

Likewise Open 6 Installation And Administration Guide

IN THIS DOCUMENT

- Downloading Likewise Open.
- Installing Likewise Open.
- Joining a Linux computer to an Active Directory domain.
- Joining a Mac OS X computer to a domain.
- Joining a Unix computer to a domain.
- Logging on with Active Directory credentials.
- Managing and troubleshooting the agent.

Abstract

Likewise Open joins Linux, Unix, and Mac OS X computers to Microsoft Active Directory so that you can centrally manage all your computers, authenticate users, and authorize access to resources. This guide describes how to install and administer Likewise Open, an open source version of Likewise Enterprise that includes the Likewise Agent. The guide covers installing the agent, joining an Active Directory domain, and troubleshooting the agent.

Likewise Open is free to download and use according to the terms of the GNU General Public License.

This guide is supplemented by the Likewise Open community mailing list, which you can join at <http://www.likewisesoftware.com/community/> and use to discuss and troubleshoot Likewise Open with other users and developers.

Table of Contents

1. Quick Start	1
1.1. Install the Agent on Linux, Join a Domain, and Log On	1
1.2. Upgrade to the Latest Version	2
2. The Likewise Agent	4
2.1. About the Likewise Agent	4
2.2. Daemons	4
2.3. The Likewise Registry	7
2.4. Ports and Libraries	7
2.5. Caches	8
2.6. Time Synchronization	9
2.7. Using a Network Time Protocol Server	9
2.8. Automatic Detection of Offline Domain Controller and Global Catalog	10
2.9. UID-GID Generation in Likewise Open and Likewise Enterprise Cells	10
2.10. Cached Credentials	10
2.11. Trust Support	11
2.12. The Likewise CIFS File Server	12
2.13. Supported Platforms	12
3. Configuring Clients Before Agent Installation	13
3.1. Configure nsswitch.conf	13
3.2. Configure resolv.conf	13
3.3. Configure Firewall Ports	14
3.4. Extend Partition Size Before Installing Likewise on IBM AIX	14
3.5. Increase Max Username Length on IBM AIX	14
3.6. Check System Health Before Installing the Agent	14
4. Installing the Agent	19
4.1. Install the Correct Version for Your Operating System	19
4.2. Requirements for the Agent	19
4.3. Install the Agent on Linux or Unix with the Shell Script	22
4.4. Install the Agent on Linux with the BitRock GUI	23
4.5. Install the Agent on Linux with glibc 2.2 or Earlier	23
4.6. Install the Agent on Linux in Unattended or Text Mode	24
4.7. Install the Agent on Unix with the Command Line	25
4.8. Install the Domain Join GUI	26
4.9. Install the Agent on a Mac Computer	26
4.10. Install the Agent on a Mac in Unattended Mode	27
4.11. Upgrading Your Operating System	28
5. Joining an Active Directory Domain	29
5.1. About Joining a Domain	29
5.2. Join Active Directory with the Command Line	30
5.3. Join Active Directory Without Changing /etc/hosts	37
5.4. Join a Linux Computer to Active Directory with the GUI	38
5.5. Join a Mac Computer to Active Directory with the GUI	40
5.6. Use Likewise with a Single OU	42
5.7. Rename a Joined Computer	42
5.8. Files Modified When You Join a Domain	44
5.9. With NetworkManager, Use a Wired Connection to Join a Domain	47
6. Logging On with Domain Credentials	48
6.1. About Logging On	48
6.2. Log On with AD Credentials	48
6.3. Log On with SSH	49
6.4. Solve Logon Problems from Windows	49

6.5. Solve Logon Problems on Linux or Unix	49
7. Troubleshooting Domain-Join Problems	54
7.1. Top 10 Reasons Domain Join Fails	54
7.2. Solve Domain-Join Problems	54
7.3. Dealing with Common Error Messages	57
7.3.1. Configuration of Krb5	57
7.3.2. Chkconfig Failed	57
7.4. Diagnose NTP on Port 123	57
8. Configuring the Likewise Services with the Registry	60
8.1. About the Registry	60
8.1.1. The Structure of the Registry	60
8.1.2. Data Types	62
8.2. Gain Access to the Registry	63
8.3. Change the Value of an Entry with the Shell	64
8.4. Change the Value of an Entry from the Command Line	65
8.5. Find a Value Entry	65
8.6. Settings in the lsass Branch	66
8.6.1. Log Level Value Entries	66
8.6.2. Turn On Event Logging	66
8.6.3. Turn Off Network Event Logging	66
8.6.4. Restrict Logon Rights	67
8.6.5. Display an Error to Users Without Access Rights	67
8.6.6. Display an MOTD	68
8.6.7. Change the Domain Separator Character	68
8.6.8. Change the Replacement Character for Spaces	69
8.6.9. Turn Off System Time Synchronization	69
8.6.10. Set the Default Domain	70
8.6.11. Set the Home Directory and Shell for Domain Users	70
8.6.12. Set the Umask for Home Directories	72
8.6.13. Set the Skeleton Directory	72
8.6.14. Force Likewise Open to Ignore Cell Information	73
8.6.15. Refresh User Credentials	73
8.6.16. Change the Duration of Cached Credentials	74
8.6.17. Change the Interval When Expired Cache Entries Are Purged	74
8.6.18. Turn Off K5Logon File Creation	75
8.6.19. Change NSS Membership Settings	75
8.6.20. Change the Duration of the Machine Password	76
8.6.21. Sign and Seal LDAP Traffic	77
8.6.22. Set the Cache Type	78
8.6.23. Cap the Size of the Memory Cache	78
8.6.24. Set the Interval for Checking the Status of a Domain	79
8.6.25. Set the Interval for Caching an Unknown Domain	79
8.6.26. NTLM Value Entries	79
8.6.27. Additional Subkeys	80
8.7. Settings in the eventlog Branch	81
8.7.1. Allow Users and Groups to Delete Events	81
8.7.2. Allow Users and Groups to Read Events	81
8.7.3. Allow Users and Groups to Write Events	82
8.7.4. Set the Maximum Disk Size	82
8.7.5. Set the Maximum Number of Events	82
8.7.6. Set the Maximum Event Timespan	83
8.7.7. Change the Purge Interval	83
8.8. Settings in the netlogon Branch	83
8.8.1. Set the Negative Cache Timeout	84

8.8.2. Set the Ping Again Timeout	84
8.8.3. Set the Writable Rediscovery Timeout	84
8.8.4. Set the Writable Timestamp Minimum Change	85
8.9. Settings in the lwio Branch	85
8.9.1. Sign Messages If Supported	85
8.9.2. Enable Security Signatures	85
8.9.3. Require Security Signatures	86
8.9.4. Set Support for SMB2	86
9. Troubleshooting the Agent	87
9.1. Run the Authentication Daemon in Debug Mode	87
9.2. Troubleshoot Likewise Daemons with the Service Manager	87
9.3. Check the Status of the Authentication Daemon	88
9.4. Check the Status of the DCE/RPC Daemon	89
9.5. Check the Status of the Network Logon Daemon	90
9.6. Check the Status of the Input-Output Service	91
9.7. Find the Likewise Daemons on a Mac	91
9.8. Check the Version and Build Number	92
9.9. Clear the Authentication Cache	93
9.9.1. Clear a Corrupted SQLite Cache	94
9.10. Determine a Computer's FQDN	95
9.11. Generate a Domain-Join Log	96
9.12. Generate a Network Trace	96
9.13. Generate a PAM Debug Log	96
9.14. Generate an Authentication Agent Debug Log	97
9.15. Generate a Debug Log for Netlogond	97
9.16. Make Sure Outbound Ports Are Open	97
9.17. Resolve an AD Alias Conflict with a Local Account	98
9.18. Allow Access to Account Attributes	99
9.19. Restart the DCE/RPC Daemon	100
9.20. Restart the Network Logon Daemon	100
9.21. Restart the Input-Output Service	101
9.22. Restart the Authentication Daemon	102
9.23. Troubleshooting Kerberos	103
9.24. Fix a Key Table Entry-Ticket Mismatch	103
9.25. Fix KRB Error During SSO in a Split-DNS Configuration	104
9.26. Fix the Shell and Home Directory Paths	105
9.27. A Note About the Home Directory on SLED 11	106
9.28. Updating PAM on SLED 11	106
9.29. Configuring PAM on RHEL 5 and CentOS 5	106
9.30. Increase Max Username Length on AIX	107
9.31. Updating AIX	107
9.32. Add Domain Accounts to Local Groups with /etc/group	107
9.33. Configure Entries in Your Sudoers Files	108
9.34. Set a Sudoers Search Path	109
9.35. Working with Solaris Zones	109
10. Command-Line Reference	112
10.1. lwsm: Manage Services	112
10.2. lwregshell: The Registry Shell	113
10.3. lw-edit-reg: Export the Registry to Your Editor	113
10.4. lw-set-log-level: Set the Log Level	113
10.5. Find a User or a Group	114
10.6. Find a User by a SID	115
10.7. List Groups for a User	116
10.8. lw-enum-groups: List Groups	116

10.9. lw-enum-users: List Users	116
10.10. lw-get-status: View the Status of the Authentication Providers	117
10.11. lw-get-current-domain	118
10.12. lw-get-dc-list	118
10.13. lw-get-dc-name: Get Domain Controller Information	118
10.14. lw-get-dc-time	118
10.15. lw-get-log-info	118
10.16. lw-get-metrics	119
10.17. Get Machine Account Information	119
10.18. Reload Changes to the Configuration File	120
10.19. lw-trace-info: Turn on Trace Markers in Log Messages	120
10.20. lw-update-dns: Dynamically Update DNS	120
10.21. lw-ad-cache: Manage the AD Cache	120
10.22. domainjoin-cli	121
10.23. lw-ypcat	121
10.24. lw-ypmatch	122
10.25. uuid	122
10.26. lwio: Input-Output Commands	122
10.26.1. lwio-fuse-mount: Gain Access to a Shared Windows Folder	122
10.26.2. lwio-copy: Copy Files Across Disparate Operating Systems	123
10.26.3. lwio-refresh: Reload the Input-Output Settings After Changes	123
10.26.4. lwio-set-log-level	123
10.26.5. lwio-get-log-info	124
10.27. Commands to Modify Local Accounts	124
10.27.1. lw-add-user: Add a Local User by Name or UID	124
10.27.2. lw-add-group: Add a Local Group Member by Name or GID	124
10.27.3. lw-del-user: Remove a Local User by Name or UID	125
10.27.4. lw-del-group: Remove a Local Group by Name or GID	125
10.27.5. lw-mod-user: Modify a Local User by Name or UID	125
10.27.6. lw-mod-group: Modify a Local Group's Members	125
10.28. Kerberos Commands	126
10.28.1. kdestroy: Destroy the Kerberos Ticket Cache	126
10.28.2. klist: View Kerberos Tickets	126
10.28.3. kinit: Obtain and Cache a TGT	127
10.28.4. kpasswd: Change a Password	127
10.28.5. ksu: Kerberized Super User	127
10.28.6. ktutil: The Keytab File Maintenance Utility	127
10.28.7. Kvno: Acquire a Service Ticket and Print Key Version Number	128
10.28.8. krb5-config: Identify Your Version of Kerberos	128
10.29. Commands and Scripts Not for Customer Use	129
10.29.1. ConfigureLogin	129
10.29.2. dceidl	129
10.29.3. demo	129
10.29.4. gpccron	129
10.29.5. gpccron.sh	129
10.29.6. gprsrmtnt.sh	129
10.29.7. idl	129
10.29.8. init-base.sh	129
10.29.9. lwmapsecurity-test	129
10.29.10. lw-migrator	130
11. Monitoring Events with the Event Log	131
11.1. Monitor Events with the Event Log	131
11.2. View the Local Event Log	131
11.3. The Event Type	134

11.4. The Event Source	134
11.5. List of Events by Source ID	134
12. Leaving a Domain and Uninstalling the Agent	137
12.1. Leave a Domain	137
12.2. Uninstall the Domain Join GUI	138
12.3. Uninstall the Agent on a Linux or Unix Computer	138
12.4. Uninstall the Agent on a Mac	139
13. Using Likewise for Single Sign-On	140
13.1. About Single Sign-On	140
13.2. Make Sure PAM Is Enabled for SSH	141
13.3. Configure PuTTY for Windows-Based SSO	143
13.4. Solve the SSO Problem on Red Hat and CentOS	145
13.5. On RHEL5 and AIX, Set Reverse PTR Host Definitions for SSO with SSH	147
13.6. Configure AIX 5.3 for Outbound Single Sign-On with SSH	147
13.7. Configure Apache for SSO	148
13.7.1. Kerberos Library Mismatch	157
13.8. Examples	158
14. Contacting Technical Support	159
14.1. Contact Support	159
14.2. Provide Diagnostic Information to Technical Support	159
15. Legal Disclaimer and Copyright Notice	162

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](#).)

