hab
85 -| Failure Audit -| 02:13:30 PM -| Likewise LSASS -| Login/
Logoff -| 1205   -| LIKEWISEDEMO\hab
86 -| Failure Audit -| 02:13:33 PM -| Likewise LSASS -| Login/
Logoff -| 1205   -| LIKEWISEDEMO\hab
87 -| Failure Audit -| 02:13:39 PM -| Likewise LSASS -| Login/
Logoff -| 1205   -| LIKEWISEDEMO\hab
88 -| Success Audit -| 02:14:57 PM -| Likewise LSASS -| Login/
Logoff -| 1220   -| LIKEWISEDEMO\hab
[root@rhel5d bin]#
```

You can also use SQL filters to query the event log by event type, source ID, and a variety of other field names. Example:

```
[root@rhel5d bin]# -/opt/likewise/bin/lw-eventlog-cli --
s -"(EventType = -'Failure Audit') AND (EventSourceId = 1205)"
localhost
Event Record: (1/3) (1 total)
=====
Event Record ID..... 85
Event Table Category.... Security
Event Type..... Failure Audit
Event Date..... 2009-07-29
Event Time..... 02:13:30 PM
Event Source..... Likewise LSASS
Event Category..... Login/Logoff
Event Source ID..... 1205
Event User..... LIKEWISEDEMO\hab
Event Computer..... rhel5d
Event Description..... Logon Failure:
```

```
Authentication provider: lsa-activedirectory-provider

Reason:                Unknown username or bad password
User Name:             LIKEWISEDEMO\hab
Login phase:           User authenticate
Event Data..... Error: The password is incorrect for the
given username [error code: 32789]
=====
```

11.3. The Event Type

The Event Type field is typically one of the following:

```
SUCCESS_AUDIT_EVENT_TYPE    -"Success Audit"
FAILURE_AUDIT_EVENT_TYPE     -"Failure Audit"
INFORMATION_EVENT_TYPE       -"Information"
WARNING_EVENT_TYPE           -"Warning"
ERROR_EVENT_TYPE             -"Error"
```

11.4. The Event Source

The Event Source is typically one of the following values: Likewise LSASS, Likewise GPAGENT, Likewise DomainJoin, Likewise NETLOGON, System Log.

11.5. List of Events by Source ID

Each source defines its own list of Event Source Id values. Here's a list of events categorized by source.

```
=====
EventSource = -"Likewise LSASS"

LSASS_EVENT_INFO_SERVICE_STARTED           1000
LSASS_EVENT_ERROR_SERVICE_START_FAILURE    1001
LSASS_EVENT_INFO_SERVICE_STOPPED           1002
LSASS_EVENT_ERROR_SERVICE_STOPPED          1003
LSASS_EVENT_INFO_SERVICE_CONFIGURATION_CHANGED 1004

// Logon events
LSASS_EVENT_SUCCESSFUL_LOGON_AUTHENTICATE   1200
LSASS_EVENT_SUCCESSFUL_LOGON_CREATE_SESSION 1201
LSASS_EVENT_SUCCESSFUL_LOGON_CHECK_USER     1203
LSASS_EVENT_FAILED_LOGON_UNKNOWN_USERNAME_OR_BAD_PASSWORD 1205
LSASS_EVENT_FAILED_LOGON_TIME_RESTRICTION_VIOLATION 1206
LSASS_EVENT_FAILED_LOGON_ACCOUNT_DISABLED    1207
LSASS_EVENT_FAILED_LOGON_ACCOUNT_EXPIRED     1208
LSASS_EVENT_FAILED_LOGON_MACHINE_RESTRICTION_VIOLATION 1209
LSASS_EVENT_FAILED_LOGON_TYPE_OF_LOGON_NOT_GRANTED 1210
LSASS_EVENT_FAILED_LOGON_PASSWORD_EXPIRED    1211
LSASS_EVENT_FAILED_LOGON_NETLOGON_FAILED     1212
```

LSASS_EVENT_FAILED_LOGON_UNEXPECTED_ERROR	1213
LSASS_EVENT_FAILED_LOGON_ACCOUNT_LOCKED	1214
LSASS_EVENT_FAILED_LOGON_CHECK_USER	1215
LSASS_EVENT_LOGON_PHASE_AUTHENTICATE	1
LSASS_EVENT_LOGON_PHASE_CREATE_SESSION	2
LSASS_EVENT_LOGON_PHASE_CHECK_USER	3
// Logoff events	
LSASS_EVENT_SUCCESSFUL_LOGOFF	1220
// User password change events	
LSASS_EVENT_SUCCESSFUL_PASSWORD_CHANGE	1300
LSASS_EVENT_FAILED_PASSWORD_CHANGE	1301
LSASS_EVENT_SUCCESSFUL_USER_ACCOUNT_KERB_REFRESH	1302
LSASS_EVENT_FAILED_USER_ACCOUNT_KERB_REFRESH	1303
// Machine password change events	
LSASS_EVENT_SUCCESSFUL_MACHINE_ACCOUNT_PASSWORD_UPDATE	1320
LSASS_EVENT_FAILED_MACHINE_ACCOUNT_PASSWORD_UPDATE	1321
LSASS_EVENT_SUCCESSFUL_MACHINE_ACCOUNT_TGT_REFRESH	1322
LSASS_EVENT_FAILED_MACHINE_ACCOUNT_TGT_REFRESH	1323
// Account management events	
LSASS_EVENT_ADD_USER_ACCOUNT	1400
LSASS_EVENT_DELETE_USER_ACCOUNT	1401
LSASS_EVENT_ADD_GROUP	1402
LSASS_EVENT_DELETE_GROUP	1403
// Lsass provider events	
LSASS_EVENT_SUCCESSFUL_PROVIDER_INITIALIZATION	1500
LSASS_EVENT_FAILED_PROVIDER_INITIALIZATION	1501
LSASS_EVENT_INFO_REQUIRE_MEMBERSHIP_OF_UPDATED	1502
LSASS_EVENT_INFO_AUDITING_CONFIGURATION_ENABLED	1503
LSASS_EVENT_INFO_AUDITING_CONFIGURATION_DISABLED	1504
// Runtime warnings	
LSASS_EVENT_WARNING_CONFIGURATION_ID_CONFLICT	1601
LSASS_EVENT_WARNING_CONFIGURATION_ALIAS_CONFLICT	1602
// Network events	
LSASS_EVENT_INFO_NETWORK_DOMAIN_ONLINE_TRANSITION	1700
LSASS_EVENT_WARNING_NETWORK_DOMAIN_OFFLINE_TRANSITION	1701
=====	
EventSource = -"Likewise DomainJoin"	
DOMAINJOIN_EVENT_INFO_JOINED_DOMAIN	1000
DOMAINJOIN_EVENT_ERROR_DOMAIN_JOIN_FAILURE	1001
DOMAINJOIN_EVENT_INFO_LEFT_DOMAIN	1002
DOMAINJOIN_EVENT_ERROR_DOMAIN_LEAVE_FAILURE	1003

```
=====
EventSource = -"Likewise GPAGENT"

GPAGENT_EVENT_INFO_SERVICE_STARTED                1000
GPAGENT_EVENT_ERROR_SERVICE_START_FAILURE          1001
GPAGENT_EVENT_INFO_SERVICE_STOPPED                 1002
GPAGENT_EVENT_ERROR_SERVICE_STOPPED                1003
GPAGENT_EVENT_INFO_SERVICE_CONFIGURATION_CHANGED    1004

// GPAgent policy update events
GPAGENT_EVENT_POLICY_UPDATED                        1100
GPAGENT_EVENT_POLICY_UPDATE_FAILURE                1101

// GPAgent policy processing issue events
GPAGENT_EVENT_INFO_POLICY_PROCESSING_ISSUE_RESOLVED 1200
GPAGENT_EVENT_ERROR_POLICY_PROCESSING_ISSUE_ENCOUNTED 1201

=====
EventSource = -"Likewise NETLOGON"

// Netlogon service events
LWNET_EVENT_INFO_SERVICE_STARTED                    1000
LWNET_EVENT_ERROR_SERVICE_START_FAILURE             1001
LWNET_EVENT_INFO_SERVICE_STOPPED                    1002
LWNET_EVENT_ERROR_SERVICE_STOPPED                   1003
LWNET_EVENT_INFO_SERVICE_CONFIGURATION_CHANGED      1004

=====
EventSource = -"System Log"

Syslog entries are parsed by the reapsysld daemon
to create Likewise eventlog entries for the following:

Text console logon failure                          1
Text console logon success                          2
SSH logon failure                                    3
SSH logon success                                    4
SUDO bad password                                    5
SUDO access denied                                   6
SUDO success                                         7
SSH with AD account failure                          8
SSH with AD account success                          9
Text console login with AD account failure           10
Text console login with AD account success           11
```

Chapter 12. Leaving a Domain and Uninstalling the Agent

12.1. Leave a Domain

When you leave a domain, Likewise reverses most Likewise-specific settings that were made to a computer's configuration when it was joined to the domain. Likewise also reverses any changes that you manually made to `/etc/likewise/lsassd.conf` or to the Likewise registry. Changes to the `nsswitch` module, however, are preserved until you uninstall Likewise, when they are reversed. Before you leave a domain, you can execute the following command to view the changes that will take place:

```
domainjoin-cli leave --advanced --preview domainName
```

Example:

```
[root@rhel4d likewise]# domainjoin-cli leave ---advanced ---preview
likewisedemo.com
Leaving AD Domain:      LIKEWISEDEMO.COM
[X] [S] ssh              -- configure ssh and sshd
[X] [N] pam              -- configure pam.d/pam.conf
[X] [N] nsswitch         -- enable/disable Likewise nsswitch module
[X] [N] stop             -- stop daemons
[X] [N] leave           -- disable machine account
[X] [N] krb5             -- configure krb5.conf
[F] keytab              -- initialize kerberos keytab
```

Key to flags

```
[F]ully configured      -- the system is already configured for
this step
[S]ufficiently configured -- the system meets the minimum
configuration
                        requirements for this step
[N]ecessary            -- this step must be run or manually
performed.
[X]                    -- this step is enabled and will make
changes
[ -]                   -- this step is disabled and will not
make changes
```

For information on advanced commands for leaving a domain, see *Join Active Directory with the Command Line*.

The Computer Account in Active Directory

When you leave a domain, the computer's account in Active Directory is not disabled and not deleted. If, however, you include the user name as part of the `leave` command, the computer's account is disabled but not deleted. You can include the user name as part of the `leave` command as follows; you will be prompted for the password of the user account:

```
domainjoin-cli leave userName
```

Example: `domainjoin-cli leave brsmith`


Remove a Linux or Unix Computer from a Domain

- On the Linux or Unix computer that you want to remove from the Active Directory domain, use a root account to run the following command:

```
/opt/likewise/bin/domainjoin-cli leave
```

Remove a Mac from a Domain

To leave a domain on a Mac OS X computer, you must have administrative privileges on the Mac.

1. In Finder, click **Applications**.
2. In the list of applications, double-click **Utilities**, and then double-click **Directory Access**.
3. On the **Services** tab, click the lock  and enter an administrator name and password to unlock it.
4. In the list, click **Likewise**, and then click **Configure**.
5. Enter a name and password of a local machine account with administrative privileges.
6. On the menu bar at the top of the screen, click the **Likewise Domain Join Tool** menu, and then click **Join or Leave Domain**.
7. Click **Leave**.

Remove a Mac with the Command Line

Execute the following command with an account that allows you to use sudo:

```
sudo /opt/likewise/bin/domainjoin-cli leave
```

12.2. Uninstall the Domain Join GUI

On a Linux computer, you can uninstall the domain join GUI from the command line by running the following command as root. The command applies only to Linux computers on which you installed the domain-join GUI as a separate component. In Likewise 6.0 or later, the domain-join GUI is included in the main installation for Linux platforms and cannot be uninstalled separately.

```
/opt/likewise/setup/djgtk/uninstall
```

12.3. Uninstall the Agent on a Linux or Unix Computer

Important: Before uninstalling the agent, you must leave the domain and uninstall the domain-join GUI if you installed it as a separate component. Then execute the `uninstall` command from a directory other than `likewise` so that the uninstall program can delete the `likewise` directory and all its subdirectories -- for example, execute the command from the root directory.

Uninstall Likewise with the Shell Script on Linux or Unix

If you installed the agent on a Linux or Unix computer by using the shell script, you can uninstall the Likewise agent from the command line by using the same shell script with the `uninstall` option. (To uninstall the agent, you must use the shell script with the same version and build number that you used to install it.) For example, on a Linux computer running `glibc`, change directories to the location of Likewise and then run the following command as root, replacing the name of the script with the version you installed:

```
./LikewiseOpen-6.0.0.94-linux-oldlibc-i386-rpm.sh uninstall
```

For information about the script's options and commands, execute the following command:

```
./LikewiseOpen-6.0.0.8011-linux-i386-rpm.sh help
```

Uninstall BitRock Installations on Linux or Unix

On a Linux or Unix computer, you can uninstall the Likewise agent from the command line if you originally installed the agent with the BitRock installer, an installer for previous versions of Likewise.

- To uninstall the agent on a Linux computer running Likewise Enterprise, run the following command as root:

```
/opt/likewise/setup/lwise/uninstall
```

- To uninstall the agent on a Linux computer running Likewise Open, run the following command as root:

```
/opt/likewise/setup/lwiso/uninstall
```

12.4. Uninstall the Agent on a Mac

On a Mac OS X computer, you must uninstall the Likewise agent by using Terminal. Before uninstalling the agent, you should leave the domain.

1. Log on the Mac by using a local account with privileges that allow you to use `sudo`.
2. Open a Terminal window: In Finder, on the **Go** menu, click **Utilities**, and then double-click **Terminal**.
3. At the Terminal shell prompt, execute the following command:

