

Likewise[®] Enterprise

Installation and Administration Guide

Version 6.0

Likewise Enterprise Installation and Administration Guide

Abstract

Last updated: June 28, 2011. "

This guide describes how to install Likewise Enterprise and connect computers running Unix, Linux, and Mac OS X to Active Directory. The guide covers installing the Likewise agent, configuring the agent, installing the Likewise Management Console on a Windows administrative workstation connected to Active Directory, configuring a domain for use with Likewise, migrating Unix users to Active Directory, logging on with domain credentials, and monitoring events.

This guide is supplemented by the Likewise community forum, which you can join at <http://www.likewise.com/community/>, and by manuals in the documentation library, including the Group Policy Administration Guide.

This Version

Likewise Enterprise **6.0**: http://www.likewise.com/resources/documentation_library/manuals/lwe/likewise-enterprise-guide.html

Select Your View:



Multiple-page HTML web site.



Single-page HTML document.



Compiled Help with folder view and advanced search. (Download the zip file and then save its .chm file to a local folder. On some versions of Windows, you must unblock a .chm file before you can view it. To unblock it after saving it locally, right-click the file, click Properties, and then click Unblock.)



PDF.

Previous Versions

Likewise Enterprise 5.2 and 5.3: http://www.likewise.com/resources/documentation_library/manuals/lwe/likewise-enterprise-53-guide.html (PDF)

Likewise Enterprise 5.1: http://www.likewise.com/resources/documentation_library/manuals/lwe/likewise-enterprise-51-guide.html (PDF)

Likewise Enterprise 5.0: http://www.likewise.com/resources/user_documentation/LikewiseEnterprise5.0_Installation_and_Administration_Guide.pdf

Likewise Enterprise 4.1 or earlier: http://www.likewise.com/resources/documentation_library/#enterprise

Table of Contents

1. Introduction	1
1.1. Task Road Map	1
1.2. Software Products	2
1.3. Software Components	2
2. Planning Your Installation and Deployment	4
2.1. Overview of the Installation Process	4
2.2. Planning Your Deployment	4
2.3. About Schema Mode and Non-Schema Mode	5
2.3.1. Changes Made by the Schema Wizard	8
2.3.2. Key Differences	8
2.3.3. Pros and Cons of the Schema Modes	9
2.4. About Likewise Cells	10
2.5. Best Practices for Modes, Cells, Group Policies, and User Rights	14
3. Installing and Using the Console	15
3.1. About the Likewise Console	15
3.2. Requirements	16
3.3. Install the Likewise Console	19
3.4. Start the Likewise Console	21
3.5. Connect to a Domain	21
3.6. Run the Schema Mode Wizard	22
3.7. Replication in a Large Forest or in Multiple Domains	23
3.8. Upgrade the Schema of a Forest	23
3.9. Add a Plug-In	24
4. Working with Cells	25
4.1. Make a Cell and Associate it with an OU or a Domain	25
4.1.1. Moving a Computer to Another Cell	26
4.2. Create a Default Cell	27
4.2.1. Use Pre-Existing RFC 2307 Data	27
4.3. Associate a User with One or More Cells	27
4.4. Add a Group to a Cell	27
4.5. Add a User to a Cell	28
4.6. Link Cells	29
4.7. Delegate Control to Create Container Objects	31
4.8. Administering Cells with Cell Manager	32
5. Managing Users, Groups, and Computers	36
5.1. Modify Likewise Settings in ADUC	36
5.2. Create a User	36
5.3. Finding Users and Groups in ADUC	38
5.4. Provision a User with Linux or Unix Access	39
5.5. Provision a Group with Linux or Unix Access	41
5.6. Specify a User's ID and Unix or Linux Settings	42
5.7. Apply Unix or Linux Settings to Multiple Users	43
5.8. Set a User Alias	43
5.9. Set a Group Alias	44
5.10. Set the Default Home Directory	45
5.11. Set the Default Login Shell	46
5.12. Assign a Group ID	47
5.13. Disable a User	48
5.14. Improve MMC Performance When Accessing Likewise Settings in ADUC	48
5.15. Extend File Mode Permissions with POSIX ACLs	49
5.15.1. Using POSIX ACLs to Grant AD Accounts Access to Subversion	51

6. Migrating Users to Active Directory	52
6.1. About Diagnostics and Migration	52
6.2. Migrate Users to Active Directory	52
6.3. Find Orphaned Objects	54
6.4. Migrate a User Profile on a Mac	55
7. The Likewise Agent	57
7.1. About the Likewise Agent	57
7.2. Daemons	57
7.3. The Likewise Registry	61
7.4. Ports and Libraries	61
7.5. Caches and Databases	61
7.6. Time Synchronization	63
7.7. Using a Network Time Protocol Server	63
7.8. Automatic Detection of Offline Domain Controller and Global Catalog	64
7.9. UID-GID Generation in Likewise Open and Likewise Enterprise Cells	64
7.10. Cached Credentials	64
7.11. Trust Support	65
7.12. Integrating with Samba	66
7.13. Supported Platforms	66
8. Configuring Clients Before Agent Installation	67
8.1. Configure nsswitch.conf	67
8.2. Configure resolv.conf	67
8.3. Configure Firewall Ports	67
8.4. Extend Partition Size Before Installing Likewise on IBM AIX	68
8.5. Increase Max Username Length on IBM AIX	68
8.6. Check System Health Before Installing the Agent	68
9. Installing the Agent	73
9.1. Install the Correct Version for Your Operating System	73
9.2. Requirements for the Agent	73
9.3. Install the Agent on Linux or Unix with the Shell Script	76
9.4. Install the Agent on Linux in Unattended Mode	76
9.5. Install the Agent on Unix with the Command Line	77
9.6. Install the Agent on a Mac Computer	77
9.7. Install the Agent on a Mac in Unattended Mode	78
9.8. Installing the Agent in Solaris Zones	79
9.9. Upgrading Your Operating System	80
10. Joining an Active Directory Domain	81
10.1. About Joining a Domain	81
10.2. Join Active Directory with the Command Line	83
10.3. Domainjoin-cli Options, Commands, and Arguments	84
10.4. Join Active Directory Without Changing /etc/hosts	90
10.5. Join a Linux Computer to Active Directory with the GUI	91
10.6. Join a Mac Computer to Active Directory with the GUI	92
10.6.1. Turn Off OS X Directory Service Authentication	95
10.7. Use Likewise with a Single OU	95
10.8. Rename a Joined Computer	96
10.9. Files Modified When You Join a Domain	98
10.10. With NetworkManager, Use a Wired Connection to Join a Domain	100
11. Logging On with Domain Credentials	101
11.1. About Logging On	101
11.2. Log On with AD Credentials	101
11.3. Log On with SSH	102
11.4. Solve Logon Problems from Windows	102
11.5. Solve Logon Problems on Linux or Unix	103

12. Troubleshooting Domain-Join Problems	108
12.1. Top 10 Reasons Domain Join Fails	108
12.2. Solve Domain-Join Problems	108
12.3. Ignore Inaccessible Trusts	111
12.4. Dealing with Common Error Messages	112
12.4.1. Configuration of Krb5	112
12.4.2. Chkconfig Failed	112
12.5. Diagnose NTP on Port 123	112
12.6. Turn Off Apache to Join a Domain	114
13. Configuring the Agent	115
13.1. Modify Settings with the Config Tool	115
13.2. Add Domain Accounts to Local Groups with /etc/group	116
13.3. Configure Entries in Your Sudoers Files	116
13.4. Set a Sudoers Search Path	117
13.5. Set Up AIX Audit Classes to Monitor Events	118
14. Troubleshooting the Agent	119
14.1. Likewise Daemons and Services	119
14.1.1. Troubleshoot Likewise Daemons with the Service Manager	119
14.1.2. Check the Status of the Authentication Daemon	120
14.1.3. Check the Status of the DCE/RPC Daemon	120
14.1.4. Check the Status of the Network Logon Daemon	121
14.1.5. Check the Status of the Input-Output Service	121
14.1.6. Restart the Authentication Daemon	122
14.1.7. Restart the DCE/RPC Daemon	122
14.1.8. Restart the Network Logon Daemon	122
14.1.9. Restart the Input-Output Service	122
14.2. Logging	123
14.2.1. Generate a Domain-Join Log	126
14.2.2. Generate an Authentication Agent Debug Log	127
14.2.3. Generate a PAM Debug Log	127
14.2.4. Generate a Directory Service Log on a Mac	128
14.2.5. Log Group Policy Debugging Data	128
14.2.6. Generate a Network Trace	129
14.3. Basics	129
14.3.1. Check the Version and Build Number	129
14.3.2. Determine a Computer's FQDN	130
14.3.3. Make Sure Outbound Ports Are Open	130
14.3.4. Check the File Permissions of nsswitch.conf	131
14.3.5. Configure SSH After Upgrading It	131
14.3.6. Upgrading an Operating System	131
14.4. Accounts	132
14.4.1. Allow Access to Account Attributes	132
14.4.2. A User's Settings Are Not Displayed in ADUC	132
14.4.3. Resolve an AD Alias Conflict with a Local Account	133
14.4.4. Fix the Shell and Home Directory Paths	134
14.4.5. Troubleshooting with the Get Status Command	134
14.4.6. Troubleshoot User Rights with Ldp.exe and Group Policy Modeling	135
14.4.7. Fix Selective Authentication in a Trusted Domain	139
14.5. Cache	140
14.5.1. Clear the Authentication Cache	140
14.5.2. Clear a Corrupted SQLite Cache	141
14.6. Kerberos	142
14.6.1. Fix a Key Table Entry-Ticket Mismatch	142
14.6.2. Fix KRB Error During SSO in a Disjoint Namespace	143

14.6.3. Eliminate Logon Delays When DNS Connectivity Is Poor	144
14.7. PAM	144
14.7.1. Dismiss the Network Credentials Required Message	145
14.8. Red Hat and CentOS	145
14.8.1. Modify PAM to Handle UIDs Less Than 500	145
14.9. SLED	145
14.9.1. A Note About the Home Directory on SLED 11	145
14.9.2. Updating PAM on SLED 11	145
14.10. AIX	146
14.10.1. Increase Max Username Length on AIX	146
14.10.2. Updating AIX	146
14.11. Mac OS X	146
14.11.1. Find the Likewise Service Manager Daemon on a Mac	146
14.12. FreeBSD	147
14.12.1. Keep Usernames to 16 Characters or Less	147
14.13. Solaris	147
14.13.1. Turn On Core Dumps on Solaris 10	147
15. Command-Line Reference	149
15.1. lwsm: Manage Services	149
15.2. lwconfig	150
15.3. lwregshell: The Registry Shell	150
15.4. lw-edit-reg: Export the Registry to Your Editor	150
15.5. lw-set-log-level: Set the Log Level	151
15.6. lw-set-machine-name: Change the Hostname in the Local Provider	151
15.7. Find a User or a Group	151
15.8. Find a User by a SID	152
15.9. List Groups for a User	153
15.10. lw-enum-groups: List Groups	153
15.11. lw-enum-users: List Users	153
15.12. lw-get-status: View the Status of the Authentication Providers	154
15.13. Get the Current Domain	155
15.14. lw-get-dc-list: List Domain Controllers	155
15.15. lw-get-dc-name: Get Domain Controller Information	155
15.16. lw-get-dc-time: Get Domain Controller Time	156
15.17. lw-get-log-info	156
15.18. lw-get-metrics	156
15.19. Get Machine Account Information	157
15.20. Reload Changes to the Configuration File	157
15.21. lw-trace-info: Turn on Trace Markers in Log Messages	157
15.22. lw-update-dns: Dynamically Update DNS	157
15.23. lw-ad-cache: Manage the AD Cache	158
15.24. domainjoin-cli: Join or Leave a Domain	159
15.25. lw-ypcat	159
15.26. lw-ypmatch	159
15.27. lw-adtool: Modify Objects in AD	159
15.28. lwio: Input-Output Commands	165
15.28.1. lwio-copy: Copy Files Across Disparate Operating Systems	166
15.28.2. lwio-refresh: Reload the Input-Output Settings After Changes	166
15.28.3. lwio-set-log-level	166
15.28.4. lwio-get-log-info	166
15.29. Commands to Modify Local Accounts	167
15.29.1. lw-add-user: Add a Local User by Name or UID	167
15.29.2. lw-add-group: Add a Local Group Member by Name or GID	167
15.29.3. lw-del-user: Remove a Local User by Name or UID	167

15.29.4. lw-del-group: Remove a Local Group by Name or GID	168
15.29.5. lw-mod-user: Modify a Local User by Name or UID	168
15.29.6. lw-mod-group: Modify a Local Group's Members	168
15.30. Kerberos Commands	168
15.30.1. kdestroy: Destroy the Kerberos Ticket Cache	168
15.30.2. klist: View Kerberos Tickets	169
15.30.3. kinit: Obtain and Cache a TGT	169
15.30.4. kpasswd: Change a Password	170
15.30.5. ktutil: The Keytab File Maintenance Utility	170
15.30.6. Kvno: Acquire a Service Ticket and Print Key Version Number	170
15.31. Commands and Scripts Not for Customer Use	171
15.31.1. ConfigureLogin	171
15.31.2. dceidl	171
15.31.3. gpcron	171
15.31.4. gpcron.sh	171
15.31.5. gprsrmtnt.sh	171
15.31.6. init-base.sh	171
15.32. Likewise Enterprise Tools Installed on Windows Computers	171
15.32.1. Lwopt.exe	171
16. Leaving a Domain and Uninstalling the Agent	173
16.1. Leave a Domain	173
16.2. Uninstall the Domain Join GUI	174
16.3. Uninstall the Agent on a Linux or Unix Computer	174
16.4. Uninstall the Agent on a Mac	175
17. Using Likewise with Smart Cards	176
17.1. Smart Card Setup	176
17.2. Log On with a Smart Card	177
17.3. Smart Card Group Policies	179
18. Managing Licenses	181
18.1. About Licenses	181
18.2. Creating a License Container	183
18.3. Import a License File	184
18.4. Assign a License to a Computer in AD	185
18.5. Manage a License Key on a Likewise Client	185
18.6. Delete a License	187
18.7. Revoke a License	187
19. Setting Up the Likewise Reporting Database	188
19.1. Introduction	188
19.2. Overview	188
19.3. Requirements	189
19.4. Setting Up SQL Server	190
19.4.1. Install and Configure SQL Server	190
19.4.2. Create a Database Named LikewiseEnterprise	194
19.4.3. Run the Likewise Database Creation Script	195
19.4.4. Install the Likewise DB Utilities	196
19.4.5. SQL Server Database Security Notes	196
19.5. Setting Up MySQL	198
19.5.1. Create a Database Named LikewiseEnterprise	198
19.5.2. Allow the Database To Accept External Connections from Account	199
19.5.3. Run the Likewise Database Creation Script	199
19.5.4. Install the Likewise DB Utilities	199
19.5.5. Customize Your MySQL Security Settings	200
19.6. Connecting the Likewise Console to the Database	201
19.6.1. Connect the Likewise Console to the Database	201

19.6.2. Make Sure the Collector Processes Are Running	201
19.6.3. Run the DB Update Script	202
19.6.4. Run the ldbupdate.exe from the Command Line	204
19.7. Connecting the Likewise Console to the Database	204
19.7.1. Connect the Likewise Console to the Database	204
19.7.2. Make Sure the Collector Processes Are Running	205
19.8. Setting Computers to Forward Events to LWCollector	206
19.8.1. Set Event Forwarding with a GPO	206
19.8.2. Forward Events by Changing Your Local Settings	207
19.8.3. Cull Events from Syslog	207
19.9. Generate a Sample Report	208
19.10. Monitoring Events with the Operations Dashboard	208
19.10.1. Start the Operations Dashboard	209
19.10.2. Connect to a Database	210
19.10.3. Change the Refresh Rate	210
19.11. Configuring the Likewise Data Collectors	210
19.11.1. LWCollector	211
19.11.2. LWEventDBReaper	212
19.12. Working with the Enterprise Database Management Plug-In	214
19.12.1. Connect to a Database	214
19.12.2. Change the Parameters of the Collectors	214
19.12.3. Set the ACL for RPC Access	215
19.13. Archiving Events	215
19.14. Troubleshooting	216
19.14.1. Check the Endpoints	217
19.14.2. Check the Collector	218
19.14.3. Check the Database	219
19.14.4. Troubleshooting Checklists	220
19.14.5. Switching Between Databases	221
20. Monitoring Events with the Event Log	223
20.1. Monitor Events with the Event Log	223
20.2. View the Local Event Log	223
20.3. The Event Type	226
20.4. The Event Source	226
20.5. List of Events by Source ID	226
21. Using Likewise for Single Sign-On	229
21.1. About Single Sign-On	229
21.2. Make Sure PAM Is Enabled for SSH	230
21.3. Configure PuTTY for Windows-Based SSO	231
21.4. Configure Apache for SSO	234
21.4.1. Kerberos Library Mismatch	244
21.5. Configure a Java Application Server for SSO	245
21.6. Examples	250
22. Configuring the Likewise Services with the Registry	251
22.1. About the Registry	251
22.1.1. The Structure of the Registry	251
22.1.2. Data Types	253
22.2. Modify Settings with the lwconfig Tool	254
22.3. Gain Access to the Registry	256
22.4. Change the Value of an Entry with the Shell	257
22.4.1. Set Common Options with the Registry Shell	258
22.5. Change the Value of an Entry from the Command Line	259
22.6. Find a Value Entry	259
22.7. Settings in the lsass Branch	259

22.7.1. Log Level Value Entries	260
22.7.2. Turn On Event Logging	260
22.7.3. Turn Off Network Event Logging	260
22.7.4. Restrict Logon Rights	261
22.7.5. Display an Error to Users Without Access Rights	261
22.7.6. Display an MOTD	262
22.7.7. Change the Domain Separator Character	262
22.7.8. Change the Replacement Character for Spaces	263
22.7.9. Turn Off System Time Synchronization	263
22.7.10. Set the Default Domain	264
22.7.11. Set the Home Directory and Shell for Domain Users	264
22.7.12. Set the Umask for Home Directories	266
22.7.13. Set the Skeleton Directory	266
22.7.14. Force Likewise Enterprise to Work Without Cell Information	267
22.7.15. Refresh User Credentials	268
22.7.16. Turn Off K5Logon File Creation	268
22.7.17. Change the Duration of the Machine Password	269
22.7.18. Sign and Seal LDAP Traffic	270
22.7.19. NTLM Value Entries	270
22.7.20. Additional Subkeys	271
22.7.21. Add Domain Groups To Local Groups	272
22.7.22. Control Trust Enumeration	272
22.7.23. Modify Smart Card Settings	273
22.7.24. Set the Interval for Checking the Status of a Domain	273
22.7.25. Set the Interval for Caching an Unknown Domain	274
22.8. Cache Settings in the Isass Branch	274
22.8.1. Set the Cache Type	274
22.8.2. Cap the Size of the Memory Cache	274
22.8.3. Change the Duration of Cached Credentials	275
22.8.4. Change NSS Membership and NSS Cache Settings	275
22.9. Settings in the eventlog Branch	277
22.9.1. Allow Users and Groups to Delete Events	277
22.9.2. Allow Users and Groups to Read Events	277
22.9.3. Allow Users and Groups to Write Events	278
22.9.4. Set the Maximum Disk Size	278
22.9.5. Set the Maximum Number of Events	278
22.9.6. Set the Maximum Event Timespan	279
22.9.7. Change the Purge Interval	279
22.10. Settings in the netlogon Branch	279
22.10.1. Set the Negative Cache Timeout	280
22.10.2. Set the Ping Again Timeout	280
22.10.3. Set the Writable Rediscovery Timeout	280
22.10.4. Set the Writable Timestamp Minimum Change	281
22.10.5. Set CLdap Options	281
22.11. Settings in the lwio Branch	281
22.11.1. Sign Messages If Supported	282
22.11.2. Enable Security Signatures	282
22.11.3. Require Security Signatures	282
22.11.4. Set Support for SMB2	282
22.12. Settings in the Lwedsplugin Branch for Mac Computers	283
23. Contacting Technical Support	285
23.1. Contact Support	285
23.2. Provide Diagnostic Information to Technical Support	285
24. Legal Disclaimer and Copyright Notice	288

Chapter 1. Introduction

Likewise connects Linux, Unix, and Mac OS X computers to Microsoft Active Directory so you can centrally manage all your computers and users from a single identity management system. Likewise Enterprise is made up of two software packages: the Likewise management tools for Active Directory, which you install on a Windows computer, and the Likewise agent, which you install on a Linux, Unix, or Mac computer to connect it to Active Directory.

This guide describes how to install and manage Likewise Enterprise. The target audience is system administrators who manage access to workstations, servers, and applications with Active Directory. The guide assumes that you know how to administer computers, users, and group policies in Active Directory and that you know how to manage computers running Unix, Linux, and Mac OS X.

1.1. Task Road Map

To	See
Set up and test a trial version of Likewise Enterprise 5.3 or later in a networked test environment.	The Likewise Evaluation Guide.
Install the Likewise Enterprise Console and the Likewise management tools on a Windows workstation in a production environment.	Install the Management Console
Determine whether to use schema or non-schema mode.	About Schema Mode and Non-Schema Mode
Find out how to use a container, known as a Likewise cell, to manage Likewise clients and Unix settings in AD.	About Likewise Cells
Create a cell in AD for Unix settings, such as a UID, so an AD user can log on a Likewise client.	Create a Cell in AD
Provide AD users and groups with access to Linux, Unix, and Mac computers.	Managing Users, Groups, and Computers
Install the Likewise agent on a Linux, Unix, or Mac OS X computer.	Install the Agent
Connect a computer running Likewise to Active Directory.	Join Active Directory with the Command Line
Troubleshoot problems joining a domain.	Troubleshooting Domain-Join Problems
Log on a Likewise client with an Active Directory user account.	Log On with AD Credentials
Troubleshoot logon problems.	Troubleshooting Logon Problems
Use Cell Manager to administer Likewise cells in AD.	Administering Cells with Cell Manager
Apply group policies to Linux, Unix, and Mac computers.	The Group Policy Administration Guide.
Use Workgroup Manager to apply managed client settings (MCX) to Mac computers as group policy objects.	The Group Policy Administration Guide.

Install the Likewise reporting and auditing components, including the Likewise database.	Setting Up the Likewise Reporting Database
Find information about Likewise commands and command-line utilities for Linux, Unix, and Mac.	Command-Line Reference
Change the local settings on a Likewise client.	Configuring the Likewise Agent
Monitor security events with the event log.	Monitoring Events with the Event Log
Configure Likewise clients for single sign-on.	Using Likewise for Single Sign-On
Migrate Unix or NIS users to Active Directory.	Migrating Users to Active Directory
Migrate a user profile on a Mac from a local user account to the home directory specified for the user in Active Directory.	Migrate a User Profile on a Mac
Set up Samba to authenticate users with Likewise Enterprise.	Samba 3 Integration Guide for Likewise 6 or Later
Install and use Likewise Open.	Likewise Open Installation and Administration Guide
View a list of documents for all Likewise products.	Documents List

1.2. Software Products

Likewise makes two closely related software products: Likewise Open and Likewise Enterprise.

Likewise Open authenticates domain users with the highly secure Kerberos 5 protocol by hashing their security identifiers from Active Directory. Likewise Open does not, however, process user identifiers or group identifiers even if they are set in Active Directory.

Likewise Enterprise is installed on a Windows administrative workstation connected to a domain controller so you can set user identifiers and group identifiers in Active Directory Users and Computers. Once the UIDs and GIDs are set, the Likewise agent uses the identifiers to authenticate users and groups and to control access to computers and applications.

Likewise Enterprise includes additional features. It not only lets you manage Unix identities in Active Directory but also lets you apply group policies to Unix computers from the Microsoft Group Policy Management Console, including policies based on the Gnome GConf project to define desktop and application preferences for Linux computers. More: Likewise Enterprise integrates Apple's Workgroup Manager with the Group Policy Object Editor to apply managed client settings to Mac OS X computers with group policy objects. Likewise Enterprise also lets you generate a range of reports to help improve regulatory compliance. The result: lower operating costs, better security, enhanced compliance.

1.3. Software Components

Likewise comprises several components, each of which provides part of the functionality necessary to manage Linux and Unix computers in Active Directory. There are, however, only two installation packages: one to install the Likewise agent on a Unix, Linux, or Mac OS X computer; the other to install Likewise Enterprise on a Windows administrative workstation that connects to an Active Directory domain controller.

Component	Function
Agent	<ul style="list-style-type: none"> Runs on a Linux, Unix, or Mac OS X computer to connect it to Active Directory with the

	<p>Likewise command-line interface or GUI. See Join Active Directory with the Command Line. Likewise Open is an open-source version of the agent that is available for free at www.Likewise.com.</p> <ul style="list-style-type: none"> • Communicates with an Active Directory domain controller to authenticate and authorize users and groups with the Likewise Identity Service. See Log On with AD Credentials. • Pulls and refreshes group policies by using the group policy daemon, which is included only with the Likewise Enterprise agent.
Management Console	<ul style="list-style-type: none"> • Runs on a Windows administrative workstation that connects to an Active Directory domain controller to help manage Linux, Unix, and Mac OS X computers within Active Directory. • Migrates users, checks status, and generates reports.
MMC Snap-Ins for ADUC and GPOE	<ul style="list-style-type: none"> • Extends Active Directory Users and Computers to include Unix and Linux users. • With Likewise Enterprise, it also extends the Group Policy Object Editor and the Group Policy Management Console to include Linux, Unix, and Mac OS X group policies as well as a way to target them at specific platforms.
Cell Manager	<ul style="list-style-type: none"> • A snap-in for the Microsoft Management Console to manage cells associated with Active Directory Organizational Units.
Reporting Database	<ul style="list-style-type: none"> • Stores security events and access logs for compliance reports.
Operations Dashboard	<ul style="list-style-type: none"> • The Likewise Operations Dashboard is a management application, or plug-in, for the Likewise Management Console. The dashboard retrieves information from the Likewise reporting database to display authentication transactions, authorization requests, network events, and other security events that take place on Likewise clients.