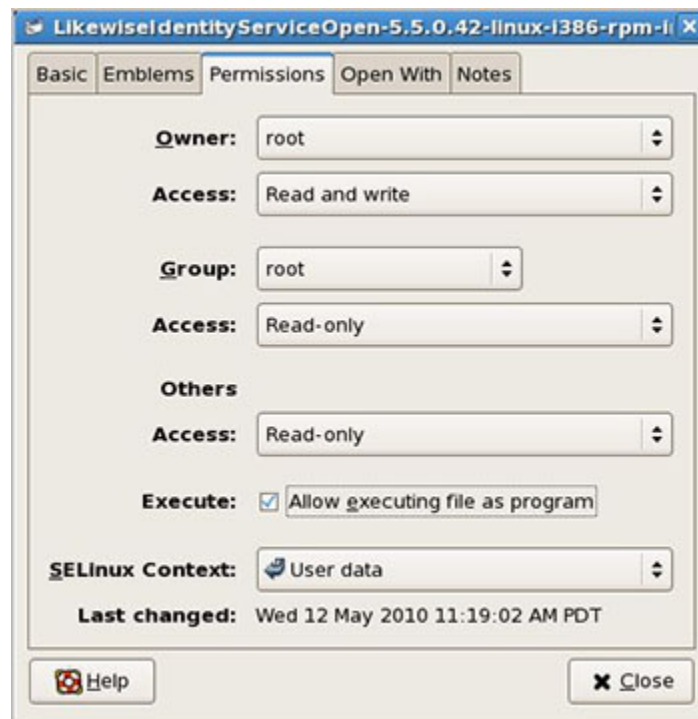
Before you deploy Likewise Open in anything other than a test environment, however, you should read the overview of the agent, the chapter on installing the agent, the chapter on joining a domain, and the chapter on configuring the Likewise services.

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

For most Linux platforms, you install Likewise Open by using a Bitrock Installer — an executable whose file name ends with `installer`. Example: `LikewiseOpen-6.0.0.3551-linux-i386-rpm-installer`



For versions of Linux running glibc 2.2 or earlier, the installer is a shell script whose file name ends in `.sh`; for instructions on how to install the shell script, see [Install the Agent on Linux with glibc 2.2 or Earlier](#).

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.

2. Double-click the installer to run it and then follow the instructions in the installation wizard.

Step 3: Join Active Directory

As root, run the following command, replacing `domainName` with the fully qualified domain name of your domain and `joinAccount` with the user name of an Active Directory 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
```

To solve problems, see [Troubleshooting Domain-Join Problems](#) or run this command: `domainjoin-cli --help`

Step 4: Log On with AD Credentials

After Likewise Open has been installed and the Linux computer has been joined to a domain, you can log on interactively or from the text login prompt with your Active Directory credentials in the following form: `DOMAIN\username`.

1. On a Linux computer, log out of the current session.
2. 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. 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 10.04 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.

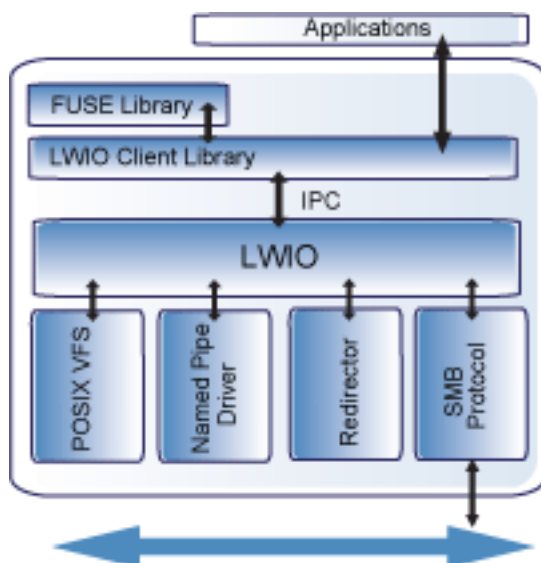
2.2. Daemons

The Likewise 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 the data. You can check its status or restart it.	None
<code>/opt/likewise/sbin/lwiod</code>	<p>The Likewise input-output service. 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>It communicates over SMB with SMB servers. You can check its status or restart it.</p> <p>For instructions on how to set up and use the Likewise CIFS/SMB file server, see the Likewise CIFS file server User Guide.</p>	<code>netlogond</code>

/opt/likewise/sbin/dcerpcd	The Likewise DCE/RPC end-point 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 end points. 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/gpagentd	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. The daemon uses LDAP to look up information about group policies and uses lwiod and its redirector to retrieve group policy objects. You can check its status or restart it.	netlogond lwiod dcerpcd eventlogd lsassd
/opt/likewise/sbin/srvsvcd	Part of the Likewise CIFS file server, included in Likewise Open as a technology preview.	lwiod
/opt/likewise/sbin/eventfwdd	Event forwarding daemon, part of the Likewise data collection service.	eventlogd
/opt/likewise/sbin/lwregd	The daemon for the registry service.	All the Likewise services depend on lwregd.
/opt/likewise/sbin/reapsysld	Part of the Likewise data collection service that is included in Likewise Enterprise.	eventlogd eventfwdd

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.

For example, when you join a domain, 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.

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
```

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)
pvfs       stopped
rdr        running (io: 2191)
srv        stopped
srvsvc     stopped
```

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

To maintain the current state and to improve performance, the Likewise authentication service (lsass) caches information about users and groups in a SQLite database. You can, however, change the cache to store the information in memory, which might improve performance; 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 cache files are in `/var/lib/likewise/db`:

Cache File	Description
<code>/var/lib/likewise/db/lsass-adcache.db</code>	Cache managed by the Active Directory authentication provider.
<code>lsass-local.db</code>	Repository managed by the local authentication provider.
<code>netlogon-cache.db</code>	Domain controller affinity cache, managed by <code>netlogond</code>
<code>pstore.db</code>	Repository storing the join state and machine password

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
\Pstore\Default]
"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 that you use 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 specify that Likewise Enterprise automatically generates 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
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

- 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
```

Aliasing and Trusts

- Aliased user names are supported in the default cell.
- Since one-way trusts do not allow LDAP queries on trusted domains, you cannot use aliases across a one-way trust.

2.12. The Likewise CIFS File Server

Likewise-CIFS is a free open source SMB file system that you can download from www.Likewise.com and use as a technology preview. It provides client-side and server-side SMB/CIFS support so Microsoft Windows clients can access folders and files on Linux computers. At the same time, the Likewise CIFS FUSE module lets you mount remote Windows shares on a Linux computer to access folders and files. For instructions on how to set up and use the Likewise CIFS file server, see the Likewise CIFS File Server User Guide.

Because Likewise-CIFS is a technology preview and because it is a separate software package from Likewise Open and Likewise Enterprise, it is not covered under your support contract.

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. To view the list, go to http://www.likewise.com/products/likewise_enterprise/supported_platforms.php.

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.

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
```

If your list of nameservers contains multiple nameservers and one of them becomes unavailable, name resolution can time out, delaying the logon process. To improve performance, set up a BIND server on each Linux or Unix computer on which you are running Likewise. Then 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.

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. 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`.

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 <code>glibc</code> 2.3 or later	Install the Agent on Linux with the BitRock GUI
Linux platforms running <code>glibc</code> 2.2 or earlier	Install the Agent on Linux with <code>glibc</code> 2.2 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	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](#).

For Likewise Enterprise, you can optionally install the agent with a shell script -- an efficient method of deploying the agent in an enterprise environment; see [Install the Agent on Linux or Unix with the Shell Script](#).

Checking Your `glibc` Version

To determine the version of `glibc` on your Linux machine, run the following command:

```
rpm -q glibc
```

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 installing and running the Likewise Management Console, which is part of Likewise Enterprise and the UID-

GID module, 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 use `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

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 `nsd`, either patch ID number 138047-02 or the patch that supercedes 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 superceded 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 software that uses PAM for processing authentication requests is 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 can 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: `LikewiseIdentityServiceEnterprise-6.0.0.3499-linux-i386-rpm.sh`.

Note: 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. For Linux computers running `glibc` 2.2 or earlier, see [Install the Agent on Linux with glibc 2.2 or Earlier](#).

Install the Agent on Linux or Unix with the Shell Script

Perform the following procedure with the root account.

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

Tip: To view information about the installer or to view a list of command-line options, run the following command:

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

4. As root, run the installer:

```
./LikewiseIdentityServiceEnterprise-6.0.0.3499-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`

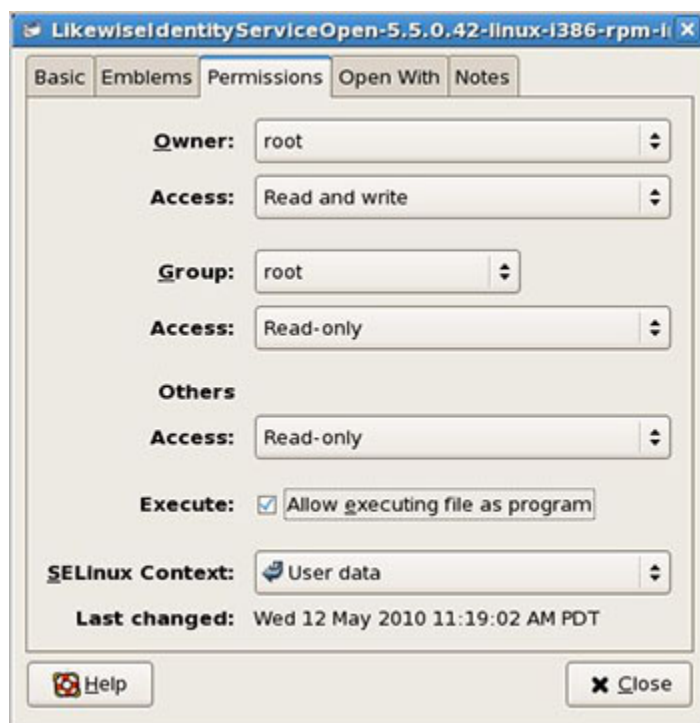
4.4. Install the Agent on Linux with the BitRock GUI

For most Linux platforms, you can install the Likewise Open agent or the Likewise Enterprise agent by using a BitRock installer — an executable whose file name ends with `installer`. Example: `LikewiseOpen-6.0.0.3842-linux-i386-rpm-installer`.