```
sudo /opt/likewise/bin/macuninstall.sh
```

Chapter 13. Using Likewise for Single Sign-On

13.1. About Single Sign-On

When you log on a Linux, Unix, or Mac OS X computer by using your Active Directory domain credentials, Likewise initializes and maintains a Kerberos ticket granting ticket (TGT). The TGT lets you log on other computers joined to Active Directory or applications provisioned with a service principal name and be automatically authenticated with Kerberos and authorized for access through Active Directory. In a transparent process, the underlying Generic Security Services (GSS) system requests a Kerberos service ticket for the Kerberos-enabled application or server. The result: single sign-on.

To gain access to another computer, you can use various protocols and applications:

- SSH (how to configure single sign-on for SSH)
- rlogin
- rsh
- Telnet
- FTP
- Firefox (for browsing of intranet sites)
- LDAP queries against Active Directory
- HTTP with an Apache HTTP Server

How Likewise Makes SSO Happen

Since Microsoft Windows 2000 was released, Active Directory's primary authentication protocol has been Kerberos. When a user logs on to a Windows computer that is joined to a domain, the operating system uses the Kerberos protocol to establish a key and to request a ticket for the user. Active Directory serves as the Kerberos key distribution center, or KDC.

Likewise configures Linux and Unix computers to interact with Active Directory in a similar way. When a user logs on a Linux and Unix computer joined to a domain, Likewise requests a ticket for the user. The ticket can then be used to implement SSO with other applications.

Likewise fosters the use of the highly secure Kerberos 5 protocol by automating its configuration on Linux and Unix computers. To ensure that the Kerberos authentication service is properly configured, Likewise does the following:

- Ensures that DNS is properly configured to resolve names associated with Active Directory (AD).
- Performs secure, dynamic DNS updates to ensure that Linux and Unix computer names can be resolved with AD-integrated DNS servers.
- Configures Kerberos. In an environment with multiple KDCs, Likewise makes sure that Kerberos selects the right server.

- Configures SSHD to support SSO through Kerberos by using GSSAPI.
- Creates a keytab for the computer in the following way: When you join a Linux or Unix computer to AD, Likewise creates a machine account for the computer. Likewise then automatically creates a keytab for the SPN and places it in the standard system location (typically `/etc/krb5.keytab`).
- Creates a keytab for the user during logon. On most systems, the user keytab is placed in the `/tmp` directory and named `krb5cc_UID`, where `UID` is the numeric user ID assigned by the system.

Overview of How to Implement SSO with Likewise

When you install Likewise on a Linux, Unix, or Mac OS X computer and join it to Active Directory, Likewise prepares it for single sign-on by creating a keytab for the computer. However, when you use Likewise to implement SSO with other applications or services, you will likely have to configure the application to use GSSAPI and Kerberos 5 authentication and you will likely have to provision each application user for external Kerberos authentication. At the very least, you will have to provision your application with a service principal name in Active Directory. A service principal name, or SPN, is the name with which a client uniquely identifies an instance of a service. Kerberos then uses the SPN to authenticate a service.

Note: Configuring an external application for SSO with Kerberos is beyond the scope of the Likewise documentation; for more information, see the vendor's manual for your application.

The following process outlines the steps for setting up an application or service to use Likewise for single sign-on. For a detailed example of how to configure an application for SSO, see [Configure Apache for SSO](#). For examples of how to create a service account in AD, register an SPN for the service account, and create a keytab for the SPN, see [creating a Kerberos service principal and keytab file for SSO on the IBM web site](#).

1. Create a service account for the application in Active Directory.
2. Associate a service principal name, or SPN, with the service account in Active Directory; see the overview of `setspn.exe` on Microsoft TechNet.
3. Create a keytab for the SPN with the `ktpass` utility.
4. Place the keytab in the appropriate location on the Linux or Unix computer.
5. Configure the authentication module to get its Kerberos key from the generated keytab.
6. Configure the authentication module to determine appropriate roles by examining Active Directory group membership.
7. Configure an application to restrict access to Active Directory authenticated users in certain roles.
8. Test SSO by accessing restricted web sites from a Windows client running Microsoft Internet Explorer or Mozilla Firefox. Repeat this step on Linux and Unix using Firefox.

13.2. Make Sure PAM Is Enabled for SSH

If your Active Directory account is not working with SSH, make sure that `UsePAM` is enabled in `sshd_config` and make sure that your `sshd` is linked to the PAM libraries.

1. Determine which `sshd` is running by executing the following command:

```
bash-3.2# ps --ef -| grep sshd
root  8199      1  0  Feb  6  -?          0:00 -/opt/ssh/sbin/sshd
```

```
root 2987 8199 0 Mar 3 -? 0:04 sshd: root@notty
root 24864 8199 0 12:16:25 -? 0:00 sshd: root@pts/0
root 2998 8199 0 Mar 3 -? 0:05 sshd: root@notty
root 24882 24880 0 12:16:54 pts/0 0:00 grep sshd
```

2. Either use `lsof` to find out which conf file it is reading, or start it up with debugging to figure out the default path. Example:

```
username@computer:~$ -/usr/sbin/sshd --dd --t
debug2: load_server_config: filename -/etc/ssh/sshd_config
debug2: load_server_config: done config len = 664
debug2: parse_server_config: config -/etc/ssh/sshd_config len 664
debug1: sshd version OpenSSH_5.1p1 Debian-3ubuntu1
Could not load host key: -/etc/ssh/ssh_host_rsa_key
Could not load host key: -/etc/ssh/ssh_host_dsa_key
```

3. Verify that UsePAM is enabled in the config file. As a best practice, make a backup copy of the configuration file before you change it.

4. Run `ldd` on `sshd` to make sure it links with `libpam`. Example from an IA64 HP system:

```
bash-3.2# ldd -/opt/ssh/sbin/sshd
libpam.so.1 => -/usr/lib/hpux64/libpam.so.1
libdl.so.1 => -/usr/lib/hpux64/libdl.so.1
libnsl.so.1 => -/usr/lib/hpux64/libnsl.so.1
libxnet.so.1 => -/usr/lib/hpux64/libxnet.so.1
libsec.so.1 => -/usr/lib/hpux64/libsec.so.1
libgssapi_krb5.so => -/usr/lib/hpux64/libgssapi_krb5.so
libkrb5.so => -/usr/lib/hpux64/libkrb5.so
libpthread.so.1 => -/usr/lib/hpux64/libpthread.so.1
libc.so.1 => -/usr/lib/hpux64/libc.so.1
libxti.so.1 => -/usr/lib/hpux64/libxti.so.1
libxti.so.1 => -/usr/lib/hpux64/libxti.so.1
libm.so.1 => -/usr/lib/hpux64/libm.so.1
libk5crypto.so => -/usr/lib/hpux64/libk5crypto.so
libcom_err.so => -/usr/lib/hpux64/libcom_err.so
libk5crypto.so => -/usr/lib/hpux64/libk5crypto.so
libcom_err.so => -/usr/lib/hpux64/libcom_err.so
libdl.so.1 => -/usr/lib/hpux64/libdl.so.1
bash-3.2#
```

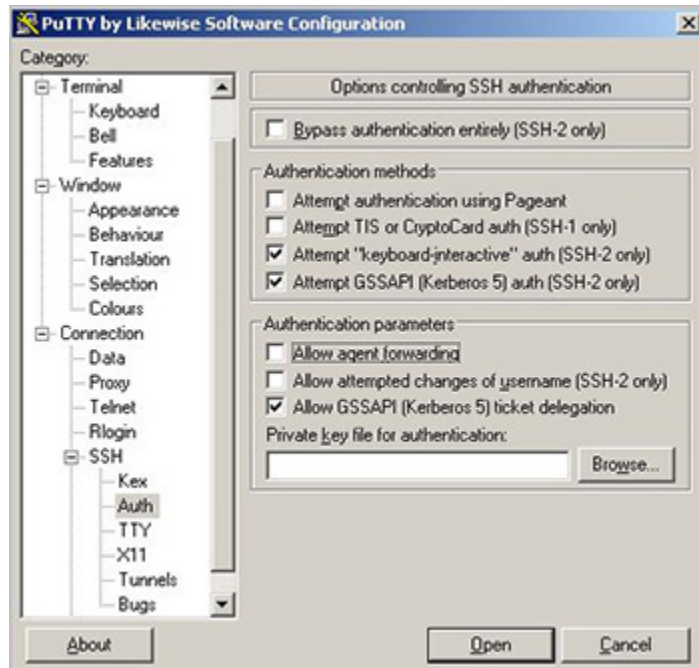
13.3. Configure PuTTY for Windows-Based SSO

To use PuTTY to connect to a Linux or Unix machine from a Windows machine and then connect to a second Linux or Unix, you must configure PuTTY to allow ticket forwarding and you must set the base Linux or Unix computer in Active Directory to be trusted for delegation.

Important: The following procedure assumes that you are using a GSSAPI-enhanced version of PuTTY, such as PuTTY by Likewise Software, which you can download at http://likewise.com/download/Likewise_PuTTY.zip. The procedure also assumes that there are DNS entries for all three computers and that you use host names to connect to the target computers. If DNS search domains are properly setup on your client systems, you can use short host names.

Configure PuTTY

1. In the PuTTY Configuration dialog, select **Allow GSSAPI (Kerberos 5) ticket delegation**. (With some versions of PuTTY, the option is named **Allow Kerberos 5 ticket forwarding (SSH 1/2)**.)
2. Select **Attempt GSSAPI (Kerberos 5) auth (SSH-2 only)**. With some versions of PuTTY, the option is named **Attempt GSSAPI/Kerberos 5 authentication**.

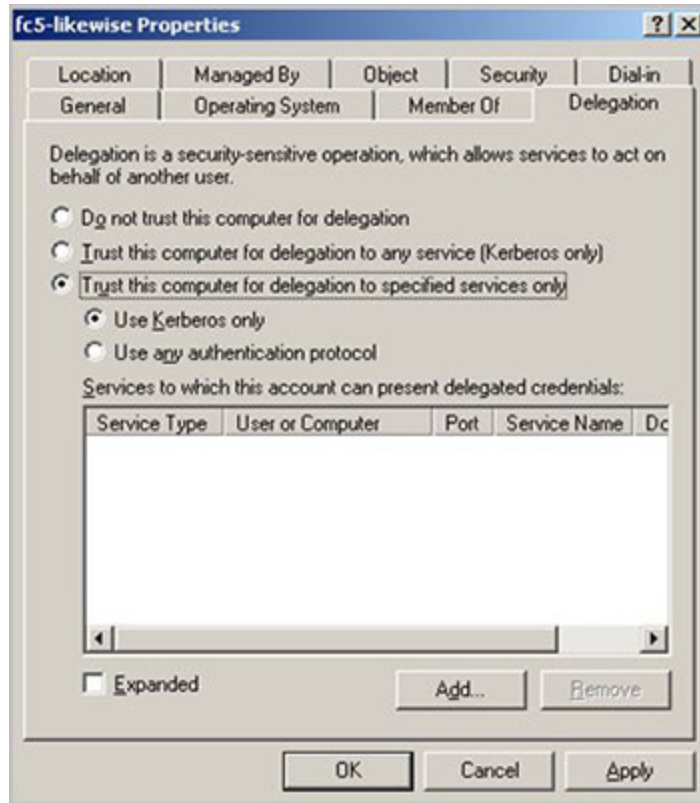


Configure the Base Linux Computer in Active Directory

This procedure assumes the base Linux or Unix computer is joined to Active Directory with Likewise. To perform this procedure, you must be a member of the Domain Administrators security group or the Enterprise Administrators security group, or you must have been delegated authority.

Windows Server 2003 R2

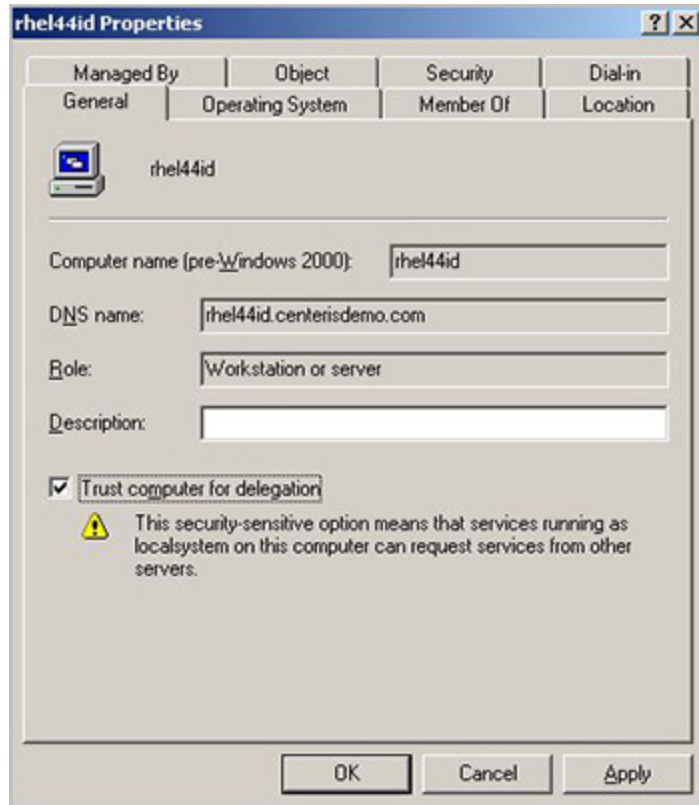
1. In Active Directory Users and Computers, in the console tree, click **Computers**.
2. In the details pane, right-click the computer that you want, and then click **Properties**.
3. On the **Delegation** tab, click **Trust this computer for delegation to specified services only**:



4. Confirm that **Use Kerberos only** is selected.
5. Click **Add** and, in **Add Services**, click **Users and Computers**.
6. In **Enter the object names to select**, type the name of the user or computer that the computer will be trusted to delegate for, and then click **OK**.
7. In **Add Services**, click the service or services that will be trusted for delegation and then click **OK**.

Windows 2000

1. In Active Directory Users and Computers, in the console tree, click **Computers**.
2. In the details pane, right-click the computer that you want, and then click **Properties**.
3. On the **General** tab, select **Trust computer for delegation**:



13.4. Configure Apache for SSO

This section describes how to configure Likewise and the Apache HTTP Server to provide single sign-on authentication through Active Directory with Kerberos 5. The instructions assume that you know how to administer Active Directory, the Apache HTTP Server, and computers running Linux.

Single sign-on for the Apache HTTP server uses the Simple and Protected GSS-API Negotiation Mechanism, or SPNEGO, to negotiate authentication with Kerberos. SPNEGO is an Internet standard documented in RFC 2478 and is commonly referred to as the negotiate authentication protocol. The Likewise `mod_auth_kerb` module lets an Apache web server running on a Linux or Unix system authenticate and authorize users based on their Active Directory domain credentials.

Important: This topic assumes that you have installed either Likewise Open 5.0 or later or Likewise Enterprise 5.0 or later, build **3946** or later, on the Linux computer running your Apache HTTP Server and that you have joined the server to Active Directory. With build 3946, Likewise 5.0 began to include the Apache `mod_auth_kerb` module in `/opt/likewise/apache`; the Likewise version of the `mod_auth_kerb` module is required to set up your Apache HTTP Server for single sign-on. Later versions of Likewise, such as 6.1, package the module independently: It is in the application integration installer, which you can obtain for free from the Likewise web site by registering to download Likewise Open. (The name of the application integration package looks like this: `LikewiseAppIntegration-6.1.0.8656-linux-i386-rpm.sh`.)

To check whether your build of Likewise Enterprise or Likewise Open includes `mod_auth_kerb`, confirm that the following components exist:

```
/opt/likewise/apache/2.0/mod_auth_kerb.a
```

```
/opt/likewise/apache/2.0/mod_auth_kerb.so
/opt/likewise/apache/2.2/mod_auth_kerb.a
/opt/likewise/apache/2.2/mod_auth_kerb.so
```

Requirements

- Likewise Open 5.0 or later or Likewise Enterprise 5.0 or later, build 3946 or later. Later versions of Likewise, such as 6.1, also require the application integration package (LikewiseAppIntegration-6.1.0.8656-linux-i386-rpm.sh).
- The Linux or Unix computer that is hosting the Apache web server is joined to Active Directory.
- An Apache HTTP Server 2.0 or 2.2 that supports dynamically loaded modules. To check whether your Apache web server supports dynamically loaded modules, execute the following command and verify that `mod_so.c` appears in the list of compiled modules:

```
httpd -l
```

```
Compiled in modules:
  core.c
  prefork.c
  http_core.c
  mod_so.c
```

For Apache installations that are compiled from the source code, make sure that `--enable-module=so` is specified when `./configure` is executed:

```
./configure --enable-module=so
```

- Your Kerberos libraries must support SPNEGO. For example, MIT Kerberos libraries that are version 1.5 and later support SPNEGO; earlier versions do not. Make sure your Kerberos libraries support SPNEGO by running `ldd`:

```
which httpd
/usr/sbin/httpd
ldd -/usr/sbin/httpd
```

In the results, find the line that references `libgssapi`:

```
libgssapi_krb5.so.2 => /usr/lib/libgssapi_krb5.so.2 (0x00231000)
```

Finally, query the version number of the library and make sure it is **1.5 or later**:

```
rpm -qif /usr/lib/libgssapi_krb5.so.2
```

```
Name           -: krb5-libs                      Relocations: (not
relocatable)
Version        -: 1.5                               Vendor: Red Hat, Inc.
Release       -: 17                               Build Date: Tue 16 Jan
2007 10:01:00 AM PST
Install Date:  Fri 14 Dec 2007 09:09:44 AM PST    Build Host: ls20-
bc1-13.build.redhat.com
Group          -: System Environment/Libraries    Source RPM:
krb5-1.5-17.src.rpm
```

```
Size           -: 1333337                               License: MIT, freely
distributable.
Signature      -: DSA/SHA1, Wed 17 Jan 2007 10:57:33 AM PST, Key ID
5326810137017186
Packager       -: Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
URL            -: http://web.mit.edu/kerberos/www/
Summary        -: The shared libraries used by Kerberos 5.
Description -:
Kerberos is a network authentication system. The krb5-libs package
contains the shared libraries needed by Kerberos 5. If you are using
Kerberos, you need to install this package.
[root@rhel5d sbin]#
```

Configure Apache HTTP Server 2.2 for SSO on RHEL 5

The following instructions demonstrate how to configure Likewise and Apache for SSO on a Red Hat Enterprise Linux 5 computer. The steps vary by operating system and by Apache version. Ubuntu, in particular, uses `apache2` instead of `httpd` for commands, the name of the daemon, the configuration directory, the name of the configuration file, and so forth.

Important: Configuring web servers is complex. Before you deploy your configuration to a production web server, implement and test it in a test environment. More: Before you change your web server's configuration, read and understand the Apache HTTP Server documentation at <http://httpd.apache.org/docs/> and the `mod_auth_kerb` documentation at <http://modauthkerb.sourceforge.net/configure.html>. Before you change a file, make a backup copy of it.

1. Determine whether your Apache server is 2.0 or 2.2 by running the following command:

```
httpd -v

Server version: Apache/2.2.3
Server built:   Nov 29 2006 06:33:19
```

2. Edit your Apache configuration file -- `/etc/httpd/conf/httpd.conf` -- to add a directive to load the Likewise `auth_kerb_module` for your version of Apache. Since my Red Hat computer is running Apache 2.2.3, I have added the 2.2 version of the module to the list after the other `auth` modules (which were already listed in the file):

```
LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule auth_kerb_module -/opt/likewise/apache/2.2/
mod_auth_kerb.so
```

3. In `/etc/httpd/conf/httpd.conf`, configure authentication for a directory and then restart the web server; example:

```
<Directory -"/var/www/html/secure">
Options Indexes MultiViews FollowSymLinks
AllowOverride None
Order deny,allow
Deny from all
Allow from 127.0.0.0/255.0.0.0 -::1/128
AuthType Kerberos
AuthName -"Kerberos Login"
KrbAuthRealms LIKWISEDEMO.COM
```



```
Krb5Keytab -/etc/apache2/http.ktb
Require valid-user
</Directory>
```

Tip: You can require that a user be a member of a security group to access the Apache web server by replacing `Require valid-user` with `Require group name-of-your-group`, as shown in the example below. To control group access by requiring group membership, however, you must first install and load `mod_auth_pam`; for instructions on how to set up `mod_auth_pam`, see http://pam.sourceforge.net/mod_auth_pam/install.html. (Because `mod_auth_pam` is no longer maintained, you should consider using `mod_authz_unixgroup` instead; see the instructions later in this section.)

```
<Directory -"/var/www/html/secure">
Options Indexes MultiViews FollowSymLinks
AllowOverride None
Order deny,allow
Deny from all
Allow from 127.0.0.0/255.0.0.0 -::1/128
AuthType Kerberos
AuthName -"Kerberos Login"
KrbAuthRealms LIKEWISEDEMO.COM
Krb5Keytab -/etc/apache2/http.ktb
Require group linuxfulladmins
</Directory>
```

4. Configure your web server for Secure Socket Layer (SSL). For instructions, see the Apache HTTP Server documentation.

Important: If SSO fails and you have not turned on SSL, your server will prompt you for an ID and password -- which will be sent in clear text. SSL encrypts all data that passes between the client browser and the web server. SSL can also perform Basic Authentication in a secure fashion, providing a fallback mechanism in the event that Kerberos authentication fails. Using SSL is especially important if the protected web site also needs to be accessible from outside the corporate network. For more information, see <http://modauthkerb.sourceforge.net/configure.html>.

5. In Active Directory, create a user account for the Apache web server in the same OU (or, with Likewise Enterprise, cell) to which the Linux computer hosting the web server is joined. Set the password of the user account to never expire. In the examples that follow, the user account for my Apache web server is named `httpUser`.
6. On the domain controller, create an RC4-HMAC keytab for the Apache web server by using Microsoft's `ktpass` utility. For information on `ktpass`, see <http://technet.microsoft.com/en-us/library/cc776746.aspx>. The keytab that you must create can vary by Windows version.

Example:

```
C:\>ktpass -/out keytabfile -/princ HTTP/
rhel5d.likewisedemo.com@LIKEWISEDEMO.COM -/pass SkiAlta2008 -/
mapuser likewisedemo\httpUser -/ptype KRB5_NT_PRINCIPAL
Targeting domain controller: steveh-dc.likewisedemo.com
Using legacy password setting method
Successfully mapped HTTP/rhel5d.likewisedemo.com to httpUser.
Key created.
Output keytab to keytabfile:
Keytab version: 0x502
```

```
keysize 80 HTTP/rhel5d.likewisedemo.com@LIKEWISEDEMO.COM ptype
0 (KRB5_NT_UNKNOWN) vno 3 etype 0x17 (RC4-HMAC) keylength 16
(0x2998807dc299940e2c6c81a08315c596)
```

Note: On Windows 2000, do not specify the domain name as part of the `/mapuser` parameter; just enter the name of the user.

7. Use secure FTP or another method to transfer the keytab file to the Linux computer that hosts your Apache web server and place the file in the location specified in your `<Directory>` configuration in `httpd.conf`. For example, using the configuration shown in Step 3 above, the keytab file would be placed in `/etc/apache2/http.ktb`.
8. Set the permissions of the keytab file to be readable by the ID under which the Apache web server runs and no one else.

Important: The Kerberos keytab file is necessary to authenticate incoming requests. It contains an encrypted, local copy of the host's key and, if compromised, might allow unrestricted access to the host computer. It is therefore crucial to protect it with file-access permissions.

Control Group Access with `mod_authz_unixgroup`

Instead of using the `mod_auth_pam`, which is no longer maintained, you can require that a user be a member of a security group to access the Apache web server by using `mod_authz_unixgroup`. First, install `mod_authz_unixgroup`:

```
yum install httpd-devel
wget http://mod-auth-external.googlecode.com/files/
mod_authz_unixgroup-1.0.2.tar.gz
tar --xzvf mod_authz_unixgroup-1.0.2.tar.gz
cd mod_authz_unixgroup-1.0.2
apxs --c mod_authz_unixgroup.c
apxs --i --a mod_authz_unixgroup.la
```

Then, in `/etc/httpd/conf/httpd.conf`, replace `Require valid-user` with `AuthzUnixgroup on` and `Require group name-of-your-group`:

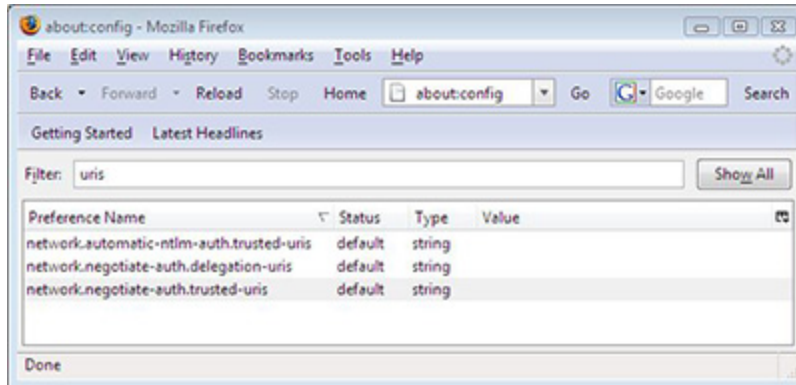
```
<Directory -"/var/www/html/secure">
...
KrbAuthRealms LIKEWISEDEMO.COM
Krb5Keytab -/etc/apache2/http.ktb
AuthzUnixgroup on
Require group linuxfulladmins
</Directory>
```

For more information, see the documentation for `mod_authz_unixgroup`.

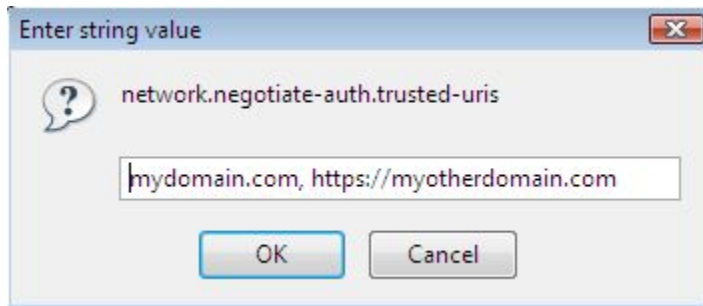
Configure Firefox for SSO

To set up Firefox for single sign-on, you must turn on the Simple and Protected GSS-API Negotiation Mechanism, or SPNEGO, to negotiate authentication with Kerberos.

1. Open Firefox.
2. In the **Go** box, type `about:config`, and then click **Go**.
3. In the **Filter** box, type `uris`.



- Double-click **network.negotiate-auth.trusted-uris**, enter a comma-separated list of URL prefixes or domains that are permitted to engage in SPNEGO authentication with the browser, and then click **OK**. Example:

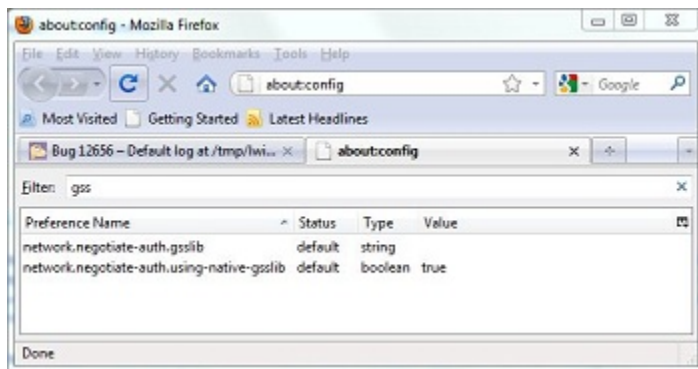


- Double-click **network.negotiate-auth.delegation-uris**, enter a comma-separated list of the sites for which the browser may delegate user authorization to the server, and then click **OK**.

For more information on how to configure Firefox, see <http://grolmsnet.de/kerbtut/firefox.html>.

- To negotiate with your web server through the GSSAPI by using NTLM as the preferred authentication protocol on a Mac OS X computer, you must also modify the GSS preferences as follows. To find the preferences, type `gss` into Firefox's filter box:

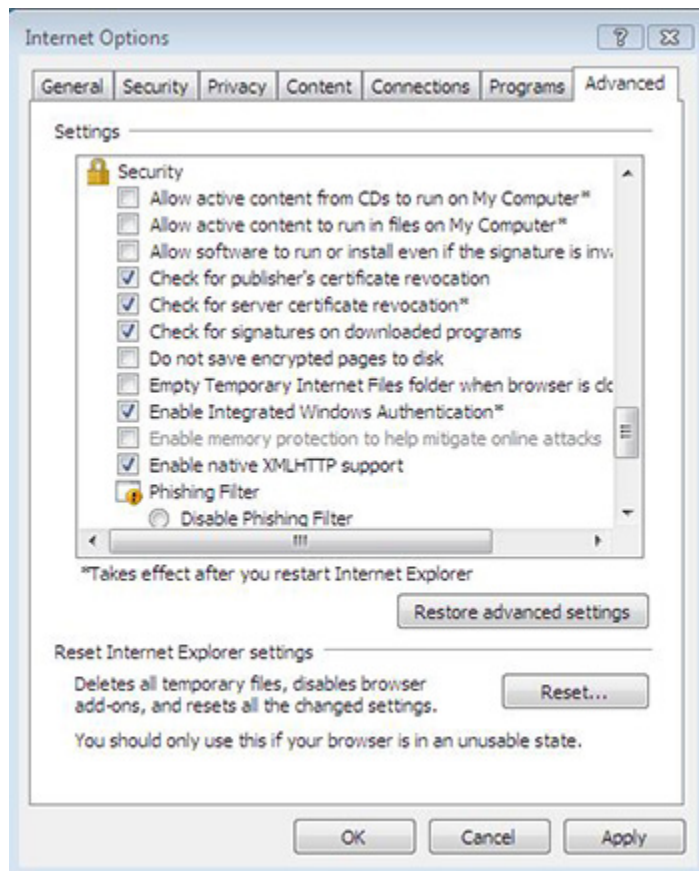
```
network.negotiate-auth.gsslib user set string -/opt/likewise/lib/
libgssapi_krb5.2.2.dylib
network.negotiate-auth.using-native-gsslib user set boolean
false
```



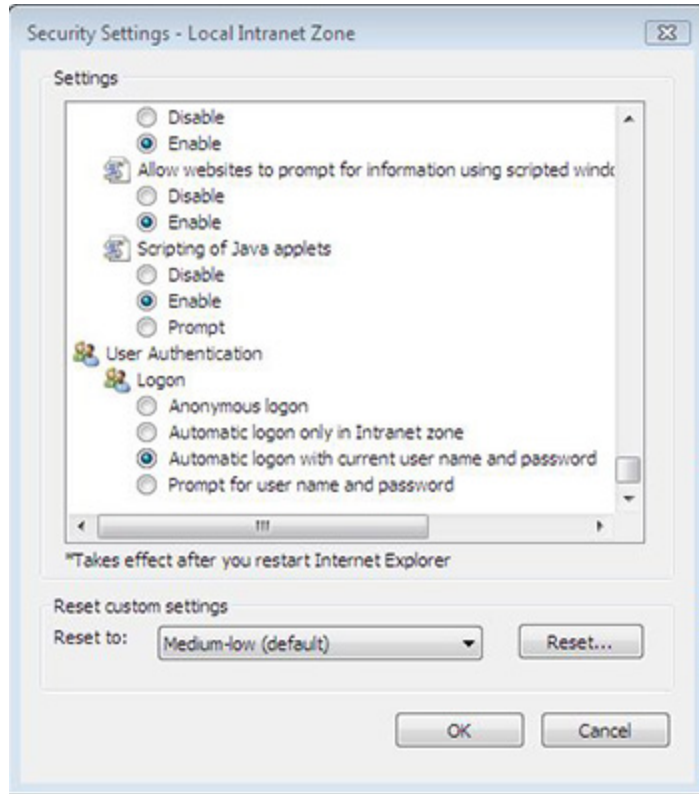
Configure Internet Explorer for SSO

Here's how to configure Internet Explorer 7.0 to use SPNEGO and Kerberos. The settings for other versions of IE might vary; see your browser's documentation for more information.

1. Start Internet Explorer 7.0.
2. On the **Tools** menu, click **Internet Options**.
3. Click the **Advanced** tab and make sure that the **Enable Integrated Windows Authentication** box is selected:



4. Click the **Security** tab.
5. Select a zone -- for example, **Local intranet** -- and then click **Custom level**.
6. In the **Settings** list, under **User Authentication**, click **Automatic logon with current user name and password** for a trusted site, or **Automatic logon only in Intranet zone** for a site you added to IE's list of Intranet sites. For more information, see your browser's documentation.



7. Return to the **Security** tab for **Internet Options** and set your web server as a trusted site.
8. Restart Internet Explorer.

Troubleshooting

The following tools can help diagnose problems with Kerberos authentication.

Apache Log File

The location of the Apache error logs is specified in the Apache configuration file under the `ErrorLog` directive. Here's an example directive from `/etc/httpd/conf/httpd.conf` on RHEL 5:

```
ErrorLog logs/error_log
```

The Microsoft Kerbtray Utility

The Microsoft Kerbtray.exe utility, part of the Windows 2000 Resource Kit, can verify whether Internet Explorer obtained a Kerberos ticket for your web server. You can download the utility at the following URL:

<http://www.microsoft.com/downloads/details.aspx?familyid=4E3A58BE-29F6-49F6-85BE-E866AF8E7A88&displaylang=en>

Klist

You can use the klist utility in `/opt/likewise/bin/klist` to check the Kerberos keytab file on a Linux or Unix computer. The command shows all the service principal tickets contained in the

keytab file so you can verify that the correct service principal names appear. Confirm that HTTP/myserver@MYDOMAIN.COM and HTTP/myserver.mydomain.com@MYDOMAIN.COM appear in the list. It is normal to see multiple entries for the same name.

Example:

```
klist --k krb5_myserver.keytab
```

```
Keytab name: FILE:krb5_myserver.keytab
```

```
KVNO Principal
```

```
-----  
 6 HTTP/myserver@MYDOMAIN.COM  
 6 HTTP/myserver@MYDOMAIN.COM  
 6 HTTP/myserver@MYDOMAIN.COM  
 6 HTTP/myserver.mydomain.com@MYDOMAIN.COM  
 6 HTTP/myserver.mydomain.com@MYDOMAIN.COM  
 6 HTTP/myserver.mydomain.com@MYDOMAIN.COM
```

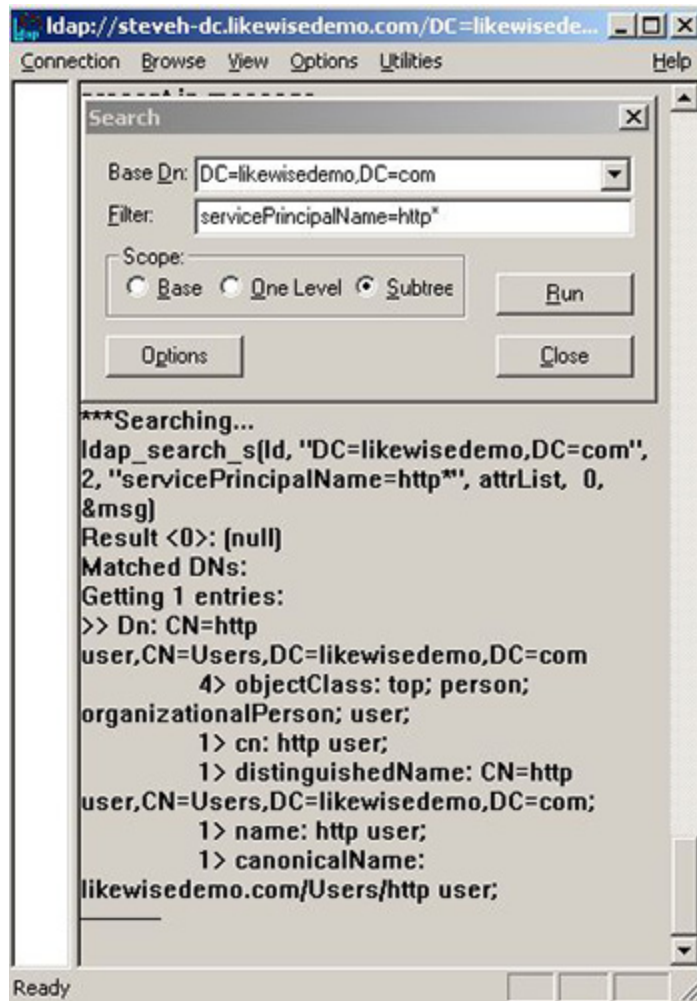
If your service principal names are incorrect, generate a new Kerberos keytab file.

Common Problems

Authentication problems can be difficult to diagnose. First, check all the configuration parameters, including the validity of the keytab file. Second, make sure none of the common problems listed in the following table are sabotaging authentication.

Problem	Solution
The system's clock is out of sync.	The Kerberos standard requires that system clocks be no more than 5 minutes apart. Make sure that the system clocks on the Active Directory domain controller, the Linux or Unix web server, and the client are synchronized.
The user accessing the web site is not on the require list	<p>If Kerberos ticket was obtained on the client or the user correctly entered his credentials during the Basic Authentication prompt, it might be because authentication worked but the authorization failed. If so, the Apache error_log will contain a line like this:</p> <pre>access to / failed, reason: user MYDOMAIN\\user not allowed access</pre> <p>Add the user to the <code>require user</code> directive or add the user's group to the <code>require group</code> directive.</p>
The user accessing the web site is logged on the wrong domain.	If the client user is logged on a domain different from the domain of the web server, one of two things will happen:

	<ol style="list-style-type: none"> 1. If the <code>KrbMethodK5Passwd</code> directive is set to on, or was not specified and thus defaults to on, the user will be prompted for credentials. 2. If <code>KrbMethodK5Passwd</code> is set to off, authentication will fail and the <code>Authorization Required</code> page will be displayed.
Internet Explorer does not consider the URL to be part of the Local Intranet zone or the Trusted sites.	<p>This problem commonly occurs when the web site is accessed by using a URL that includes the full domain name, such as <code>https://myserver.mydomain.com</code>. Internet Explorer tries to obtain Kerberos tickets only for web sites that are in the Local Intranet zone.</p> <p>Try to access the web site by using only the server name, for example <code>https://myserver</code>.</p> <p>Or, you can add the URL to a list of Local Intranet sites or the trusted sites by changing your options in Internet Explorer.</p>
The service principal name of the web site is mapped to more than one object in the Active Directory.	<p>Although this problem is rare, it is difficult to diagnose because the error messages are vague. The problem can occur after the <code>ktpass</code> utility was used repeatedly to generate a Kerberos keytab file for the web server.</p> <p>To check for this problem, log on your Active Directory domain controller and open the Event Viewer. Look for an event of type=Error, source=KDC, and event ID=11. The text of the event will be similar to the message below:</p> <p>There are multiple accounts with name <code>HTTP/myserver.mydomain.com</code> of type <code>DS_SERVICE_PRINCIPAL_NAME</code>.</p> <p>To fix the problem, find the computer or user objects that were used to map the service principal name in Active Directory and then use the ADSI Edit to manually remove the “<code>HTTP/myserver.mydomain.com</code>” string from the <code>servicePrincipalName</code> object property.</p> <p>Below the table is a screen shot that provides an example of how to find an object named <code>HTTP</code> by using <code>Ldp</code>:</p>



13.4.1. Kerberos Library Mismatch

Problem: Because some operating systems, such as the 64-bit version of Red Hat Enterprise Linux 5, use an outdated version of `/lib/libcom_err.so`, the Likewise authentication agent cannot locate the proper system library, leading to an error that looks like this:

```

httpd: Syntax error on line 202 of /etc/httpd/conf/httpd.conf:
Cannot load /opt/likewise/apache/2.2/mod_auth_kerb.so into server:
/opt/likewise/lib/libcom_err.so.3: symbol krb5int_strncpy, version
krb5support_0_MIT not defined in file libkrb5support.so.0
with link time reference
  
```

Solution: Force the `httpd` daemon to use the Likewise `krb5` libraries by opening the startup script for the Apache HTTP Server -- `/etc/init.d/httpd` -- and adding the path to the Likewise Kerberos libraries on the line that starts Apache. The line that starts the daemon can vary by operating system. Example on a 64-bit system:

```

LD_LIBRARY_PATH=/opt/likewise/lib64 LANG=$HTTPD_LANG daemon $httpd
$OPTIONS
  
```

On a 32-bit system, the path would look like this:


```
/opt/likewise/lib
```

Note: This modification changes the version of the Kerberos libraries that are used by the Apache HTTP Server. The change might result in compatibility issues with other modules of Apache that use Kerberos.

13.5. Configure a Java Application Server for SSO

This section describes how to set up Likewise and a Java web server to provide secure single sign-on through Active Directory with Integrated Windows Authentication. The instructions use Apache Tomcat as an example to demonstrate how to implement single sign-on with servlet authentication filters. Because servlet authentication filters are a generic Java technology common to most Java application servers, the procedure is similar for other Java application servers, such as JBoss. The instructions assume that you know how to configure Active Directory, Tomcat, and computers running Linux.

Before you can integrate Likewise 6.1 with a Java application servers, you must install a separate application integration package, which you can download for free from the Likewise web site by registering to download Likewise Open. (The name of the application integration package looks like this: `LikewiseAppIntegration-6.1.0.8656-linux-i386-rpm.sh`.)

Once you have installed the application integration package, here's how to configure your Tomcat server for SSO with Likewise. This section assumes you have installed Likewise 6.1 or later on the computer running the Java application server and have joined the server to an Active Directory domain.

Requirements

- Root access to the Linux or Unix computer.
- The Linux or Unix computer is joined to Active Directory with Likewise 6.1.
- The Linux or Unix computer is running Apache Tomcat Server version 5.5 or 6.0.
- The server is running JRE 1.5.0 or higher.
- The Likewise application integration package is installed.

Important: Configuring Java application servers is complex. Before you deploy your configuration to a production web server, implement and test it in a test environment. More: Before you change your application server's configuration, read and understand the Apache Tomcat documentation. Before you change a file, make a backup copy of it.

Components

The following Likewise components relevant to Apache integration are installed at `/opt/likewise/{lib, lib64}`:

Component name	Description
<code>lwjplatform.jar</code>	Likewise Platform Library
<code>lwservlets.jar</code>	Likewise authentication modules, including Servlet Filter and JAAS Module.
<code>lwtomcat.jar</code>	Likewise authentication modules specific to implementing the Tomcat authentication valve.

jna.jar	Java Native Access Library patched for UCS-2 support.
commons-codec-1.4.jar	Base64 and other encoding routines
commons-net-2.2.jar	Network utilities

Install the Authentication Components

The components from the integration package must be installed. Typically, an Apache Tomcat installation uses the following environment variables:

Environment Variable	Value
CATALINA_HOME_DIR	/usr/share/tomcat5 or /usr/share/tomcat6
CATALINA_BASE_DIR	/var/lib/tomcat5 or /var/lib/tomcat6

For the servlet filter and the required JAAS module, you must install the following components in `${CATALINA_HOME_DIR}/webapps/<web application>/lib`:

```
lwservlets.jar, lwjplatform.jar, jna.jar,  
commons-codec-1.4.jar, commons-net-2.2.jar
```

Symbolic links can be created to these jar files from the target directory.

Generate Kerberos Keytab File

The Kerberos keytab file is necessary to authenticate incoming requests. It contains an encrypted, local copy of the host's key. If compromised may allow unrestricted access to the host computer. It is therefore important to protect it with file access permissions. The file must be readable by the user group under which the Apache Tomcat server is running, typically `tomcat` on most Linux systems.

Next, you must get the server name of the web site that will require authentication. If you don't know the server name, try doing a reverse DNS name lookup on the IP address of the host or just use the `hostname` of the Linux or Unix system.

You will also need to know the full domain name of the domain to which the Linux or Unix system is joined.

Finally, you will need to figure out where to save the generated keytab file.

The steps below use a sample Apache user account name named `tomcat`, a sample server name of `myserver`, a sample full domain name of `MYDOMAIN.COM`, and a sample Kerberos keytab file named `/etc/krb5_myserver.keytab`. You must substitute the correct names from your system and configuration.

1. Set the `KRB5_KTNAME` environment variable to point to the Kerberos keytab file to be generated. This can be set in the `tomcat` init script at `/etc/init.d/tomcat`:

```
# export KRB5_KTNAME=FILE:/etc/krb5_myserver.keytab
```

2. Select a user in Active Directory. If you create a user, make sure to set the password for the user account to never expire. Also make sure "Use DES Encryption types for this account" is not checked in the user account properties in Active Directory. In this example, we are using the following user: `MYDOMAIN\tomcat`

3. Generate keytab entry on your Windows domain controller for the default HTTP service principal:

```
# ktpass
  -/out          c:\krb5_myserver.keytab
  -/pType       KRB5_NT_PRINCIPAL
  -/crypto      RC4-HMAC-NT
  -/princ       HTTP/myserver.mydomain.com@MYDOMAIN.COM
  -/mapuser     tomcat@MYDOMAIN.COM
  -/mapop       set
  -/pass        *
```

4. Change the group ownership of the keytab file:

```
# chown tomcat:tomcat /etc/ krb5_myserver.keytab
```

5. Set appropriate file permissions of the keytab file:

```
# chmod 600 /etc/krb5_myserver.keytab
```

6. If you choose not to create a separate keytab and the Tomcat server process is running in the context of the local tomcat user, you must provide read access to the default keytab file (typically at `/etc/krb5.keytab`) to the local tomcat user:

```
# chgrp tomcat -/etc/krb5.keytab
# chmod g+r -/etc/krb5.keytab
```

Modify the Web Application Configuration File

The only configuration that remains is to modify the Apache Tomcat configuration file -- `web.xml` -- by adding directives in each application container that is to be protected. Remember to replace `/etc/krb5_myserver.keytab` with your own keytab file name and replace `MYDOMAIN` with your short domain name. Servlet filters can be applied only to specific web applications.

Include the following configuration in the `web.xml` for the web application requiring authorization:

```
<filter>
  <filter-name>LikewiseAuth</filter-name>
  <filter-
class>com.likewise.auth.filter.spnego.LikewiseNegotiateFilter</filter-
class>
  <init-param>
    <param-name>deny-role</param-name>
    <param-value>MYDOMAIN\guests</param-value>
  </init-param>
  <init-param>
    <param-name>allow-role</param-name>
    <param-value>MYDOMAIN\domain^users</param-value>
  </init-param>
  <init-param>
    <param-name>remote-address-accept-filter</param-name>
    <param-value>10.100.0.0/24</param-value>
  </init-param>
  <init-param>
    <param-name>remote-address-accept-filter</param-name>
    <param-value>10.100.1.0,255.255.255.0</param-value>
  </init-param>
</filter>
```

```
<filter-mapping>
<filter-name>LikewiseAuth</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>
```

The configuration above ensures that only users who are in the MYDOMAIN\domain^users group can access the web pages from this application. Users who belong to the MYDOMAIN\guests group will be denied access. It is possible to configure multiple deny and allow roles. The user is checked for membership in the deny roles before being checked in the allow roles.

The remote-address-accept-filter configuration parameter can be used to specify IP addresses in the CIDR format or by using an IP Address, Subnet mask format. If this configuration is specified, the servlet performs authentication only on requests whose remote IP Address is in the range of one of the permitted addresses.

Protect the Web Pages

When trying to protect the web pages in a web application, the corresponding web.xml file should include the following configuration to protect all the web pages so they are accessible only to users who belong to the MYDOMAIN\domain^users group.