Chapter 2. Planning Your Installation and Deployment

2.1. Overview of the Installation Process

The installation and deployment process typically proceeds in the following order:

1. Make sure your computers meet the installation requirements and then obtain the Likewise software package from www.Likewise.com.
2. Plan your installation, test environment, and production deployment. Make decisions about whether to use Likewise in schema mode or non-schema mode; whether to manage a single forest or multiple forests and to assign UID-GID ranges accordingly; how to configure a Likewise cell topology for your unique needs; whether to migrate NIS users and what to do with local user accounts after migration; and whether to use specific cells for aliasing.
3. Before you install the Likewise Management Console, check Active Directory to make sure it is ready for Likewise by meeting our remediation requirements.
4. Install the Likewise Management Console, which includes management tools, on a Windows administrative workstation that you use to manage Active Directory.
5. Optionally, install a reporting database on a Windows administrative workstation connected to a domain controller. The reporting database, which can be either MySQL or SQL Server, stores access information and security events for compliance reports.
6. Use a Likewise wizard to configure your Active Directory domain in either schema or non-schema mode.
7. Configure a cell topology in Active Directory Users and Computers.
8. Optionally use the console's migration tool to migrate Unix and Linux users and groups to Active Directory.
9. Check the system health, or readiness, of your Linux, Unix, and Mac computers before installing the Likewise agent. For example, you must make sure `resolv.conf` is configured for Likewise.
10. Install the Likewise agent on each Unix, Linux, or Mac OS X computer that you want to join to the Active Directory domain.
11. Join your Unix and Linux computers to Active Directory.
12. Optionally plan and deploy group policies to manage your Unix, Linux, and Mac OS X computers in Active Directory.
13. Troubleshoot any deployment issues and optimize the deployment for your unique mixed network.

2.2. Planning Your Deployment

The key to a successful deployment is planning. Before you begin deploying Likewise in an enterprise, develop a plan that addresses at least the following aspects of installation and deployment:

- Set up a test environment. It is recommended that you first deploy Likewise in a test environment so that you can identify and resolve any issues specific to your mixed network before you put the system into production.
- Determine whether to use Likewise in schema or non-schema mode. The advantages and disadvantages of both approaches are discussed later. When you configure your domain with the Likewise domain configuration wizard, you must choose whether to use schema or non-schema mode.

Important: Back up Active Directory before you run the Likewise domain configuration wizard.

- Decide whether to configure Likewise to manage a single forest or multiple forests. If you manage multiple forests, the UID-GID range assigned to a forest should not overlap with the range of another forest.
- Determine how you will migrate Linux, Unix, and Mac OS X users to Active Directory. For example, if you are using NIS, decide whether you will migrate those accounts to Active Directory and whether you will migrate local accounts and then delete them or leave them. It is usually recommended that you delete interactive local accounts other than the root account.
- Identify the structure of the organizational units -- or cell topology -- that you will need, including the UID-GID ranges. If you have multiple NIS servers in place, your users may have different UID-GID maps in each NIS domain. You may want to eliminate the NIS servers but retain the NIS mapping information in Active Directory. To do so, you can use Likewise cells.
- Determine whether you will use aliasing. If you plan to use aliasing, you must associate users with a specific Likewise cell; you cannot use the default cell.

2.3. About Schema Mode and Non-Schema Mode

Likewise has two operating modes: schema mode and non-schema mode. Schema mode takes advantage of the Unix- and Linux-specific RFC 2307 object classes and attributes to store Linux and Unix user and group information. In contrast, non-schema mode stores Linux and Unix data without requiring RFC 2307 object classes and attributes and without modifying the schema. Instead, non-schema mode uses existing object classes and attributes to store its data. To store information about a cell, Likewise creates a `container` object and stores data in its `description` attribute. To store information about a group or user, Likewise creates a `serviceConnectionPoint` object and stores data in its `keywords` attribute. Both `keywords` and `description` are multi-valued attributes that can have multiple values while still allowing AD searches for specific values.

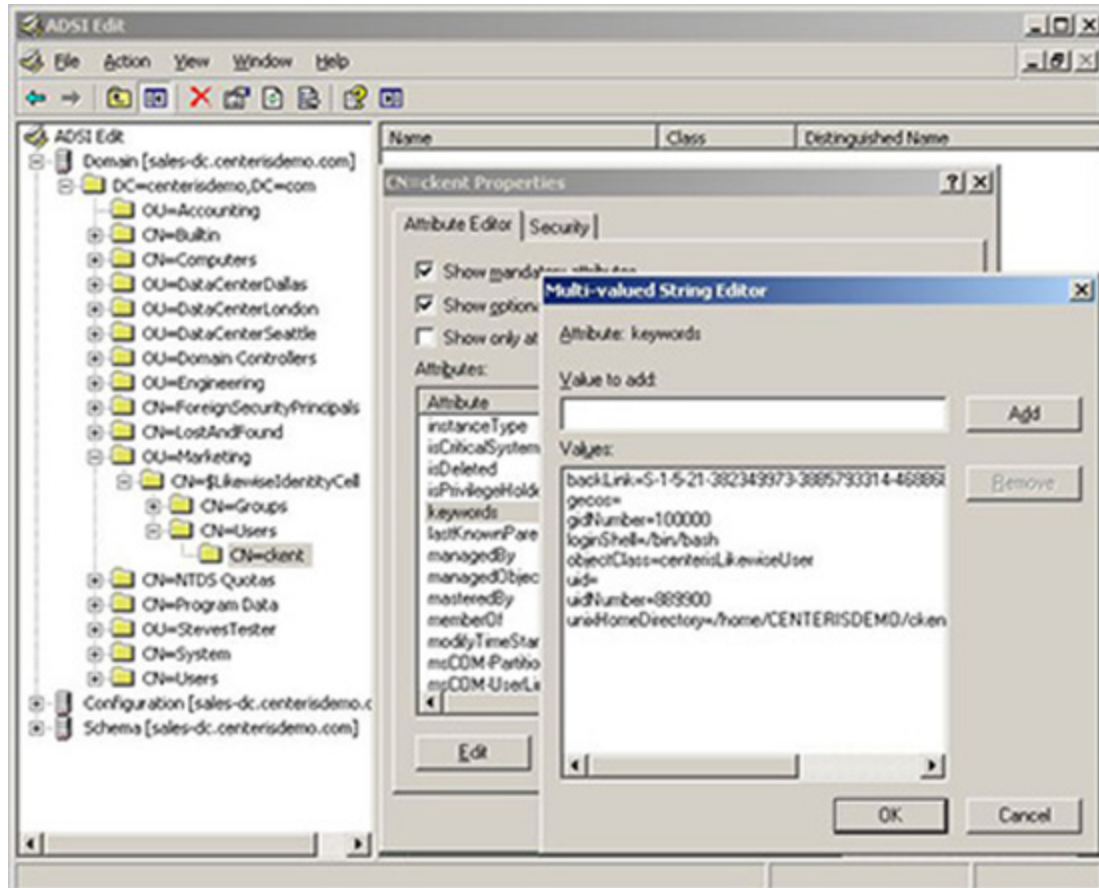
Specifically, in non-schema mode Likewise uses RFC 2307 attribute names to store values in the `keywords` and `description` attributes in the form `name=value`, where `name` is the attribute name and `value` is its value. Here's an example of how the `keywords` attribute name-value pairs can contain Unix and Linux information for an AD user:

```
uid=
uidNumber=1016
gidNumber=100000
loginShell=/bin/bash
unixHomeDirectory=/home/joe
gecos=
backlink=[securityIdentifierOfUser]
objectClass=CenterisLikewiseUser
```

Planning Your Installation and Deployment

In the example, the `uid` attribute is empty. It is needed only when you want to specify a name alias so that the AD user can log on a computer with something other than his or her AD account name.

In ADSI Edit, the properties for a user look like this:

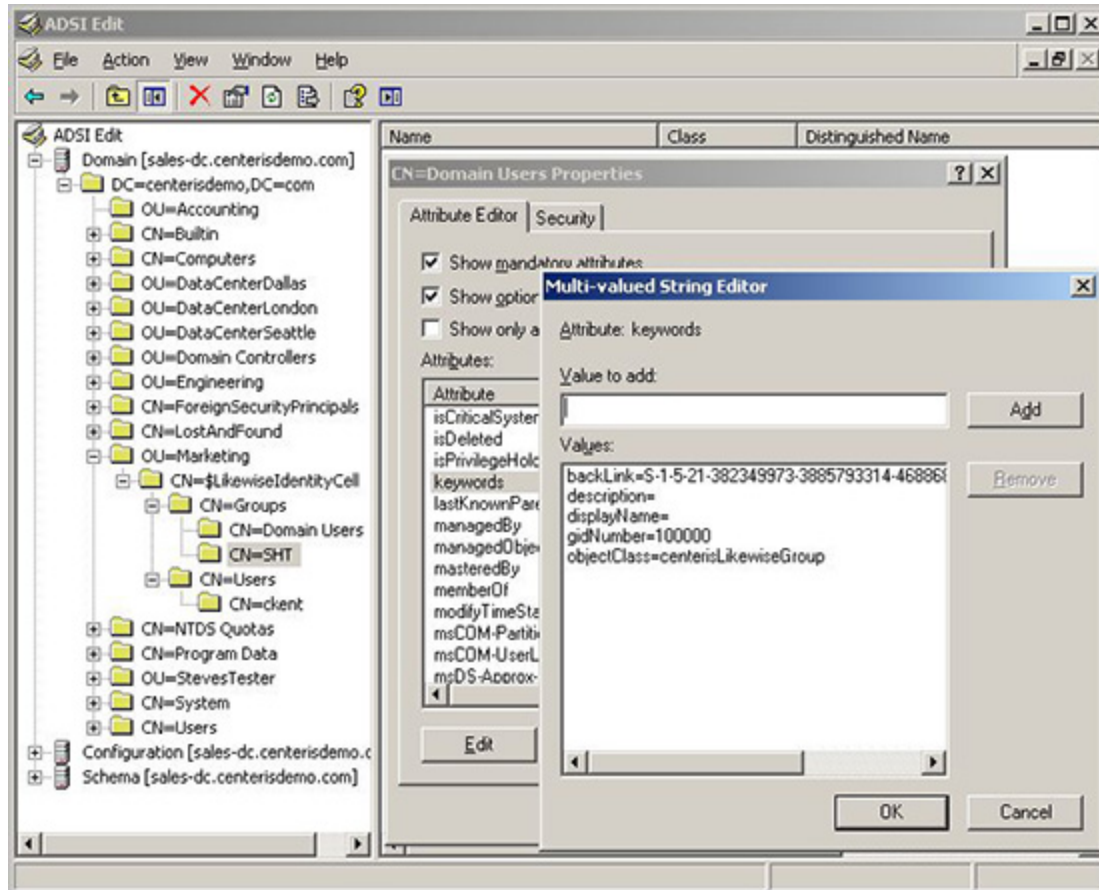


The `keywords` attribute is also used to store Linux and Unix group information. Here's an example of how the attribute name-value pairs can contain Unix and Linux information for a group:

```
backLink=[securityIdentifierOfGroup] description= displayName=  
gidNumber=100000 objectClass=centerisLikewiseGroup
```

When you set an alias for a group, it is stored in the `displayName` attribute (for the group in the example above, no alias has been set, and thus `displayName` is empty).

In ADSI Edit, the values of the `keywords` attribute look like this:



Schema mode takes a slightly different approach. To store Linux and Unix user and group information, schema mode takes advantage of the Unix- and Linux-specific RFC 2307 object classes and attributes, namely the `posixAccount` and `posixGroup` object classes. For example, the `posixAccount` and `posixGroup` object classes include attributes -- `uidNumber` and `gidNumber` -- that Likewise uses for UID and GID mapping. In addition, Likewise uses `serviceConnectionPoint` objects to store the same information as in non-schema mode by using the `keywords` attribute.

For example, when you create a cell in schema mode, Likewise creates a container object -- `CN=$LikewiseIdentityCell` -- in the domain root, or in the OU where you created the cell. If the container is created in an OU, which is called a named or non-default cell, the Unix-specific data is stored in `CN=Users` and `CN=Groups` in the `$LikewiseIdentityCell` container object. The objects point to the Active Directory user or group information with a backlinked security identifier.

If the container is created at the level of the root domain, it is known as a default cell. In this case, the Unix-specific data is stored directly in the AD user or group account.

If you choose to use schema mode and your schema does not comply with RFC 2307, you must modify the schema. The Likewise Domain Extension Wizard, which is a tool in the console, can automatically upgrade your schema to comply with RFC 2307. (Windows Server 2003 R2 or later complies with RFC 2307.) When you use schema mode with a schema that already complies with RFC 2307, Likewise does not change the schema, but you still must run the Domain Extension Wizard to include the RFC 2307 attributes in the global catalog and to index them for faster searches.

2.3.1. Changes Made by the Schema Wizard

The Active Directory schema changes are applied from a set of LDAP Data Interchange Format (LDIF) files. The standard installation places these files in the following directory:

```
/Program Files/Likewise/Enterprise/Resources/LDF
```

After you have raised the domain and forest to 2003 functional levels, the Likewise domain configuration wizard makes the following changes, which are required for Likewise to run in schema mode:

1. Adds the Windows Server 2003 R2 schema extensions for Unix if they are not already part of the schema. Specifically, the wizard adds `uid`, `uidNumber`, `gidNumber`, `gecos`, `unixHomeDirectory`, and `loginShell`.
2. Promotes the `uid`, `uidNumber`, and `gidNumber` attributes to the global catalog.
3. Indexes the `uid` attribute.

2.3.2. Key Differences

The following table summarizes the differences between schema mode and non-schema mode:

Mode	Use Case	Storage Method
Non-schema mode	AD installations that have not migrated to the latest AD schema; administrators are reluctant or unwilling to change the schema. AD installations that use Windows 2000 domain controllers.	Likewise uses the <code>description</code> and the <code>keywords</code> attributes of <code>container</code> and <code>serviceConnectionPoint</code> objects to store Unix and Linux information for users, groups, and cells.
Schema mode	AD installations that comply with RFC 2307, such as Windows Server 2003 R2 or later. Or, administrators who are willing to change the schema to RFC 2307 and to raise the forest functional level to Windows Server 2003. AD installations that do not use Windows 2000 domain controllers. (You cannot raise the forest functional level of a Windows 2000 domain controller to that of Windows Server 2003; see http://support.microsoft.com/kb/322692 .)	Likewise uses the Unix- and Linux-specific attributes that are built into the RFC 2307 schema as well as the <code>container</code> object and the <code>keywords</code> attribute.

Both schema mode and non-schema mode provide a method for storing Unix and Linux information in Active Directory -- including UIDs and GIDs -- so that Likewise can map SIDs to UIDs and GIDs and vice versa. The mapping lets Likewise use an Active Directory user account to grant a user access to a Unix or Linux resource that is governed by a UID-GID scheme. When an AD user logs on a Unix

or Linux computer, the Likewise agent communicates with the Active Directory Domain Controller through standard LDAP protocols to obtain the following authorization data:

- UID
- Primary GID
- Secondary GIDs
- Home directory
- Login shell

Likewise uses this information to control the user's access to Unix and Linux resources.

The advantages and disadvantages of the schema modes are further discussed in the next section.

2.3.3. Pros and Cons of the Schema Modes

Likewise has two operating modes: schema mode and non-schema mode. There are advantages and disadvantages to both. The mode that you choose depends on your unique situation.

The optimal setup is schema mode with a default cell. Schema mode is preferred because lookups use attributes indexed in Active Directory, reducing network traffic and the processing load on domain controllers. Forests that are in Windows 2008 Forest Mode are already in Likewise schema mode. Forests in Windows 2003 Forest Mode with Windows 2003 R2 domain controllers can be moved to schema mode without extending the AD schema.

Because of the performance benefits of schema mode, you should avoid non-schema mode whenever you can. Non-schema mode, however, remains fully supported by Likewise.

Non-Schema Mode: Advantages and Disadvantages

The benefit of using non-schema mode is that it does not require you to upgrade the Active Directory schema. This may be preferable in an environment that places special controls around how Active Directory is managed. This mode is sufficient for use in small deployments, such as a single server or workstation that will be added to a single domain controller.

Advantages of non-schema mode include the following:

- Supports Windows 2000 domain controllers.
- Does not change the current schema. Likewise objects are contained in their own `serviceConnectionPoints`.
- Does not affect settings in a global manner.
- Does not affect other Unix schema extensions that may be in place.

A disadvantage of non-schema mode is that if you're using third-party software to manipulate AD objects, it will not recognize how Likewise stores data in Active Directory.

Schema Mode: Advantages and Disadvantages

Schema mode raises the version of the schema to match that of Windows Server 2003 R2 -- the schema extensions are added to comply with the standard defined in RFC 2307. These changes are prescribed by Microsoft and are built into Windows Server 2003 R2.

Advantages of schema mode include the following:

- Uses indexed searching, which makes lookups faster when there are a large number of UID-GID mappings to process.
- Improves compatibility with other tools.
- Enhances ADSI scripting capabilities.

Drawbacks of schema mode include the following:

- Significantly modifies the Active Directory schema in cases where it must be upgraded to RFC 2307. If you are already using the RFC 2307-compliant schema, the schema adds the `uid`, `uidNumber`, and `gidNumber` attributes to the global catalog, which could marginally increase the size of the catalog and might marginally affect performance in a large Active Directory implementation.
- Requires you to raise the forest functional level to Windows Server 2003.

Important: If you upgrade your schema to RFC 2307, you cannot roll back the changes.

- Cannot use schema mode if you have Windows 2000 domain controllers; you must first upgrade them to Windows Server 2003.

There is background information about functional levels at <http://technet.microsoft.com/en-us/library/cc738038.aspx> and reference information about functional level features at <http://technet.microsoft.com/en-us/library/cc771132.aspx>.

2.4. About Likewise Cells

A Likewise cell contains Unix settings for Active Directory users and groups so they can log on to Linux, Unix, and Mac OS X computers. For each user, the settings include a Unix user identifier (UID), the group identifier (GID) of the primary group, a home directory, and a shell.

When an Active Directory user logs on a Likewise client, Likewise searches Active Directory for the user's cell information. The search typically begins at the node where the computer is joined and moves up the directory's structure until a cell is found. To operate properly, the Likewise Enterprise agent must find a cell.

There are two types of cells:

- A cell associated with the domain. Such a cell is known as a *default cell*.
- A cell associated with an organizational unit (OU). Such a cell is sometimes referred to as a *named cell*. Since Likewise Enterprise applies group policies to organizational units, associating cells with OUs is a natural way to organize computers and users.

In a named cell, Likewise searches for a user or group's attributes in the cell associated with the computer.

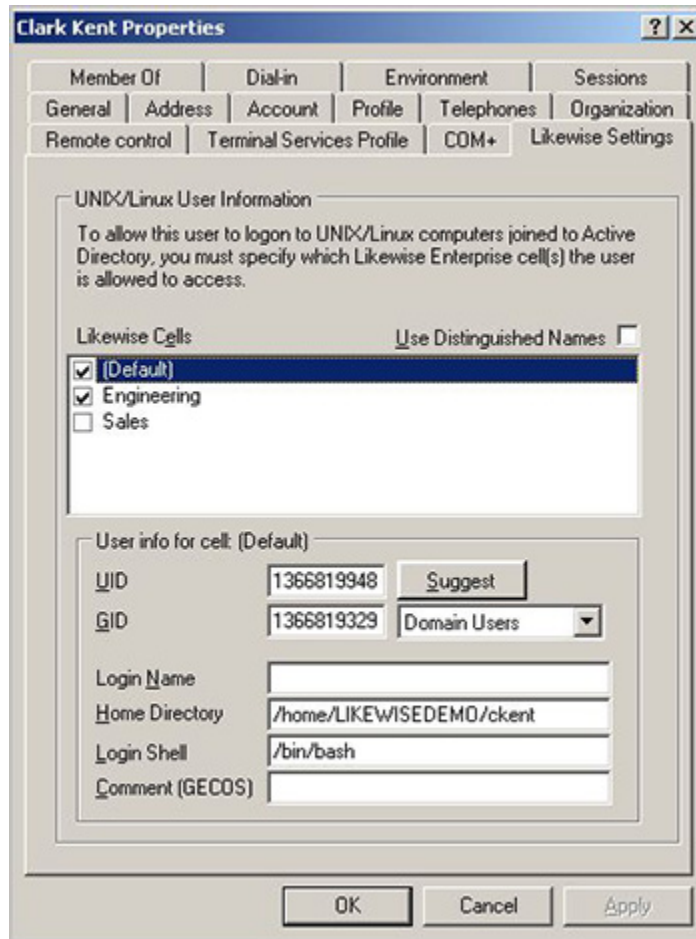
A default cell is processed in a different way. With a default cell, Likewise searches for a user or group's attributes in the default cell of the domain where the user or group resides. As a result, in a two-domain topology that, for example, uses a separate domain for users and a separate domain for computers, there must be two default cells:

- A default cell in the domain where user and group objects reside.

- A default cell in the domain where computers objects are joined.

In a multi-domain topology, then, you must create a default cell *in each domain*.

Cells can also map a user to different UIDs and GIDs for different computers. In the following screen shot, the example user, Clark Kent, is allowed to access the computers that are in the selected cells:



Creating Cells

Likewise modifies the Active Directory User and Computers MMC snap-in so that you can create a cell associated with an OU and then use the cell to manage UID-GID numbers. To create a cell, use Active Directory Users and Computers to select the OU you want, click the Likewise Settings tab of the object's Properties sheet, and then select the check box to associate a cell with the OU. You can then assign UID-GID numbers manually or let Likewise do it for you.

When a Likewise client connects to Active Directory, the Likewise agent determines the OU of which the computer is a member and checks whether a cell is associated with it. If a cell is not associated with the OU, the Likewise agent on the Unix computer searches the parent and grandparent OUs until it finds an OU that has a cell associated with it. If an OU with an associated cell is not found, the agent uses the default cell to map its username to UID and GID information.

Important: Before you associate a cell with an organizational unit, make sure you have chosen the schema mode that you want. You cannot change the schema mode after you create a cell, including a default cell.

For instructions on how to make a cell, see [Create a Cell](#).

The Default Cell

Likewise lets you define a default cell. It 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.

When you use a default cell, Likewise searches across all your trusted domains for Unix and Linux information directly on the user objects. In schema mode, Likewise searches all trusted global catalogs, which are shared across a forest -- Likewise queries the trusted global catalogs as a set. In non-schema mode, Likewise queries each trusted domain individually.

The default cell does not contain Unix or Linux data. It is a method for managing client Linux and Unix users and computers. When a client finds the default cell object, it searches all trusted domains and forests, enterprise wide, for Linux and Unix information, even if the default cell object has not been created in those trusted domains and forests.

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 group policies associated with the OU apply to the Linux and Unix computer, but user UID-GID mappings follow the policy of the nearest parent cell, or the default cell. Likewise does not require you to have a default cell.

Linking Cells

To provide a mechanism for inheritance and to ease system management, Likewise can link cells. Linking specifies that users and groups in a linked cell can access resources in the target cell. For example, if your default cell contains 100 system administrators and you want those administrators to have access to another cell, called Engineering, you do not need to provision those users in the Engineering cell. You can simply link the Engineering cell to the default cell, and then the Engineering cell will inherit the settings of the default cell. Then, to make management easier, in the Engineering cell you can just specify the mapping information that deviates from the default cell.

Although you can use linking to in effect set up a hierarchy of cells, linking is not transitive. If, for example, a cell called Civil is linked to the Engineering cell and the Engineering cell is linked to the default cell, the Civil cell does not inherit the settings of the default cell.

When you link to multiple cells, the order that you set is important because it controls the search order. Suppose that Kathy, a system administrator, has a UID of 100,000 set in the default cell and a UID of 150,000 set in the Engineering cell. In the Civil cell, however, he must use his UID from the Engineering cell to log on Civil computers. If the Civil cell is linked to both the default cell and Engineering cell, the order becomes important. If Engineering does not precede the default cell in the search order, Kathy will be assigned the wrong UID and will be unable to log on computers in the Civil cell.

For instructions on how to link cells, see [Link Cells](#).

Cell Manager

Cell Manager is a Likewise MMC snap-in for managing cells associated with Active Directory organizational units. With Cell Manager, you can view all your cells in one place. Cell Manager complements Active Directory Users and Computers by letting you delegate management of a cell --

that is, give others the ability to add users and groups to a cell. Cell Manager is automatically installed when you install the Likewise Console. For more information, see [Manage Cells](#).

Migrating NIS Domains

If use Likewise to migrate all your Unix and Linux users to Active Directory, in most cases you will assign these users a UID and GID that is consistent across all the Unix and Linux computers that are joined to Active Directory -- a simple approach that reduces administrative overhead.