The following procedure assumes that you downloaded or copied the Likewise installer to the desktop of your Linux computer.

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 this 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 with `chmod a+x`.

2. Double-click the installer to run it, and then follow the instructions in the installation wizard.

4.5. Install the Agent on Linux with glibc 2.2 or Earlier

Linux platforms running `glibc` 2.2 or earlier require you to use the `oldlibc` installer -- a shell script that includes `oldlibc` in its name; example: `LikewiseIdentityServiceOpen-6.0.0.7111-linux-oldlibc-i386-rpm.sh`.

To check the version of `glibc` on your Linux computer, execute the following query:

`rpm - q glibc`

The following platforms are running `glibc` 2.2 or earlier and thus require the `oldlibc` installer:

- Red Hat Enterprise Linux AS 2.1
- Red Hat Enterprise Linux ES 2.1
- Red Hat Enterprise Linux WS 2.1
- Red Hat Linux 7.2
- Red Hat Linux 7.3
- Red Hat Linux 8
- Red Hat Linux 9
- SUSE 8.2

Install the Agent on `glibc` 2.2 or Earlier

Perform the following procedure with the root account.

1. Download or copy the `oldlibc` installer to the Linux computer's desktop.

Important: If you FTP the file to the desktop of the target Linux 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 LikewiseIdentityServiceOpen-6.0.0.3494-linux-oldlibc-i386-rpm.sh
```

Tip: To view information about the installer or to view a list of command-line options, run the following command:

```
./LikewiseIdentityServiceOpen-6.0.0.3494-linux-oldlibc-i386-rpm.sh --help
```

4. As root, run the installer:

```
./LikewiseIdentityServiceOpen-6.0.0.3494-linux-oldlibc-i386-rpm.sh
```

5. Follow the instructions in the installer.

4.6. Install the Agent on Linux in Unattended or Text Mode

When you use the BitRock installer, command-line tools can help deploy the Likewise agent to multiple computers or install the agent remotely.

You can use the command-line tools to automatically install the agent, join the computer to a domain, and obtain credentials. For example, you can automate the installation of the agent by using the installation command in unattended mode:

```
LikewiseEnterprise-6.0.0.7111-linux-x86_64-rpm-installer --mode unattended
```

For Unix and Linux hosts, you can run the installer from the shell prompt with no special treatment. The installer detects that it is running in character mode and displays a character mode user interface, or you can force it into character mode with the option `--mode text`:

```
LikewiseEnterprise-6.0.0.7111-linux-x86_64-rpm-installer --mode text
```

4.7. Install the Agent on Unix with the Command Line

You can install the Likewise Open agent or the Likewise Enterprise agent on Sun Solaris, HP-UX, and IBM AIX by using a BitRock installer — an executable whose file name ends with `installer`. Example: `LikewiseIdentityServiceEnterprise-6.0.0.3499-solaris-sparc-pkg-installer`.

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 `LikewiseIdentityServiceEnterprise-6.0.0.3499-solaris-sparc-pkg-installer`.

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 LikewiseIdentityServiceEnterprise-6.0.0.3499-solaris-sparc-pkg-installer
```

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

```
./LikewiseIdentityServiceEnterprise-6.0.0.3499-solaris-sparc-pkg-installer --help
```

4. As root, run the installer:

```
./LikewiseIdentityServiceEnterprise-6.0.0.3499-solaris-sparc-pkg-installer
```

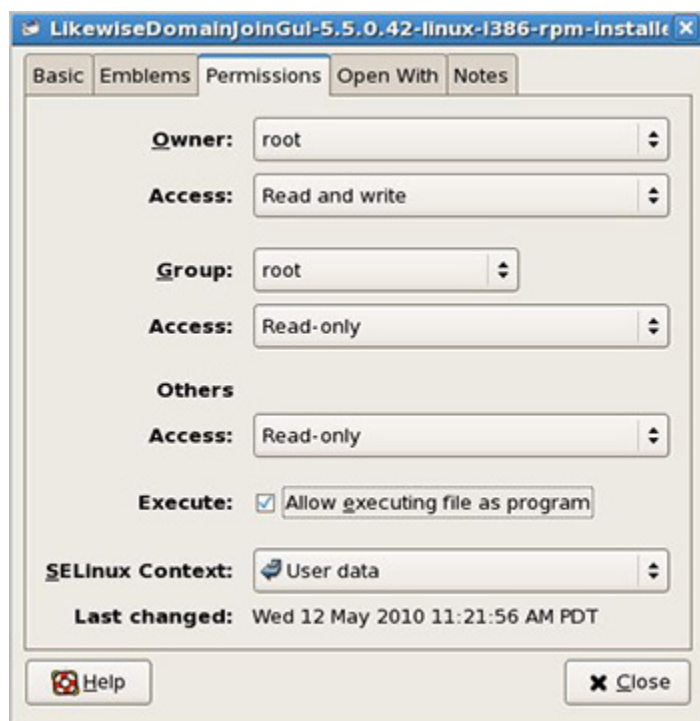
5. Follow the instructions in the installer.

4.8. Install the Domain Join GUI

You can install the optional graphical user interface version of the Likewise domain join tool on a Linux computer after you have installed the Likewise agent. The domain join tool can be installed on Linux platforms that are running GTK+ version 2.6 or later.

Note: You do not need to install the domain join GUI to join a domain; for more information, see Join Active Directory with the Command Line.

1. Obtain the BitRock installer for the domain join tool for your platform from Likewise Software at <http://www.Likewise.com>.
2. Copy the installer to the desktop of the target Linux computer.
3. As root, on the desktop, right-click the icon for the installer, click **Properties**, and then click the **Permissions** tab.
4. The dialog box varies by platform: You must set the owner to be the root account and you must set the program to be executable by the root account with read and write permissions. On Red Hat Enterprise Linux, for example, you must make sure the owner is the root account and select **Read and Write** access for the owner. You must also select **Allow executing file as program**:




5. On the desktop, double-click the icon of the installer to run it, and then follow the instructions in the installation wizard.

4.9. 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.

4.10. 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-6.0.0.3628-i386.dmg`. For Macs that do not have Intel chips, use the **powerpc** version of the .dmg installer; for example: `LikewiseEnterprise-6.0.0.3628-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-6.0.0.3628-i386.dmg
```

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

```
/usr/bin/open Volumes/LikewiseEnterprise-6.0.0.3628-i386
```

4. Execute the following command to install the agent:

```
sudo installer -pkg /Volumes/LikewiseEnterprise-6.0.0.3628-i386/  
LikewiseEnterprise-6.0.0.3628-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`

4.11. 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 within Active Directory. You can, however, choose to create machine accounts in Active Directory before you join your Unix, Linux, and Mac OS X computers to the domain. When you join a computer to a domain by running the Domain Join Tool, Likewise associates the Unix or Linux host with the pre-existing machine account. 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 any service or daemon that looks up users or groups through the standard nsswitch interface, which includes most services that authenticate users, groups, or computers.

For Linux computers, there is an optional graphical version of the Likewise Domain Join Tool. It can be installed on Linux platforms that are running GTK+ version 2.6 or later. For more information, see [Install the Domain Join GUI and 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](#).

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

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 computer's 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](#).

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.

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 user 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
```

Example of how to join a deeply nested OU:

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

Options and Basic Commands

The following tables list the options and commands of the command-line interface for joining a domain.

Options

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 commands.	<code>domainjoin-cli --help-internal</code>
<code>--log {. path}</code>	Generates a log file or prints the log to the console.	<code>domainjoin-cli --log /var/log/domainjoin.log</code> <code>join likewisedemo.com Administrator</code> <code>domainjoin-cli --log .</code> <code>join likewisedemo.com Administrator</code>

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 be with the domain 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>domainjoin-cli join -- notimesync 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, 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 module 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
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 <code>krb5.conf</code>
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:

```
[root@rhel4d bin]# 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 lwidthentity module in -/usr/lib/security/methods.cfg (AIX
only)

* Add lwidthentity to passwd and group/groups line -/etc/
nsswitch.conf or

-/etc/netssvc.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.