```
<security-role>
  <role-name>MYDOMAIN\domain^users</role-name>
</security-role>

<security-constraint>
  <display-name>Likewise Security Constraint</display-name>
  <web-resource-collection>
    <web-resource-name>Protected Area</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>MYDOMAIN\domain^users</role-name>
  </auth-constraint>
</security-constraint>
```

Likewise supports programmatic security. In addition, Likewise extends the standard Principal class. Once a request has been authenticated, you can get access to the additional principal information like this:

```
Principal p = request.getUserPrincipal();
If(p != null)
    LikewiseUser lwUser = (LikewiseUser) p;
```

Configure the JAAS Module

Likewise depends on the JAAS module: To integrate Likewise with a your servlet filters, the JAAS module is required. Here's how to set up the JAAS module to complete the integration of your Java application server with Likewise.

1. Create a file named /opt/likewise/share/config/jaas.policy and add the following lines to it:

```
grant Principal * * {
```

```
        permission java.security.AllPermission -"/**";
    -};
```

Create a file name `/opt/likewise/share/config/login.conf` and add the following lines to it:

```
    Jaas {
        com.likewise.auth.jaas.LikewiseLoginModule
sufficient;
    -};
```

2. Include the above files in your Tomcat startup environment, using the following variables as part of `CATALINA_OPTS`:

```
--Djava.security.auth.login.config=/opt/likewise/share/
config/login.conf
--Djava.security.auth.policy=/opt/likewise/share/config/
jaas.policy
```

3. Add the following configuration to `${CATALINA_BASE_DIR}/webapps/<web application>/WEB-INF/web.xml`:

```
<login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>Jaas</realm-name>
</login-config>

<security-role>
    <role-name>MYDOMAIN\domain^users</role-name>
</security-role>

<security-constraint>
    <display-name>Likewise Security Constraint</display-
name>
    <web-resource-collection>
        <web-resource-name>Protected Area</web-resource-
name>
        <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <role-name>MYDOMAIN\domain^users</role-name>
    </auth-constraint>
</security-constraint>
```

4. Add the following configuration to `${CATALINA_BASE_DIR}/webapps/<web application>/META-INF/context.xml` to add a realm named Jaas and to protect all the pages accessible by AD domain users:

```
<Context>
    <Realm className="org.apache.catalina.realm.JAASRealm"
        appName="Jaas"
        userClassNames="com.likewise.auth.LikewiseUser"
        roleClassNames="com.likewise.auth.LikewiseGroup"
```

```
        useContextClassLoader="false"  
        debug="true" -/>  
</Context>
```

Restart the Tomcat Server

Finally, restart the Tomcat server:

```
/etc/init.d/tomcat restart
```

Set Up Firefox and Internet Explorer for SSO

Follow the directions in the following sections and then you're ready to use your Java web application for SSO with Likewise:

Configure Firefox for SSO

Configure Internet Explorer for SSO

Troubleshooting

In the case of an authentication failure, the Apache Tomcat log file may contain information to help solve the problem. The Tomcat logs are typically located under `${CATALINA_HOME_DIR}/logs`. It is possible to set the “`java.security.debug`” variable in the Tomcat environment to elevate the log level and to help check for security issues.

```
$SU -- $TOMCAT_USER --c -"KRB5_KTNAME=/etc/keytab.likewise  
CATALINA_OPTS=-Djava.security.debug=access,failure  
$TOMCAT_SCRIPT start" >> $TOMCAT_LOG 2>&1
```

13.6. Examples

To view sample code that shows you how to use Likewise for single sign-on with protocols such as FTP and Telnet, see [Single Sign-On Examples](#).

Chapter 14. Configuring the Likewise Services with the Registry

14.1. About the Registry

The Likewise registry is a hierarchical database that stores configuration information for Likewise daemons, authentication providers, drivers, and other services. On Linux, Unix, and Mac computers, the Likewise services continually access the registry to obtain settings for their parameters. The Likewise authentication service, for example, queries the registry to determine which log level to use or which home directory template to apply to a user. In Likewise 5.4 or later, the registry replaces the text-based configuration files like `lsassd.conf` that were used in Likewise 5.3 or earlier.

When you install the Likewise agent on a Linux, Unix, or Mac computer but do not install Likewise Enterprise on a Windows administrative workstation connected to Active Directory, you cannot configure local Likewise settings with group policies. Instead, you must edit the local Likewise registry. You can access the registry and modify its settings by using the Likewise registry shell `-- lwregshell` `--` in `/opt/likewise/bin/`.

This chapter describes the structure of the registry, demonstrates how to change a value in it, and lists the local Likewise configuration options.

Most of the registry settings can be centrally managed with group policies when you use Likewise Enterprise; see [About Group Policies in the Group Policy Administration Guide](#). If you modify a setting in the registry that is managed by a group policy, the change will not persist: It will be overwritten by the setting in the policy as soon as the group policy object is updated, which typically takes place once every 30 minutes. Likewise Open does not apply group policies.

14.1.1. The Structure of the Registry

The Likewise registry contains one predefined top-level, or root, key: `HKEY_THIS_MACHINE`. Within the root key, the structure of the registry is delineated by service into branches of keys, subkeys, and values. A key is similar to a folder; it can contain additional keys and one or more value entries. A value entry is an ordered pair with a name and a value. A subkey, similar to a subfolder, is simply a child key that appears under another key, the parent. A branch describes a key and all of its contents, including subkeys and value entries.

The upper level of the Likewise registry's hierarchical structure looks like this:

```
\> ls
[HKEY_THIS_MACHINE]

\> cd HKEY_THIS_MACHINE\
HKEY_THIS_MACHINE\> ls

[HKEY_THIS_MACHINE\Services]

HKEY_THIS_MACHINE\> cd Services\
HKEY_THIS_MACHINE\Services> ls

[HKEY_THIS_MACHINE\Services\]
```

```
[HKEY_THIS_MACHINE\Services\dcerpc]
[HKEY_THIS_MACHINE\Services\eventlog]
[HKEY_THIS_MACHINE\Services\lsass]
[HKEY_THIS_MACHINE\Services\lwio]
[HKEY_THIS_MACHINE\Services\lwreg]
[HKEY_THIS_MACHINE\Services\netlogon]
[HKEY_THIS_MACHINE\Services\npfs]
[HKEY_THIS_MACHINE\Services\pvfs]
[HKEY_THIS_MACHINE\Services\rdr]
[HKEY_THIS_MACHINE\Services\srv]
[HKEY_THIS_MACHINE\Services\svs\svcs]
```

Each of the services corresponds to a Likewise daemon, driver, or other service. The subkeys within each service contain value entries. A value specifies the setting for an entry, often presented under the parameters key. The following output illustrates the hierarchy of keys, subkeys, and their value entries for the upper levels of the lsass service.

```
[HKEY_THIS_MACHINE\Services\lsass\] ❶
  -"Arguments"      REG_SZ          -"/opt/likewise/sbin/lsassd ---
syslog" ❷
  -"Dependencies"   REG_SZ          -"netlogon lwio lwreg rdr npfs" ❸
  -"Description"    REG_SZ          -"Likewise Security and
Authentication Subsystem"
  -"Path"           REG_SZ          -"/opt/likewise/sbin/lsassd" ❹
  -"Type"           REG_DWORD       0x00000001 (1) ❺

[HKEY_THIS_MACHINE\Services\lsass\Parameters] ❻

HKEY_THIS_MACHINE\Services\lsass> cd Parameters
HKEY_THIS_MACHINE\Services\lsass\Parameters> ls

[HKEY_THIS_MACHINE\Services\lsass\Parameters\]
  -"EnableEventlog"      REG_DWORD       0x00000000 (0) ❼
  -"LogLevel"            REG_SZ          -"error"
  -"LogNetworkConnectionEvents" REG_DWORD       0x00000001 (1)

[HKEY_THIS_MACHINE\Services\lsass\Parameters\NTLM] ❽
[HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM]
[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers]
[HKEY_THIS_MACHINE\Services\lsass\Parameters\RPCServers]
```

- ❶ The key for the lsass service. Lsass is the Likewise authentication and security subsystem.
- ❷ The value entry for the command that is run to start the service, including command-line arguments. For the lsass daemon, the default argument routes messages to syslog.
- ❸ Other services that the service depends on. The Likewise Service Manager starts the dependencies before it starts the lsassd service. It is recommended that you do not change a service's list of dependencies or start order.
- ❹ The system path to the lsassd daemon. It is recommended that you do not change the path to a daemon or other service.
- ❺ The data type of the daemon. Its boolean value is set to the hexadecimal representation of 1, for true: It is turned on. Data types are discussed below.
- ❻ The branch for the service's parameters.
- ❼ The value entry for EnableEventlog. By default, this entry is set to 0, for false: It is turned off.
- ❽ The branch for the NTLM subkey.

The `lsass` service is the primary location for configurations targeted at system administrators and end users. It contains nearly all the configuration options for the Likewise authentication and security service.

14.1.1.1. Additional Branches

The following branches contain a minimal set of value entries, most of which are used by their corresponding service to function properly. It is recommended that you do not change them.

```
[HKEY_THIS_MACHINE\Services\dcerpc]
"Dependencies"=" "
"Description"="Likewise DCE/RPC Endpoint Mapper"
"Path"="/opt/likewise/sbin/dcerpcd"

[HKEY_THIS_MACHINE\Services\lwreg]
"Dependencies"=" "
"Description"="Likewise Registry Service"
"Path"="/opt/likewise/sbin/lwregd"

[HKEY_THIS_MACHINE\Services\npfs]
"Dependencies"="lwio"
"Description"="Likewise Named Pipe Filesystem"
"Path"="/opt/likewise/lib/libnpfs.sys.so"

[HKEY_THIS_MACHINE\Services\pvfs]
"Dependencies"="lwio"
"Description"="Likewise POSIX VFS Filesystem"
"Path"="/opt/likewise/lib/libpvfs.sys.so"

[HKEY_THIS_MACHINE\Services\rdr]
"Dependencies"="lwio"
"Description"="Likewise CIFS Redirector"
"Path"="/opt/likewise/lib/librdr.sys.so"

[HKEY_THIS_MACHINE\Services\srv]
"Dependencies"="lwio pvfs npfs lsass"
"Description"="Likewise CIFS Server"
"Path"="/opt/likewise/lib/libsrv.sys.so"

[HKEY_THIS_MACHINE\Services\svsvcd]
"Dependencies"="dcerpc lwio srv npfs"
"Description"="Likewise Server Service"
"Path"="/opt/likewise/sbin/svsvcd"
```

14.1.2. Data Types

The Likewise registry employs four data types to store values. The values of data types are case sensitive. The following table lists the data types that are defined and used by Likewise. The maximum size of a key is 255 characters (absolute path).

Name	Data Type	Description
------	-----------	-------------

Binary Value	REG_BINARY	A sequence of bytes. Displayed in the registry shell in hexadecimal format. The maximum size is 1024 bytes.
DWORD Value	REG_DWORD	Data represented by a 32-bit integer. Parameters and services are typically set as this data type. The values are displayed in the registry shell in hexadecimal and decimal format. When a parameter is turned off, it is set to 0; when a parameter is turned on, it is set to 1.
Multi-String Value	REG_MULTI_SZ	A multiple string. Values that include lists or multiple values typically use this data type. Values are strings in quotation marks separated by spaces. In an import of a Likewise registry file, the multi-string values typically contain an <code>sza:</code> prefix. In an export of the registry, the multi-string values typically contain an <code>hex(7):</code> prefix. The maximum size of a REG_MULTI_SZ is 1024 bytes, total, not each string in the multi string. There are, however, null bytes between strings that contribute to the count, so the actual byte count is slightly less.
String Value	REG_SZ	A text string. The maximum size of a REG_SZ value is 1023 characters (1024 bytes, including the null terminator).

14.2. Modify Settings with the lwconfig Tool

To quickly change an end-user setting in the registry that is not managed by a group policy, you can run the `lwconfig` command-line tool as root:

```
/opt/likewise/bin/lwconfig
```

The syntax to change the value of a setting is as follows, where `setting` is replaced by the registry entry that you want to change and `value` by the new value that you want to set:

```
/opt/likewise/bin/lwconfig setting value
```

Here's an example of how to use `lwconfig` to change the `AssumeDefaultDomain` setting:

```
[root@rhel5d bin]# ./lwconfig ---detail AssumeDefaultDomain ❶
Name: AssumeDefaultDomain
```

Description: Apply domain name prefix to account name at login
Type: boolean
Current Value: false
Accepted Values: true, false
Current Value is determined by local policy.

```
[root@rhel5d bin]# ./lwconfig AssumeDefaultDomain true ❷
```

```
[root@rhel5d bin]# ./lwconfig --show AssumeDefaultDomain ❸  
boolean  
true  
local policy
```

- ❶ Use the `--detail` option to view the setting's current value and to determine the values that it accepts.
- ❷ Set the value to `true`.
- ❸ Use the `--show` option to confirm that the value was set to `true`.

To view the registry settings that you can change with `lwconfig`, execute the following command:

```
/opt/likewise/bin/lwconfig --list
```

You can also import and apply a number of settings with a single command by using the `--file` option combined with a text file that contains the settings that you want to change followed by the values that you want to set. Each setting-value pair must be on a single line. For example, the contents of my flat file, named `newRegistryValuesFile` and saved to the desktop of my Red Hat computer, looks like this:

```
AssumeDefaultDomain true  
RequireMembershipOf -"likewisedemo\\support" -"likewisedemo\  
\domain^admins"  
HomeDirPrefix -/home/ludwig  
LoginShellTemplate -/bash/sh
```

To import the file and automatically change the settings listed in the file to the new values, I would execute the following command as root:

```
/opt/likewise/bin/lwconfig --file /root/Desktop/newRegistryValuesFile
```

Another Example

Here's another example of how to use `lwconfig` to find a setting and change it. Let's say you want to view the available trust settings because you know there are inaccessible trusts in your Active Directory network and you want to set Likewise to ignore all the trusts before you try to join a domain.

To do so, use `grep` with the `list` option:

```
/opt/likewise/bin/lwconfig --list | grep -i trust
```

The results will look something like this:

```
DomainManagerIgnoreAllTrusts  
DomainManagerIncludeTrustsList  
DomainManagerExcludeTrustsList
```

Next, use the `details` option to list the values that the `DomainManagerIgnoreAllTrusts` setting accepts:

```
[root@rhel5d bin]# ./lwconfig ---details DomainManagerIgnoreAllTrusts
Name: DomainManagerIgnoreAllTrusts
Description: When true, ignore all trusts during domain enumeration.
Type: boolean
Current Value: false
Accepted Values: true, false
Current Value is determined by local policy.
```

Now change the setting to `true` so that Likewise will ignore trusts when you try to join a domain.