In cases when multiple NIS domains are in use and you want to eliminate these domains over time and migrate all users and computers to Active Directory, mapping an Active Directory user to a single UID and GID might be too difficult. When multiple NIS domains are in place, a user typically has different UID- GID maps in each NIS domain. With Likewise, you can eliminate these NIS domains but retain the different NIS mapping information in Active Directory because Likewise lets you use a cell to map a user to different UIDs and GIDs depending on the Unix or Linux computer that they are accessing.

To move to Active Directory when you have multiple NIS servers, you can create an OU (or choose an existing OU) and join to the OU all the Unix computers that are connected to the NIS server. You can then use cells to represent users' UID-GID mapping from the previous identity management system.

Using Multiple Cells

If you have multiple Unix and Linux hosts but are not using a centralized scheme to manage UIDs and GIDs, it is likely that each host has unique UID-GID mappings. You may also have more than one centralized IMS, such as multiple NIS domains. You can use multiple cells to represent the UID-GID associations that the NIS domain provided, allowing those Unix and Linux users to continue to use their existing UID-GID information while using Active Directory credentials.

When using multiple cells, it is useful to identify what Unix and Linux objects the cell will represent, such as the following:

- Individual Unix, Linux, or Mac OS X computers
- A single NIS domain
- Multiple NIS domains (which requires multiple cells)

Migration Tool

The Likewise Console provides a migration tool to import Linux, Unix, and Mac OS X passwd and group files -- typically `/etc/passwd` and `/etc/group` -- and automatically map their UIDs and GIDs to users and groups defined in Active Directory. The migration tool can also generate a Windows automation script to associate the Unix and Linux UIDs and GIDs with Active Directory users and groups. For more information, see [Migrate Users to Active Directory](#).

Orphaned Objects Tool

The Likewise console provides a tool for finding and removing orphaned objects. An orphaned object is a linked object, such as a Unix or Linux user ID or group ID, that remain in a cell after you delete a group or user's security identifier, or SID, from an Active Directory domain. Removing orphaned objects from Active Directory can clean up manually assigned user IDs and improve search speed. For more information, see [Find Orphaned Objects](#).

2.5. Best Practices for Modes, Cells, Group Policies, and User Rights

In general, the optimal setup is schema mode with a default cell. Schema mode is strongly preferred because lookups use attributes indexed in Active Directory, reducing network traffic and the processing load on domain controllers. When Unix identity information does not overlap, you should use schema mode with a default cell. If you require multiple cells to keep Unix identities from coming into conflict, use schema mode with named cells. Try to minimize the number of named cells you use, preferably no more than four.

Forests that are in Windows 2008 Forest Mode are already in Likewise schema mode. Forests in Windows 2003 Forest Mode with Windows 2003 R2 domain controllers can be moved to schema mode without extending the AD schema.

Because of the performance benefits of schema mode, you should avoid non-schema mode whenever you can. Non-schema mode, however, remains fully supported by Likewise.

Migrating from a non-schema default cell to a default cell in schema mode requires more work and is riskier than any other kind of cell migration. So, to ease migration in the future and to improve support, non-schema mode cells should be created only as named cells -- that is, cells associated with organizational units.

Although you could use cells to limit access to a computer, doing so goes against the design of Active Directory. It is recommended that you control access and authorize users with methods other than cells. Instead, you can control access by using the `RequireMembershipOf` setting in the registry or the group policy, named Allow Logon Rights, that manages the `RequireMembershipOf` setting.

Likewise recommends the following additional best practices:

- You should either pre-stage Unix computer accounts or you should delegate to Unix system administrators control of the OU to which the Unix computers will be joined. For information on how to delegate control, see [Best Practices for Delegating Active Directory Administration](#). For information on how to pre-create computer accounts, see [Domain Users Cannot Join Workstation or Server to a Domain](#).
- You should follow the same best practices for applying group policy objects that Microsoft recommends at [TechNet](#).
- To simplify troubleshooting across multiple operating systems, you should avoid heavy use of Likewise's target platform filter for group policies.

There are additional best practices for managing the security of the Likewise database; see the chapter on installing and configuring the Likewise database.

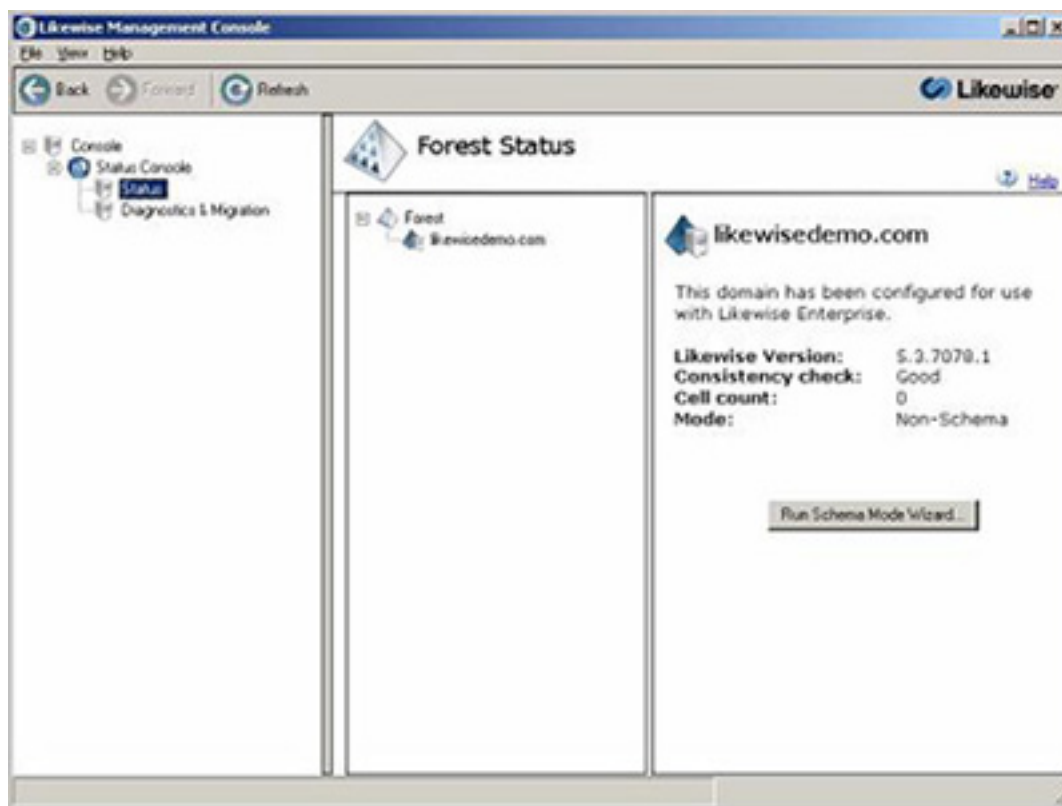
Finally, more best practices are listed in Likewise professional services' [Best Practices Guide](#).

Chapter 3. Installing and Using the Console

3.1. About the Likewise Console

You install the Likewise Management Console on a Windows administrative workstation connected to a domain controller to administer Linux, Unix, and Mac OS X computers in Active Directory. When you install the console, it adds extension tabs to the properties sheets of most objects in Active Directory Users and Computers (ADUC). The extension tabs, named Likewise Settings and Likewise NIS Maps, let you manage Unix settings in ADUC. In addition, the Likewise group policies are added to the Group Policy Management Console and the Group Policy Object Editor.

After you install the console, you can use Active Directory Users and Computers to manage Unix and Linux users and groups, including their UID and GID information, their default logon shell, and their default home directory. You can also use the Group Policy Object Editor to create and edit Linux- and Unix-specific group policies, and you can use the Group Policy Management Console to view information about Likewise group policies.



You can use the console to perform the following tasks:

- Run multiple instances of the console and point them at different domains.
- Run the console with a different user account.
- Upgrade your Active Directory schema.

- Obtain status information about your Active Directory forests and domains.
- Migrate Unix and Linux users and groups by importing `passwd` and `group` files and mapping the information to users and groups in Active Directory.
- Remove orphaned objects.
- Generate reports about users, groups, and computers.

3.2. Requirements

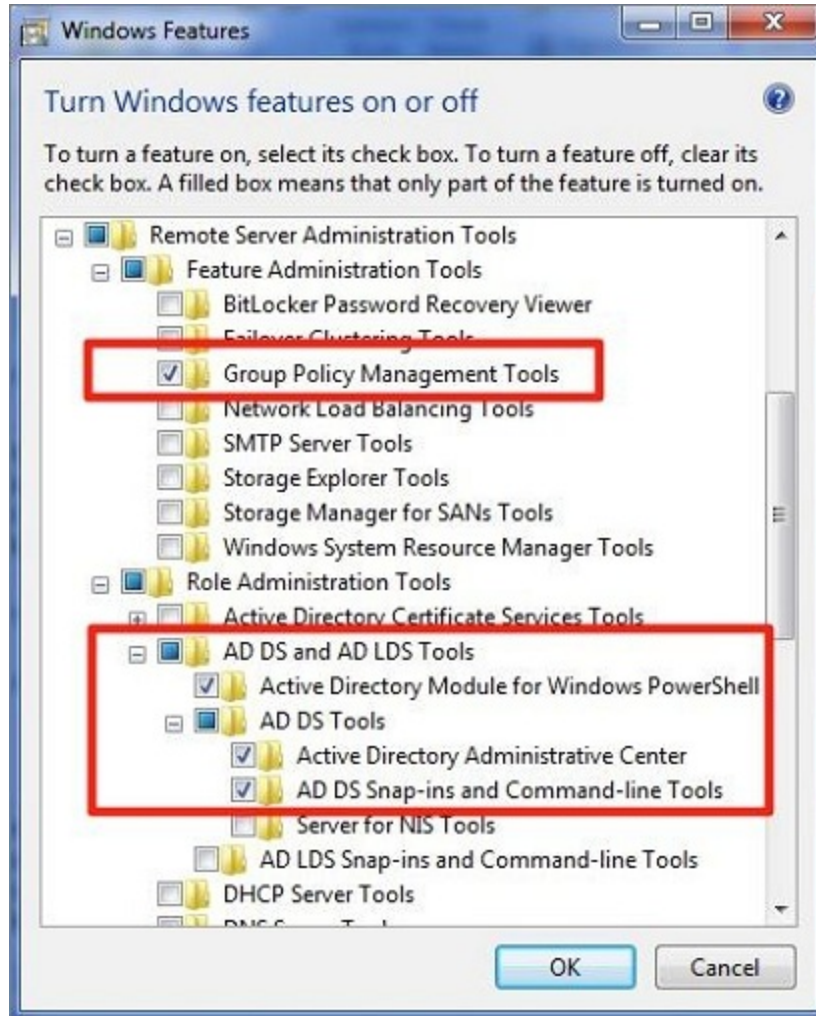
This section lists the requirements to use Likewise Enterprise with Active Directory. Requirements for the Likewise agent -- the software that runs on the Linux, Unix, and Mac OS X computers that you want to connect to AD -- are listed in About Installing the Agent.

You must have at least the following components:

1. An Active Directory domain controller.
2. A Windows administrative workstation that is running ADUC and is connected to your Active Directory domain controller.

Because Likewise enhances ADUC, GPOE, and GPMC to support Unix computers, you must make sure that the Microsoft management tools for Active Directory are installed **before** you install Likewise. The Microsoft management tools vary by Windows version, but typically include the Admin Pack for Windows XP and Windows Vista and the Remote Server Administration Tools (RSAT) for Windows 7 and Windows Server 2008 R2.

With Windows 7 and Windows 2008 R2, you must turn on the following features of the Remote Server Administration Tools by going to the Control Panel, selecting Programs, and then selecting Turn Windows features on or off: Group Policy Administration Tools, Active Directory Module for Windows PowerShell, Active Directory Administrative Center, AD DS Snap-ins and Command-Line Tools. For more information, see the description of the Remote Server Administration Tools for Windows 7 and your Microsoft Windows documentation.



3. One or more Unix or Linux computers running an operating system that Likewise supports, such as versions of Mac OS X, Red Hat, SUSE Linux, Fedora, CentOS, Debian, Sun Solaris, IBM AIX, HP-UX, and Ubuntu. For a complete list of supported platforms, see the list at www.Likewise.com.

Administrator Privileges

- Root access or sudo permission on the Unix, Linux, and Mac OS X computers that you want to join to the domain.
- Active Directory credentials that allow you to add computers to an Active Directory domain -- for example, membership in the Domain Administrators security group or the Enterprise Administrators security group.

Active Directory Requirements

- Windows 2003 SP1 or R2 Standard and Enterprise
- Windows Server 2008
- Windows 2000 SP4 Server

Windows Requirements for the Console

- Windows 2003 SP1 or R2 (or later)
- Windows XP Professional, SP3 -- requires the Windows Admin Pack

Note: The 64-bit version of Windows Server 2003 and the 64-bit version of Windows XP are not supported.

- Windows Server 2008 SP1 or R2
- Windows 7 Professional
- Windows Vista SP1
- Microsoft .NET 1.1 Framework
- Microsoft .NET 2.0 Framework
- MSXML 6.0 Parser (for displaying reports in the GPMC)
- MMC 3.0 Update

Note: You cannot install MMC 3.0 on a Windows 2000 computer, and thus you cannot install the Likewise Console on a Windows 2000 computer.

- 50 MB of free space

Requirements to Run Likewise in Schema Mode

- Active Directory installations that comply with RFC 2307, such as Windows Server 2003 R2.
- Domain and forest functional levels have been raised to Windows Server 2003 or higher.
- No Windows 2000 domain controllers (raising the forest functional level to Windows Server 2003 excludes Windows 2000 domain controllers from the domain).

For more information, see About Schema Mode and Non-Schema Mode and Pros and Cons of the Schema Modes.

Remediation Requirements for Active Directory

Networking

The subnets with your Linux, Unix, and Mac computers must be added to Active Directory sites before joining the computers to Active Directory so that the Likewise agent can detect the optimal domain controller and global catalog.

Replication

Make sure your AD replication system is up to date and functioning properly by using the following diagnostic tools from <http://www.microsoft.com/download> to test replication. For instructions, see the Microsoft documentation for each tool.

1. **DCDiag.** Part of Microsoft's support tools for Windows Server 2003, dcdiag.exe should be run with the /v /c /e switches to test all the domain controllers in all your sites.
2. **FRSDiag.** Use frsdiag.exe tool, available from the Microsoft Resource Kit tools, to check the File Replication Service (FRS).

In addition, the following tools can help you review and troubleshoot FRS problems.

Sonar. Optionally use it to perform a quick review of FRS status.

Ultrasound. Optionally use it to monitor and troubleshoot FRS.

ReplMon. Included in the Microsoft Resource Kit Tools, use it to investigate replication problems across links where DCDiag showed failures.

3.3. Install the Likewise Console

You install the Likewise Management Console on a Windows administrative workstation that can connect to your Active Directory domain controller. It is recommended that you do not install the console on a domain controller. (For instructions on how to use the Likewise metainstaller to install the console and other components, see the Likewise Evaluation Guide.)

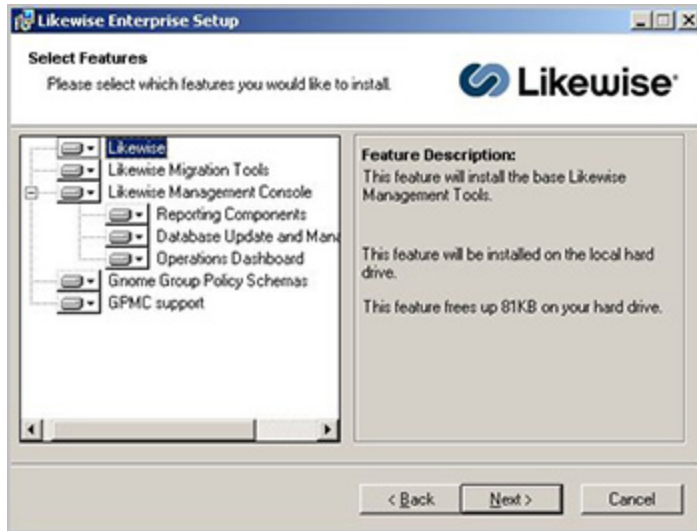
In addition to the console, the Likewise Enterprise installer for Windows includes several components: the Likewise migration tools, Gnome group policy schemas, and GPMC support.

Important Note About Upgrading: To upgrade to the latest version of Likewise Enterprise on your Windows administrative workstation, first uninstall the existing version. Then, before installing the latest version of Likewise Enterprise, install the latest version of the Microsoft Group Policy Management Console and run Windows update to make sure your workstation has the latest XML patches.

1. Verify that your administrative workstation is running a version of Windows that Likewise supports (see the list in the section on requirements) and has 50 MB of free disk space.
2. Because Likewise enhances ADUC, GPOE, and GPMC to support Unix computers, make sure that the Microsoft management tools for Active Directory are installed **before** you install the console.

The Microsoft management tools vary by Windows version, but typically include the AdminPak for Windows XP and Windows Vista and the Remote Server Administration Tools (RSAT) for Windows 7.

3. Locate `LikewiseEnterprise.exe` on your installation media. (The file name might also contain a version and build number.) It is a standard MSI installer. Copy it to the desktop of your Windows administrative workstation.
4. Execute `LikewiseEnterprise.exe` with an Active Directory account that has privileges to modify objects and child objects in Active Directory -- for example, an account that is a member of the Domain Administrators or the Enterprise Administrators security group.
5. Follow the instructions in the installation wizard.
6. Select the Likewise features you want to install:




To	Install
Install the Likewise extension tabs for ADUC and other base tools and code that Likewise uses to manage Unix information in Active Directory. This component is required.	Likewise
Install the Likewise migration tools, including the tool to import Linux, Unix, and Mac OS X passwd and group files and the tool to upgrade a previous version of Likewise to the current version.	Likewise Migration Tools
Install the Likewise Management Console. It runs on a Windows administrative workstation that connects to an Active Directory domain controller to help you manage Linux and Unix computers in Active Directory. The console lets you view status and start several Likewise tools, such as Cell Manager. The console also serves as an extensible service for running several other Likewise management applications, called snap-ins or plug-ins. A plug-in named Provisioning Management is included when you install the Likewise Management Console and it is loaded by default when you run the console. The other plug-ins include Enterprise Data Management, the Operations Dashboard, and Audit and Access Reporting, all three of which are new components provided as a technology preview.	Likewise Management Console and its components
Install the Gnome GConf group policy schemas. The schemas are used to apply user settings to Gnome desktops.	Gnome Group Policy Schemas

Install features that support managing and viewing Likewise group policies in the Microsoft Group Policy Management Console.	GPMC support
------------------------------------------------------------------------------------------------------------------------------	--------------

7. If you do not have MMC 3.0 installed, you are prompted to install it.
8. If you do not have .NET 2.0 installed, you are prompted to install it.

3.4. Start the Likewise Console

Before you can start the Likewise Management Console, it must be installed on your administrative desktop. Depending on the options chosen during installation, the console can be started in the following ways:

-  Double-click on the Likewise Management Console desktop shortcut.
- Click **Start**, point to **All Programs**, click **Likewise**, and then click **Likewise Management Console**.
- At the command prompt, execute the following commands:

```
cd %ProgramFiles%\Likewise\Enterprise\  
  
iconsole.lmc
```

Tip: You can run multiple instances of the Likewise Console and point them at different domains.

The Likewise Console page is the first screen that is displayed after you start the console. From the page, you can navigate to all other pages in the console, including the Status page. You can also start Active Directory Users and Computers (ADUC), Cell Manager, and the Migration tool.

The Forest Status page displays the following information for the selected Active Directory forest. After you start the console, it may take a few moments to retrieve information about your domains.

Likewise Version: The Likewise version and build number. Technical support personnel may ask you for this information when you contact them for assistance.

Consistency check: Indicates whether Active Directory has been properly prepared for the current operating mode. Typically this status indicator reads as `Good`.

Cell count: Displays the number of cells that are associated with organizational units in the selected domain, including the default cell.

Mode: Either schema or non-schema. Schema indicates that the selected forest is using the RFC 2307-compliant schema. Non-schema indicates that it is not.

3.5. Connect to a Domain

If Likewise detects more than one Active Directory forest, it displays them on the Likewise Console's Forest Status page. You can connect to a forest by double-clicking the forest name.

You can connect to another domain as follows:

1. In the Likewise Management Console tree, right-click the **Provisioning Management** node, and then click **Connect to Domain**.
2. In the **Fully Qualified Domain Name** box, enter the FQDN of the domain that you want to connect to.
3. In the **NT4-style Domain Name** box, enter the short name of the domain.
4. In the **Username** and **Password** boxes, enter the credentials of an Active Directory administrator. It is recommended that you use the AD Enterprise Administrators security group account.

3.6. Run the Schema Mode Wizard

After you install the Likewise Management Console for the first time, you can run the Schema Mode Wizard to upgrade your Active Directory schema to that of Microsoft Windows Server 2003 R2, which provides support for RFC 2307. The **Run Schema Mode Wizard** button appears only if you have not run the Schema Mode Wizard and if you have not created any Likewise cells. In non-schema mode, the button will reappear after you remove all your Likewise cells.

Likewise has two operating modes: schema mode and non-schema mode. Non-schema mode stores Linux and Unix data without requiring RFC 2307 object classes and attributes and without modifying the existing schema. Non-schema mode is Likewise's default mode, and you do not need to run the schema mode wizard to use it.

Schema mode takes advantage of the Unix- and Linux-specific RFC 2307 object classes and attributes, namely the `posixAccount` and `posixGroup` object classes. The wizard upgrades your schema to RFC 2307. If you are already using Windows Server 2003 R2, running the wizard indexes frequently searched attributes in the Active Directory global catalog.

Before you decide which schema mode is right for your environment, see [About Schema Mode and Non-Schema Mode](#) and [Pros and Cons of the Schema Modes](#).

Important: You cannot roll back the changes that the schema mode wizard makes to the Active Directory schema. Back up Active Directory before you run the wizard.

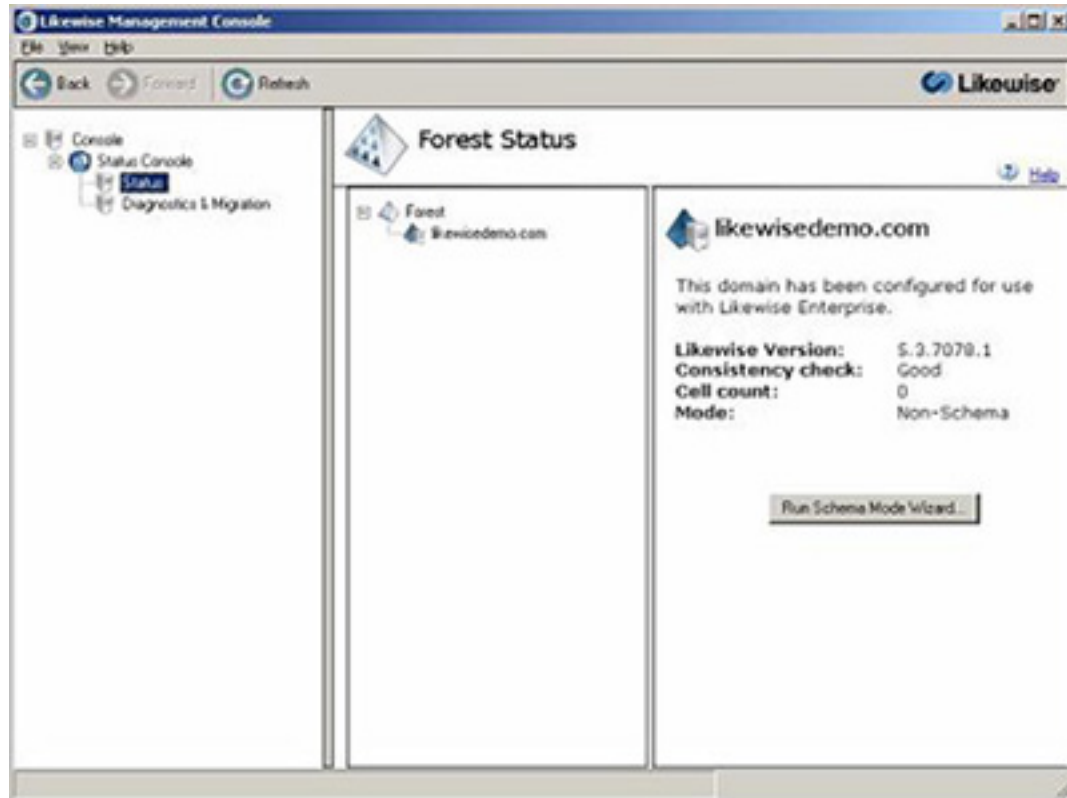
Run the Schema Mode Wizard

To raise the forest functional level and to upgrade the schema, you must be a member of the Enterprise Administrators security group or the Schema Administrators security group for the forest.

1. On your Windows administrative workstation, use Active Directory Domains and Trusts to raise the forest functional level of your Active Directory forest to `Windows 2003`. To raise the forest functional level to `Windows 2003`, you must first raise the domain functional level for each domain in your forest to `Windows 2003`. For more information, see [Active Directory Domains and Trusts Help](#).

Note: Raising the forest functional level to Windows Server 2003 will exclude Windows 2000 domain controllers from the domain.

2. In the Likewise Management Console tree, click **Status**.
3. In the left pane, click the forest for which you want to upgrade the schema.
4. Click **Run Schema Mode Wizard**:



Note: The **Run Schema Mode Wizard** button appears only if the forest has not been configured for Likewise and if you have not created any Likewise cells.