To disable a module, execute either the following join or leave command:

```
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

See Also

Generate a Domain Join Log

5.3. 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 then 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 at the shell prompt 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`.

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

After you install the Likewise agent, you can install the Likewise Domain Join Tool, a graphical user interface for joining a domain. The domain join tool is not included when you install the agent; you must install the utility separately. For more information, see [Install the Domain Join Utility](#).

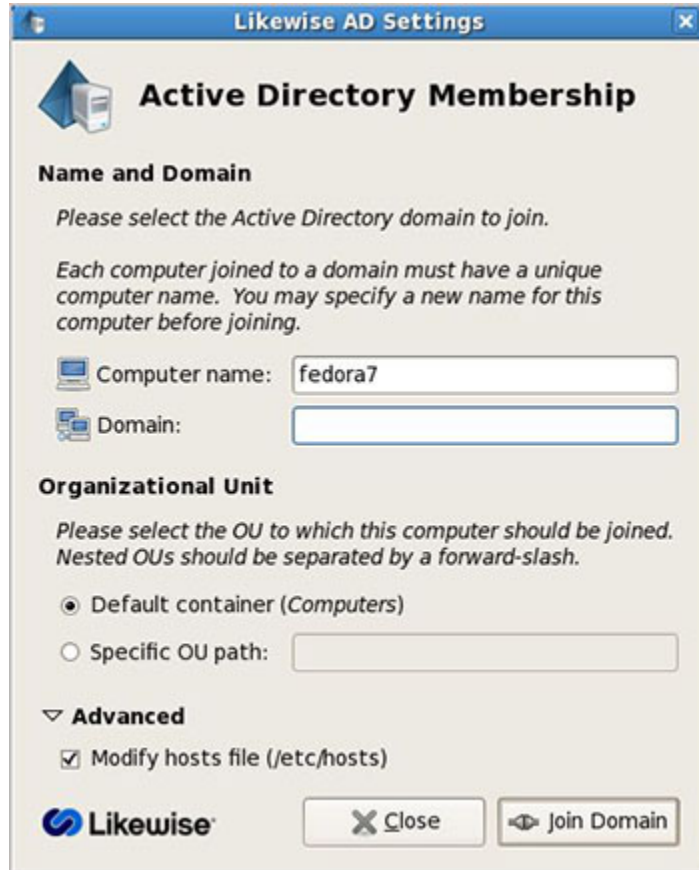
Important: To join a computer to a domain, you must have the user name and password of a user who has privileges to join computers to a domain and the full name of the domain that you want to join.

1. 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

1. On the Likewise AD Settings panel, in the **Domain** box, enter the Fully Qualified Domain Name (FQDN) of the Active Directory domain.

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.



2. 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. 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 to container (Computers)**.

3. Click **Join Domain**.
4. Enter the user name and password of an Active Directory user with the right to join a machine to the Active Directory 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.

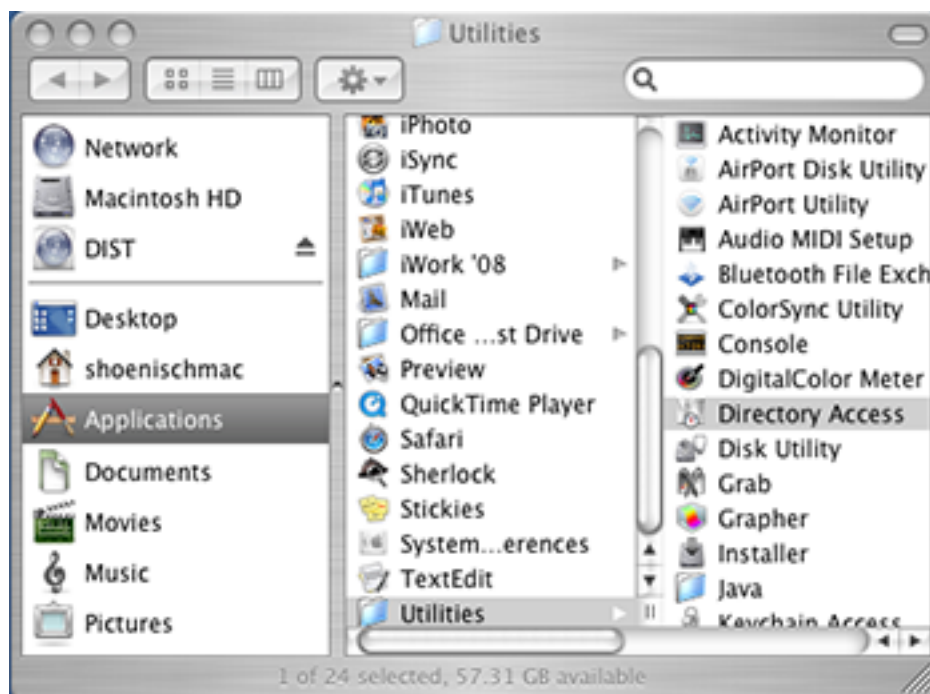
After you join a domain for the first time, you must restart the computer before you can log on.


5.5. 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.

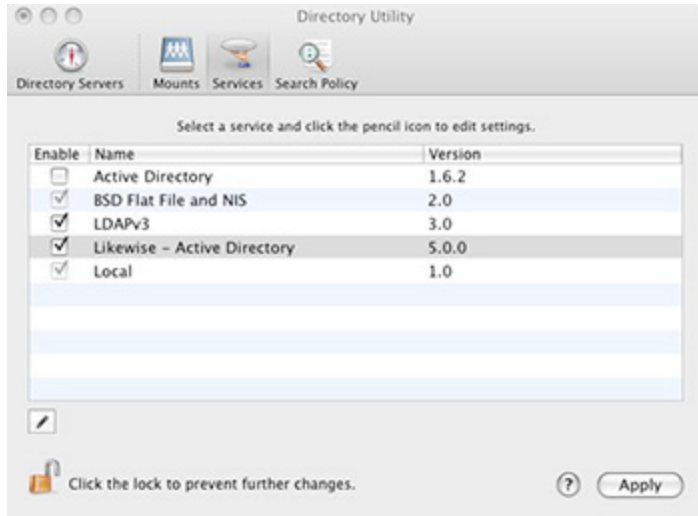


2. On Mac OS X 10.5, click **Show Advanced Settings**.
3. On the **Services** tab, click the lock  and enter an administrator name and password to unlock it.
4. In the list, make sure that the check box for **Active Directory** is not selected.


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**.

See Also

Migrate a User Profile on a Mac

5.6. Use Likewise with a Single OU

If you have only write privileges for an organizational unit in Active Directory, you can still use Likewise. You should enable an organizational unit (OU) for Likewise only when you want to manage your Linux, Unix, and Mac OS X computers within a single OU and you do not have Domain Administrator or Enterprise Administrator privileges, but you have been given rights to create objects in an OU. (See Delegate Control to Create Container Objects.) You can use the write privileges that you have been given for an OU to join Linux and Unix computers to that OU.

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 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 domain 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.

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.

5.7. 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.

Rename a Computer by Using the Domain Join Tool

To execute the following procedure, the Likewise Domain Join Tool, a graphical user interface for joining a domain, must be installed on your computer. For more information, see [Install the Likewise Domain Join Tool](#).

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
```

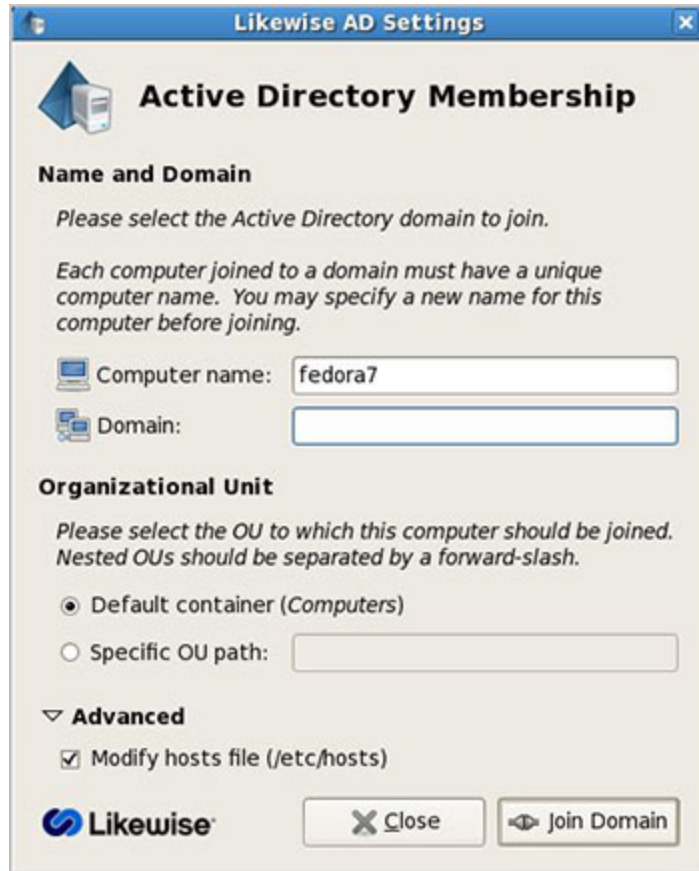
2. Click **Leave**, and then click **OK**.

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.

5.8. Files Modified When You Join a Domain

When Likewise joins 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 installation* 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.)	#	#			#

/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	#	#	#	#	#
/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	#	#			

5.9. 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](#).

See Also

[About Single Sign-On](#)

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

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

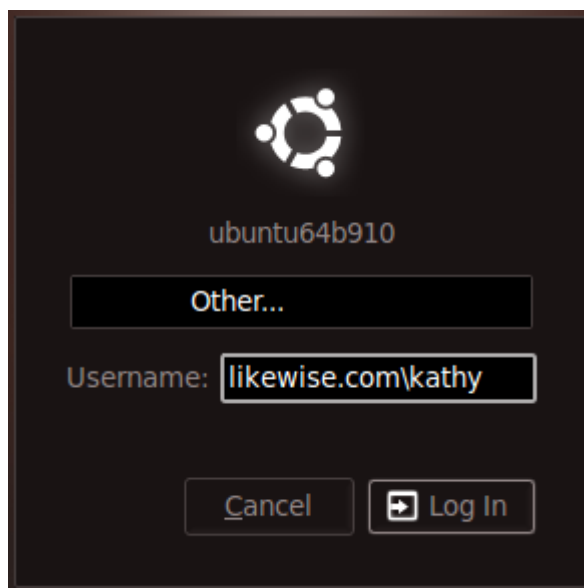
6.2. Log On with AD Credentials

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 to 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 to a Linux or Unix computer with SSH from Windows, 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.
2. Try to SSH to the target Linux or Unix computer again with the user's full NT4-style credentials, not 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, on a Windows administrative workstation connected to your Active Directory domain controller, 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. 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 at the shell prompt 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 at the shell prompt as the root user:

```
/sbin/service lsassd status
```

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: <code>domainjoin-cli query</code> 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. 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
```

```
[root@rhel4d bin]#
```

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.
```

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 switch user 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`

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 output the log to the console by executing the following 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`

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 ADrootDomain.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 domainName
```

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. This is likely to be the IP address 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 `--log` denotes that the information is to be shown in the console:

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

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

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

Example:

```
domainjoin-cli --log /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 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 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 source `w32tm`, the Windows time service.

7.3. Dealing with Common Error Messages

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

7.3.1. 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.

7.3.2. 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.

7.4. 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
```

Chapter 8. Configuring the Likewise Services with the Registry

8.1. 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 settings can be centrally managed with group policies when you use Likewise Enterprise; see *About Group Policies* in the Likewise Enterprise guide. Likewise Open does not apply group policies.

8.1.1. 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\svsvcs]
```

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] ❸
[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 syslod.
- 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.
- ❸ 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.

8.1.1.1. 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"
```

8.1.2. 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).

8.2. 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
```

```
\>
```

8.3. 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 -- `lwsm --` 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/lwsm refresh lsass
```

8.4. 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"
```

8.5. 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.

8.6. Settings in the Lsass Branch

This section lists value entries in the registry's lsass branch.

8.6.1. 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"
```

8.6.2. 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
```

8.6.3. 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
```

8.6.4. 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 Likewise Enterprise guide.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

RequireMembershipOf

Notes

Add the users and groups 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 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" "jane"  
"S-1-5-21-3447809367-3151979076-456401374-513" "sales^admins"
```

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.

8.6.5. 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"
```

8.6.6. 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
```

8.6.7. 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:

- whitespace -- spaces and tabs
- 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\Providers\ActiveDirectory]
```

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.

8.6.8. 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\Providers\ActiveDirectory]
```

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.

8.6.9. 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
```

8.6.10. 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
```

8.6.11. 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 with Likewise Enterprise you 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 three 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.

The variables are used in the following order: %H/%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.

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

8.6.12. 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"
```

8.6.13. 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.

8.6.14. Force Likewise Open to Ignore Cell Information

When there is cell information from Likewise Enterprise in Active Directory, it can prevent users from logging on a computer running Likewise Open. To allow Active Directory users, regardless of whether they have been provisioned with UID-GID information or other cell information, to access a computer running Likewise Open, you can force the Likewise authentication daemon to ignore cell information when the daemon queries Active Directory. Since Likewise Open does not require the following information, you can set the authentication daemon to ignore it:

- Home directory
- UID
- GID
- Unix shell

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

CellSupport

Notes

Value must be set as one of the following: `full` or `unprovisioned`.

Example with the value set to `unprovisioned` to force Likewise Open to ignore Unix settings in AD:

```
"CellSupport"="unprovisioned"
```

If you are using Likewise Enterprise with cells and you want to use the Unix settings in AD, leave `cell-support` set to its default value of `full`. Example:

```
"CellSupport"="full"
```

8.6.15. 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

8.6.16. 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). Features that are using offline cached credentials reattempt to log on the Active Directory domain controller at the interval that you set. When online, the Likewise agent also caches the information for the specified time period.

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.

8.6.17. Change the Interval When Expired Cache Entries Are Purged

You can change the interval when expired entries are purged from the cache. Purging expired entries from the cache can improve the performance of the authentication daemon.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

CachePurgeTimeout

Example with default value:


```
"CachePurgeTimeout"=dword:00278d00
```

Set the value to a time span, in seconds. The minimum value is 5 minutes, expressed in seconds, and the maximum value is 60 days, expressed in seconds.

8.6.18. Turn Off K5Login 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
```

8.6.19. Change NSS Membership 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	Specifies whether to discard cached information from a Privilege Attribute Certificate (PAC) entry