```
[root@rhel5d bin]# ./lwconfig DomainManagerIgnoreAllTrusts true
```

Finally, check to make sure the change took effect:

```
[root@rhel5d bin]# ./lwconfig ---show DomainManagerIgnoreAllTrusts
boolean
true
local policy
```

In the example output that shows the setting's current values, `local policy` is listed -- meaning that the policy is managed locally through `lwconfig` because a Likewise Enterprise group policy is not managing the setting. You cannot locally modify a setting that is managed by a group policy.

For more information on the arguments of `lwconfig`, run the following command:

```
/opt/likewise/bin/lwconfig --help
```

14.3. Gain Access to the Registry

You can access and modify the registry by using the registry shell -- `lwregshell` -- in `/opt/likewise/bin`. The shell works in a way that is similar to `BASH`. You can navigate the registry's hierarchy with the following commands:

```
cd
ls
pwd
```

You can view a list of commands that you can execute in the shell by entering `help`:

```
/opt/likewise/bin/lwregshell
\> help
usage: regshell [--file -| --f] command_file.txt
        add_key [[KeyName]]
        list_keys [[keyName]]
        delete_key [KeyName]
        delete_tree [KeyName]
        cd [KeyName]
        pwd
        add_value [[KeyName]] -"ValueName" Type -"Value" ["Value2"]
[...]
        set_value [[KeyName]] -"ValueName" -"Value" ["Value2"] [...]
        list_values [[keyName]]
```

```
delete_value [[KeyName]] -"ValueName"
set_hive HIVE_NAME
import file.reg
export [[keyName]] file.reg
upgrade file.reg
exit -| quit -| ^D

Type: REG_SZ -| REG_DWORD -| REG_BINARY -| REG_MULTI_SZ
      REG_DWORD and REG_BINARY values are hexadecimal
Note: cd and pwd only function in interactive mode
Note: HKEY_THIS_MACHINE is the only supported hive

\>
```

Note: In the unlikely event that you want to restore all the registry's default values, you must leave the domain, stop all the Likewise services, manually delete `/var/lib/likewise/db/registry.db`, and then reinstall Likewise.

14.4. Change the Value of an Entry with the Shell

You can change a value in the registry by executing the `set_value` command with the shell. The following procedure demonstrates how to change the value of the PAM key's `LogLevel` entry. The procedure to change other keys is similar. After you modify a registry setting for a Likewise service, you must refresh the corresponding service with the Likewise Service Manager for the changes to take effect.

1. With the root account, start `lwregshell`:

```
/opt/likewise/bin/lwregshell
```

2. Change directories to the location of the PAM key and list its current settings:

```
[root@rhel5d bin]# ./lwregshell
\> cd HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM
HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM> ls

[HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM\]
-"DisplayMotd"          REG_DWORD          0x00000001 (1)
-"LogLevel"             REG_SZ             -"error"
-"UserNotAllowedError"  REG_SZ             -"Access denied"
```

3. Execute the `set_value` command with the name of the value as the first argument and the new value as the second argument:

```
HKEY_THIS_MACHINE\services\lsass\Parameters\PAM> set_value
LogLevel debug
```

4. List the key's value entries to confirm that the value was changed:

```
HKEY_THIS_MACHINE\services\lsass\Parameters\PAM> ls

[HKEY_THIS_MACHINE\services\lsass\Parameters\PAM\]
-"DisplayMotd"          REG_DWORD          0x00000001 (1)
-"LogLevel"             REG_SZ             -"debug"
```

```
- "UserNotAllowedError" REG_SZ          - "Access denied"
```

5. Exit the shell:

```
HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM> quit
```

6. After you change a setting in the registry, you must use the Likewise Service Manager -- `lws` -- to force the service to begin using the new configuration. Because we changed a configuration of the `lsass` service, we must refresh it by executing the following command with super-user privileges:

```
/opt/likewise/bin/lws refresh lsass
```

14.4.1. Set Common Options with the Registry Shell

This section shows you how to modify several common Likewise settings by using the registry shell: the default domain, the home directory, and the shell.

1. As root or with `sudo`, start the registry shell:

```
/opt/likewise/bin/lwregshell
```

2. Change directories to the following location:

```
cd HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers  
\ActiveDirectory
```

3. Change the shell to, for example, `bash`:

```
set_value LoginShellTemplate /bin/bash
```

For more information, see [Set the Home Directory and Shell for Domain Users](#).

4. Set the option to use the default domain:

```
set_value AssumeDefaultDomain 1
```

5. Leave the shell:

```
quit
```

6. After you change a setting in the registry, you must use the Likewise Service Manager -- `lws` -- to force the service to begin using the new configuration. Because we changed a configuration of the `lsass` service, we must refresh it by executing the following command with super-user privileges:

```
/opt/likewise/bin/lws refresh lsass
```

Here's how the string of commands looks in the registry shell:

```
[root@rhel5d docs]# -/opt/likewise/bin/lwregshell  
\> cd HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers  
\ActiveDirectory  
HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers  
\ActiveDirectory> set_value AssumeDefaultDomain 1  
HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers  
\ActiveDirectory> set_value LoginShellTemplate -/bin/bash  
HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers  
\ActiveDirectory> quit
```

```
[root@rhel5d docs]# -/opt/likewise/bin/lwsm refresh lsass
```

14.5. Change the Value of an Entry from the Command Line

You can also change a value in the registry by executing the `set_value` command from the command line. The following code block demonstrates how to change the value of the PAM key's `LogLevel` entry without using the shell. After you modify a registry setting for a Likewise service, you must refresh the corresponding service with the Likewise Service Manager for the changes to take effect.

```
/opt/likewise/bin/lwregshell ls -'[HKEY_THIS_MACHINE\Services\lsass
\Parameters\PAM\]'
[HKEY_THIS_MACHINE\\Services\lsass\Parameters\PAM]
  -"DisplayMotd"          REG_DWORD          0x00000001 (1)
  -"LogLevel"             REG_SZ          -"error"
  -"UserNotAllowedError"  REG_SZ          -"Access denied"

/opt/likewise/bin/lwregshell set_value -'[HKEY_THIS_MACHINE\Services
\lsass\Parameters\PAM\]' LogLevel debug

/opt/likewise/bin/lwregshell ls -'[HKEY_THIS_MACHINE\Services\lsass
\Parameters\PAM\]'
[HKEY_THIS_MACHINE\\Services\lsass\Parameters\PAM]
  -"DisplayMotd"          REG_DWORD          0x00000001 (1)
  -"LogLevel"             REG_SZ          -"debug"
  -"UserNotAllowedError"  REG_SZ          -"Access denied"
```

14.6. Find a Value Entry

When you're unsure where to find a setting that you want to change, you can export the registry's structure to a file and then search the file for the value entry's location.

Important: You must export the registry as root.

1. With the root account, start `lwregshell`:

```
/opt/likewise/bin/lwregshell
```

2. In the shell, execute the `export` command with the root key as the first argument and a target file as the second argument:

```
export HKEY_THIS_MACHINE\ lwregistry.reg
```

The file is exported to your current directory unless you specify a path.

In a text editor such as `vi`, open the file to which you exported the registry and search for the entry that you are want to find.

14.7. Settings in the Lsass Branch

This section lists value entries in the registry's Lsass branch.

14.7.1. Log Level Value Entries

There is a `LogLevel` value entry under several keys, including `lsass/Parameters` and `PAM`. Although the default value is typically `error`, you can change it to any of the following values: `disabled`, `error`, `warning`, `info`, `verbose`.

Locations

[HKEY_THIS_MACHINE\Services\lsass\Parameters]

[HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM]

Value Entry

`LogLevel`

Example with default value:

```
"LogLevel"="error"
```

14.7.2. Turn On Event Logging

You can capture information about authentication transactions, authorization requests, and other security events by turning on event logging. For information about managing and viewing events, see [Monitoring Events with the Event Log](#).

Note: With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see [Turn on Event Logging with a GPO](#).

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters]

Value Entry

`EnableEventlog`

Example with default value:

```
"EnableEventlog"=dword:00000000
```

14.7.3. Turn Off Network Event Logging

After you turn on event logging, network connection events are logged by default. On laptop computers, computers with a wireless connection, or other computers whose network status might be in flux, you can turn off event logging so that the event log is not inundated with connectivity events.

Note: With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see [Turn Off Logging of Network Events](#).

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters]

Value Entry

LogNetworkConnectionEvents

Example with default value:

```
"LogNetworkConnectionEvents"=dword:00000001
```

14.7.4. Restrict Logon Rights

With Likewise Open and Likewise Enterprise, you can require that a user be a member of a group to log on a computer, or you can limit logon to only the users that you specify. With Likewise Enterprise, you can also restrict logon rights with a Likewise group policy; see Allow Logon Rights in the Group Policy Administrators Guide. Likewise checks `require_membership_of` information in both the authentication phase and the account phase.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

RequireMembershipOf

Notes

Add each user or group to the value entry by using an NT4-style name (the short domain name with the group name) or an Active Directory security identifier (SID). Aliases are not supported. The entries must be in the form of a list of quoted entries: Each entry must be enclosed in quotation marks. A slash character must be escaped by being preceded by a slash. Example:

```
"RequireMembershipOf"="likewisedemo\\support"  
"likewisedemo\\domain^admins" "likewisedemo\\joe"  
"S-1-5-21-3447809367-3151979076-456401374-513"
```

Only the users that you specify and the users who are members of the groups that you specify are allowed to log on the computer.

14.7.5. Display an Error to Users Without Access Rights

You can set Likewise to display an error message when a user attempts to log on a computer without the right to access it. With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see Display a Message of the Day at Logon in the Likewise Enterprise guide.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM]

Value Entry

UserNotAllowedError

Notes

Add the text of the error message that you want to display to the value of the entry. Example with default value:

```
"UserNotAllowedError"="Access denied"
```

14.7.6. Display an MOTD

You can set Likewise to display a message of the day. It appears after a user logs on but before the logon script executes to give users information about a computer. The message can, for instance, remind users of the next scheduled maintenance window.

With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see Display a Message of the Day at Logon in the Likewise Enterprise guide.

Location in registry:

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM]
```

Value Entry

DisplayMotd

Example with the value set to 1, or true, to display a message:

```
"DisplayMotd"=dword:00000001
```

14.7.7. Change the Domain Separator Character

The default domain separator character is set to \. So, by default, the Active Directory group DOMAIN\Administrators appears as DOMAIN\administrators on target Linux and Unix computers. The Likewise authentication daemon renders all names of Active Directory users and groups lowercase.

You can, however, replace the slash that acts as the separator between an Active Directory domain name and the SAM account name with a character that you choose by modifying the DomainSeparator value entry in the registry.

The following characters cannot be used as the separator:

- alphanumeric characters -- letters and digits
- @
- #
- And not the character that you used for the `space-replacement` setting; for more information, see [Change the Replacement Character for Spaces](#).

Location

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters]
```

Value Entry

DomainSeparator

Example entry with default value:

```
"DomainSeparator"="\\"
```

Notes

In the default value, the slash character is escaped by the slash that precedes it.

14.7.8. Change the Replacement Character for Spaces

The default replacement character is set to `^`. So, by default, the Active Directory group `DOMAIN\Domain Users` appears as `DOMAIN\domain^users` on target Linux and Unix computers. You can, however, replace the spaces in Active Directory user and group names with a character that you choose by editing the `SpaceReplacement` value entry in the registry.

With Likewise Enterprise, you can manage this setting with a Likewise group policy; see [Replace Spaces in Names with a Character](#) in the Likewise Enterprise guide.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters]

Value Entry

`SpaceReplacement`

Example with default value:

```
"SpaceReplacement" = "^"
```

Notes

The following characters cannot be used as the separator:

- whitespace -- spaces and tabs
- alphanumeric characters -- letters and digits
- `@`
- `\`
- `#`

The Likewise authentication daemon renders all names of Active Directory users and groups lowercase.

14.7.9. Turn Off System Time Synchronization

With Likewise Open and Likewise Enterprise, you can specify whether a joined computer synchronizes its time with that of the domain controller. By default, when a computer is joined to a domain without using the `notimesync` command-line option, the computer's time is synchronized with the domain controller's when there is a difference of more than 60 seconds but less than the maximum clock skew, which is typically 5 minutes. With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see [Turn Off System Time Synchronization with a GPO](#) in the Likewise Enterprise guide.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

`SyncSystemTime`

Example with default value:

```
"SyncSystemTime"=dword:00000001
```

14.7.10. Set the Default Domain

If your Active Directory environment has only one domain, you can set Likewise to assume the default domain, liberating users from typing the domain name before their user or group name each time they log on a computer or switch users. With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see Prepend Domain Name for AD Users and Groups in the Likewise Enterprise guide.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

AssumeDefaultDomain

Example with default value:

```
"AssumeDefaultDomain"=dword:00000000
```

14.7.11. Set the Home Directory and Shell for Domain Users

When you install Likewise on a Linux, Unix, or Mac computer but not on Active Directory, you cannot associate a Likewise cell with an organizational unit, and thus you have no way to define a home directory or shell in Active Directory for users who log on the computer with their domain credentials. To set the home directory and shell for a Linux, Unix, or Mac computer that is using Likewise Open or Likewise Enterprise without cell, edit the value entry in registry.

If you use Likewise Enterprise to set the shell and home directory both in Active Directory and in the registry, the settings in Active Directory take precedence.

After you change the home directory or shell in the registry, you must clear the Likewise authentication cache, log off, and then log on before your changes will take effect.

In the lsass branch, there are two keys that contain value entries for the home directory and shell. One is for the local provider, the other is for the Active Directory provider. Locations:

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\Local]

The following value entries for the home directory and shell, shown with their default settings, appear under both the Active Directory and Local provider keys:

```
"LoginShellTemplate"="/bin/sh"
"HomeDirTemplate"="%H/local/%D/%U"
"HomeDirPrefix"="/home"
"CreateHomeDir"=dword:00000001
```

Set the Shell

Under the key for a provider, modify the value of the following entry to set the shell that you want:

LoginShellTemplate

Example with default value:

```
"LoginShellTemplate"="/bin/sh"
```

Note: /bin/bash might not be available on all systems.

Set the Home Directory

You can modify the HomeDirTemplate value entry to set the home directory that you want by using these variables:

Variable	Description
%U	The default user name. It is required.
%D	The default domain name. It is optional.
%H	The default home directory. It is optional. If used, it must be set as an absolute path. This value, if used, is typically the first variable in the sequence.
%L	The hostname of the computer. It is optional.

Here's an example with all four variables set: %H/%L/%D/%U

Example with default value:

```
"HomeDirTemplate"="%H/local/%D/%U"
```

In the example above, the HomeDirTemplate is using the %H variable for the HomeDirPrefix to set the user's home directory. In the example, the HomeDirPrefix is not preceded by a slash because the slash is included in the default HomeDirPrefix to ensure that the path is absolute. By default, the %H variable automatically changes to be compatible with the operating system to generate a home directory path. On Solaris, for example, the %H variable maps to /export/home. On Mac OS X it maps to /Users; on Linux, it maps to /home.

Optionally, you can set the HomeDirPrefix by changing the prefix to the path that you want.

However, the HomeDirPrefix must be an absolute path -- so you must precede it with a slash.

Example with default value:

```
"HomeDirPrefix"="/home"
```

You must use the default user name variable (%U). You may specify the default domain name by using the domain name variable (%D), but it is not required.

All the users who log on the computer by using their Active Directory domain credentials will have the shell and home directory that you set under the Providers\ActiveDirectory key. All the users who log on the computer by using their local Likewise provider credentials will have the shell and home directory that you set under the Providers\Local key.

Important: On Solaris, you cannot create a local home directory in /home, because /home is used by autofs, Sun's automatic mounting service. The standard on Solaris is to create local home directories in /export/home.

On Mac OS X, to mount a remote home directory, you must first create the directory on the remote server as well as the folders for music, movies, and so forth. See [Use the createhomedir Command to Create Home Directories](#) and other information on Apple's web site.

Turn Off Home Directories

By default, a user's home directory is created upon login. To turn off the creation of home directories, change value of the following entry to 0, for false:

CreateHomeDir

Example with default setting of 1, which creates a home directory:

```
"CreateHomeDir"=dword:00000001
```

See Also

[Fix the Shell and Home Directory Paths](#)

14.7.12. Set the Umask for Home Directories

Likewise presets the umask for the home directory and all the files in it to 022. With a umask value of 022, the default file permissions for your AD user account are as follows: Read-write access for files and read-write-search for directories you own. All others have read access only to your files and read-search access to your directories. You can, however, set the umask for home directories by modifying its value entry in the registry.

With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see [Set Permissions with a File Creation Mask](#) in the Likewise Enterprise guide.

Locations

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\Local]

Value Entry

HomeDirUmask

Example with default value:

```
"HomeDirUmask"="022"
```

14.7.13. Set the Skeleton Directory

By default, Likewise adds the contents of `/etc/skel` to the home directory created for a new user account on Linux and Unix computers. Using `/etc/skel` or a directory that you designate ensures that all users begin with the same settings or environment.

On Mac OS X computers, the default skeleton directory is as follows:

```
System/Library/User Template/Non_localized,  
/System/Library/User Template/English.lproj
```

Note: With Likewise Enterprise, you can manage this setting by using a Likewise group policy.

Locations

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\Local]

Value Entry

SkeletonDirs

Example with default value:

"SkeletonDirs"="/etc/skel"

Notes

Add the skeleton directory that you want to set to the entry. You can add multiple entries, but each entry must be enclosed in quotation marks and separated by a space.

14.7.14. Force Likewise Enterprise to Work Without Cell Information

To use the Likewise Enterprise agent to join a Linux, Unix, or Mac OS X computer to a domain that has not been configured with cell information, you must change the value of `CellSupport` to `unprovisioned`. This setting, which applies only to Likewise Enterprise, forces the authentication service to ignore the following Unix information even though it is set in Active Directory:

- Home directory
- UID
- GID
- Unix shell

Instead of using the information from Active Directory, the `unprovisioned` value sets the authentication service to hash the user's security identifier and use local settings for the Unix shell and the home directory.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

CellSupport

Notes

The value must be set as one of the following: `no-unprovisioned`, `full` or `unprovisioned`.

The default is `no-unprovisioned`, a setting that requires you to create a cell in Active Directory before you join a Likewise client to it. If you are using Likewise Enterprise with cells and you want to

use the Unix settings in AD, it is recommended that you leave `cell-support` set to its default value of `no-unprovisioned`:

```
"CellSupport"="no-unprovisioned"
```

Here's an example with the value set to `unprovisioned` to force Likewise Enterprise to ignore Unix settings and other cell information in AD:

```
"CellSupport"="unprovisioned"
```

Setting the value to `full` configures the Likewise Enterprise agent to use cell information when it appears in AD and local settings when no cells are in AD:

```
"CellSupport"="full"
```

14.7.15. Refresh User Credentials

By default, Likewise automatically refreshes user credentials, but you can turn off automatic refreshes by modifying the configuration of the Likewise authentication daemon.

Location

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]
```

Value Entry

RefreshUserCredentials

Example with default setting:

```
"RefreshUserCredentials"=dword:00000001
```

14.7.16. Turn Off K5Logon File Creation

By default, Likewise creates a `.k5login` file in the home directory of an Active Directory user who is authenticated by Kerberos when logging on a Linux, Unix, or Mac OS X computer. You can, however, stop the creation of a `.k5login` file.

The `.k5login` file contains the user's Kerberos principal, which uniquely identifies the user within the Kerberos authentication protocol. Kerberos can use the `.k5login` file to check whether a principal is allowed to log on as a user. A `.k5login` file is useful when your computers and your users are in different Kerberos realms or different Active Directory domains, which can occur when you use Active Directory trusts.

With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see [Create a .k5login File in a User's Home Directory in the Likewise Enterprise guide](#).

Location

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]
```

Value Entry

CreateK5Login

Example with default value:


```
"CreateK5Login"=dword:00000001
```

14.7.17. Change the Duration of the Machine Password

You can set the machine account password's expiration time. The expiration time specifies when a machine account password is reset in Active Directory if the account is not used. The default is 30 days.

Active Directory handles machine accounts for Linux, Unix, and Mac in the same way as those for Windows computers; for more information, see the Microsoft Active Directory documentation.

With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see [Set the Machine Account Password Expiration Time](#) in the Likewise Enterprise guide.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

MachinePasswordLifespan

Example with default value, which is shown as seconds in hexadecimal format:

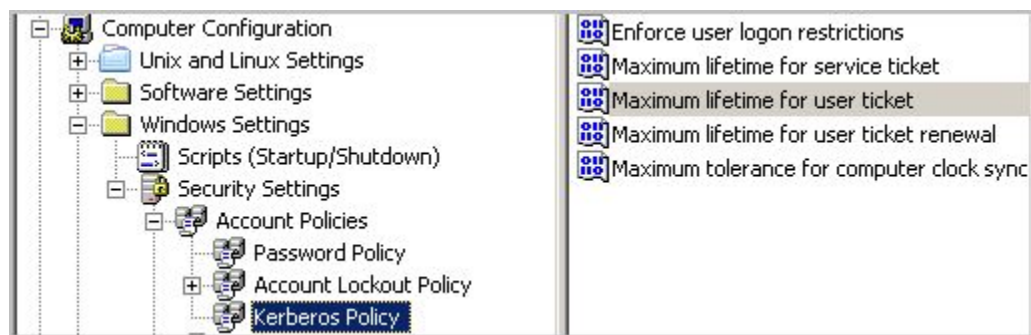
```
"MachinePasswordLifespan"=dword:000927c0
```

Notes

Setting the value to 0 disables expiration. The minimum value is 1 hour, expressed in seconds, and the maximum is 60 days, expressed in seconds. To avoid issues with Kerberos key tables and single sign-on, the `MachinePasswordLifespan` must be at least twice the maximum lifetime for user tickets, plus a little more time to account for the permitted clock skew. The expiration time for a user ticket is set by using an Active Directory group policy called **Maximum lifetime for user ticket**. The default user ticket lifetime is 10 hours; the default Likewise machine password lifetime is 30 days.

Check the Maximum Lifetime for a User Ticket in the Group Policy Object Editor

1. Open the default domain policy in the Group Policy Object Editor.
2. In the console tree under **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Account Policies**, and then click **Kerberos policy**.



3. In the details pane, double-click **Maximum lifetime for user ticket**.

4. In the **Ticket expires in** box, make sure that the number of hours is no more than half that of the `MachinePasswordLifespan` you set in the registry.

See Also

Fix a Key Table Entry-Ticket Mismatch

14.7.18. Sign and Seal LDAP Traffic

You can sign and seal LDAP traffic to certify it and to encrypt it so that others cannot see your LDAP traffic on your network. This setting can help improve network security.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

`LdapSignAndSeal`

Example with default value:

```
"LdapSignAndSeal"=dword:00000000
```

14.7.19. NTLM Value Entries

There are a number of NTLM settings that system administrators can use to manage NTLM sessions.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\Local]

Value Entry with Default Values

```
"AcceptNTLMv1"=dword:00000001
```

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\NTLM]

Value Entries with Default Values

```
"SendNTLMv2"=dword:00000000
"Support128bit"=dword:00000001
"Support56bit"=dword:00000001
"SupportKeyExchange"=dword:00000001
"SupportNTLM2SessionSecurity"=dword:00000001
"SupportUnicode"=dword:00000001
```

Each NTLM value entry is described in the following table. For additional information, see Microsoft's description of the LAN Manager authentication levels.

Value Entry	Description
AcceptNTLMv1	Controls whether the Likewise local provider accepts the older and less secure NTLM protocol

	for authentication in addition to NTLMv2. This setting does not apply to the Active Directory provider because it passes off NTLM and NTLMv2 authentication to a domain controller through schannel; it is the domain controller's settings that determine which versions of NTLM are allowed.
SendNTLMv2	Forces lsassd to use NTLMv2 rather than the older and less secure NTLM when lsassd acts as a client. (Lsassd typically serves as an NTLM client in relation to domain controllers.)
Support128bit and Support56bit	Control the length of the encryption key. They are intended to serve as a mechanism for debugging NTLM sessions. There are no corresponding settings in Windows.
SupportKeyExchange	Allows the protocol to exchange a session key -- Kerberos has a similar feature. During authentication, an alternate key is exchanged for subsequent encryption to reduce the risk of exposing a password. It is recommended that you use the default setting.
SupportNTLM2SessionSecurity	Permits the client to use a more secure variation of the protocol if the client discovers that the server supports it. Corresponds to a similar setting in Windows.
SupportUnicode	Sets NTLM to represent text according to the Unicode industry standard. It is recommended that you use the default setting -- which is to support Unicode.

14.7.20. Additional Subkeys

There are additional subkeys in the lsass branch that the lsass service uses to store information for the Likewise application. It is recommended that you do not change these subkeys or their value entries.

- [HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin\YourDNSdomainName\DomainTrust]

Stores information about domain trusts.

- [HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin\YourDNSdomainName\ProviderData]

Stores data used by the Active Directory authentication provider.

- [HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin\YourDNSdomainName\Pstore]

Caches information about the computer and the user's Active Directory account, including the machine password. The machine password is visible only to root users when they view or export the registry.

- [HKEY_THIS_MACHINE\Services\lsass\Parameters\RPCServers]

Stores information that the system uses to execute remote procedure calls.

14.7.21. Add Domain Groups To Local Groups

This value entry controls whether the domain-join process adds domain groups to the local Likewise groups and whether the domain-leave process removes domain groups from the local Likewise groups. The default setting is 0, for disabled -- no domain groups are added to local groups.

When the setting is enabled, the AD group `Domain Admins` is added to `BUILTIN\Administrators`, and `Domain Users` is added to `BUILTIN\Users`.

After joining or leaving a domain, you can verify that the domain groups were added to or removed from the local groups by running the `lw-lsa enum-members` command for the `BUILTIN\Administrators` group and the `BUILTIN\Users` group.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

AddDomainToLocalGroupsEnabled

14.7.22. Control Trust Enumeration

Likewise includes the following settings for controlling how the domain manager component of the authentication service enumerates trusts. The settings can help improve performance of the authentication service in an extended AD topology. With Likewise Enterprise, you can manage these settings with their corresponding group policies.

Important: The setting that specifies an include list is dependent on defining the setting for ignoring all trusts: To use the include list, you must first enable the setting to ignore all trusts. The include-list setting must explicitly contain every domain that you want to enumerate. It is insufficient to include only the forests that contain the domains.

For a domain that is added to the include list, Likewise tries to discover its trust. If some of the domains are not included in the space-separated list, the resulting trust relationships might run counter to your intentions: The Likewise agent might process the trust as a one-way forest child trust when it is not.

Changes to the trust enumeration settings take effect when you restart either the computer or the Likewise authentication service (`lsass`).

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entries

Value Entry	Description
DomainManagerIgnoreAllTrusts	Determines whether the authentication service discovers domain trusts. In the default configuration of disabled, the service enumerates all the parent and child domains as

	<p>well as forest trusts to other domains. For each domain, the service establishes a preferred domain controller by checking for site affinity and testing server responsiveness, a process that can be slowed by WAN links, subnet firewall blocks, stale AD site topology data, or invalid DNS information.</p> <p>When it is unnecessary to enumerate all the trusts -- because, for example, the intended users of the target computer are only from the forest that the computer is joined to -- turning on this setting can improve startup times of the authentication service.</p>
DomainManagerIncludeTrustsList	When the setting <code>DomainManagerIgnoreAllTrusts</code> is turned on, only the domain names in the space-separated include list are enumerated for trusts and checked for server availability. Each item in the list must be separated by a space.
DomainManagerExcludeTrustsList	When the setting <code>DomainManagerIgnoreAllTrusts</code> is turned off (its default setting), the domain names in the space-separated exclude list are not enumerated for trusts and not checked for server availability. Each item in the list must be separated by a space.

14.7.23. Modify Smart Card Settings

The following settings are available only with Likewise Enterprise.

Location in registry:

[HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM]

Value Entries

SmartCardPromptGecos

SmartCardServices

14.7.24. Set the Interval for Checking the Status of a Domain

This value entry determines how frequently the Likewise domain manager checks whether a domain is online. The default is 5 minutes.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

DomainManagerCheckDomainOnlineInterval

Example with default value:

```
"DomainManagerCheckDomainOnlineInterval"=dword:0000012c
```

14.7.25. Set the Interval for Caching an Unknown Domain

This value entry determines how long the Likewise domain manager caches an unknown domain as unknown. The default is 1 hour.

Location

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]
```

Value Entry

DomainManagerUnknownDomainCacheTimeout

Example with default value:

```
"DomainManagerUnknownDomainCacheTimeout"=dword:00000e10
```

14.8. Cache Settings in the lsass Branch

Many of the following cache settings can be managed by the group policies of Likewise Enterprise. For more information, see the Likewise Enterprise Group Policy Administration Guide.

14.8.1. Set the Cache Type

By default, the lsass service uses SQLite to cache information about users, groups, and the state of the computer. You can, however, change the cache to store the information in memory, which might improve the performance of your system.