5. Follow the instructions in the wizard.

3.7. Replication in a Large Forest or in Multiple Domains

When you set up Likewise in an environment with a large forest or multiple domains, it may take some time for the Likewise objects and the schema update to replicate to the rest of the domain.

Replication must complete before the domain and its child domains are fully enabled for Likewise. You will be unable to connect to a child domain until replication finishes.

3.8. Upgrade the Schema of a Forest

One or more domains that share a common schema and global catalog are known as a forest. With Likewise, you can upgrade the schema of a forest. To do so, you must be a member of the Enterprise Administrators security group or the Schema Administrators security group for the forest.

Important: To apply the schema extensions only to a single forest, select only the forest that you want.

1. In the Likewise Management Console, click the **Status** tab.
2. In the **Forest** tree, select the forest, domain, or child domain that you want to configure.

3. In the right pane, click **Run Schema Mode Wizard**.

Note: The **Run Schema Mode Wizard** button appears only if the forest has not been configured for Likewise.

4. Follow the instructions in the wizard. For more information, see [Run the Schema Mode Wizard](#).

3.9. Add a Plug-In

The console includes several plug-ins: Access and Audit Reporting, Enterprise Database Management, and the Operations Dashboard.

1. In the console, on the **File** menu, click **Add/Remove Plug-in**.
2. Click **Add**.
3. Click the plug-in that you want, and then click **Add**.
4. Click **Close**, and then click **OK**.

Chapter 4. Working with Cells

4.1. Make a Cell and Associate it with an OU or a Domain

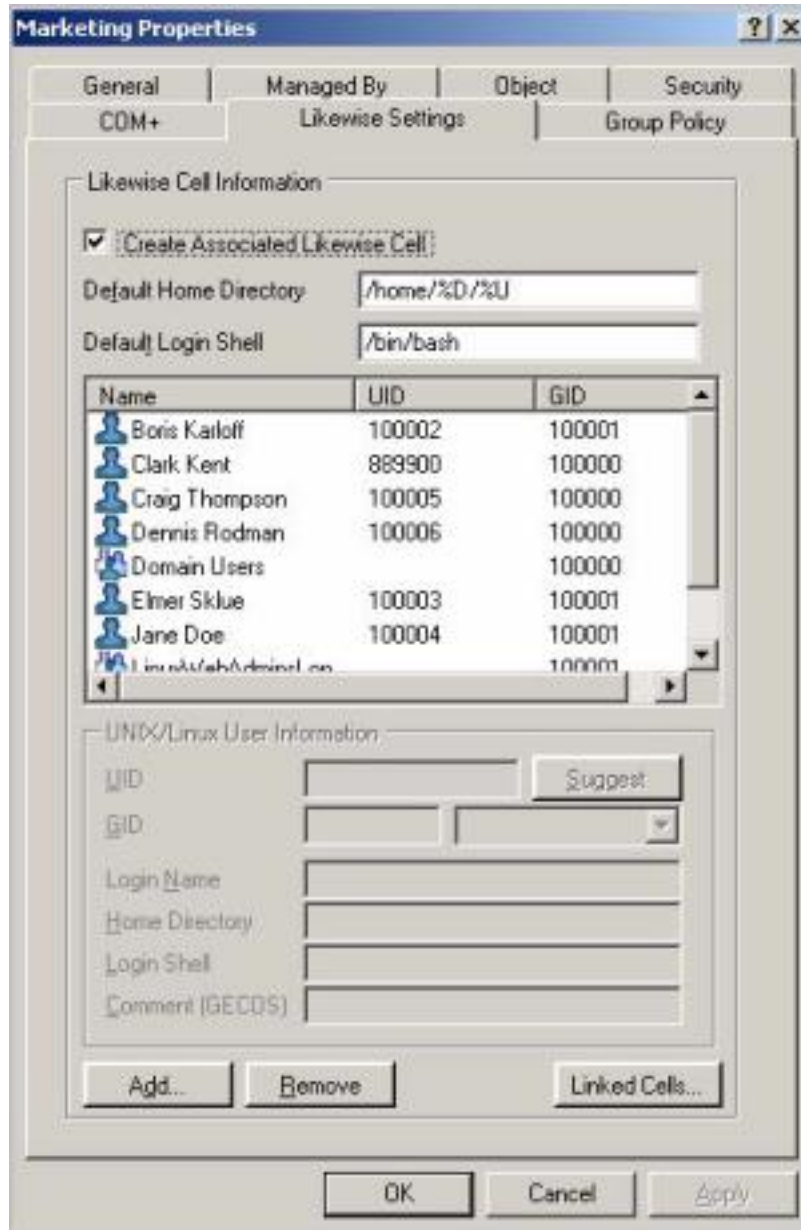
To create a Likewise cell and associate it with a domain or an organizational unit (OU), you must have Active Directory administrative privileges that allow you to create container objects within an OU or a domain. To associate a cell with an OU, for example, you must be a member of the Domain Administrators security group, or you must have been delegated control to create container objects within the OU.

Important: Before you associate a cell with an organizational unit, make sure you have chosen the schema mode that you want. You cannot easily change the schema mode after you create a cell, including a default cell.

1. On your Windows administrative workstation, start Active Directory Users and Computers.
2. In the console tree, right-click the OU or the domain for which you want to create a cell, click **Properties**, and then click the **Likewise Settings** tab.

Important: Do not create a cell in the built-in OU named `Domain Controllers`.

3. Under **Likewise Cell Information**, select the **Create Associated Likewise Cell** check box, and then click **OK**.



You can now associate users with the cell.

4.1.1. Moving a Computer to Another Cell

When you move a computer from one cell to another, you must do the following if you want the cell information to be updated immediately on the client:

- Clear the authentication cache for user and group membership: `lsass-adcache.db`. For instructions, see [Clear the Authentication Cache](#).
- Restart the Likewise authentication daemon by running this command as root: `/opt/likewise/bin/lwsm restart lsass`

- Force the computer to refresh its group policies by running this command as root: `/opt/likewise/bin/gporefresh`

4.2. Create a Default Cell

Likewise gives you the option of defining a default cell. It 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. Likewise Enterprise does not require a default cell.

A Linux or Unix computer can be a member of an OU that does not have a cell associated with it. In such cases, the group policies associated with the OU apply to the Linux and Unix computer, but user UID-GID mappings follow the policy of the nearest parent cell, or the default cell.

To create a default cell, in the Active Directory Users and Computers console tree, right-click the name of your domain, click **Properties**, click the **Likewise Settings** tab, and then click **Create Associated Likewise Cell**.

4.2.1. Use Pre-Existing RFC 2307 Data

To recognize and use pre-existing Unix data that is stored in Active Directory with RFC 2307 attributes, make sure Likewise is in schema mode and then create a default cell.

4.3. Associate a User with One or More Cells

In Active Directory Users and Computers, you can associate a user with one or more Likewise cells to give the user access to the Linux, Unix, and Mac OS X computers that are members of each cell.

Note: To associate a user with a cell, you must log on with sufficient administrative privileges -- for example, as a member of the Domain Administrators group.

1. Start Active Directory Users and Computers.
2. In the console tree, click **Users**.
3. In the details pane, right-click the user that you want, and then click **Properties**.
4. Click the **Likewise Settings** tab.
5. Under **Likewise Cells**, select the check box for the cell that you want to associate the user with. You can associate the user with multiple cells by selecting the check boxes for the cells that you want.

Under **User info for cell**, a default GID value, typically 100000, is automatically populated in the **GID** box.

Note: The user's settings can vary by cell.

6. To set the UID, click **Suggest**, or type a value in the **UID** box.

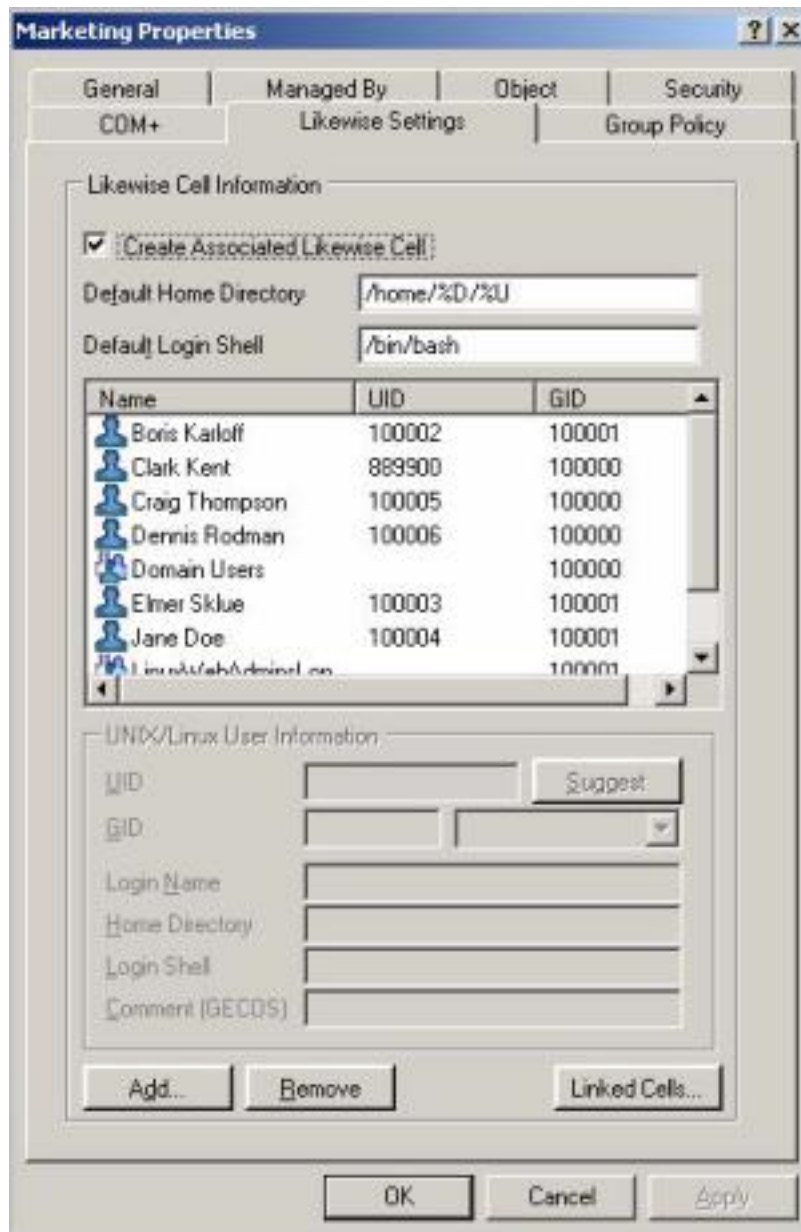
See Also

[Assign a Group ID](#)

4.4. Add a Group to a Cell

You can add an Active Directory group to a cell after you have associated a cell with an organizational unit (OU).

1. On your Windows administrative workstation, start Active Directory Users and Computers.
2. In the console tree, right-click the OU with an associated cell to which you want to add a group, click **Properties**, and then click the **Likewise Settings** tab:



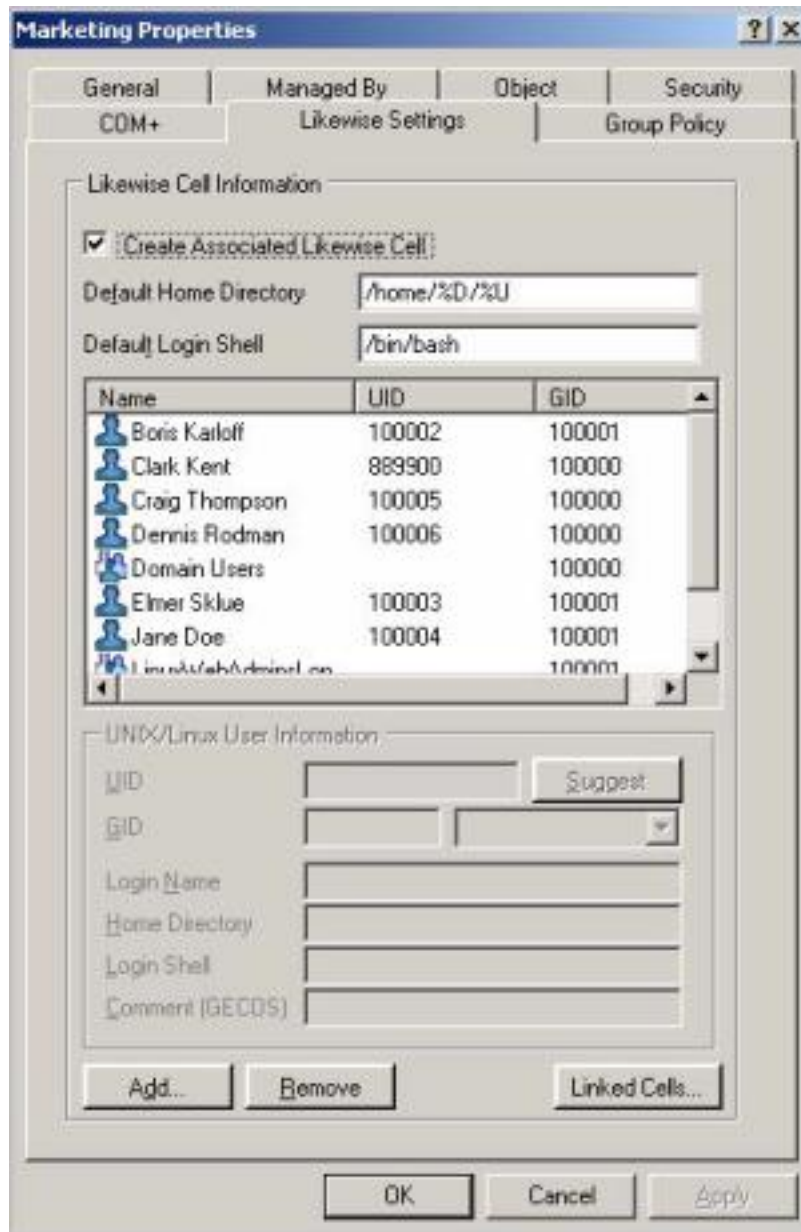
3. Click **Add**, select the group that you want to add, and then click **OK**.

4.5. Add a User to a Cell

You can add an Active Directory user to a cell after you have associated a cell with an organizational unit (OU).

1. On your Windows administrative workstation, start Active Directory Users and Computers.

- In the console tree, right-click the OU with an associated cell to which you want to add a user, click **Properties**, and then click the **Likewise Settings** tab:

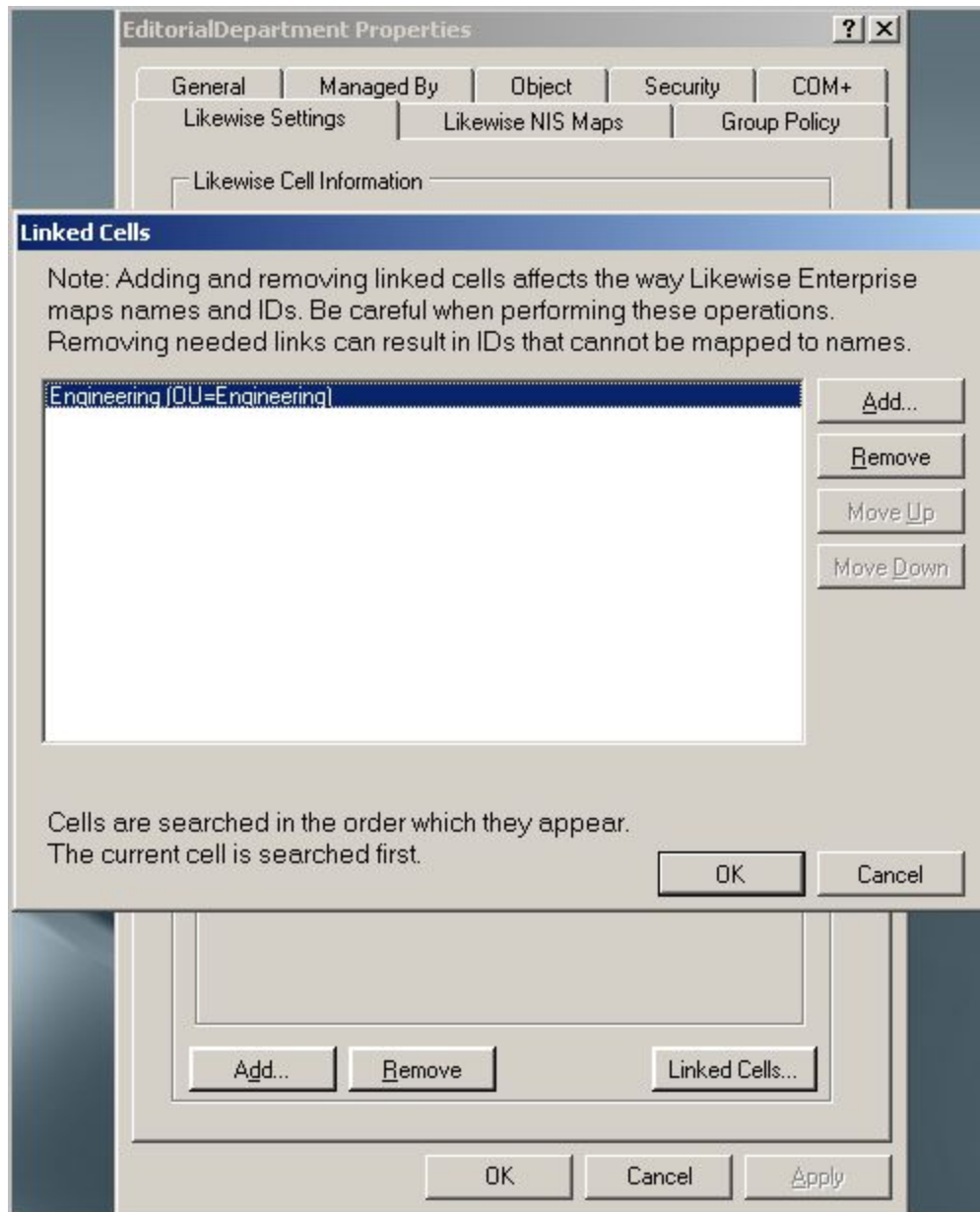


- Click **Add**, locate and select the user that you want to add, and then click **OK**.

4.6. Link Cells

Linking specifies that the computers in the current cell can be accessed by the users in the cell that you link to (the linked cell).

In the scenario shown in the screenshot below, the current cell is `EditorialDepartment`. When you link to the `Engineering` cell from the `Likewise Settings` tab for `EditorialDepartment`, the users in `Engineering` can access the computers in `EditorialDepartment`.



The following example demonstrates how linking cells can be useful:

If your default cell contains 100 system administrators and you want those administrators to have access to the computers in another cell, called `Engineering`, you do not need to provision those users in the `Engineering` cell. You can simply link the `Engineering` cell to the default cell, and then the `Engineering` cell inherits the settings of the default cell. For more information on linking cells, see [About Cells](#).

1. On your administrative workstation, start Active Directory Users and Computers.
2. In the console tree, right-click the organizational unit that is associated with the cell you want to link to another cell, and then click **Properties**.
3. Click the **Likewise Settings** tab.
4. Click **Linked Cells**, click **Add**, click the cell that you want, and then click **OK**.

5. When you link to multiple cells, the order that you set is important because it controls the search order. The cells are searched in the order listed. Use **Move Up** or **Move Down** to set the order of the cells.

For an example of how the search order can be important, see About Cells.

6. Click **OK**.

4.7. Delegate Control to Create Container Objects

To associate a Likewise cell with an Active Directory organizational unit, an administrator must have permission to create `container` objects within the OU. A member of the Domain Administrators or Enterprise Administrators security group can delegate control of the OU to another administrator.

1. In Active Directory Users and Computers, in the console tree, right-click the OU for which you want to delegate permissions, and then click **Delegate Control**.
2. Click **Next**.
3. Click **Add**, find the user that you want, click **OK**, and then click **Next**.
4. Select **Create a custom task to delegate**, and then click **Next**.
5. Select **This folder, existing objects in this folder, and creation of new objects in this folder**, and then click **Next**.
6. Under **Permissions**, select the following, and then click **Next**:

- Read
- Write
- Create All Child Objects
- Delete All Child Objects
- Read All Properties
- Write All Properties



7. Click **Finish**.

Tip: For more information about delegating control, see *Delegating Administration in Active Directory Users and Computers Help*.

4.8. Administering Cells with Cell Manager

Cell Manager is a Likewise MMC snap-in for managing cells associated with Active Directory organizational units.

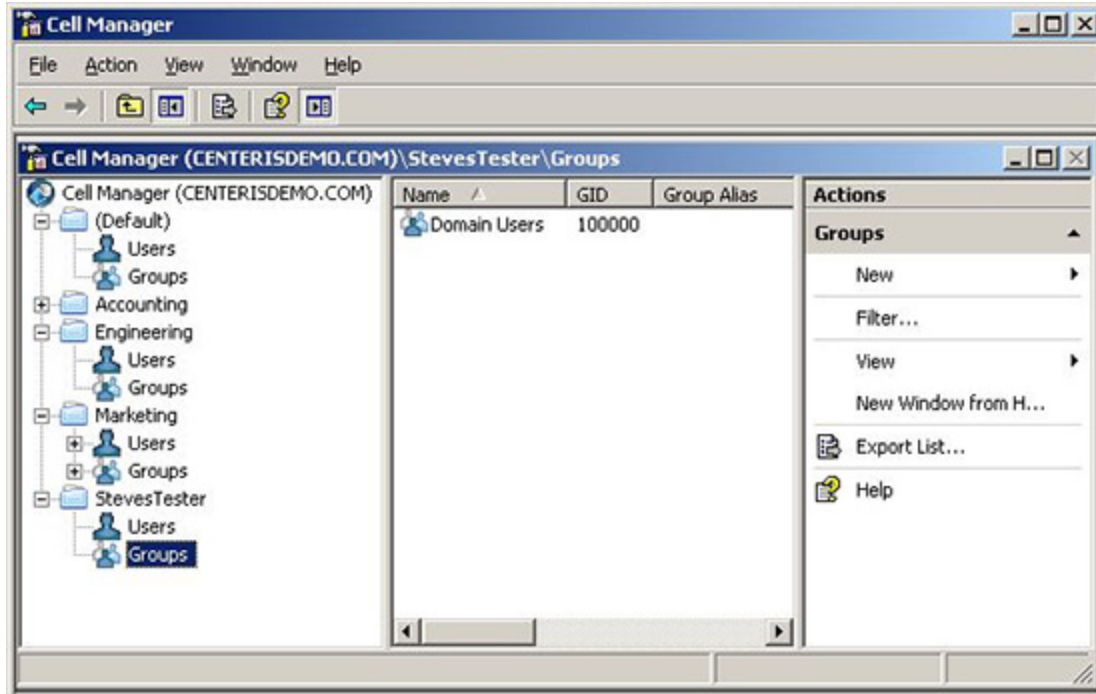
With Cell Manager, you can delegate management, change permissions for a cell, add cells, view cells, and associate cells with OUs to provide users and groups with Linux and Unix access. Cell Manager also lets you connect to another domain and filter cells to reduce clutter.

Cell Manager is automatically installed when you install the Likewise Console.

Start Cell Manager

1. In the Likewise Enterprise Console tree, click **Diagnostics & Migration**.
2. Under **Tasks**, click **Launch Cell Manager**.

Tip: To start Cell Manager from the Start menu, click **Start**, point to **All Programs**, click **Likewise**, and then click **Likewise Cell Manager**.



Delegate Management

You can use Cell Manager to create an access control list (ACL) that allows users or groups without administrative privileges to perform the administrative operations that you specify. For example, you can delegate management for the cell manager node to allow other users to create and delete cells. You can delegate management of a cell, a group, or a user.

1. In the Cell Manager console tree, right-click the folder of the cell that you want to delegate management for, and then click **Delegate Control**.
2. Follow the instructions in the Delegate Control Wizard.

Change Permissions of a Cell, Group, or User

1. In the Cell Manager console tree or in the details pane, right-click the object that you want to change permissions for, and then click **Properties**.

Tip: To select multiple users or groups, in the details pane, hold down CTRL and click the users or groups that you want to change.

2. Click **Permissions**.
3. Make the changes that you want.

Add a Cell

When you add a cell, you must attach it to an Organizational Unit in Active Directory.

1. In the Cell Manager console tree, right-click the top-level **Cell Manager** domain node, point to **New**, and then click **Cell**.

2. In the list of OUs, expand the tree and then click the OU to which you want to attach the cell.

Note: You cannot attach a cell to the top-level node (the domain).

3. In the **First available user ID** box, enter the number that you want. Keep in mind that the user ID range cannot overlap with the ID range of another cell.
4. In the **First available group ID** box, enter the number that you want. Keep in mind that the user ID range cannot overlap with the ID range of another cell.
5. In the **Home directory template** box, type the path for the home directory that you want to set for users in the cell -- for example, /home/%D/%U.

Important: When you set the home directory, you must use the default user name variable (%U). You may specify the default domain name by using the domain name variable (%D) but, unlike the user name variable, it is not required.

6. In the **Default login shell** box, type the path to the default shell that you want to use -- for example, /bin/sh.

Give a User Access to a Cell

When you give a user access to a cell by using Cell Manager, you can add the new user to the cell only with default attributes. You can change the attributes later by using Active Directory Users and Computers; see Specify a User's ID and Unix or Linux Settings.