	<p>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 change this setting to 1, but performance might be affected.</p>

8.6.20. 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:

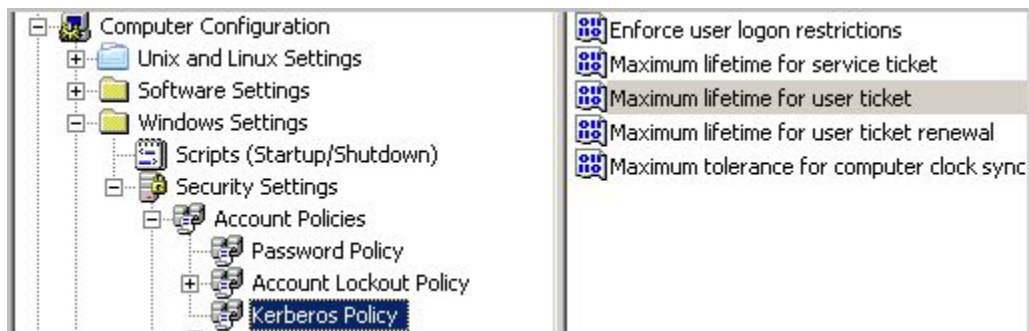
"MachinePasswordLifespan"=dword:000927c0

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

8.6.21. 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.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

LdapSignAndSeal

Example with default value:

```
"LdapSignAndSeal"=dword:00000000
```

8.6.22. 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"
```

8.6.23. 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.

8.6.24. 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
```

8.6.25. 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
```

8.6.26. 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.

8.6.27. 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\DomainTrust]

Stores information about domain trusts.

- [HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\ProviderData]

Stores data used by the Active Directory authentication provider.

- [HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\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.

8.7. Settings in the eventlog Branch

This section lists value entries in the registry's eventlog branch.

8.7.1. 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"
```

8.7.2. 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"
```

8.7.3. 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"
```

8.7.4. 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
```

8.7.5. 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
```

8.7.6. 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
```

8.7.7. 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
```

8.8. 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
```

8.8.1. Set the Negative Cache Timeout

This setting determines how long netlogond waits before it attempts to look up something it could not previously find.

Location

```
[HKEY_THIS_MACHINE\Services\netlogon\Parameters]
```

Value Entry

NegativeCacheTimeout

Example with default value:

```
"NegativeCacheTimeout"=dword:0000003c
```

8.8.2. 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
```

8.8.3. 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
```

8.8.4. 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
```

8.9. 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.

8.9.1. 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\lwio\Parameters\Drivers\rdr]
```

Value Entry

`SignMessagesIfSupported`

Example with default value:

```
"SignMessagesIfSupported"=dword:00000000
```

8.9.2. Enable Security Signatures

This value entry, which is turned on by default, sets the CIFS file server to sign response when it receives signed messages from a client.

Location

[HKEY_THIS_MACHINE\Services\lwp\Parameters\Drivers\srp]

Value Entry

EnableSecuritySignatures

Example with default value:

"EnableSecuritySignatures"=dword:00000001

8.9.3. 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\lwp\Parameters\Drivers\srp]

Value Entry

RequireSecuritySignatures

Example with default value:

"RequireSecuritySignatures"=dword:00000001

8.9.4. 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\lwp\Parameters\Drivers\srp]

Value Entry

SupportSmb2

Example with default value:

"SupportSmb2"=dword:00000000

Chapter 9. Troubleshooting the Agent

9.1. 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 output the log to the console by stopping the daemon with the Likewise Service Manager and then running the authentication daemon in debug mode. Execute the following commands as root:

```
/opt/likewise/bin/lwsm stop lsass
/opt/likewise/sbin/lsassd ---loglevel debug
```

9.2. Troubleshoot Likewise Daemons with the Service Manager

Although you can manage the Likewise daemons individually -- see the sections on checking the status of and restarting each daemon later in this chapter -- 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. 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)
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 see the logging destination:

/opt/likewise/bin/lwsm get-log

To see the logging level:

/opt/likewise/bin/lwsm get-log-level

To change the logging level:

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

Examples:

```
[root@rhel5d bin]# -/opt/likewise/bin/lwsm get-log
syslog: LOG_DAEMON
[root@rhel5d bin]# -/opt/likewise/bin/lwsm get-log-level
INFO
[root@rhel5d bin]# -/opt/likewise/bin/lwsm set-log-level warning
[root@rhel5d bin]# -/opt/likewise/bin/lwsm get-log-level
WARNING
```

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

/opt/likewise/bin/lwsm --help

9.3. 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:

```
/sbin/service lsassd status
```

or

```
/etc/init.d/lsassd status
```

(On HP-UX, the command is `/sbin/init.d/lsassd status`.)

If the authentication daemon is running, the result should look like this:

```
lsassd (pid 25753) is running...
```

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

```
/sbin/service lsassd start
```

or

```
/etc/init.d/lsassd start
```

(On HP-UX, the command is `/sbin/init.d/lsassd start`.)

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 `lsassd` 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**.

9.4. Check the Status of the DCE/RPC Daemon

The Likewise DCE/RPC daemon handles communication between Linux, Unix, and Mac computers 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:

```
/sbin/service dcerpcd status
```

or

```
/etc/init.d/dcerpcd status
```

If the daemon is running, the result should look like this:

```
dcerpcd (pid 21538) is running...
```

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

```
/sbin/service dcerpcd start
```

or

```
/etc/init.d/dcerpcd start
```

On HP-UX

The commands are different on HP-UX:

```
/sbin/init.d/dcerpcd status
```

```
/sbin/init.d/dcerpcd start
```

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**.

9.5. 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:

```
/sbin/service netlogond status
```

or

```
/etc/init.d/netlogond status
```

If the daemon is running, the result should look like this:

```
netlogond (pid 21438) is running...
```

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

```
/sbin/service netlogond start
```

or

```
/etc/init.d/netlogond start
```

On HP-UX

The commands are different on HP-UX:

```
/sbin/init.d/netlogond status
```

```
/sbin/init.d/netlogond start
```

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**.

9.6. Check the Status of the Input-Output Service

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

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:

```
/sbin/service lwiod status
```

or

```
/etc/init.d/lwiod status
```

If the daemon is running, the result should look like this:

```
lwiod (pid 21638) is running...
```

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

```
/sbin/service lwiod start
```

or

```
/etc/init.d/lwiod start
```

On HP-UX

The commands are different on HP-UX:

```
/sbin/init.d/lwiod status
```

```
/sbin/init.d/lwiod start
```

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**.

9.7. Find the Likewise Daemons on a Mac

To locate the Likewise processes on a Mac OS X computer, execute the following command in Terminal:

```
sudo launchctl list | grep likewise
```

There are typically four Likewise daemons running on a Mac:

```
com.likewisesoftware.lwiod
```

```
com.likewisesoftware.netlogond
```

```
com.likewisesoftware.dcerpcd
```

```
com.likewisesoftware.lsassd
```

With the Likewise Enterprise agent, the group policy daemon is also running:

```
com.likewisesoftware.gpagentd
```

9.8. 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 your domain controller:

1. In Active Directory Users and Computers, right-click the Linux, Unix, or Mac OS X 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>lsllpp -l grep likewise</code>
HP-UX	<code>swlist grep -i likewise</code>

9.9. 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. 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
```

9.9.1. 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:

```
/sbin/service lsassd 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:

```
/sbin/service lsassd start
```

Clear the Cache on a Mac

1. In Terminal, stop the Likewise authentication daemon by executing the following command as sudo:

```
sudo launchctl stop com.likewisesoftware.lsassd
```

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:

```
sudo launchctl start com.likewisesoftware.lsassd
```

Clear the Cache on a Unix Computer

1. Stop the Likewise authentication daemon by executing the following command as root:

```
/etc/init.d/lsassd 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:

```
/etc/init.d/lsassd start
```

9.10. 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

9.11. Generate a Domain-Join Log

To help troubleshoot problems with joining 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 `--log` denotes that the information is to be shown in the console:

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

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

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

Example:

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

9.12. 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
```

9.13. 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 error, warning, info, and verbose.

1. Log on as root user.
2. Edit the registry so that the `log-level` line in the `pam` section is set to the log level that you want.

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`

9.14. Generate an Authentication Agent Debug Log

By editing the entries for the `lsass` service in the Likewise registry, you can specify the level of logging for the Likewise authentication daemon's interaction with PAM. The following log levels are available: `error`, `warning`, `info`, `verbose`. The default is `error`.

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

1. Log in as root user.
2. Modify the registry to set the debug log for the `lsass` service to `verbose`.
3. Restart the Likewise authentication daemon by executing the following command from the command line (On HP-UX, the path to the command is `/sbin/init.d`):

```
/sbin/service lsassd restart
```

On a Mac:

```
sudo launchctl stop com.likewisesoftware.lsassd
sudo launchctl start com.likewisesoftware.lsassd
```

4. After you finish troubleshooting, set the `log-level` back to `error` and restart the daemon again.

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

9.15. Generate a Debug Log for Netlogond

The `netlogond` daemon detects the optimal domain controller and global catalog and caches the data. You can obtain debugging information about the daemon's lookup requests for domain controllers by executing the following command as root:

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

9.16. 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
```

9.17. 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

9.18. Allow Access to Account Attributes

Likewise Enterprise and the UID-GID module are 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 determine 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 either Likewise Enterprise or the UID-GID module in schema mode.
uidNumber	Required when you use either Likewise Enterprise or the UID-GID module in schema mode.
gidNumber	Required when you use either Likewise Enterprise or the UID-GID module 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 without the Likewise UID-GID Module.

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 login 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

9.19. 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 and a list of inter-daemon dependencies, see [About the Likewise Agent](#).

On Linux and Unix

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

```
/sbin/service dcerpcd restart
```

or

```
/etc/init.d/dcerpcd restart
```

To stop the daemon, type this command:

```
/sbin/service dcerpcd stop
```

To start the daemon, type this command:

```
/sbin/service dcerpcd start
```

Note: On Unix systems, the location of the daemon may vary.

On HP-UX

Restart: `/sbin/init.d/dcerpcd restart`

Stop: `/sbin/init.d/dcerpcd stop`

Start: `/sbin/init.d/dcerpcd start`

On Mac OS X

On a Mac, use the following `stop` and `start` commands (you cannot use the `restart` command on a Mac):

```
sudo launchctl stop com.likewisesoftware.dcerpcd
```

```
sudo launchctl start com.likewisesoftware.dcerpcd
```

9.20. 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](#).

On Linux and Unix

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

```
/sbin/service netlogond restart
```

or

```
/etc/init.d/netlogond restart
```

To stop the daemon, type this command:

```
/sbin/service netlogond stop
```

To start the daemon, type this command:

```
/sbin/service netlogond start
```

Note: On Unix systems, the location of the daemon may vary.

On HP-UX

Restart: `/sbin/init.d/netlogond restart`

Stop: `/sbin/init.d/netlogond stop`

Start: `/sbin/init.d/netlogond start`

On Mac OS X

On a Mac, use the following `stop` and `start` commands (you cannot use the `restart` command on a Mac):

```
sudo launchctl stop com.likewissoftware.netlogond
```

```
sudo launchctl start com.likewissoftware.netlogond
```

9.21. Restart the Input-Output Service

The Likewise input-output service -- `lwiod` -- communicates over SMB with SMB servers; authentication is with Kerberos 5. For a list of start-order dependencies, see [About the Likewise Agent](#).