Location

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]
```

Value Entry

CacheType

Example with default value:

```
"CacheType"="sqlite"
```

Notes

To use the memory cache, change the value to memory. Example:

```
"CacheType"="memory"
```

14.8.2. Cap the Size of the Memory Cache

By default, the lsass service caches information about users, groups, and the state of the computer in a SQLite database. If, however, you change the cache to store the data in memory, you can limit the size of the cache to prevent it from consuming too much memory. It is suggested that the size of the cache be

between 1 MB and 10 MB, but the size limit that you choose will depend on your environment. Groups with many members call for a larger memory cache to enumerate all the users.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

MemoryCacheSizeCap

Example with default value:

"MemoryCacheSizeCap"=dword:00000000

Notes

To limit the memory cache to a maximum value, change the value to the byte count that you want. When the total cache size exceeds the limit, old data is purged. The default value is 0: no limit is set.

14.8.3. Change the Duration of Cached Credentials

You can specify how long the Likewise agent caches information about an Active Directory user's home directory, logon shell, and the mapping between the user or group and its security identifier (SID). This setting can improve the performance of your system by increasing the expiration time of the cache.

Note: With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see Set the Cache Expiration Time in the Likewise Enterprise guide.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

CacheEntryExpiry

Example with default value:

"CacheEntryExpiry"=dword:00003840

Notes

Set the value to an interval, in seconds. The minimum entry is 0 seconds and the maximum is 1 day, expressed in seconds.

14.8.4. Change NSS Membership and NSS Cache Settings

To customize Likewise to meet the performance needs of your network, you can specify how the Likewise agent parses and caches group and user membership information with the following value entries in the registry:

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entries

Here are the value entries with their default values:

```
"TrimUserMembership"=dword:00000001
"NssGroupMembersQueryCacheOnly"=dword:00000001
"NssUserMembershipQueryCacheOnly"=dword:00000000
"NssEnumerationEnabled"=dword:00000000
```

Each setting is described in the table that follows.

Setting	Description
TrimUserMembership	<p>Specifies whether to discard cached information from a Privilege Attribute Certificate (PAC) entry when it conflicts with new information retrieved through LDAP. Otherwise, PAC information, which does not expire, is updated the next time the user logs on.</p> <p>The default setting is 1: It is turned on.</p>
NssGroupMembersQueryCacheOnly	<p>Specifies whether to return only cached information for the members of a group when queried through nsswitch. More specifically, the setting determines whether nsswitch-based group APIs obtain group membership information exclusively from the cache, or whether they search for additional group membership data through LDAP.</p> <p>This setting is made available because, with large amounts of data, the LDAP enumeration can be slow and can affect performance. To improve performance for groups with more than 10,000 users, set this option to <i>yes</i>. Without the LDAP enumeration, only when a user logs on can that user's complete group membership be retrieved based on the PAC.</p> <p>The default setting is 1: It is turned on.</p>
NssUserMembershipQueryCacheOnly	<p>When set to <i>yes</i>, enumerates the groups to which a user belongs using information based solely on the cache. When set to <i>no</i>, it checks the cache and searches for more information over LDAP.</p> <p>The default setting is 0: It is turned off.</p>
NssEnumerationEnabled	<p>Controls whether all users or all groups can be incrementally listed through NSS. On Linux computers and Unix computers other than Mac, the default setting is 0, or turned off. On Mac OS X computers, the default setting is 1, or turned on.</p> <p>To allow third-party software show Active Directory users and groups in lists, you can</p>

change this setting to 1, but performance might be affected.

Note: When you run the `id` command for an Active Directory user other than the current user on some Linux systems, such as SLES 10 and SLED 10, the command returns only that user's primary group. The command enumerates all the groups and searches for the user in the groups' membership. To properly find another user's membership with the `id` command on SLES 10 and SLED 10, you must turn on NSS enumeration.

14.9. Settings in the eventlog Branch

This section lists value entries in the registry's eventlog branch.

14.9.1. Allow Users and Groups to Delete Events

This entry specifies the Active Directory users and groups who can delete events from the Likewise event log.

Location

[HKEY_THIS_MACHINE\Services\eventlog\Parameters]

Value Entry

AllowDeleteTo

Notes

Add the users and groups, separated by commas, to the value entry by using NT4-style names (the short domain name with the group name), the user's or group's alias, or an Active Directory security identifier (SID). The comma-separated list must be enclosed in quotation marks. Example:

```
AllowDeleteTo="likewisedemo\support, likewisedemo\domain^admins,  
likewisedemo\joe, jane, S-1-5-21-3447809367-3151979076-456401374-513,  
sales^admins"
```

14.9.2. Allow Users and Groups to Read Events

This value entry specifies the Active Directory users and groups who can read events in the Likewise event log.

Location

[HKEY_THIS_MACHINE\Services\eventlog\Parameters]

Value Entry

AllowReadTo

Notes

Add the users and groups, separated by commas, to the value entry by using NT4-style names (the short domain name with the group name), the user's or group's alias, or an Active Directory security identifier (SID). The comma-separated list must be enclosed in quotation marks. Example:

```
AllowReadTo="likewisedemo\support, likewisedemo\domain^admins,  
likewisedemo\joe, jane, S-1-5-21-3447809367-3151979076-456401374-513,  
sales^admins"
```

14.9.3. Allow Users and Groups to Write Events

This value entry specifies the Active Directory users and groups who can write events in the Likewise event log.

Location

[HKEY_THIS_MACHINE\Services\eventlog\Parameters]

Value Entry

AllowWriteTo

Notes

Add the users and groups, separated by commas, to the value entry by using NT4-style names (the short domain name with the group name), the user's or group's alias, or an Active Directory security identifier (SID). The comma-separated list must be enclosed in quotation marks. Example:

```
AllowWriteTo="likewisedemo\support, likewisedemo\domain^admins,  
likewisedemo\joe, jane, S-1-5-21-3447809367-3151979076-456401374-513,  
sales^admins"
```

14.9.4. Set the Maximum Disk Size

This value entry specifies the maximum size of the event log. The default is 512 KB. The minimum size is 64 KB. The maximum is 419424 KB.

Location

[HKEY_THIS_MACHINE\Services\eventlog\Parameters]

Value Entry

MaxDiskUsage

Example with default value:

```
"MaxDiskUsage"=dword:06400000
```

14.9.5. Set the Maximum Number of Events

This value entry defines the maximum number of events that can reside in the event log. The default is 100,000. The minimum number is 100. The maximum is 2,000,000.

Location

[HKEY_THIS_MACHINE\Services\eventlog\Parameters]

Value Entry

MaxNumEvents

Example with default value:

```
"MaxNumEvents"=dword:000186a0
```

14.9.6. Set the Maximum Event Timespan

This value entry defines maximum length of time, in days, that events can remain in the event log. Events older than the specified time span are removed. The default is 90 days. The maximum is 365 days.

Location

```
[HKEY_THIS_MACHINE\Services\eventlog\Parameters]
```

Value Entry

MaxEventLifespan

Example with the default value of 90 days:

```
"MaxEventLifespan"=dword:0000005a
```

14.9.7. Change the Purge Interval

This value entry defines the number of days after which to purge the database of events. The default is 1 day.

Location

```
[HKEY_THIS_MACHINE\Services\eventlog\Parameters]
```

Value Entry

EventDbPurgeInterval

Example with default value of 1 day:

```
"EventDbPurgeInterval"=dword:00000001
```

14.10. Settings in the netlogon Branch

The `netlogon` branch contains value entries for setting the expiration of the cache that holds information for the site affinity service, including the optimal domain controller and global catalog. The `netlogon` service generates the value entries under the `[HKEY_THIS_MACHINE\Services\netlogon\cachedb]` subkey to cache information about your domain controllers and global catalog. It is recommended that you do not change the values of entries under the `cachedb` subkey. Only the value entries under the `Parameters` subkey are documented in this section.

```
[HKEY_THIS_MACHINE\Services\netlogon]
"Arguments"="/opt/likewise/sbin/netlogond ---syslog"
"Dependencies"="lwreg"
```

```
"Description"="Likewise Site Affinity Service"
"Path"="/opt/likewise/sbin/netlogond"
"Type"=dword:00000001

[HKEY_THIS_MACHINE\Services\netlogon\cachedb]

[HKEY_THIS_MACHINE\Services\netlogon\Parameters]
"NegativeCacheTimeout"=dword:0000003c
"PingAgainTimeout"=dword:00000384
"WritableRediscoveryTimeout"=dword:00000708
"WritableTimestampMinimumChange"=dword:00000000
```

14.10.1. Set the Negative Cache Timeout

This setting is reserved for internal use only.

Location

```
[HKEY_THIS_MACHINE\Services\netlogon\Parameters]
```

Value Entry

NegativeCacheTimeout

Example with default value:

```
"NegativeCacheTimeout"=dword:0000003c
```

14.10.2. Set the Ping Again Timeout

The netlogon service periodically tests whether cached domain controllers are available. This setting controls how often it does so.

Location

```
[HKEY_THIS_MACHINE\Services\netlogon\Parameters]
```

Value Entry

PingAgainTimeout

Example with default value:

```
"PingAgainTimeout"=dword:00000384
```

14.10.3. Set the Writable Rediscovery Timeout

When a service requests a writable domain controller and one does not exist in the local site, this setting controls how long the service stays affinitized to the writable domain controller before reaffinitizing to a closer read-only domain controller.

Location

```
[HKEY_THIS_MACHINE\Services\netlogon\Parameters]
```

Value Entry

WritableRediscoveryTimeout

Example with default value:

```
"WritableRediscoveryTimeout"=dword:00000708
```

14.10.4. Set the Writable Timestamp Minimum Change

Netlogond keeps track of when a writable domain controller was last requested. Related to `WritableDiscoveryTimeout`, this setting controls how often that timestamp is changed.

Location

[HKEY_THIS_MACHINE\Services\netlogon\Parameters]

Value Entry

WritableTimestampMinimumChange

Example with default value:

```
"WritableTimestampMinimumChange"=dword:00000000
```

14.10.5. Set CLdap Options

The netlogon service uses multiple asynchronous CLDAP searches in a single thread to find servers that act as domain controllers and global catalogs. To improve performance in the context of your unique network, you can adjust the following settings for the Connection-less Lightweight Directory Access Protocol.

Location

[HKEY_THIS_MACHINE\Services\netlogon\Parameters]

Value Entries

`CLdapMaximumConnections` is the maximum number of servers that will be pinged simultaneously. The default is 100.

`CLdapSearchTimeout` is the timeout for the entire search (in seconds). The default is 15 seconds.

`CLdapSingleConnectionTimeout` is the timeout for pinging a single server (in seconds). The default is 15 seconds.

14.11. Settings in the Lwio Branch

The `lwio` branch contains value entries for the input-output service, `lwio`, that plays a fundamental role in the operation of the CIFS file server.

The value entries under the `shares` subkey define shared folders and the security descriptors that control access to them. It is recommended that you do not directly change the values under the `shares` subkey while the `lwiod` service is running.

14.11.1. Sign Messages If Supported

Although signing messages is turned off by default, you can set the input-output service to sign messages. Doing so, however, can degrade performance. When signing is turned off, the input-output service will reject clients that require signing.

Location

[HKEY_THIS_MACHINE\Services\lwo\Parameters\Drivers\rdr]

Value Entry

SignMessagesIfSupported

Example with default value:

"SignMessagesIfSupported"=dword:00000000

14.11.2. Enable Security Signatures

This value entry, which is turned on by default, sets the CIFS file server to sign responses when it receives signed messages from a client.

Location

[HKEY_THIS_MACHINE\Services\lwo\Parameters\Drivers\srv]

Value Entry

EnableSecuritySignatures

Example with default value:

"EnableSecuritySignatures"=dword:00000001

14.11.3. Require Security Signatures

This value entry determines whether the CIFS file server will reject clients that do not support signing.

Location

[HKEY_THIS_MACHINE\Services\lwo\Parameters\Drivers\srv]

Value Entry

RequireSecuritySignatures

Example with default value:

"RequireSecuritySignatures"=dword:00000001

14.11.4. Set Support for SMB2

This value entry determines whether the CIFS file server will engage the SMB2 protocol module. When the setting is turned off, the server will not negotiate with SMB2.

Location

[HKEY_THIS_MACHINE\Services\lwiio\Parameters\Drivers\srv]

Value Entry

SupportSmb2

Example with default value:

"SupportSmb2"=dword:00000000

14.12. Settings in the Lwedsplugin Branch for Mac Computers

The Likewise registry includes the following settings to manage the directory services plugin on a Mac OS X computer. Each of these settings can be managed by a corresponding Likewise Enterprise group policy; for more information, see the Group Policy Administration Guide. Here's an example configuration in the registry:

```
[HKEY_THIS_MACHINE\Services\lwedsplugin\Parameters\]
- "AllowAdministrationBy"          REG_SZ          - "CORP\
\EnterpriseTeam"
- "EnableForceHomedirOnStartupDisk" REG_DWORD        0x00000001 (1)
- "EnableMergeAdmins"             REG_DWORD        0x00000001 (1)
- "UncProtocolForHomeLocation"     REG_SZ          - "smb"
- "UseADUncForHomeLocation"        REG_DWORD        0x00000001 (1)
```

Each setting is described in the following table.

DS Plugin Setting in the Registry	Description
Allow administration by	Specifies the administrators included the local admin group (GID: 80) on the computer. The setting can specify Active Directory users or groups. Local entries are overwritten unless you also set the parameter to merge administrators who are defined locally.
Force home directory on startup disk	Sets a computer to use a local home directory path. When a user with a home folder connection defined in Active Directory logs on, the connection is created in the dock under / Network/Servers/homeFolderName.
Merge Administrators	Preserves members of the admin group who are defined locally but are not specified in the allow administration by policy.
Set the UNC Protocol for the Home Location	Sets the protocol for the home location.
Use UNC path from Active Directory to create home location	Sets the computer to connect to the network share defined in the Active Directory user account. The UNC path is converted to SMB when the target share is running Windows or AFP when the target is running Mac OS X.

If the setting for forcing the home directory on the startup disk is enabled, the UNC path is used to create a folder in the user's dock and the home directory is set to the user's local home directory path.

To set the path for the home directory, go to the **Profile** tab of the user's properties in ADUC and under **Home folder** select **Connect**, choose a drive letter (which is ignored by a Mac OS X computer), and then in the **To** box type the UNC path that you want.

Here's the form the path takes: \\server
\\share\\folder

Here's an example of a path: \
\\lwdemo01\\homes\\fanthony

Chapter 15. Contacting Technical Support

15.1. Contact Support

For either post-sales technical support or for free technical support during an evaluation period, please visit the Likewise support web page at <http://www.likewise.com/support/>. You can use the support web page to register for support, submit incidents, and receive direct technical assistance.

Technical support may ask for your Likewise version, Linux or Unix version, and Microsoft Windows version. To find the Likewise Enterprise product version, in the Likewise Console, on the menu bar, click **Help**, and then click **About**.

15.2. Provide Diagnostic Information to Technical Support

When you work with Likewise technical support staff to troubleshoot a problem, it is useful to provide a set of information to help solve the problem. The list below outlines the information that, as a best practice, you should collect and provide to Likewise technical support staff.

Information for All Problems

1. Operating system version.
2. Likewise version and build number. See Check the Version and Build Number.

Problem: Segmentation Faults

1. Core dump of the Likewise application:

```
ulimit - c unlimited
```
2. Exact patch level or exact versions of all installed packages. See Check the Version and Build Number.

Problem: Program Freezes

1. Debug logs.
2. tcpdump.
3. An `strace` of the program.

Problem: Domain Join Errors

1. Debug logs. See Generate a Domain-Join Log or grab the log file from `/var/log/likewise-join.log`.

2. `tcpdump`.

See Solve Domain-Join Problems.

Problem: All Active Directory Users Are Missing

1. Run `/opt/likewise/bin/lw-get-status`

See Get the Status of the Authentication Providers.

2. Contents of `nsswitch.conf`.

See Solve Logon Problems on Linux or Unix.

Problem: All Active Directory Users Cannot Log On

1. Output of `id <user>`
2. Output of `su -c 'su <user>' <user>`
3. Lsass debug logs. See Generate an Authentication Agent Debug Log.
4. Contents of `pam.d/pam.conf`.
5. The `sshd` and `ssh` debug logs and `syslog`.

Problem: AD Users or Groups Are Missing

1. The debug logs for `lsass`.
2. Output for `getent passwd` or `getent group` for the missing object.
3. Output for `id <user>` if user.
4. `tcpdump`.
5. Copy of `lsass` cache file. For the file name and location of the cache files, see About the Likewise Agent.

Problem: Poor Performance When Logging On or Looking Up Users

1. Output of `id <user>`

2. The lsass debug log.
3. Copy of lsass cache file. For the file name and location of the cache files, see About the Likewise Agent.
4. tcpdump.

Chapter 16. Legal Disclaimer and Copyright Notice

The information contained in these documents represents the current view of Likewise Software on the issues discussed as of the date of publication. Because Likewise Software must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Likewise, and Likewise Software cannot guarantee the accuracy of any information presented after the date of publication.

These documents are for informational purposes only. LIKEWISE SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form, by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Likewise Software.

Likewise may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Likewise, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. For complete information on the software licenses and terms of use for Likewise products, see www.likewise.com.

Likewise and the Likewise logos are either registered trademarks or trademarks of Likewise Software in the United States and/or other countries. All other trademarks are property of their respective owners.

Likewise Software
15395 SE 30th Place, Suite 140
Bellevue, WA 98007
USA

Terms of Use.

For more information, contact info@likewise.com or visit www.Likewise.com.

Copyright © 2011 Likewise Software. All rights reserved.