1. In the Cell Manager console tree, right-click the cell that you want to give a user access to, point to **New**, and then click **User**.
2. Find and select the user that you want to add, and then click **OK**.

Give a Group Access to a Cell

When you give a group access to a cell by using Cell Manager, you can add the new group to the cell only with default attributes. You can change the attributes later by using Active Directory Users and Computers.

1. In the Cell Manager console tree, right-click the cell that you want to give a user access to, point to **New**, and then click **Group**.
2. Find and select the group that you want to add, and then click **OK**.

Filter Cells

You can use filtering to set the maximum number of cells to display and show only the cells that match a pattern.

1. In the Cell Manager console tree, right-click the top-level **Cell Manager** domain node, and then click **Filter**.
2. Set the filtering values that you want to use.

Connect to a Different Domain

Even though users and groups imported from a different domain appear in Cell Manager, you cannot modify their settings from outside their original domain. Instead, to modify the settings of a user or

group imported from another domain, use Cell Manager to connect to that domain and then make the changes that you want.

1. In the Cell Manager console tree, right-click the top-level **Cell Manager** domain node, and then click **Connect To Domain**.
2. In the **Domain** box, type the domain that you want, or click **Browse**, and then locate the domain that you want.

Chapter 5. Managing Users, Groups, and Computers

5.1. Modify Likewise Settings in ADUC

In Microsoft Active Directory Users and Computers, you can modify your Likewise settings for a domain, an organizational unit, a group, or a user. Likewise adds a tab to the property sheet of the following objects in the Active Directory Users and Computers MMC snap-in:

- Domain: Likewise Settings
- Users: Likewise Settings
- Groups: Likewise Settings
- Organizational Units:
 - Likewise Settings (for the associated cell)
 - Group Policy (with Likewise Enterprise)

Important: To change the settings, you must log on as a member of the Domain Administrators security group, the Enterprise Administrators security group, or another group that gives you sufficient privileges to modify objects in Active Directory. Or you must have been delegated privileges to modify the settings of the objects that you want to change; for more information, see [Delegate Management](#).

1. On your Windows administrative workstation, start Active Directory Users and Computers.
2. In the console tree, right-click the object that you want to change, click **Properties**, and then click the **Likewise Settings** tab.
3. Make the changes that you want.

5.2. Create a User

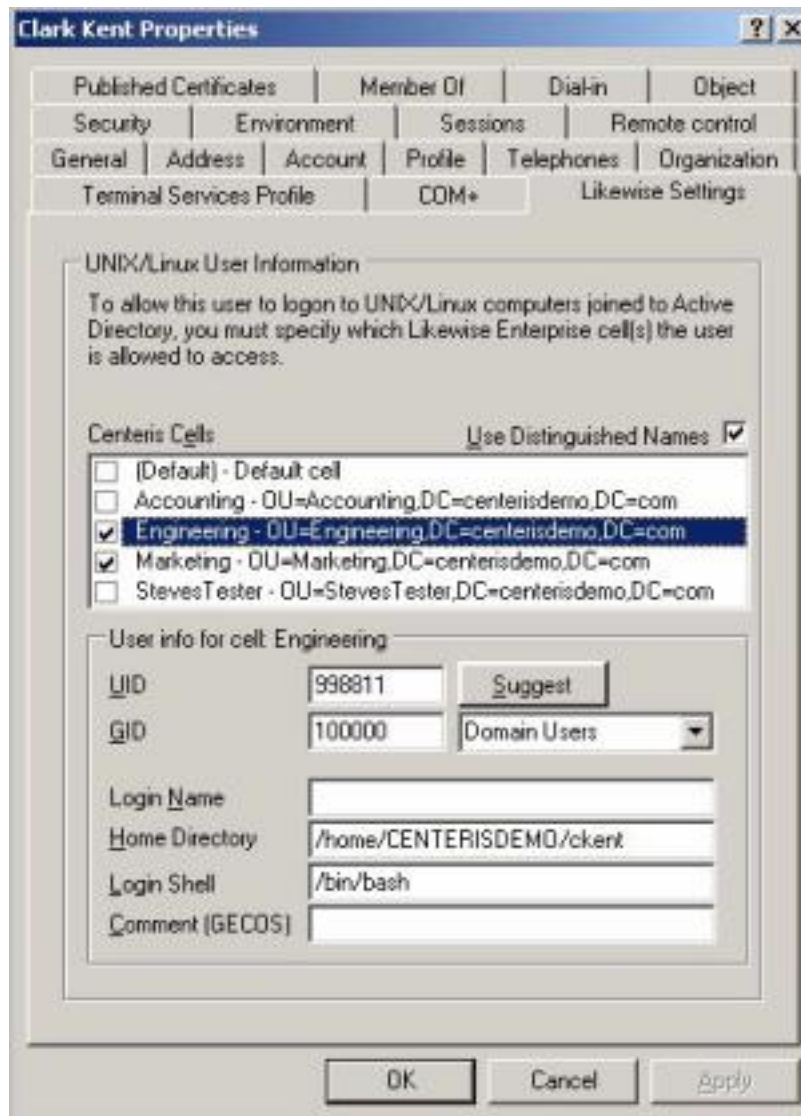
To create a Unix or Linux user account in Active Directory, you must have sufficient administrative privileges -- for example, as a member of the Enterprise Administrators group, the Domain Administrators group, or as a delegate.

1. On your Windows administrative workstation, start Active Directory Users and Computers.
2. In the console tree, right-click **Users**, point to **New**, and then click **User**.
3. Enter the name and logon name information for the user, and then click **Next**.

Tip: For more information, see [Create a New User Account in Active Directory Users and Computers Help](#).

4. In the **Password** box and the **Confirm password** box, type a password for the user, select the password options that you want, and then click **Next**.
5. Click **Finish**.

6. In the console tree, right-click the user that you just created, and then click **Properties**.
7. Click the **Likewise Settings** tab.



8. Under **Likewise Cells**, select the check box for the cell that you want to associate the user with. The user's settings can vary by cell.

Under **User info for cell**, a default value, typically 100000, is automatically populated in the **GID** box.

9. To set the UID, click **Suggest**, or type a value in the **UID** box.
10. To override the default home directory and login shell settings, in the **Home Directory** box, type the directory that you want to set for the user, and then in **Login Shell** box, type the login shell that you want.
11. Optionally, you can set a login name for the user in the **Login Name** box and add a comment in the **Comment** box. You use the **Login Name** box to set a login name for the user that is different from

the user's Active Directory login name. If you leave the **Login Name** box empty, the user logs on Linux and Unix computers by using his or her Active Directory login name.

See Also

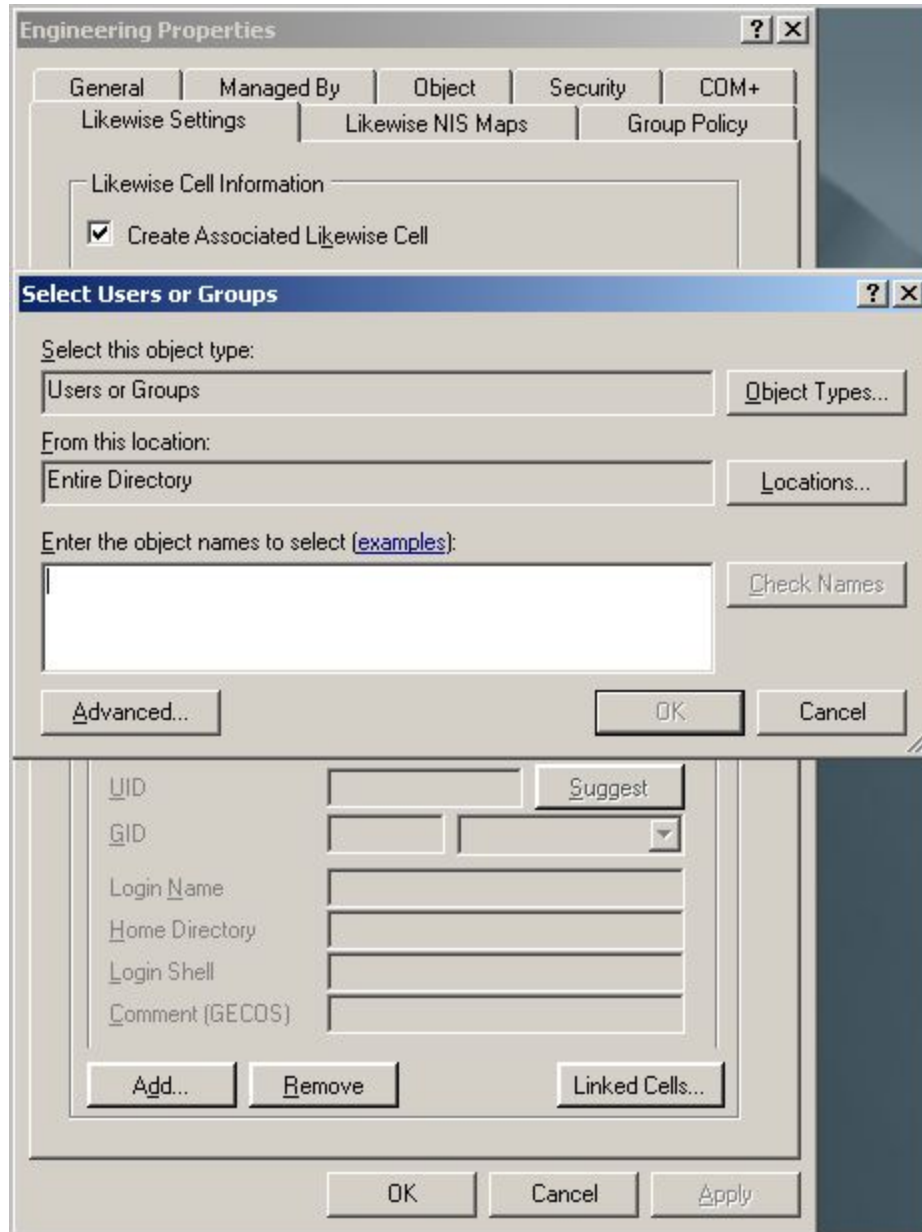
Create a Cell

5.3. Finding Users and Groups in ADUC

Because of a limitation with the Active Directory Users and Computers snap-in, when you try to find a Likewise user or group by right-clicking an organizational unit and then clicking **Find**, the user or group will not appear in the results even when the user or group is in the OU. The Find command does, however, work at the level of the domain.

As an alternative, you can find Likewise users and groups in an OU by using the following procedure:

1. In the console tree, right-click the OU with an associated cell in which you want to find a user or a group, click **Properties**, and then click the **Likewise Settings** tab:



2. Click Add and use the dialog box that appears to find the object that you want.

5.4. Provision a User with Linux or Unix Access

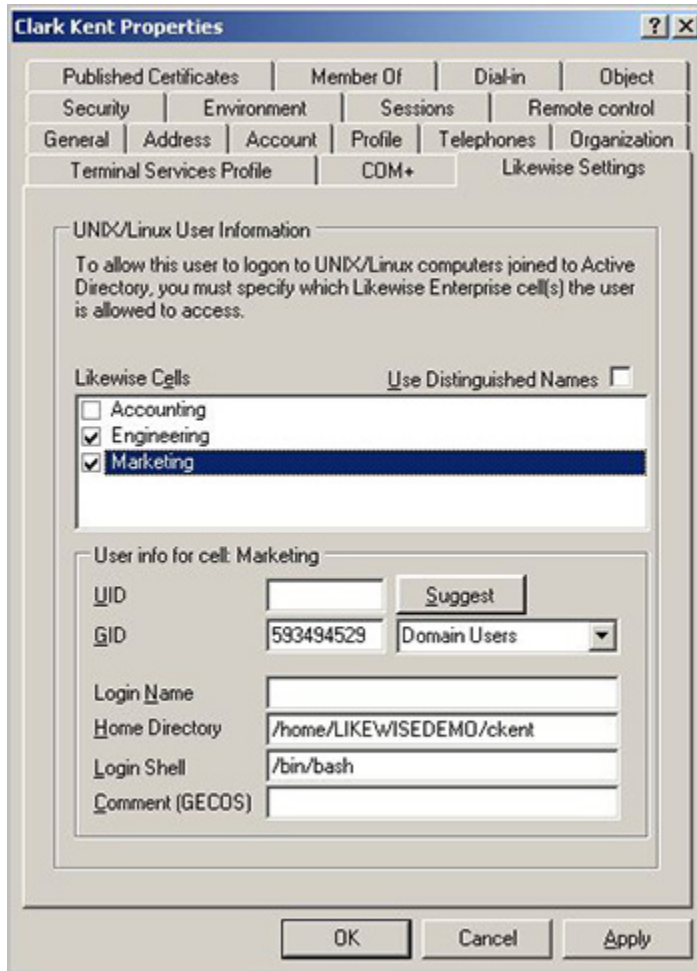
To provide an Active Directory user with Unix, Linux, or Mac access, you must have sufficient administrative privileges -- for example, as a member of the Enterprise Administrators group, the Domain Administrators group, or as a delegate.

Tip: For a Mac OS X user, limit group membership to less than 45 groups that are enabled for Unix access. Because of a limitation with Mac OS X, membership in groups other than the primary group is not enumerated for a user who belongs to more than 45 groups.

1. On your Windows administrative workstation, start Active Directory Users and Computers.

2. In the console tree, right-click the user that you want, and then click **Properties**.
3. Click the **Likewise Settings** tab.
4. Under **Likewise Cells**, select the check box for the cell that you want to give the user Linux or Unix access.

Note: If no cells appear under Likewise Cells, see Create a Cell or Create a Default Cell.



5. Under **User info for cell**, to set the UID, click **Suggest**, or type a value in the **UID** box.

Note: The user's settings can vary by cell.

6. In the **GID** box, a default value, typically the GID for the Domain Users group, is automatically populated in the **GID** box. To change the GID, click the drop-down list, and select the group that you want.

Note: If the group that you want is unavailable, you must first add the group to the cell; see Add a Group to a Cell.

7. To override the default home directory and login shell settings, in the **Home Directory** box, type the directory that you want to set for the user, and then in **Login Shell** box, type the login shell that you want.

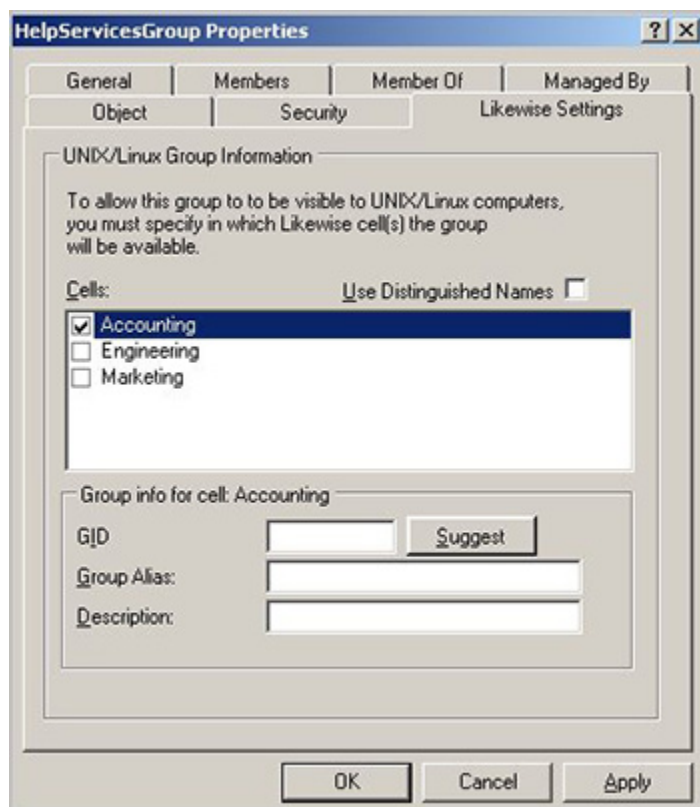
8. Optionally, you can set a login name for the user in the **Login Name** box and add a comment in the **Comment** box. You use the **Login Name** box to set a login name for the user that is different from the user's Active Directory login name. If you leave the **Login Name** box empty, the user logs on Linux and Unix computers by using his or her Active Directory login name.

5.5. Provision a Group with Linux or Unix Access

To provide an Active Directory group with Unix, Linux, or Mac access, you must have sufficient administrative privileges -- for example, as a member of the Enterprise Administrators group, the Domain Administrators group, or as a delegate.

1. On your Windows administrative workstation, start Active Directory Users and Computers.
2. In the console tree, right-click the group that you want, and then click **Properties**.
3. Click the **Likewise Settings** tab.
4. Under **Cells**, select the check box for the cell that you want to provide the group access to.

Note: If no cells appear under Likewise Cells, see Create a Cell or Create a Default Cell.



5. Under **Group info for cell**, to set the GID for the group in the cell you selected, click **Suggest**, or type a value in the **GID** box.
6. Optionally, you can set an alias for the group: In the **Group Alias** box, type an alias. The alias applies only within the cell.

5.6. Specify a User's ID and Unix or Linux Settings

You can set a user's identifier (UID) and specify the user's Unix, Linux, or Mac OS X settings.

Note: To provide a user with a UID and Unix or Linux settings, you must have sufficient administrative privileges -- for example, as a domain administrator or as a delegate. To delegate administrative privileges to another user, see Delegate Management.

1. On your administrative workstation, start Active Directory Users and Computers.
2. In the console tree, click **Users**.
3. In the details pane, right-click the user that you want, and then click **Properties**.
4. Click the **Likewise Settings** tab.

The screenshot shows the 'Clark Kent Properties' dialog box with the 'Likewise Settings' tab selected. The 'UNIX/Linux User Information' section contains a list of 'Likewise Cells' with checkboxes: Accounting (unchecked), Engineering (checked), and Marketing (unchecked). Below this, the 'User info for cell: Engineering' section has several fields: UID (593495123), GID (593494529), Login Name (empty), Home Directory (/home/LIKEWISEDEMO/ckent), and Login Shell (/bin/bash). There are also 'Suggest' and 'Domain Users' buttons.

5. Under **Likewise Cells**, select the check box for the cell that you want to associate the user with.

Under **User info for cell**, a default value is automatically populated in the **GID** box. You can change the user's primary group by select the group that you want from the drop-down list.

6. To set the UID, click **Suggest**, or type a value in the **UID** box.

Tip: To generate a report that shows duplicate UIDs, see Show Duplicate UIDs, GIDs, Login Names, and Group Aliases.

7. To override the default home directory and login shell settings, in the **Home Directory** box, type the directory that you want to set for the user, and then in **Login Shell** box, type the login shell that you want.
8. Optionally, you can set a login name for the user in the **Login Name** box and add a comment in the **Comment** box. You use the **Login Name** box to set a login name for the user that is different from the user's Active Directory login name. If you leave the **Login Name** box empty, the user logs on Linux and Unix computers by using his or her Active Directory login name.

See Also

Resolve an AD Alias Conflict with a Local Account

5.7. Apply Unix or Linux Settings to Multiple Users

Likewise lets you apply Unix, Linux, and Mac OS X settings to multiple users at the same time. For example, you can assign multiple users to a cell and then set their home directory.

The users must be members of a group that is associated with a cell and each user must have a UID-GID mapping.

Note: To change users' settings, you must log on as a member of the Domain Administrators security group or the Enterprise Administrators security group. Or, you must have been delegated privileges to modify the settings of the user objects that you want to change; for more information, see Delegate Management.

1. On your Windows administrative workstation, start Active Directory Users and Computers.
2. In the console tree, click **Users**, or expand the container that holds the users that you want.
3. In the details pane, hold down CTRL and click the users that you want.
4. Right-click the selected range of users, click **Properties**, and then click the **Likewise Settings** tab.
5. Under **UNIX/Linux User Information**, select the check box for the cell to which you want to assign the users.

By assigning the users to a cell, you are enabling them for access to the Unix, Linux, and Mac OS computers that are in the cell.

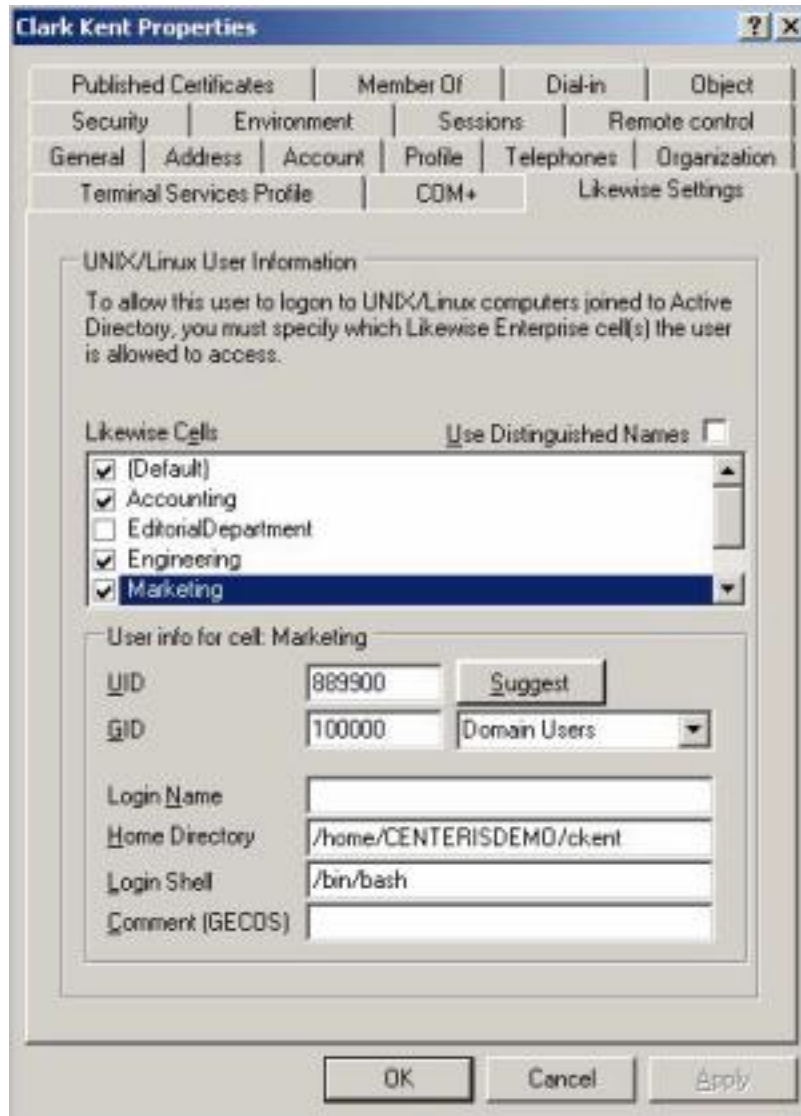
6. Under **User Info**, make the changes that you want.

You can specify a GID for the users, and you can set their login shell and home directory.

5.8. Set a User Alias

You can set an alias for an Active Directory user so that the user can use the alias to log on a Linux, Unix, or Mac OS X computer joined to Active Directory. The alias is set only for the cell that you select when you set it.

1. On your Windows administrative workstation, in Active Directory Users and Computers, expand the folder for your domain, and then expand **Users**.
2. Right-click the user that you want, click **Properties**, and then click the **Likewise Settings** tab.
3. Under **Likewise Cells**, click the cell that you want the user's alias to apply in.



4. In the **Login Name** box, type an alias for the user.

5.9. Set a Group Alias

You can create an alias for a group that is part of a Likewise cell, including the default cell. The group can use the alias within the cell.

1. On your Windows administrative workstation, start Active Directory Users and Computers.
2. In the console tree, click **Users**.

3. In the list of users, right-click the group that you want, click **Properties**, and then click the **Likewise Settings** tab.
4. Under **Cells**, select the check box for the cell that you want to set a group alias for, and then in the **Group Alias** box, type an alias for the group.

Tip: To generate a report that shows duplicate group aliases, see Show Duplicate UIDs, GIDs, Login Names, and Group Aliases.

5.10. Set the Default Home Directory

There are three ways that you can set the default home directory for Linux, Unix, and Mac OS X users:

- Set a cell's default home directory by using the Likewise Settings tab for an organizational unit's properties in Active Directory Users and Computers.
- Select multiple users in Active Directory Users and Computers and then set their default home directory.
- Set an individual user's default home directory by using the Likewise Settings tab for the user's properties in Active Directory Users and Computers.

When you set the default home directory, you must use the default user name variable (%U). You may specify the default domain name by using the domain name variable (%D) but, unlike the user name variable, it is not required.

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.

Set the Home Directory for a Cell

To set a default home directory for a cell, you must have Active Directory administrative privileges to modify OU objects.

1. On your Windows administrative workstation, start Active Directory Users and Computers.
2. In the console tree, right-click the OU for which you want to set a home directory, click **Properties**, and then click the **Likewise Settings** tab.
3. Under **Likewise Cell Information**, in the **Default Home Directory** box, type the home directory that you want to set for the groups and users in the cell.

Set the Home Directory for Multiple Users

To change users' settings, you must log on as a member of the Domain Administrators security group or the Enterprise Administrators security group. Or, you must have been delegated privileges to modify user settings; see Delegate Management.

1. On your administrative workstation, start Active Directory Users and Computers.
2. In the console tree, expand **Users**, or expand the container that holds the users that you want.
3. In the details pane, hold down CTRL and click the users that you want.

4. Right-click on the selected range of users, click **Properties**, and then click the **Likewise Settings** tab.
5. Under **UNIX/Linux User Information**, select the check box for the cell that contains the users whose home directory you want to set.