On Linux and Unix

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

```
/sbin/service lwiod restart
```

or

```
/etc/init.d/lwiod restart
```

To stop the daemon, type this command:

```
/sbin/service lwiod stop
```

To start the daemon, type this command:

```
/sbin/service lwiod start
```

Note: On Unix systems, the location of the daemon may vary.

On HP-UX

Restart: `/sbin/init.d/lwiod restart`

Stop: `/sbin/init.d/lwiod stop`

Start: `/sbin/init.d/lwiod start`

On Mac OS X

On a Mac, use the following `stop` and `start` commands (you cannot use the `restart` command on a Mac):

`sudo launchctl stop com.likewisesoftware.lwiod`

`sudo launchctl start com.likewisesoftware.lwiod`

9.22. Restart the Authentication Daemon

The authentication daemon handles authentication, authorization, caching, and idmap lookups. When you restart the authentication daemon (`lsassd`), you should also restart the `lwiod` daemon. For more information and a list of inter-daemon dependencies, see [About the Likewise Agent](#).

On Linux and Unix

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

`/sbin/service lsassd restart`

or

`/etc/init.d/lsassd restart`

To stop the daemon, type this command:

`/sbin/service lsassd stop`

To start the daemon, type this command:

`/sbin/service lsassd start`

Note: On Unix systems, the location of the daemon may vary.

On HP-UX

Restart: `/sbin/init.d/lsassd restart`

Stop: `/sbin/init.d/lsassd stop`

Start: `/sbin/init.d/lsassd start`

On Mac OS X

On a Mac, use the following `stop` and `start` commands (you cannot use the `restart` command on a Mac):

```
sudo launchctl stop com.likewisesoftware.lsassd
```

```
sudo launchctl start com.likewisesoftware.lsassd
```

9.23. Troubleshooting 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/tkerrberr.mspx>

- Kerberos and LDAP Troubleshooting Tips:

<http://www.microsoft.com/technet/solutionaccelerators/cits/interopmigration/unix/usecdirw/17wsdsu.mspx>

9.24. 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
```

9.25. Fix KRB Error During SSO in a Split-DNS Configuration

When you are working in a network with a split-DNS configuration in which the domain for users is different from the domain 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 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 instance) will work:

```
KRB ERROR BAD OPTION
```

Assume your computer's 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.

9.26. 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

Set the Default Login Shell

9.28. Updating PAM on SLED 11

9.29. Configuring PAM on RHEL 5 and CentOS 5

9.30. 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. 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.

9.31. 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
```

9.32. 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:115:LIKEWISEDEMO\bakhtin
```

9.33. 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: Jorgen Habermas:/home/local/
LIKEWISEDEMO/ hab:/bin/ sh
```

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

9.34. 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";
```

9.35. Working with Solaris Zones

Solaris zones are a virtualization technique created by Sun Microsystems to consolidate servers. Primarily used for application isolation, they give the appearance that the various applications are running on individual servers.

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 file spaces, including `/usr` and others, which are mounted read-only. These file spaces are writable only for the global zone.

As a result, you cannot install most applications -- including Likewise -- in a zone except by installing it in the global zone. Installing Likewise in the global zone automatically results in it being installed in all the non-global zones. This behavior can be over-ridden with a flag to `pkgadd`.

Although Likewise installs on all zones, they are not joined to Active Directory (AD) as a group. Each individual zone, including the global zone, can be joined to AD independently of any other zones.

Make Sure `/opt/likewise` Exists

To work with Solaris zones, the `/opt/likewise` directory must be present on the target computer. Typically, the Likewise installation script creates it. Solaris zones typically share `/opt`, so Likewise installations on machines with a shared `/opt` configuration for zones, called a small zones configuration, can create the `likewise` directory. However, a big zones configuration in which

nothing is shared can result in `/opt` being different in the global and non-global zones. Thus, even though the Likewise installer can create `/opt/likewise` in the global zone but cannot create the directory in the non-global zones, and the installation of fails. In such cases, as a work around, pre-create `/opt/likewise` in the 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. This is because the root user of the non-global zone does not have root access to the underlying (global) system, and therefore cannot set the system clock.

If the clocks are within the five-minute spread required by Kerberos, this will not be an issue. If this is not the case, you can resolve this 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. If you create a new global zone after installing the Likewise product, you may receive errors similar to the following:

```
Installation of these packages generated errors: <likewiseLibXML2
likewiseOpenLDAP likewiseKrb5 likewiseExpat likewiseGroupPolicy
likewiseAuth likewiseDomainJoin>
```

```
Installation of these packages generated warnings: <SMCx11vnc NXnode
NXserver>
```

The file `</zones/zone02/root/var/sadm/system/logs/install_log>` contains a log of the zone installation.

The `install_log` file will show issues related to the packages requiring user interaction. This interaction is simply `pkgadd` asking if you are sure you want to over-write the package files that already exist in the global zone.

You may safely ignore these messages, since the required files are already installed in the shared file spaces.

3. Some group policies may log PAM errors in the non-global zones even though they function as expected. Cron is one example, as shown below:

```
Wed Nov 7 16:26:02 PST 2007 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 be due to file access permissions, attempts to write to read-only file spaces, or both.

4. 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 cause an undesirable amount of chatter on the console or mangle the graphic desktop.

To redirect this traffic to a file instead of being displayed 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 cause Syslog to ignore the entire line.

Chapter 10. Command-Line Reference

This chapter presents an overview of the commands in `/opt/likewise/bin`. 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. lwsmd: Manage Services

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 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/lwsmd list`

Example:

```
[root@rhel5d bin]# -/opt/likewise/bin/lwsmd 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/lwsmd 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/lwsmd refresh lsass`

To view information about the `lsass` service, including its dependencies, run the following command:

`/opt/likewise/bin/lwsmd 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, execute the following command:

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

10.2. 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](#).

10.3. 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
```

10.4. lw-set-log-level: Set the Log Level

You can set the Likewise log level from the shell prompt by executing the following command and replacing `level` with one of the four available logging levels: `error`, `warning`, `info`, `verbose`.

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

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

The configuration for the Likewise authentication daemon in the registry is modified to include the level you specified in the command.

You can also set the logon level by editing an entry for the lsass service in the registry; see the chapter on configuring Likewise with the registry.

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

10.5. Find a User or a Group

On a Unix or Linux computer that is joined to the 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\\hoenstiv`

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
```

```
/opt/likewise/bin/lw-find-user-by-name ---level 2 likewisedemo\\hab
```

```
User info (Level-2):
```

```
=====
```

```
Name:                LIKEWISEDEMO\\hab
UPN:                  hab@likewisedemo.com
Uid:                  593495196
Gid:                  593494529
Gecos:                Jurgen Habermas
Shell:                -/bin/sh
Home dir:              -/home/LIKEWISEDEMO/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
```

10.6. 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
```

10.7. 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
```

10.8. 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
```

10.9. 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:                LIKEWISEDEMO\sduval
UPN:                 SDUVAL@LIKEWISEDEMO.COM
Generated UPN:       NO
Uid:                 593495151
Gid:                 593494529
Gecos:               Shelley Duval
Shell:               -/bin/sh
Home dir:            -/home/LIKEWISEDEMO/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
```

10.10. 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, 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: 5.4.0
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.

10.11. lw-get-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-get-current-domain

10.12. lw-get-dc-list

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

10.13. lw-get-dc-name: Get Domain Controller Information

/opt/likewise/bin/lw-get-dc-name DomainName

10.14. lw-get-dc-time

This command displays the time of the current domain controller for the domain that you specify. 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
```

10.15. 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
```

10.16. 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
```

10.17. 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-dump-machine-acct domainDNSName

Example: `/opt/likewise/bin/lw-dump-machine-acct likewisedemo.com`

The result looks like this:

```
/opt/likewise/bin/lw-dump-machine-acct likewisedemo.com

DomainSID              = S-1-5-21-382349973-3885793314-468868962
DomainName             = LIKEWISEDEMO
Domain DNS Name        = LIKEWISEDEMO.COM
HostName               = RHEL5D
Machine Account Name   = RHEL5D$
```

Machine Account Password = xoiy8X!k/BdfiVUj

10.18. 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
```

10.19. 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.

```
/opt/likewise/bin/lw-trace-info
```

Example usage:

```
lw-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-trace-info --help
```

10.20. lw-update-dns: Dynamically Update DNS

This command registers an IP address for the computer in DNS. Running this 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
```

Example usage:

To view the command's syntax and arguments, execute the following command:

```
/opt/likewise/bin/lw-update-dns --help
```

10.21. 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, execute the following command as root:

```
/opt/likewise/bin/sqlite3 /var/lib/likewise/db/lsass-adcache.db 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
```

10.22. domainjoin-cli

`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](#).

10.23. 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-yocat -d likewisedemo.com -k map-name
```

To view the command's syntax and arguments, execute the following command:

```
/opt/likewise/bin/lw-yocat --help
```

10.24. 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
```

10.25. uuid

This command displays the UUID of the user.

/opt/likewise/bin/uuid

Example:

```
[root@rhel5d bin]# ./uuid
836d9daa-a3b6-11de-885e-000c2961e58e
[root@rhel5d bin]#
```

10.26. 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.

10.26.1. lwio-fuse-mount: Gain Access to a Shared Windows Folder

The `lwio-fuse-mount` command lets you gain access to a shared folder on a Windows computer. For this command to work, your Linux or Unix computer must have File System in User Space, or FUSE, a loadable kernel module that gives non-privileged users the power to create their own file systems without editing the kernel code. FUSE is preinstalled on several Linux platforms. It is freely available from SourceForge at <http://sourceforge.net/projects/fuse/files/fuse-2.X/>.

The location of the Likewise tool is as follows:

/opt/likewise/bin/lwio-fuse-mount

Example:


```
/opt/likewise/bin/lwio-fuse-mount --server steveh-dc --share  
winshare /rhelshare
```

To view the tool's arguments, execute the following command:

```
/opt/likewise/bin/lwio-fuse-mount --help
```

10.26.2. **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
```

10.26.3. **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
```

10.26.4. **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
```

10.26.5. 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
```

10.27. 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 administrators 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.)

10.27.1. 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
```

10.27.2. 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
```

10.27.3. 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
```

10.27.4. 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
```

10.27.5. 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
```

10.27.6. 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
```

10.28. 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.

10.28.1. 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 `-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 -
```

10.28.2. 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  
  
-sh-3.00$
```

Note: To address Kerberos issues, see Troubleshooting Kerberos Errors at <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/tkerberr.msp>.

10.28.3. 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
```

10.28.4. kpasswd: Change a Password

The kpasswd command changes 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
```

10.28.5. ksu: Kerberized Super User

This command is a Kerberized version of the su program. It has two main uses: To securely change the real and effective user ID to that of the target user and to create a new security context. The command's location is as follows:

/opt/likewise/bin/ksu

To view the command's options and arguments, execute the following command:

```
man ksu
```

10.28.6. 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

10.28.7. 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

10.28.8. krb5-config: Identify Your Version of Kerberos

This command provides details about your computer's version of Kerberos, including its libraries. The command's location is as follows:

/opt/likewise/bin/krb5-config

Example usage:

```
[root@rhel5d bin]# ./krb5-config --all
Version:      Kerberos 5 release 1.7
Vendor:       Massachusetts Institute of Technology
Prefix:       -/opt/likewise
Exec_prefix:  -/opt/likewise
```

To view the command's options and arguments, execute the following command:

/opt/likewise/bin/krb5-config --help

Example:

```
[root@rhel5d bin]# ./krb5-config --help
Usage: ./krb5-config [OPTIONS] [LIBRARIES]
Options:
    [--help]           Help
    [--all]            Display version, vendor, and various values
    [--version]        Version information
    [--vendor]         Vendor information
    [--prefix]         Kerberos installed prefix
    [--exec-prefix]    Kerberos installed exec_prefix
    [--cflags]         Compile time CFLAGS
    [--libs]           List libraries required to link [LIBRARIES]

Libraries:
    krb5               Kerberos 5 application
    gssapi             GSSAPI application with Kerberos 5 bindings
    kadm-client        Kadmin client
    kadm-server        Kadmin server
    kdb                Application that accesses the kerberos
    database
[root@rhel5d bin]#
```

10.29. 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.