Note: Selecting a check box for a cell assigns the selected users to the cell and gives them access to the Unix, Linux, and Mac OS computers that are in the cell.

If the check box for the cell that you want is already selected, click the name of the cell.

6. In the **Home Directory** box, type the path for the home directory that you want to set -- for example, /home/%D/%U.

Set the Home Directory for a Single User

To change a user's settings, you must log on as a member of the Domain Administrators security group or the Enterprise Administrators security group. Or, you must have been delegated privileges to modify user settings; see Delegate Management.

1. On your administrative workstation, start Active Directory Users and Computers.
2. In the console tree, expand **Users**.
3. Right-click the user that you want, click **Properties**, and then click the **Likewise Settings** tab.
4. In the list under **Likewise Cells**, click the cell for which you want to set the user's home directory.
5. In the **Home Directory** box, type the path for the home directory that you want to set -- for example, /home/%D/%U.

5.11. Set the Default Login Shell

By using Likewise, there are two ways that you can set the default login shell for Linux, Unix, and Mac OS X users:

- Set a cell's default login shell by using the Likewise Settings tab for an organizational unit's properties in Active Directory Users and Computers.
- Select multiple users in Active Directory Users and Computers and then set their default login shell.
- Set an individual user's default login shell by using the Likewise Settings tab in Active Directory Users and Computers.

Set the Login Shell for a Cell

To set a default login shell for a cell, you must have Active Directory administrative privileges to modify OU objects.

1. On your Windows administrative workstation, start Active Directory Users and Computers.
2. In the console tree, right-click the OU for which you want to set a login shell, click **Properties**, and then click the **Likewise Settings** tab.
3. Under **Likewise Cell Information**, in the **Default Login Shell** box, type the login shell that you want to set for the users and groups in the cell.

Set the Login Shell for Multiple Users

To change users' settings, you must log on as a member of the Domain Administrators security group or the Enterprise Administrators security group. Or, you must have been delegated privileges to modify user settings; see Delegate Management.

1. On your administrator workstation, start Active Directory Users and Computers.
2. In the console tree, expand **Users**, or expand the container that holds the users that you want.
3. In the details pane, hold down CTRL and click the users that you want.
4. Right-click on the selected range of users, click **Properties**, and then click the **Likewise Settings** tab.
5. Under **UNIX/Linux User Information**, select the check box for the cell that contains the users whose home directory you want to set.

Note: Selecting a check box for a cell assigns the selected users to the cell and gives them access to the Unix, Linux, and Mac OS computers that are in the cell.

If the check box for the cell that you want is already selected, click the name of the cell.

6. In the **Login Shell** box, type the login shell that you want to set -- for example, `/bin/sh`.

Set the Login Shell for a Single User

To change a user's settings, you must log on as a member of the Domain Administrators security group or the Enterprise Administrators security group. Or, you must have been delegated privileges to modify user settings; see Delegate Management.

1. On your administrator workstation, start Active Directory Users and Computers.
2. In the console tree, expand **Users**.
3. Right-click the user that you want, click **Properties**, and then click the **Likewise Settings** tab.
4. In the list under **Likewise Cells**, click the cell for which you want to set the user's home directory.
5. In the **Login Shell** box, type the login shell that you want to set -- for example, `/bin/bash`.

5.12. Assign a Group ID

You can assign a group identifier (GID) to an Active Directory group by associating the group object with a cell and specifying a GID value for the group object.

The GID information that you enter is applied to all objects within the group. However, subgroups nested within the settings do not carry down; you must apply the GID information to subgroups individually.

Note: To assign a group ID, you must log on with privileges sufficient to modify the object.

1. On your Windows administrative workstation, Start Active Directory Users and Computers.
2. In the console tree, click **Users**.
3. In the details pane, right-click a group object or any container object, and then click **Properties**.

4. Click the **Likewise Settings** tab.
5. Under **Cells**, select the check box for the cell that you want to associate with the group object.
6. To assign a GID, click **Suggest**, or in the **GID** box type the group identifier that you want to assign to the group.

Tip: To generate a report that shows duplicate GIDs, see Show Duplicate UIDs, GIDs, Login Names, and Group Aliases.
7. In the **Group Alias** box, you may type an alias for the group, but it is not required.
8. In the **Description** text box, you may enter a description, but it is not required.

5.13. Disable a User

To disable a user, you must log on as a domain administrator or as a member of another group that gives you privileges sufficient to modify Active Directory user objects.

Note: When a computer cannot communicate with a domain controller, a user with a disabled account who has recently logged on to the computer can continue to log on until you clear the cache or until the cache expires. By default, the cache expires after 4 hours, or the interval that you set by using a Likewise group policy or by modifying the local configuration file (lsassd.conf).

1. On your Windows administrative workstation, start Active Directory Users and Computers.
2. In the console tree, click **Users**.
3. In the details pane, right-click the user that you want to disable, and then click **Properties**.
4. Click the **Likewise Settings** tab.
5. Under **Likewise Cells**, clear the check boxes for the cells in which you want to disable the user.

To disable the user's access to all Linux, Unix, and Mac OS X computers, in the list of cells under **Likewise Cells**, clear all the check boxes.

5.14. Improve MMC Performance When Accessing Likewise Settings in ADUC

When the Microsoft Management Console loads a snap-in such as ADUC, it checks for certificate revocations. To improve MMC performance after Likewise is installed on your Windows administrative workstation, you can reconfigure Internet Explorer's security options to not check for certificate revocation and reconfigure Windows to not update root certificates.

Important: Although these changes can improve performance, they can also affect your administrative workstation's security policy. Before making these changes, determine whether they are permitted by your IT security policy.

1. Close all instances of the Microsoft Management Console. Windows Task Manager should show no instances of `mmc.exe`.
2. Start Internet Explorer. The following steps assume you are using IE 7; for additional information or instructions for other versions of Windows, see Microsoft.com.

3. On the **Tools** menu, click **Internet Options**.
4. Click the **Advanced** tab, and then in the list under **Security** clear the check boxes for the following options:
 - Check for publisher's certificate revocation
 - Check for server certificate revocation
 - Check for signatures on downloaded programs
 - Allow software to run or install even if the signature is invalid
5. Click **OK**.
6. In Control Panel, go to **Add or Remove Programs**. The following steps assume you are using Windows Server 2003.

For additional information and instructions for other versions of Windows, see Microsoft.com. For computers running Windows 2008, for instance, you can turn off automatic root certificates updates by using a Microsoft group policy; see Certificate Support and the Update Root Certificates Component.
7. Click **Add/Remove Windows Components**, and then in the list under **Components** clear the **Update Root Certificates** checkbox.
8. Apply the changes and then restart the Microsoft Management Console.

5.15. Extend File Mode Permissions with POSIX ACLs

When you have to grant multiple users or groups access to a file, directory, or Samba share on a Linux server, you can use POSIX access control lists to extend the standard file mode permissions.

Because Linux and Unix file mode permissions control access only for a single user, a single group, and then everyone else, the only means of granting access to more than one group with the standard file modes is to either nest the groups together or to give everyone access -- approaches that are often unacceptable. Nested groups can be a maintenance burden, and granting access to everyone can undermine security. As for Samba shares, it is insufficient to add multiple users and groups to the `valid users` parameter in `smb.conf` if the underlying file system does not allow them access.

Prerequisites

You must have the `acl` package installed. You can determine this as follows:

```
# rpm -- qa -| grep acl
libacl-2.2.23-5
acl-2.2.23-5
```

The file system must be mounted with `acl` in the option list. You can determine this using the `mount` command:

```
# mount
/dev/sda1 on -/ type ext3 (rw,acl)
```

As shown above, the root file system has been mounted with read-write (`rw`) and `acl` options. If you don't see `acl` in the options for the file system you are working with, modify `/etc/fstab` to include this option, and then remount the file system. In the case of the root file system, you may need to reboot the system.

All users and groups must be created before adding them to the ACL. In the case of Active Directory users, they must be preceded by the domain unless user aliases have been configured (for example, `DOMAIN\username`).

Example

This example uses a directory called `testdir`. The process is the same for files.

Here are the standard file mode permissions of the `testdir` directory.

```
[aciarochi@rhel4-devel tmp]$ ls --ld testdir
drwxrwx--- 2 root root 4096 Dec 14 13:28 testdir
```

You can view the extended ACL using the `getfacl` utility. In this case, it shows the same information, in a different format:

```
[aciarochi@rhel4-devel tmp]$ getfacl testdir
# file: testdir
# owner: root
# group: root
user::rwx
group::rwx
other::---
```

With these permissions, only the root user and members of the root group are allowed to open the directory. Since the `aciarochi` user is not in the root group, he is denied access:

```
[aciarochi@rhel4-devel tmp]$ cd testdir
-bash: cd: testdir: Permission denied
```

However, we can grant access to `aciarochi` by using the `setfacl` utility to add him to the ACL. We must switch to the root user, of course, since that is the directory owner. Once the ACL is set, `aciarochi` can open the directory:

```
[root@rhel4-devel ~]# setfacl --m u:aciarochi:rwx -/tmp/testdir/
[root@rhel4-devel ~]# exit
logout
[aciarochi@rhel4-devel tmp]$ cd testdir
[aciarochi@rhel4-devel testdir]$ pwd
/tmp/testdir
```

Notice that the standard file mode permissions have not changed, except for the addition of a `+` at the end, indicating that extended file permissions are in effect:

```
[aciarochi@rhel4-devel tmp]$ ls --ld -/tmp/testdir/
drwxrwx---+ 2 root root 4096 Dec 14 13:28 -/tmp/testdir/
```

Additional groups can be added in the same manner -- using a `g:` instead of a `u:` -- to indicate a group. In the following example, we grant read and execute (open) access to the `ftp` group:

```
[root@rhel4-devel ~]# setfacl --m g:ftp:r-x -/tmp/testdir
```

```
[root@rhel4-devel ~]# getfacl testdir
# file: testdir
# owner: root
# group: root
user::rwx
user:aciarochi:rwx
group::rwx
group:ftp:r-x
mask::rwx
other:----
```

5.15.1. Using POSIX ACLs to Grant AD Accounts Access to Subversion

With Likewise, you can use AD accounts with Subversion. The trick is to use POSIX ACLs to give a domain group write access to the SVN repository.

Here's an example:

```
$ svnadmin create -/data/foo

## Add domain admins to the default directory ace
$ find -/data/foo --type d -| xargs setfacl --d --m -"g:AD
\domain^admins:rwx"

## Add domain admins to the directory ace
$ find -/data/foo --type d -| xargs setfacl --m -"g:AD
\domain^admins:rwx"

## Add domain admins to the ace for files
$ find -/data/foo --type f -| xargs setfacl --m -"g:AD
\domain^admins:rw"

$ getfacl -/data/foo
# file: foo
# owner: AD\134gjones
# group: AD\134unixusers
user::rwx
group::r-x
group:AD\134domain^admins:rwx
mask::rwx
other::r-x
default:user::rwx
default:group::r-x
default:group:AD\134domain^admins:rwx
default:mask::rwx
default:other::r-x
```

Don't forget to use only one forward slash (\) in `/etc/group`. Note too that the entry is case sensitive. You must specify the domain name in uppercase and the username in lowercase.

Chapter 6. Migrating Users to Active Directory

6.1. About Diagnostics and Migration

The Likewise Diagnostics and Migration page in the Likewise Management Console includes two tools to help manage a mixed network:

- Find Orphaned Objects
- Run Migration Tool

An orphaned object is a linked object, such as a Unix user ID or group ID, that remains in a cell after you delete a group or user's security identifier, or SID, from an Active Directory domain. The Find Orphaned Objects tool cleans up manually assigned user IDs and improves search speed.

The NIS migration tool imports Linux and Unix passwd files and group files and maps them to users and groups in Active Directory. The tool lets you resolve conflicts and ambiguous user names before you commit the changes.

The migration tool includes options to ease your NIS migration to Active Directory and to handle various requirements:

- Migrate account information to the organizational units that you want.
- Create groups in Active Directory to match your Linux and Unix groups.
- Generate scripts to repair file ownership and group settings.
- Change the GID of imported users to that of the AD Domain Users group.
- Automatically set an alias for each migrated user.
- Generate Visual Basic scripts to migrate users and groups in an automated and custom way.
- Modify GIDs during migration.
- Select only the groups and users that you want to migrate from your full list of groups and users.
- Set the home directory and shell for migrated users.
- Filter out standard Unix and Linux accounts, such as mail and news.
- Modify UID information during migration.
- Use NIS map files to migrate netgroups, automounts, and other services to Active Directory.

6.2. Migrate Users to Active Directory

The Likewise NIS migration tool can import Linux, Unix, and Mac OS X password and group files -- typically /etc/passwd and /etc/group -- and automatically map their UIDs and GIDs to users and groups defined in Active Directory.

You can also generate a Windows automation script to associate the Unix and Linux UIDs and GIDs with Active Directory users and groups. Before you commit the changes, you can resolve ambiguous user names and other conflicts.

Important: Before you migrate users to a domain that operates in non-schema mode, it is recommended that you find and remove orphaned objects. The IDs associated with orphaned objects are reserved until you remove the orphaned objects. See Find Orphaned Objects.

What You Need Before You Begin

Before running the migration tool, you should have the following information ready:

- The name of the domain to which you want to migrate the account information.
- Credentials that allow you to modify the domain.
- The Unix or Linux passwd file and corresponding group file that you want to add to Active Directory and manage with Likewise. The password and group files can be from a computer or an NIS server.

Run the Migration Tool

1. In the Likewise Management Console tree, under **Provisioning Management**, click the **Diagnostics & Migration**.
2. Under **Tasks**, click **Run Migration Tool**.
3. Click **Next**.
4. In the **Domain** box, type the domain name that you want to migrate the account information to.
5. If your logon credentials allow you to modify the domain, under **Credentials**, select **Use logon credentials**.

Or, if your logon credentials are not allowed to modify the domain, select **Use alternate credentials**, and then enter credentials that have the appropriate privileges.

6. Click **Next**.
7. Click **Import**, and then in the **Map name** box, type a name that corresponds to the computer that the passwd and group files are from.

The migration tool imports the passwd file and group file into the map file, which is then matched to existing Active Directory user and group names.

8. In the **Passwd file** box, type the path and name of the file that you want to import, or click **Browse** and then find the file that you want.
9. In the **Group file** box, type the path and name of the passwd file's corresponding group file, or click **Browse** and then find the file.
10. To import default Unix or Linux user accounts such as `root` and `public`, clear the **Omit standard Linux/UNIX user accounts** check box.

11. Click **Import**.

12. In the list under **Users**, clear the **Import** check box for any user that you do not want to import, and then click **Next**.

13. Select the organizational unit to which you want to migrate the Linux or Unix account information.

If you select the top of your domain, the information is migrated to the default Likewise cell of your Active Directory forest and UID numbers are automatically assigned within the domain's range.

If you select an organizational unit, Likewise creates a cell for the organizational unit and migrates the account information to it, maintaining your UIDs and GIDs if the passwd and group files agree and if the UIDs and GIDs do not conflict with existing users or groups. The migrated account information applies only to computers that are members of the organizational unit.

14. Click **Next**.

15. Under **Migration Options**, do any of the following:

To	Do This
Create groups in Active Directory that match your Linux or Unix groups	Select the Create groups in Active Directory to match Linux/UNIX groups check box.
Create all groups in Active Directory -- not just the references ones. To select this option, you must first you must first select the Create groups in Active Directory to match Linux/UNIX groups check box.	Select the Create all groups in AD (not just referenced ones) check box.
Generate script that can repair ownership and group settings	Select the Generate scripts to repair file ownership and group settings check box.
Change the GID of imported users to "Domain Users"	Select the Change GID of imported users to "Domain Users" check box.
Set the alias even if it is the same as sAMAccountName	Select the Always set Login Name (alias), even when same as sAMAccountName check box.
Generate a Visual Basic script to perform migration	Select the Generated VBScript to perform migration check box, and then in the Script name box, type a name for the script. In the Folder for generated scripts box, enter the directory that you want.

16. Click **Next**.

17. Click the **Users** tab and verify that the information is correct.

18. Click the **Groups** tab and verify that the information is correct.

19. To import the passwd and group files after you verify that the information is correct, click **Next**.

6.3. Find Orphaned Objects

You can use the Likewise Management Console to find and remove orphaned objects. An orphaned object is a linked object, such as a Unix or Linux user ID or group ID, that remains in a cell after you delete a group or user's security identifier, or SID, from an Active Directory domain.

Removing orphaned objects from Active Directory can clean up manually assigned user IDs and improve search speed. It is recommended that you remove orphaned objects before you use the migration tool with a domain that operates in non-schema mode.

1. In the Likewise Management Console tree, under **Provisioning Management**, click the **Diagnostics & Migration**.
2. Under **Tasks**, click **Find Orphaned Objects**.

3. Click **Select Domains**, select the domains that you want to scan, and then click **OK**.
4. Click **Begin Scan**.
5. To remove the objects that appear in the **Orphaned objects to delete** box, click **Delete Objects**.

6.4. Migrate a User Profile on a Mac

On a Mac OS X computer, the Likewise domain join utility includes a tool to migrate a user's profile from a local user account to the home directory specified for the user in Active Directory.

When you migrate the user's profile, you can either copy or move it from the local account to the user's Active Directory account. Copying the profile leaves a copy of the user's files in their original location, but doubles the space on the hard disk required to keep the user's files.

You can migrate a user by using the GUI or by using the command line. In addition, you can customize the migration shell script to suit your requirements.

Important: To migrate a user's profile, you must have a local or AD account with administrative privileges. The account that you use must not be the account that you are migrating.

Migrate a User's Profile with the GUI

1. Save and close any documents that the user has open.
2. Log on with an administrator account that is not being migrated.
3. In Terminal, execute the following command to open the Likewise Domain Join dialog:

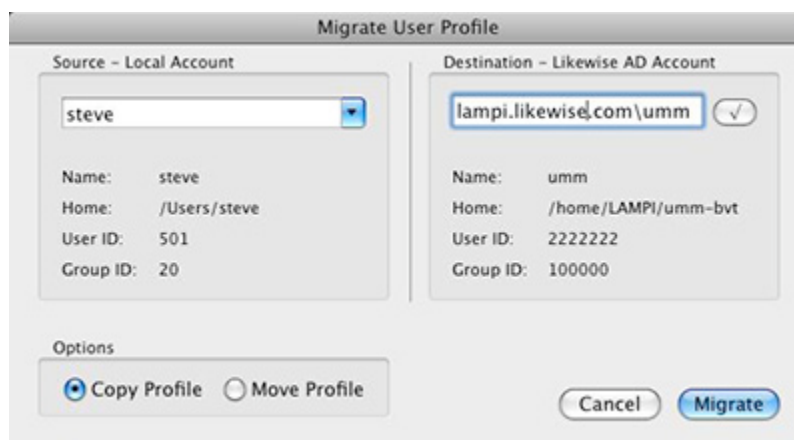
```
open /opt/likewise/bin/Likewise\ Domain\ Join.app
```


If prompted, enter a name and password of an account with administrative privileges. The account can be either a local machine account or an AD account, but must not be the account that you are migrating.

4. In the **Likewise Domain Join** dialog, Click **Migrate**.

Note: The **Likewise Domain Join** dialog might be behind your Terminal window or behind another window.

5. Under **Source - Local Account**, in the list, click the user that you want.



- In the box under **Destination - Likewise AD Account**, type the name of the Active Directory user account to which you want to migrate the local account, and then click  to check that the account is in Active Directory.
- Under **Options**, do one of the following:

To	Do This
Move the user's files and data from the user's home directory to a home directory specified in Active Directory.	Select Move Profile .
Copy a user's files and data from the user's home directory to a home directory specified in Active Directory. Note: This option doubles the amount of hard disk space required to store the user's files and data on the computer.	Select Copy Profile .

- Click **Migrate**.

Migrate a User's Profile from the Command Line

You can migrate a user's profile by using the command line. On a Mac OS X computer, the location of the migration shell script is as follows:

```
/opt/likewise/bin/lw-local-user-migrate.sh
```

You can execute the migration script either locally or remotely by connecting to a Mac with SSH. Connecting to a Mac with SSH and then running the migration script from the command line lets you remotely migrate users from another computer.

For information about the command's syntax and arguments, execute the following command in Terminal:

```
/opt/likewise/bin/lw-local-user-migrate.sh --help
```

Customize the Migration Script

You can customize the migration script to suit your needs by opening the script and editing it. The script is written in Bash shell.

Important: There is no Likewise support for customizing the script or for modified scripts. Changes to the script preclude Likewise support.

Chapter 7. The Likewise Agent

7.1. 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.

7.2. Daemons

Likewise Open

The Likewise Open agent comprises the following daemons:

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

	SMB servers. For instructions on how to set up and use the Likewise CIFS/SMB file server, see the Likewise CIFS file server user guide.	
/opt/likewise/sbin/dcerpcd	The Likewise DCE/RPC endpoint mapper. DCE/RPC stands for Distributed Computing Environment/Remote Procedure Calls. The daemon handles communication between Linux, Unix, and Mac computers and Microsoft Active Directory by mapping data to 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/lwregd	The daemon for the registry service.	All the Likewise services depend on lwregd.
/opt/likewise/sbin/lwsmd	The Likewise service manager. It manages all the other Likewise daemons and services.	All the Likewise services depend on lwsmd.

Likewise Enterprise

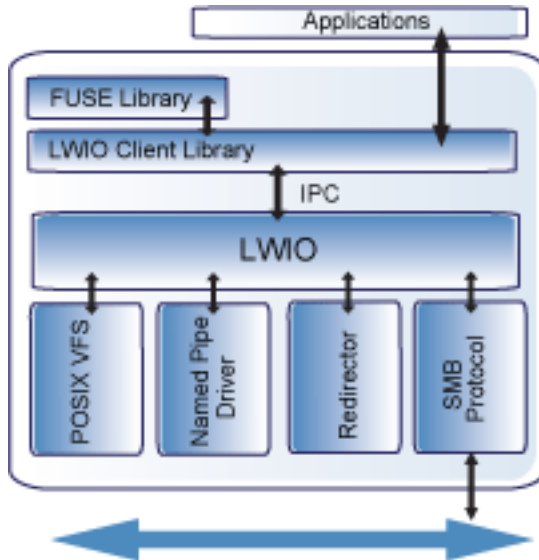
Likewise Enterprise includes all the daemons that are in Likewise Open. The following additional daemons are in Likewise Enterprise to apply group policies, handle smart cards, and monitor security events:

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

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

The Likewise Input-Output Service


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



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

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

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

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

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

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

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

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

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

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

PAM Options

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

Managing the Likewise Daemons

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

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

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

Example:

```
[root@rhel15d bin]# /opt/likewise/bin/lwsm list
lwreg      running (standalone: 1920)
dcerpc     running (standalone: 2544)
eventlog   running (standalone: 2589)
lsass      running (standalone: 2202)
lwio       running (standalone: 2191)
netlogon   running (standalone: 2181)
npfs       running (io: 2191)
rdr        running (io: 2191)
```

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

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

7.3. 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](#).

7.4. 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

7.5. Caches and Databases

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

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

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

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

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

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

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

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

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

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

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

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

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

7.6. 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.

7.7. 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.

7.8. 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.

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

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

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

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

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

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

7.10. 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.

7.11. Trust Support

The Likewise agent supports the following Active Directory trusts:

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

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

Notes on Trusts

The following list contains general information about working with trusts.

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

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

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

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

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

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

Trusts and Cells in Likewise Enterprise

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

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

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

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

7.12. Integrating with Samba

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

7.13. Supported Platforms

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

Chapter 8. Configuring Clients Before Agent Installation

8.1. Configure `nsswitch.conf`

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

```
hosts: files dns
```

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

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

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

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

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

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

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

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

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

8.2. Configure `resolv.conf`

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

Example:

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

search likewisedemo.com
nameserver 192.168.100.132
```

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

8.3. 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](#).

8.4. 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.

8.5. Increase Max Username Length on IBM AIX

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

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

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

Example:

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

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

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

You must reboot for the changes to take effect:

```
# shutdown -Fr
```

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

8.6. Check System Health Before Installing the Agent

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

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

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

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

Configuring Clients
Before Agent Installation

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

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

Configuring Clients
Before Agent Installation

<p>Contents of <code>nsswitch.conf</code> (or, for AIX, <code>netstvc.conf</code>)</p>	<p>Displays information about the <code>nsswitch</code> configuration.</p>	<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>
<p>FQDN</p>	<p>Determines the fully qualified domain name of the computer to ensure that it is set properly.</p>	<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>	Returns the address for the <code>nameserver</code> set in <code>resolv.conf</code> . 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. 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.	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 9. Installing the Agent

9.1. Install the Correct Version for Your Operating System

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

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

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

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

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

Checking Your Linux Kernel Release Number

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

```
uname -r
```

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

Package Management Commands

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

9.2. Requirements for the Agent

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

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

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

Patch Requirements

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

Sun Solaris

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

Sun Solaris 10 requires update 5 or later. The Solaris 10 05/08 (or later) patch bundle is available at <http://sunsolve.sun.com/>. Solaris 10_x86 requires the patch for nscd, either patch ID number 138047-02 or the patch that 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 programs that uses PAM for processing authentication requests are compatible with Likewise.

Networking Requirements

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

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

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

Disk Space Requirements

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

Memory and CPU Requirements

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

Clock Skew Requirements

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

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

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

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

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

Install the Agent on Linux or Unix with the Shell Script

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

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

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

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

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

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

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

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

4. As root, run the installer:

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

5. Follow the instructions in the installer.

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

9.4. Install the Agent on Linux in Unattended Mode

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

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

9.5. Install the Agent on Unix with the Command Line

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

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

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

Perform the following procedure with the root account.

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

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

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

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

4. As root, run the installer:

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

5. Follow the instructions in the installer.

9.6. Install the Agent on a Mac Computer

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

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

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

2. Log on the Mac with a local account.

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

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

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

9.7. Install the Agent on a Mac in Unattended Mode

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

The commands in this procedure require administrative privileges.

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

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

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

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

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

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

4. Execute the following command to install the agent:

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

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

```
man installer
```

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

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

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

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

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

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

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

9.8. Installing the Agent in Solaris Zones

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

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

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

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

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

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

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

Caveats

There are some caveats when using Likewise with Solaris Zones:

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

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

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

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

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

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

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

Change this:

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

To this:

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

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

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

9.9. Upgrading Your Operating System

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

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

Chapter 10. Joining an Active Directory Domain

10.1. About Joining a Domain

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

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

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

/opt/likewise/bin/domainjoin-cli

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

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

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

Privileges and Permissions

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

Removing a Computer from a Domain

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

Creation of Local Accounts

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

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

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

Example output:

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

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

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

10.2. Join Active Directory with the Command Line

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

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

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

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

Before Joining a Domain

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

```
nslookup domainName
```

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

```
ping domainName
```

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

Join a Linux or Unix Computer to Active Directory

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

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

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

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

Join a Mac Computer to Active Directory

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

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

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

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

Join a Linux or Unix Computer to an Organizational Unit

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

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

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

Join a Linux or Unix Computer to a Nested Organizational Unit

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

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

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

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

10.3. Domainjoin-cli Options, Commands, and Arguments

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

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

Basic Commands

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

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

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

Advanced Commands

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



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

Preview the Stages of the Domain Join for Your Computer

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

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

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

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

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

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

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

Check Required Configurations

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

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

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

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

The result varies by computer:

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

Key to flags

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

View Details about a Module

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

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

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

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

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

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

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

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

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

The result varies depending on your system's configuration:

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

Key to flags

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

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

```
requirements for this step
```

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

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

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

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

The following steps are required and can be performed automatically:

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

- and `-/opt/likewise/lib64` directories

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

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

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

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

Turn On or Turn Off Domain Join Modules

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

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

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

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

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

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

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

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

Configuration and Debugging Commands

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

domainjoin-cli configure --enable nsswitch

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

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

```

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

```

10.4. Join Active Directory Without Changing /etc/hosts

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

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

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

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

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

If the Computer Fails to Join the Domain

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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


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

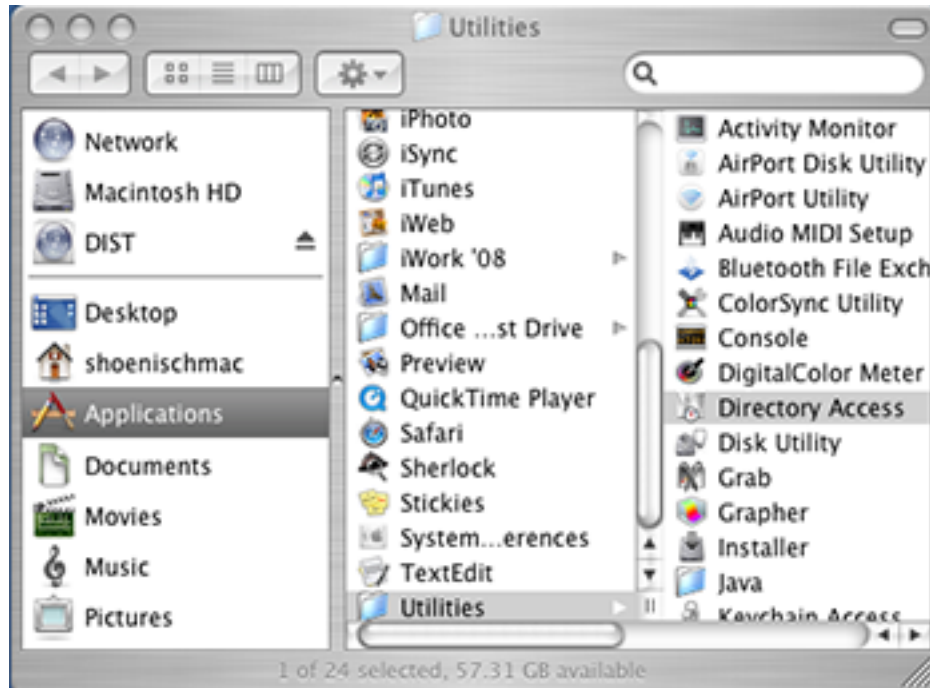
After you join a domain for the first time, you must restart the computer before you can log on.

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

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


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

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



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

3.

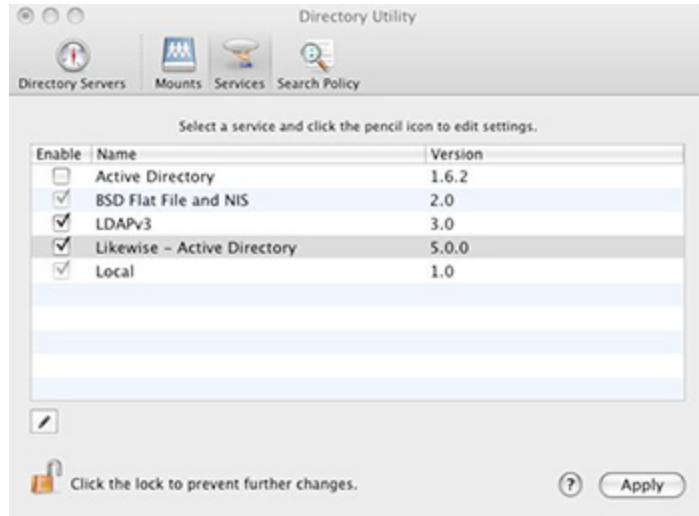
On the **Services** tab, click the lock  and enter an administrator name and password to unlock it.

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


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

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

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





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

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

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

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

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

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

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

10.6.1. Turn Off OS X Directory Service Authentication

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

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

10.7. Use Likewise with a Single OU

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

There are additional limitations to this approach:

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

Join a Linux Computer to an Organizational Unit

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

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

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

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

Example of how to join a nested OU:

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

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

10.8. Rename a Joined Computer

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

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

Rename a Computer by Using the Command-Line Tool

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

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

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

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

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

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

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

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

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

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

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

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

Rename a Computer by Using the Domain Join Tool GUI

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

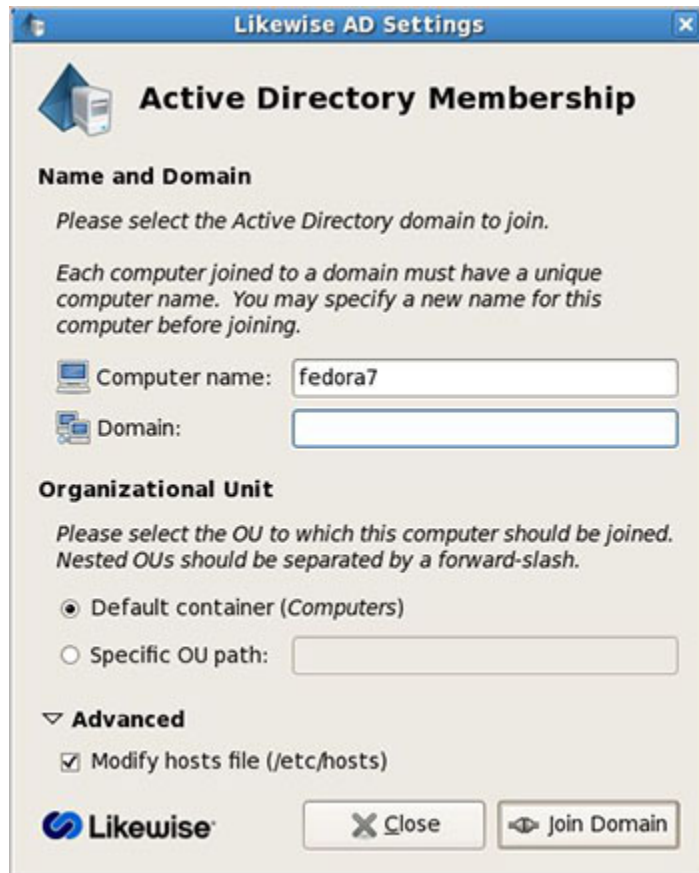
```
/opt/likewise/bin/domainjoin-gui
```

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

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

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

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



6. In the **Domain to join** box, enter the Fully Qualified Domain Name (FQDN) of the Active Directory domain.

7. Under **Organizational Unit**, you can join the computer to an OU in the domain by selecting **OU Path** and then typing a path in the **OU Path** box.

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

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

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

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

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

10.9. Files Modified When You Join a Domain

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

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

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

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

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

- /etc/inet/ipnodes

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

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

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

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

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

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

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

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

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

Chapter 11. Logging On with Domain Credentials

11.1. About Logging On

Likewise includes the following logon options:

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

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

- Cached credentials

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

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

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

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

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

See Also

[About Single Sign-On](#)

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

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

11.2. Log On with AD Credentials

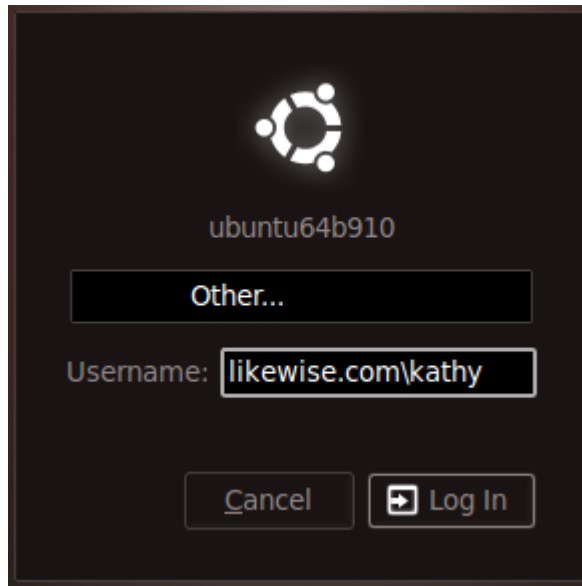
After the Likewise agent has been installed and the Linux or Unix computer has been joined to a domain, you can log on with your Active Directory credentials, either from the command line or

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

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

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

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



11.3. 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`

11.4. Solve Logon Problems from Windows

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

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

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

11.5. Solve Logon Problems on Linux or Unix

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

Make Sure You Are Joined to the Domain

Execute the following command:

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

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

Check Whether You Are Using a Valid Logon Form

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

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

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

Clear the Cache

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

Destroy the Kerberos Cache

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

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


Check the Status of the Likewise Authentication Daemon

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

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

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

Check Communication between the Likewise Daemon and AD

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

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

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

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

Verify that Likewise Can Find a User in AD

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

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

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

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

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

Make Sure the AD Authentication Provider Is Running

Likewise includes two authentication providers:

1. The local provider
2. The Active Directory provider

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

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

A healthy result should look like this:

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

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

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

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

Run the `id` Command to Check the User

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

```
id DOMAIN\\username
```

Example: `id likewisedemo\\kathy`

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

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

Switch User to Check PAM

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

```
su DOMAIN\\username
```

Example: `su likewisedemo\\hoenstiv`

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

Test SSH

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

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

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

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

Run the Authentication Daemon in Debug Mode

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

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

Check Nsswitch.Conf

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

On HP-UX, Escape Special Characters at the Console

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

Additional Diagnostic Tools

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

`/opt/likewise/bin`

See Also

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

Chapter 12. Troubleshooting Domain-Join Problems

12.1. Top 10 Reasons Domain Join Fails

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

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

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

```
/etc/sysconfig/selinux
```

or

```
/etc/selinux/config
```

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

See Also

[Generate a Domain-Join Log](#)

12.2. Solve Domain-Join Problems

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

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

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

Verify that the Name Server Can Find the Domain

Run the following command as root:

```
nslookup YourADrootDomain.com
```

Make Sure the Client Can Reach the Domain Controller

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

```
ping YourDomainName
```

Verify that Outbound Ports Are Open

Run the following command as root:

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

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

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

Check DNS Connectivity

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

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

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

```
hosts: files dns
```

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

Generate a Domain-Join Log

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

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

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

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

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

Example:

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

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

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

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

Determine Whether the DNS Server Is Configured to Return SRV Records

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

Diagnose it by executing the following command:

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

Make Sure that the Global Catalog Is Accessible

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

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

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

```
telnet 192.168.100.20 3268
```

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

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

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

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

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

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

For more information, see Diagnose NTP on Port 123.

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

12.3. Ignore Inaccessible Trusts

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

First, list the available trust settings:

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

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

```
DomainManagerIgnoreAllTrusts
DomainManagerIncludeTrustsList
DomainManagerExcludeTrustsList
```

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

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

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

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

Finally, check to make sure the change took effect:

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

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

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

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

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

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

12.4. Dealing with Common Error Messages

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

12.4.1. Configuration of Krb5

Error Message:

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

Solution:

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

12.4.2. Chkconfig Failed

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

Error Message:

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

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

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

```
chkconfig --add netlogond
```

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

12.5. Diagnose NTP on Port 123

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

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

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

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

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

```
[root@rhel44id ~]# ntpdate --d --u sales-dc
2 May 14:19:20 ntpdate[20232]: ntpdate 4.2.0a@1.1190-r Thu Apr 20
11:28:37 EDT 2006 (1)
Looking for host sales-dc and service ntp
host found -: sales-dc.likewisedemo.com
transmit(192.168.100.20)
receive(192.168.100.20)
transmit(192.168.100.20)
receive(192.168.100.20)
transmit(192.168.100.20)
receive(192.168.100.20)
transmit(192.168.100.20)
receive(192.168.100.20)
transmit(192.168.100.20)
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)
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
```

12.6. Turn Off Apache to Join a Domain

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

Chapter 13. Configuring the Agent

13.1. Modify Settings with the Config Tool

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

```
/opt/likewise/bin/lwconfig
```

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

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

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

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

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

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

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

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

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

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

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

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

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

13.2. Add Domain Accounts to Local Groups with /etc/group

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

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

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

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

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

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

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

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

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

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

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

13.3. Configure Entries in Your Sudoers Files

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

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

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

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

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

```
DOMAIN\\username
```

```
DOMAIN\\groupname
```

Example entry of a group:

```
% LIKWISEDEMO\\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
```

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

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

13.4. Set a Sudoers Search Path

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

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

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

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

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

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

13.5. Set Up AIX Audit Classes to Monitor Events

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

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

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

The sample Likewise `auditclasses` file looks like this:











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

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

Chapter 14. Troubleshooting the Agent

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

Additional troubleshooting information is in the following chapters:

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

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

14.1. Likewise Daemons and Services

14.1.1. Troubleshoot Likewise Daemons with the Service Manager

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

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

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

Here's an example:

```
[root@rhel15d bin]# -/opt/likewise/bin/lwsm list
lwreg          running (standalone: 1920)
dcerpc         running (standalone: 2544)
eventlog       running (standalone: 2589)
lsass          running (standalone: 2202)
```



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

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

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

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

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

14.1.2. Check the Status of the Authentication Daemon On Linux and Unix

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

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

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

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

14.1.3. Check the Status of the DCE/RPC Daemon

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

On Linux and Unix

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

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

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

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

On Mac OS X

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

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

14.1.4. Check the Status of the Network Logon Daemon

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

On Linux and Unix

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

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

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

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

On Mac OS X

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

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

14.1.5. Check the Status of the Input-Output Service

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

On Linux and Unix

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

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

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

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

On Mac OS X

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

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

14.1.6. Restart the Authentication Daemon

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

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

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

To stop the daemon, type this command:

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

To start the daemon, type this command:

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

14.1.7. Restart the DCE/RPC Daemon

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

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

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

To stop the daemon, type this command:

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

To start the daemon, type this command:

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

14.1.8. Restart the Network Logon Daemon

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

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

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

To stop the daemon, type this command:

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

To start the daemon, type this command:

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

14.1.9. Restart the Input-Output Service

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

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

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

To stop the daemon, type this command:

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

To start the daemon, type this command:

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

14.2. Logging

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

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

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

- `gpagent`, the group policy agent. Generate a debug log for `gpagent` to troubleshoot the application or processing of group policy objects.
- `eventfwd`, the event forwarding daemon. Generate a debug log to verify the service is properly receiving events and forwarding them to a collector server.
- `reapsysl`, part of the data collection service. Capture a debug log for `reapsysl` to investigate the collection and processing of events.
- `lwsc`, the smart card service. Gather logging information for the smart card service when card-insertion or card-removal behavior is other than expected.
- `lwpkcs11d`, a daemon that aids in logging on and logging off with a smart card. Gather logging information about it when there is a problem logging on or logging off with a smart card.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Instantly Change the Log Level for Other Services

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

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

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

Change the Log Level to Debug Until the Service Restarts

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

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

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

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

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

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

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

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

Permanently Change the Log Level by Editing the Registry

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

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

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

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

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

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

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

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

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

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

14.2.1. Generate a Domain-Join Log

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

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

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

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

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

Example:

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

14.2.2. Generate an Authentication Agent Debug Log

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

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

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

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

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

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

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

14.2.3. Generate a PAM Debug Log

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

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

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

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

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

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



```

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

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

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

Finally, confirm that the change took effect:

```

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

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

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

14.2.4. Generate a Directory Service Log on a Mac

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

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

```

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

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

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

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

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

```

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

14.2.5. Log Group Policy Debugging Data

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

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

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

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

14.2.6. Generate a Network Trace

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

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

The result should look something like this:

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

14.3. Basics

14.3.1. Check the Version and Build Number

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

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

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

Another option is to execute the following command:

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

Check the Version and Build Number of the Agent with ADUC

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

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

Check the Build Number of the Agent

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

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

The result shows the build version after the version number:

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

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

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

14.3.2. Determine a Computer's FQDN

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

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

On HP-UX

The command is different on HP-UX:

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

On Solaris

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

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

See Also

[Join Active Directory Without Changing /etc/hosts](#)

14.3.3. Make Sure Outbound Ports Are Open

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

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

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

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

```
iptables - nL
```

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

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

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

14.3.5. Configure SSH After Upgrading It

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

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

14.3.6. Upgrading an Operating System

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

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

14.4. Accounts

14.4.1. Allow Access to Account Attributes

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

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

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

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

Allow Access to Account Attributes

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

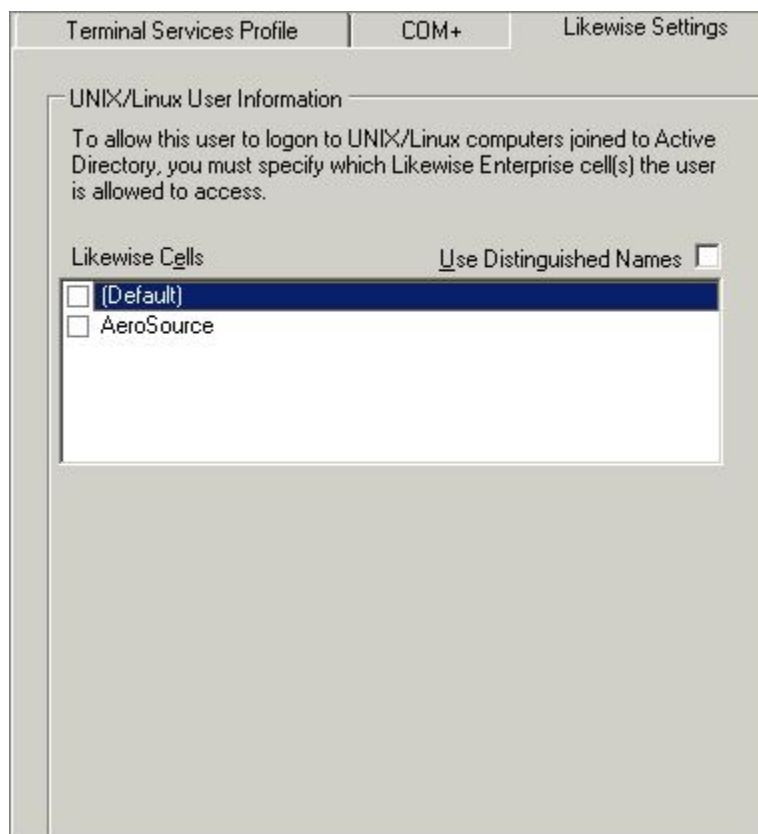
See Also

About Schema Mode and Non-Schema Mode

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

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

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



14.4.3. Resolve an AD Alias Conflict with a Local Account

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

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

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

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

Change Ownership

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

```
cd <users home directory root>

chown -R <AD user UID>:<AD primary group ID> *.*

Or: chown -R <short domain name>\\<account name>:<short domain name>\\
<AD group name> *.*
```

See Also

Show Duplicate UIDs, GIDs, Login Names, and Group Aliases

14.4.4. Fix the Shell and Home Directory Paths

Symptom: A local directory is in the home directory path and the home directory path does not match the path specified in Active Directory or in `/etc/passwd`.

Example: `/home/local/DOMAIN/USER` instead of `/home/DOMAIN/USER`

The shell might also be different from what is set in Active Directory -- for example, `/bin/ksh` instead of `/bin/bash`.

Problem: The computer is not in a Likewise cell in Active Directory.

Solution: Make sure the computer is in a Likewise cell. For more information, see Associate a Cell with an OU or a Domain, or create a default cell.

A default cell handles mapping for computers that are not in an OU with an associated cell. The default cell can contain the mapping information for all your Linux and Unix computers. For instance, a Linux or Unix computer can be a member of an OU that does not have a cell associated with it. In such a case, the home directory and shell settings are obtained from the nearest parent cell or the default cell. If there is no parent cell and no default cell, the computer will not receive its shell and home directory paths from Active Directory.

See Also

Set the Default Home Directory and Login Shell

14.4.5. Troubleshooting with the Get Status Command

The `/opt/likewise/bin/lw-get-status` command shows whether the domain or the Likewise AD provider is offline. The results of the command include information useful for general troubleshooting.

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

Here's an example of the information the command returns:

```
[root@rhel5d bin]# -/opt/likewise/bin/lw-get-status
LSA Server Status:
Compiled daemon version: 6.1.272.54796
Packaged product version: 6.1.272.54796
Uptime:                15 days 21 hours 24 minutes 1 seconds

[Authentication provider: lsa-activedirectory-provider]

      Status:           Online
      Mode:             Un-provisioned
      Domain:          LIKWISEDEMO.COM
```

```
Forest:          likewisedemo.com
Site:           Default-First-Site-Name
Online check interval: 300 seconds
[Trusted Domains: 1]
```

```
[Domain: LIKEWISEDEMO]
```

```

DNS Domain:          likewisedemo.com
Netbios name:       LIKEWISEDEMO
Forest name:        likewisedemo.com
Trustee DNS name:
Client site name:  Default-First-Site-Name
Domain SID:
S-1-5-21-3190566242-1409930201-3490955248
Domain GUID:       71c19eb5-1835-f345-ba15-0595fb5b62e3
Trust Flags:       [0x000d]
                   [0x0001 -- In forest]
                   [0x0004 -- Tree root]
                   [0x0008 -- Primary]
Trust type:        Up Level
Trust Attributes:  [0x0000]
Trust Direction:  Primary Domain
Trust Mode:        In my forest Trust (MFT)
Domain flags:      [0x0001]
                   [0x0001 -- Primary]

```

```
[Domain Controller (DC) Information]
```

```

DC Name:           w2k3-r2.likewisedemo.com
DC Address:        192.168.92.20
DC Site:           Default-First-Site-Name
DC Flags:          [0x000003fd]
DC Is PDC:         yes
DC is time server: yes
DC has writeable DS: yes
DC is Global Catalog: yes
DC is running KDC: yes

```