10.29.1. ConfigureLogin

ConfigureLogin is used by `domainjoin-cli`. It is recommended that you do not execute the ConfigureLogin command manually.

10.29.2. dceidl

dceidl is used by dcerpcd; the command is not for end users.

10.29.3. demo

demo is used by the application; it is not for end users.

10.29.4. gpccron

gpccron is used by the application. It is recommended that you do not execute it manually.

10.29.5. gpccron.sh

gpccron.sh is used by the application. It is recommended that you do not execute it manually.

10.29.6. 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.

10.29.7. idl

idl is used by the application. It is recommended that you do not execute it manually.

10.29.8. init-base.sh

init-base.sh is included by the initiation scripts. It is recommended that you do not execute it manually.

10.29.9. lwmapsecurity-test

This command tests the `lwmapsecurity` library.

`/opt/likewise/bin/lwmapsecurity-test`

Example usage:

```
/opt/likewise/bin/lwmapsecurity-test Administrator
```

To view the command's arguments, execute the following command:

```
/opt/likewise/bin/lwmapsecurity-test --help
```

10.29.10. lw-migrator

This command is not implemented yet.

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
```

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..... glennn-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:

```
/opt/likewise/setup/djgtk/uninstall
```

12.3. Uninstall the Agent on a Linux or Unix Computer

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.

Important: Before uninstalling the agent, you must leave the domain and uninstall the domain-join GUI. 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.

- 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
```

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:

```
./LikewiseIdentityServiceOpen-5.0.0.3494-linux-oldlibc-i386-rpm.sh  
uninstall
```

For information about the script's options and commands, execute the following command:

```
./LikewiseIdentityServiceOpen-5.4.0.8011-linux-i386-rpm.sh help
```

12.4. Uninstall the Agent on a Mac

On a Mac computer, you must uninstall the Likewise agent by using the 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 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 infrastructure is properly configured, Likewise does the following:

- Ensures that DNS is properly configured to resolve names associated with Active Directory (AD).
- Provides tools to join Linux, Unix, and Mac OS X computers to 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 appropriate 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.

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 SSH for SSO](#).

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.
3. Create a keytab for the SPN.
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#

```

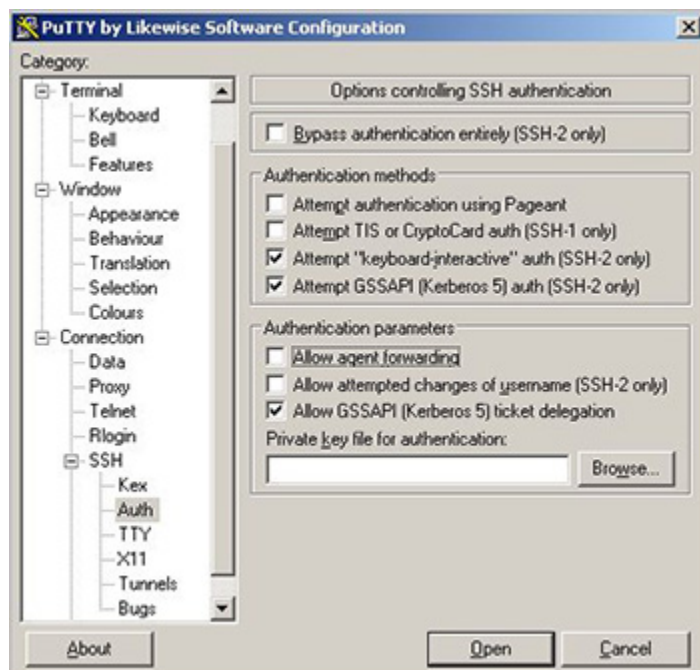
13.3. Configure PuTTY for Windows-Based SSO

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**.

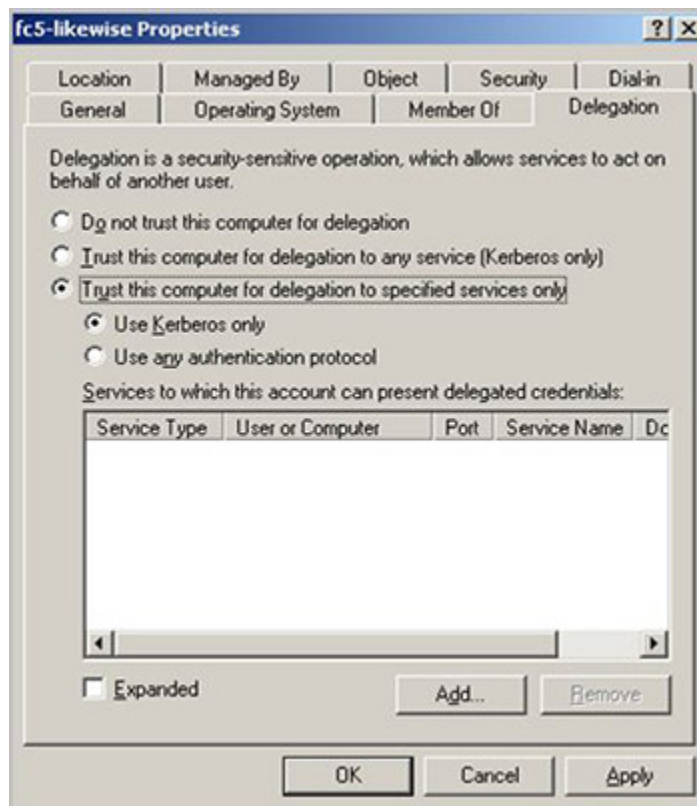


Configure the Base Linux Computer in Active Directory

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

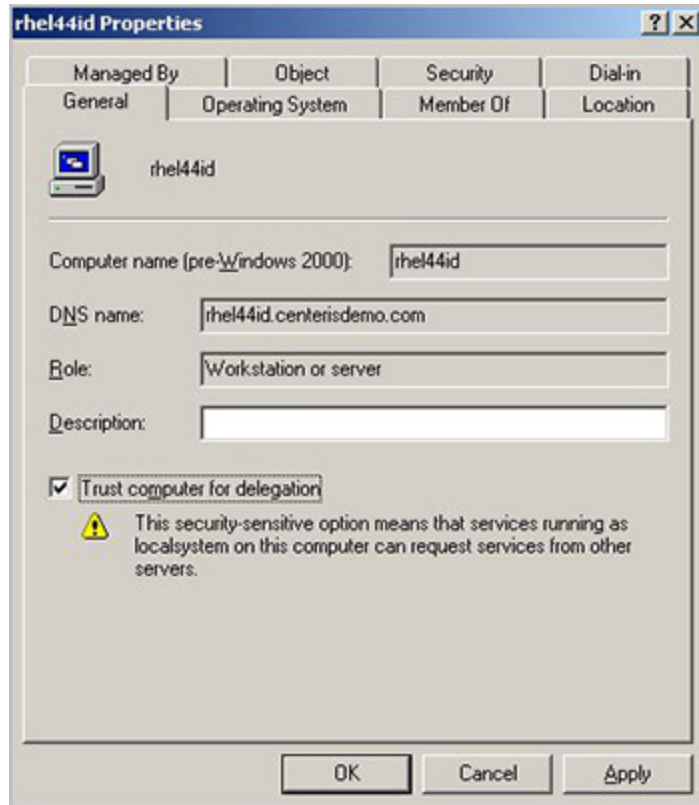
1. In Active Directory Users and Computers, in the console tree, click **Computers**.
2. In the details pane, right-click the computer that you want, and then click **Properties**.
3. On the **Delegation** tab, click **Trust this computer for delegation to specified services only**:



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. Solve the SSO Problem on Red Hat and CentOS

There is a known bug with some versions of Red Hat and CentOS that prevents SSO from working with SSH, SSHD, and PuTTY. The following versions are known to be affected:

- CentOS 5
- Red Hat Enterprise Linux 5

Problem

The system incorrectly concatenates the Kerberos ticket's service principal name on the target Linux computer. For example, in the final entry of the results of the `klist` command below, the full name of the service principal is cut off after the `@` symbol:

```
[LIKEWISEDEMO\fanthony@centos52 ~]$ -/opt/likewise/bin/klist
```

```
Ticket cache: FILE:/tmp/krb5cc_1689257039
```

```
Default principal: fanthony@LIKEWISEDEMO.COM
```

Valid starting	Expires	Service principal
07/31/08 09:25:13	07/31/08 19:25:31	krbtgt/ LIKEWISEDEMO.COM@LIKEWISEDEMO.COM

```
renew until 08/07/08 09:25:13

07/31/08 09:25:31 07/31/08 19:25:31 CENTOS52$@LIKEWISEDEMO.COM

renew until 08/07/08 09:25:13

07/31/08 09:30:04 07/31/08 19:25:31 host/centos52.likewisedemo.com@

renew until 08/07/08 09:25:13
```

Test

To determine whether you need to implement the solution below on your Red Hat or CentOS computer, execute the following series of tests:

1. Connect to your target machine with SSH by using PUTTY and a valid Active Directory user. Be sure to use the FQDN of the host.
2. Execute the following command:

```
/opt/likewise/bin/klint
```

The results should look like this:

```
LIKEWISEDEMO\fanthony@centos52 ~]$ klist
Ticket cache: FILE:/tmp/krb5cc_1689257039
Default principal: fanthony@LIKEWISEDEMO.COM
Valid starting      Expires              Service principal
07/31/08 09:25:13  07/31/08 19:25:31  krbtgt/
LIKEWISEDEMO.COM@LIKEWISEDEMO.COM
renew until 08/07/08 09:25:13
07/31/08 09:25:31  07/31/08 19:25:31  CENTOS52$@LIKEWISEDEMO.COM
renew until 08/07/08 09:25:13
```

3. SSH again to the same host and when prompted for the password, type CNTL+C.
 4. Execute the klist command again:
- is in the following output:

```
[LIKEWISEDEMO\fanthony@centos52 ~]$ klist
Ticket cache: FILE:/tmp/krb5cc_1689257039
Default principal: fanthony@LIKEWISEDEMO.COM
Valid starting      Expires              Service principal
07/31/08 09:25:13  07/31/08 19:25:31  krbtgt/
LIKEWISEDEMO.COM@LIKEWISEDEMO.COM
renew until 08/07/08 09:25:13
07/31/08 09:25:31  07/31/08 19:25:31  CENTOS52$@LIKEWISEDEMO.COM
renew until 08/07/08 09:25:13
07/31/08 09:30:04  07/31/08 19:25:31  host/
centos52.likewisedemo.com@
renew until 08/07/08 09:25:13
```


Solution

1. On Red Hat Enterprise Linux 5, make sure that the reverse PTR host definitions are defined in DNS.
2. On the target Linux computer, add the following line to `/etc/krb5.conf` under the `[domain_realm]` entry of the file:

```
.yourdomainname.com = YOURDOMAINNAME.COM
```

Example:

```
[domain_realm]
.likewisedemo.com = LIKEWISEDEMO.COM
```

3. Restart SSHD by running the following command at the shell prompt:

```
/sbin/service sshd restart
```

13.5. On RHEL5 and AIX, Set Reverse PTR Host Definitions for SSO with SSH

For single sign-on with SSH to work on Red Hat Enterprise Linux 5 and AIX, reverse PTR host definitions must be set in DNS.

13.6. Configure AIX 5.3 for Outbound Single Sign-On with SSH

On AIX 5.3, client-side SSH is not set up by default. Here's how to configure it so that it will work with Likewise.

1. On your AIX 5.3 computer, make sure the network authentication service, version 1.4.0.8, is installed; example:

```
-bash-3.00$ lslpp -l -| grep krb
krb5.client.rte 1.4.0.8 COMMITTED Network Authentication Service
```

If it is not installed, obtain it from the IBM AIX web site at http://www.ibm.com/developerworks/aix/library/au-nas_relatedtech/index.html and install it.

2. After joining an Active Directory domain with Likewise, append the following lines to the end of `/etc/krb5/krb5.conf`:

```
[domain_realm]
.demo.likewise.com = DEMO.LIKEWISE.COM
demo.likewise.com = DEMO.LIKEWISE.COM
```

3. Make sure that `/etc/krb5/krb5.conf` links to `/etc/krb5.conf`.
4. Also make sure that `/etc/krb5/krb5.keytab` links to `/etc/krb5.keytab`.
5. Make a backup of the credentials directory by executing the following command as root:

```
mv /var/krb5/security/creds /var/krb5/security/creds_old
```

6. As root, make a symbolic link to the /tmp directory so that the AIX Kerberos libraries can access the directory in which Likewise stores its credential caches:

```
ln -s /tmp /var/krb5/security/creds
```

7. Open /etc/environment -- which contains the list of environmental variables that are set when a user logs on -- and add the following line to the end of it:

```
KRB5_CONFIG=/var/lib/likewise/krb5-affinity.conf:/etc/krb5.conf
```

8. If you are logged on the machine whose environmental variable you changed, you must log off and log on again for the change to take effect.

13.7. 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 at <http://www.ietf.org/rfc/rfc2478.txt> 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 configure your Apache HTTP Server for single sign-on.

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.
- 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:

```
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 LIKEWISEDEMO.COM

Krb5Keytab -/etc/apache2/http.ktb

Require valid-user

</Directory>
```

4. Configure your web server for Secure Socket Layer (SSL).

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.

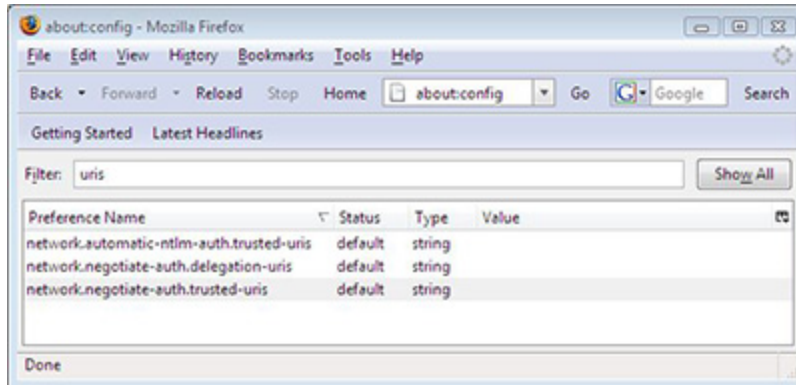
7. Use secure FTP or another method to transfer the keytab file to the Linux computer that hosts your Apache web server and place the file in the location specified in your `<Directory>` configuration in `httpd.conf`. For example, using the configuration shown in Step 3 above, the keytab file would be 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.

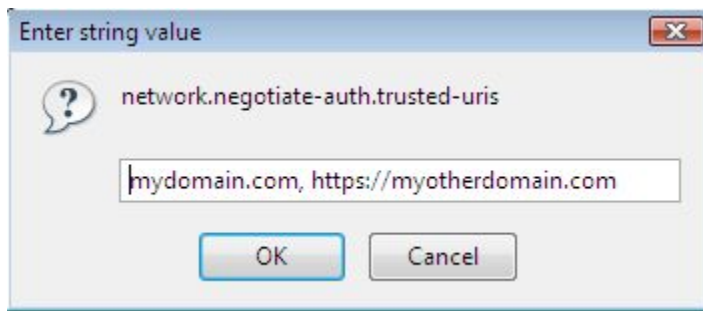
Configure Firefox for SSO

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`.



4. 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:



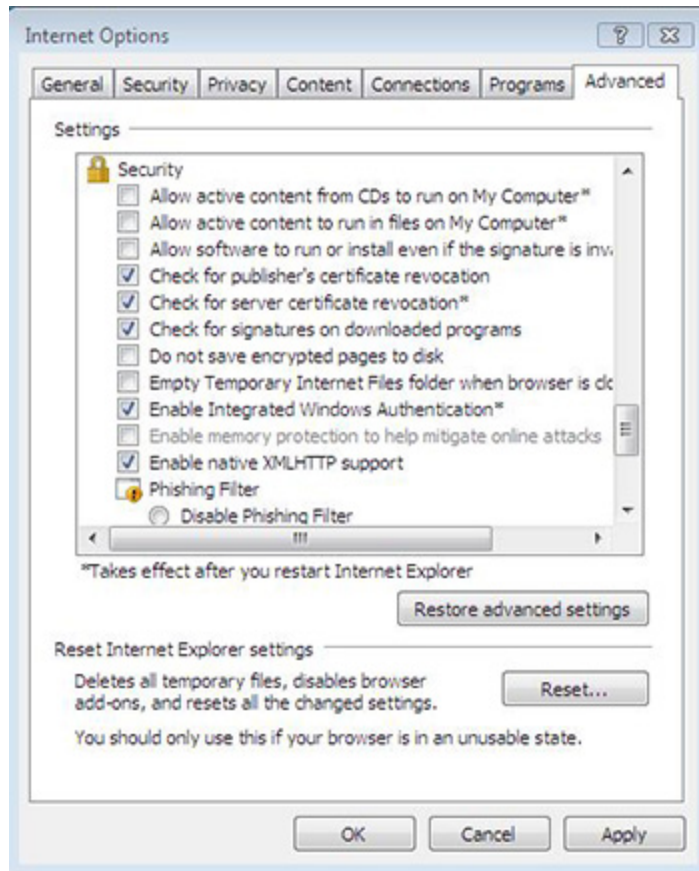
5. Double-click **network.negotiate-auth.delegation-uris**, enter a comma-separated list of the sites for which the browser may delegate user authorization to the server, and then click **OK**.

For more information on how to configure Firefox, see <http://groklmsnet.de/kerbtut/firefox.html>.

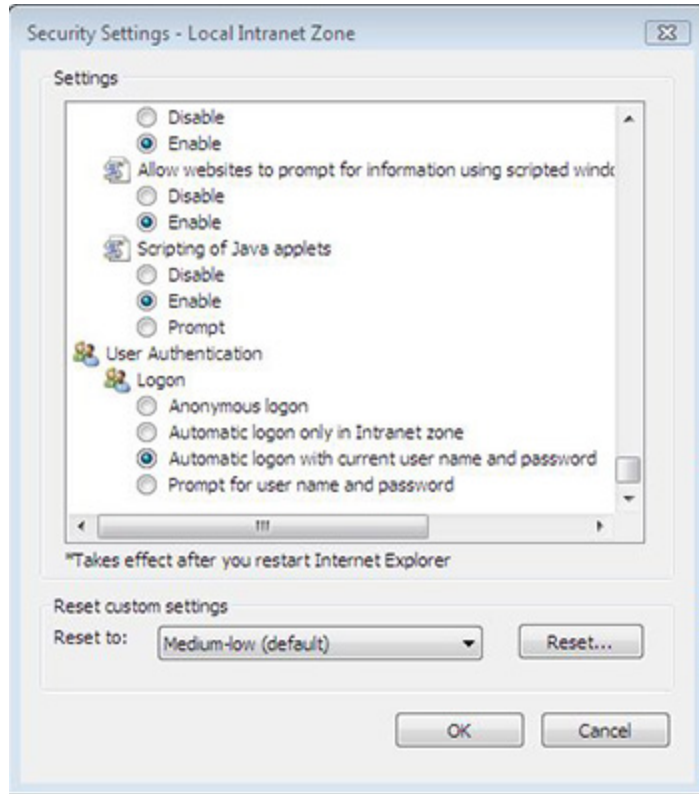
Configure Internet Explorer for SSO

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. 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
```

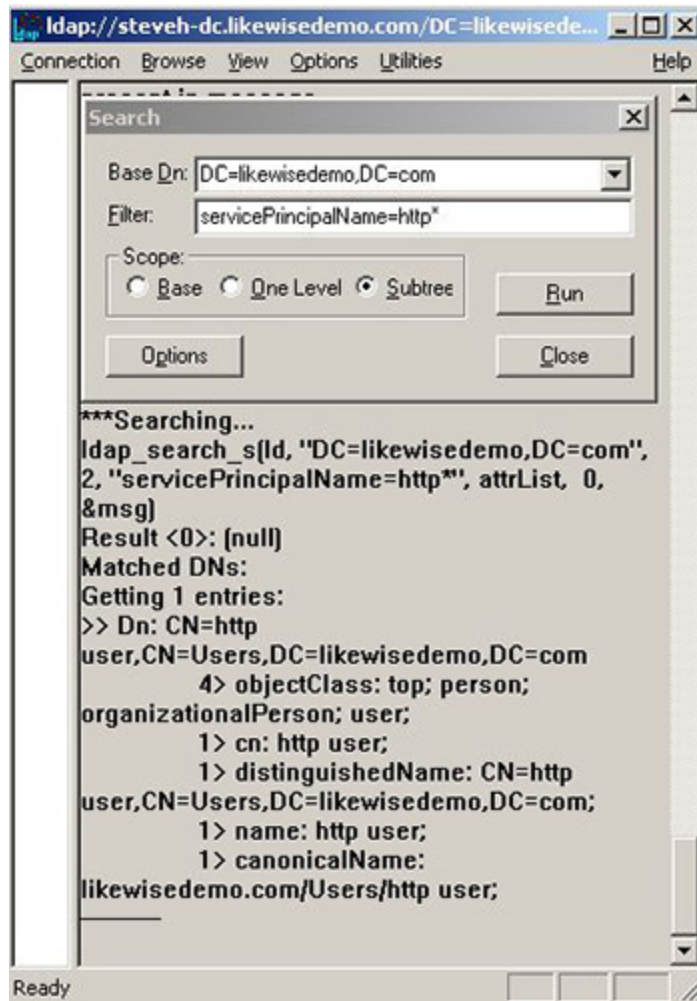
If your service principal names are incorrect, generate a new Kerberos keytab file.

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>



13.7.1. 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.

13.8. 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. Contacting Technical Support

14.1. 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**.

14.2. 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.
 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 15. 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.

The Likewise Open software is free to download and use according to the terms of the Limited GPL 2.1 for client libraries and the GPL 2 for daemons. The licenses for Likewise Enterprise and for Likewise UID-GID Module are different. 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 © 2010 Likewise Software. All rights reserved.