```
[Authentication provider: lsa-local-provider]
```

```

Status:           Online
Mode:             Local system
Domain:           RHEL5D

```

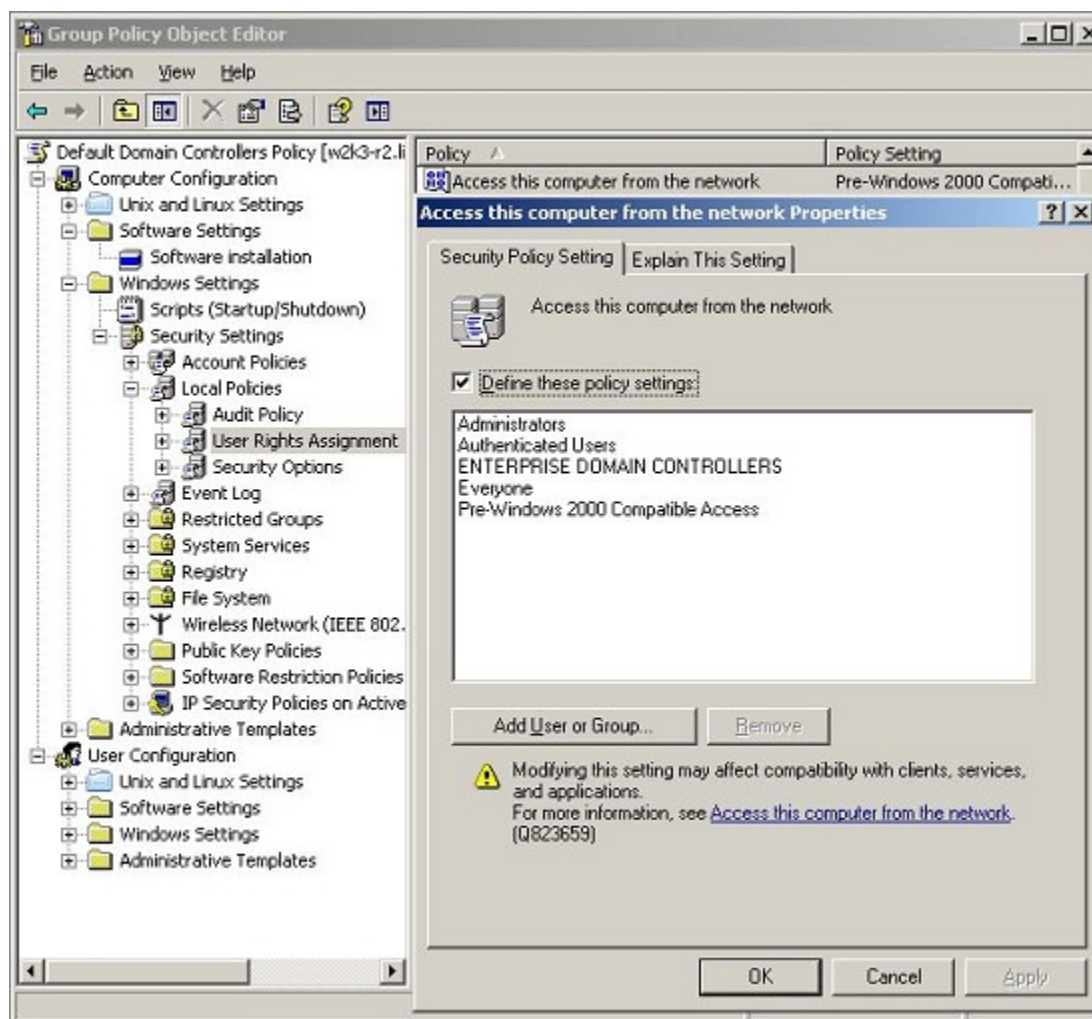
14.4.6. Troubleshoot User Rights with Ldp.exe and Group Policy Modeling

The following Microsoft default domain policies and default domain controller policies can cause a Likewise client to fail to join a domain or to fail to enumerate trusts:

- Access this computer from the network. Users and computers that interact with remote domain controllers require the access-this-computer-from-network user right. Users, computers, and service accounts can lose the user right by being removed from a security group that has been granted the

right. Removing the administrators group or the authenticated users group from the policy can cause domain join to fail. Microsoft says, "There is no valid reason for removing Enterprise Domain Controllers group from this user right." For more information, see <http://support.microsoft.com/kb/823659>.

- Deny access to this computer from the network. Including the domain computers group in the policy, for instance, causes domain-join to fail.



The symptoms of a user-right problem can include the following:

- An attempt to join the domain is unsuccessful.
- The Likewise authentication service, lsass, does not start.
- The `/opt/likewise/bin/lw-get-status` command shows the domain or the AD provider as offline.

You can pin down the issue by using the `ldp.exe` tool to check whether you can access AD by using the machine account and machine password. `Ldp.exe` is typically included in the support tools (`suptools.msi`) for Windows and located on the Windows installation CD (Support folder, Tools subfolder). You might also be able to download the support tools that contain `ldp.exe` from the Microsoft web site.

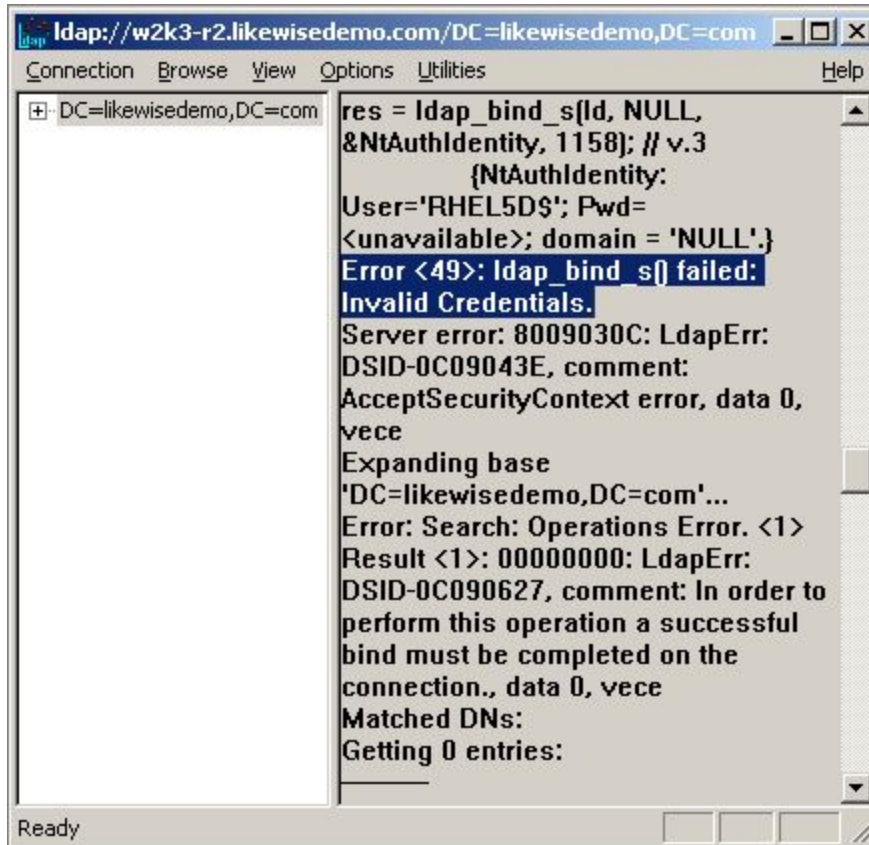
To resolve a user-right issue, you can use group policy modeling in the GPMC to find the offending policy and then modify it with the GPOE.

1. On the Likewise client, run the `/opt/likewise/bin/lw-lsa ad-get-machine password` command as root to get the machine password stored in Active Directory:

```
/opt/likewise/bin/lw-lsa ad-get-machine password
Machine Password Info:
  DNS Domain Name: LIKEWISEDEMO.COM
  NetBIOS Domain Name: LIKEWISEDEMO
  Domain SID: S-1-5-21-3190566242-1409930201-3490955248
  SAM Account Name: RHEL5D$
  FQDN: rhel5d.likewisedemo.com
  Join Type: 1
  Key Version: 0
  Last Change Time: 129401233790000000
  Password: i(2H2e41F7tHN275
```

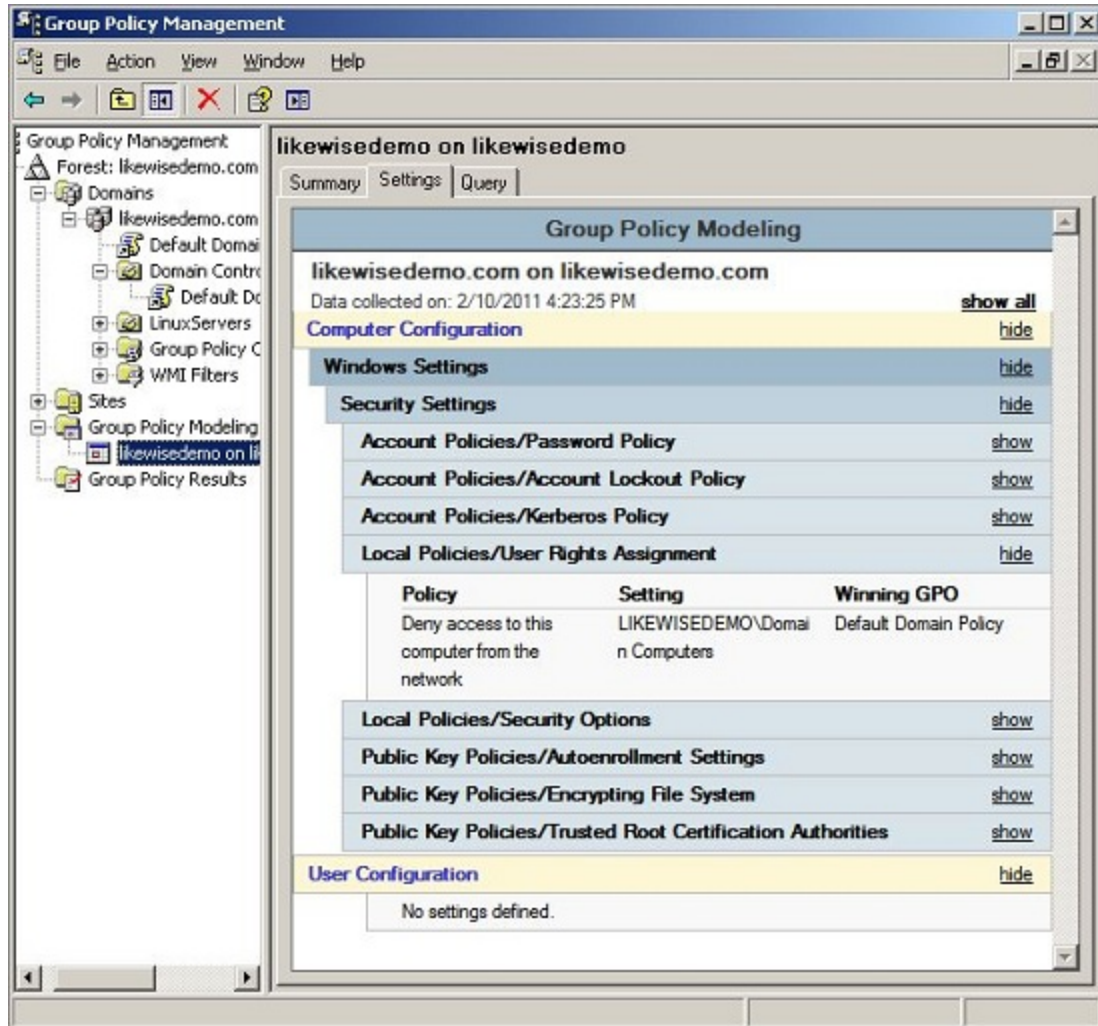
2. On a Windows administrative workstation that can connect to AD, start `ldp.exe` and connect to the domain. (See the LDP UI article for more information.)
3. In LDP, on the **Connection** menu, click **Bind**, and then use the Likewise client's SAM account name and machine password from the output of the `lw-lsa ad-get-machine password` command to bind to the directory.

If the attempt to bind with the machine account and the machine password fails because of invalid credentials, as shown in the LDP output below, go to the Group Policy Management Console and use group policy modeling to try to identify the policy causing the problem.



4. In the GPMC, run the group policy modeling tool to pinpoint the offending policy and then modify the policy to grant the correct level of user right to the computer or user. For more information, see Group Policy Modeling.

In the following screen shot, for example, the cause of the problem is that the deny-access-to-this-computer-from-the-network default domain policy contains the domain computers group.



14.4.7. Fix Selective Authentication in a Trusted Domain

When you turn on selective authentication for a trusted domain, Likewise can fail to look up users in the trusted domain because the machine account is not allowed to authenticate with the domain controllers in the trusted domain. Here's how to grant the machine account access to the trusted domain:

1. In the domain the computer is joined to, create a global group and add the computer's machine account to the group.
2. In the trusted domain, in Active Directory Users and Computers, select the **Domain Controllers** container and open **Properties**.
3. On the **Security** tab, click **Advanced**, click **Add**, enter the global group, and then click **OK**.
4. In the **Permission Entry** box, under **Apply onto**, select **Computer objects**. Under **Permissions**, find **Allowed to Authenticate** and enable it. Click **OK** and then click **Apply** in the **Advanced Security Settings** box.
5. If you have already joined the Likewise client computer to the domain, restart the Likewise authentication service:

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

14.5. Cache

14.5.1. Clear the Authentication Cache

There are certain conditions under which you might need to clear the cache so that a user's ID is recognized on a target computer.

By default, the user's ID is cached for 4 hours. If you change a user's UID for a Likewise cell with Likewise Enterprise, during the 4 hours after you change the UID you must clear the cache on a target computer in the cell before the user can log on. If you do not clear the cache after changing the UID, the computer will find the old UID until the cache expires.

There are three Likewise Enterprise group policies that can affect the cache time:

- The Cache Expiration Time, which stores UID-SID mappings, user/group enumeration lists, `getgrnam()` and `getpwnam()`, and so forth. Its default expiration time is 4 hours.
- The ID Mapping Cache Expiration Time, which caches the mapping tables for SIDs, UIDs, and GIDs. Its default is 1 hour. This policy applies only to Likewise Enterprise 4.1 or earlier.
- The ID Mapping Negative Cache Expiration Time, which stores failed SID-UID-GID lookups to prevent an overload of resolution requests. Its default is 5 minutes. This policy applies only to Likewise Enterprise 4.1 or earlier.

Tip: While you are deploying and testing Likewise, set the cache expiration time of the Likewise agent's cache to a short period of time, such as 1 minute.

Clear the Cache on a Unix or Linux Computer

To delete all the users and groups from the Likewise AD provider cache on a Linux or Unix computer, execute the following command with superuser privileges:

```
/opt/likewise/bin/lw-ad-cache --delete-all
```

You can also use the command to enumerate users in the cache, which may be helpful in troubleshooting. Here's an example:

```
[root@rhel5d bin]# ./lw-ad-cache ---enum-users
TotalNumUsersFound:      0
[root@rhel5d bin]# ssh likewisedemo.com\hab@localhost
Password:
Last login: Tue Aug 11 15:30:05 2009 from rhel5d.likewisedemo.com
[LIKEWISEDEMO\hab@rhel5d ~]$ exit
logout
Connection to localhost closed.
[root@rhel5d bin]# ./lw-ad-cache ---enum-users
User info (Level-0):
=====
Name:      LIKEWISEDEMO\hab
Uid:      593495196
Gid:      593494529
Gecos:    <null>
```

```
Shell:    -/bin/bash
Home dir: -/home/LIKEWISEDEMO/hab
TotalNumUsersFound:    1
[root@rhel5d bin]#
```

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

```
/opt/likewise/bin/lw-ad-cache --help
```

Clear the Cache on a Mac OS X Computer

On a Mac OS X computer, clear the cache by running the following command with superuser privileges in Terminal:

```
dscacheutil -flushcache
```

14.5.2. Clear a Corrupted SQLite Cache

To clear the cache when Likewise is caching credentials in its SQLite database and the entries in the cache are corrupted, use the following procedure for your type of operating system.

Clear the Cache on a Linux Computer

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

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

2. Clear the AD-provider cache and the local-provider cache by removing the following two files:

```
rm -f /var/lib/likewise/db/lsass-adcache.db
```

```
rm -f /var/lib/likewise/db/lsass-local.db
```

Important: Do not delete the other .db files in the /var/lib/likewise/db directory.

3. Start the Likewise authentication daemon:

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

Clear the Cache on a Mac

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

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

2. Clear the AD-provider cache and the local-provider cache by removing the following two files:

```
sudo rm -f /var/lib/likewise/db/lsass-adcache.db
```

```
sudo rm -f /var/lib/likewise/db/lsass-local.db
```

Important: Do not delete the other .db files in the /var/lib/likewise/db directory.

3. Restart the Likewise authentication daemon:

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

Clear the Cache on a Unix Computer

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

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

2. Clear the AD-provider cache and the local-provider cache by removing the following two files:

```
rm -f /var/lib/likewise/db/lsass-adcache.db
```

```
rm -f /var/lib/likewise/db/lsass-local.db
```

Important: Do not delete the other .db files in the /var/lib/likewise/db directory.

3. Start the Likewise authentication daemon:

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

14.6. Kerberos

The following resources can help troubleshoot time synchronization and other Kerberos issues:

- Kerberos Authentication Tools and Settings:

<http://technet2.microsoft.com/windowsserver/en/library/b36b8071-3cc5-46fa-be13-280aa43f2fd21033.mspx>

- Authentication Errors Caused by Unsynchronized Clocks:

<http://technet2.microsoft.com/windowsserver/en/library/6ee8470e-a0e8-40b2-a84f-dbec6bcbd8621033.mspx>

- Kerberos Technical Supplement for Windows:

<http://msdn2.microsoft.com/en-us/library/aa480609.aspx>

- The Kerberos Network Authentication Service (V5) RFC:

<http://www.ietf.org/rfc/rfc4120.txt>

- Troubleshooting Kerberos Errors:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/tkerberr.mspx>

- Kerberos and LDAP Troubleshooting Tips:

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

14.6.1. Fix a Key Table Entry-Ticket Mismatch

Problem

When an AD machine account password changes two or more times during the lifetime of a domain user's credentials, the computer's entry that matches the Kerberos service ticket is dropped from the

Kerberos key table. Even though the service ticket has not expired, an action that depends on the entry, such as reading the event log or using single sign-on, will fail.

To avoid issues with Kerberos key tables, keytabs, and single sign-on, the machine password expiration time must be at least twice the maximum lifetime for user tickets, plus a little more time to account for the permitted clock skew.

The expiration time for a user ticket is set by using an Active Directory group policy called Maximum lifetime for user ticket. The default user ticket lifetime is 10 hours; the default Likewise machine password lifetime is 30 days.

Causes

The machine account password can change more frequently than the user's AD credentials under the following conditions:

1. Joining a domain two or more times.
2. Setting the expiration time of the machine account password group policy to be less than twice the maximum lifetime of user tickets. For more information, see [Set the Machine Account Password Expiration Time](#).
3. Setting the local `machine-password-lifespan` for the `lsass` service in the Likewise registry to be less than twice the maximum lifetime for user tickets.

Solution

If a computer's entry is dropped from the Kerberos key table, you must remove the unexpired service tickets from the user's credentials cache by reinitializing the cache. Here's how:

On Linux and Unix, reinitialize the credentials cache by executing the following command with the account of the user who is having the problem:

```
/opt/likewise/bin/kinit
```

On Mac, you must run both the native `kinit` command and the Likewise `kinit` command with the account of the user who is having the problem. You must run both commands because the native `ssh` client uses the native credentials cache while the Likewise processes, such as those that access the event log, use the MIT credentials cache:

```
/opt/likewise/bin/kinit
kinit
```

14.6.2. Fix KRB Error During SSO in a Disjoint Namespace

When you are working in a network with a disjoint namespace in which the Active Directory domain name is different from the DNS domain suffix for computers, you may need to modify the `domain_realm` section of `/etc/krb5.conf` on your target computer even though your DNS A and PTR records are correct for both DNS domains and can be found both ways.

The following error, in particular, indicates that you might have to modify your `krb5.conf` file before single sign-on (with SSH, for example) will work:

```
KRB ERROR BAD OPTION
```


Assume your computer's Active Directory domain is `bluesky.likewisedemo.com` and your computer's FQDN is `somehostname.green.likewisedemo.com` and you have already created the following entries in DNS:

```
_kerberos._tcp.green.likewisedemo.com 0 100 389
ad2.bluesky.likewisedemo.com
_kerberos._udp.green.likewisedemo.com 0 100 389
ad2.bluesky.likewisedemo.com
```

Meantime, on the target computer, the `[domain_realm]` entry of your `/etc/krb5.conf` file looks like this:

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

To resolve the error, add the following two lines to the `[domain_realm]` entry of your `/etc/krb5.conf` file:

```
.green.likewisedemo.com = BLUESKY.LIKEWISEDEMO.COM
green.likewisedemo.com = BLUESKY.LIKEWISEDEMO.COM
```

After adding the two lines above, the complete `[domain_realm]` entry now looks like this:

```
[domain_realm]
.bluesky.likewisedemo.com = BLUESKY.LIKEWISEDEMO.COM
bluesky.likewisedemo.com = BLUESKY.LIKEWISEDEMO.COM
.green.likewisedemo.com = BLUESKY.LIKEWISEDEMO.COM
green.likewisedemo.com = BLUESKY.LIKEWISEDEMO.COM
```

Finally, make sure that you have a correct `.k5login` file and then try to log on again.

14.6.3. Eliminate Logon Delays When DNS Connectivity Is Poor

If connectivity to your DNS servers is tenuous or becomes unavailable, name resolution can time out, delaying the logon process. Because Active Directory is heavily dependent on a well-functioning DNS system, you should work to resolve your DNS issues.

If you cannot fix your DNS system, however, you can as a last resort set up a caching-forwarding name server on the Likewise client to eliminate the logon delay. For instance, you can set up a BIND server on each Linux or Unix computer on which you are running Likewise. Then you can configure BIND as a local caching resolver and add your nameserver addresses to the forwarder list, leaving `/etc/resolv.conf` with only the local loopback address:

```
search likewisedemo.com
nameserver 127.0.0.1
```

For instructions on how to set up BIND, see the BIND documentation.

14.7. PAM

For instructions on how to generate a PAM debug log, see the section on Logging.

14.7.1. Dismiss the Network Credentials Required Message

After leaving the screen saver on a Gnome desktop that is running the Gnome Display Manager, or GDM, you might see a pop-up notification saying that network authentication is required or that network credentials are required. You can ignore the notification. The GDM process that tracks the expiration time of a Kerberos TGT might not recognize the updated expiration time of a Kerberos TGT after it is refreshed by Likewise.

14.8. Red Hat and CentOS

14.8.1. Modify PAM to Handle UIDs Less Than 500

By default, the configuration file for PAM system authentication – `/etc/pam.d/system-auth` – on Red Hat Enterprise Linux 5 and CentOS 5 contains the following line, which blocks a user with a UID value less than or equal to 500 from logging on to a computer running the Likewise agent. The symptom is a login failure with a never-ending password prompt.

```
auth requisite pam_succeed_if.so uid >= 500 quiet
```

Solution: Either delete the line from `/etc/pam.d/system-auth` or modify it to allow users with UIDs lower than 500:

```
auth requisite pam_succeed_if.so uid >= 50 quiet
```

For more information on the PAM test of account characteristics, see http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/sag-pam_succeed_if.html.

14.9. SLED

14.9.1. A Note About the Home Directory on SLED 11

SUSE Linux Enterprise Desktop 11 includes Likewise Enterprise. When a user gains access to SLED 11 through Nomad -- a remote desktop using RDP protocol with session management -- the default home directory specified in `/lib/security/pam_lsass.so` is ignored. To correct the issue, change `/etc/pam.d/xrdp-sesman` to include the following line:

```
session sufficient /lib/security/pam_lsass.so
```

14.9.2. Updating PAM on SLED 11

SUSE Linux Enterprise Desktop 11 includes Likewise Enterprise. Novell has issued a PAM update (pam-config-0.68-1.22) for SLED 11 that modifies the `common-session-pc` file to include the following entry:

```
session optional pam_gnome_keyring.so auto_start_if=gdm
```

Because the PAM update makes a backup of the file and replaces it with the modified version, the changes that Likewise had made to the file are no longer present, which blocks new AD users from logging on. The following error messages may appear:

```
Could not update ICEauthority file -/home/john/.ICEauthority
```

There is a problem with the configuration server.
 (/user/lib/gconf/2/gconf-sanity-check-2 exited with status 256)

Solution: After you update PAM, run the following command as root:

```
/opt/likewise/bin/domainjoin-cli configure --enable pam
```

Or, you can make the changes manually: Open the backed up version of the common-session-pc file, add the following line to it, and then use it to overwrite the new version of the common-session-pc file:

```
session optional          pam_gnome_keyring.so      auto_start_if=gdm
```

14.10. AIX

14.10.1. Increase Max Username Length on AIX

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

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

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

Example:

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

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

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

You must reboot for the changes to take effect:

```
# shutdown -Fr
```

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

14.10.2. Updating AIX

When you update AIX, the authentication of users, groups, and computers might fail because the AIX upgrade process overwrites changes that Likewise makes to system files. Specifically, upgrading AIX to version 6.1tl3 overwrites `/lib/security/methods.cfg`, so you must manually add the following code to the last lines of the file after you finish upgrading:

```
LSASS:
  program = -/usr/lib/security/LSASS
```

14.11. Mac OS X

14.11.1. Find the Likewise Service Manager Daemon on a Mac

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

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

On a Mac computer, the name of the daemon for the service manager is as follows:

```
com.likewiseoftware.lwsmd
```

14.12. FreeBSD

14.12.1. Keep Usernames to 16 Characters or Less

On FreeBSD, user names that are longer than 16 characters, including the domain name, exceed the FreeBSD username length limit. Attempts to connect by ssh, for example, to a FreeBSD computer with a user name that exceeds the limit can result in the following notification:

```
bvt-fbs72-64# ssh testuser1@localhost
Password:
Connection to localhost closed by remote host.
Connection to localhost closed.
```

The log for sshd, meanwhile, might show an error that looks something like this:

```
Oct  7 18:22:57 vermont02 sshd[66387]: setlogin(LIKEWISEDEMO
\adm.kathy):
Invalid argument
Oct  7 18:25:02 vermont02 sshd[66521]: setlogin(LIKEWISEDEMO
\adm.kathy):
Invalid argument
```

Although `testuser1` is less than 16 characters, when you use the `id` command to check the account, something longer than 16 characters is returned:

```
[root@bvt-fbs72-64 ~/home/testuser]# id testuser1
uid=1100(BVT-FBS72-64\testuser1) gid=1801(BVT-FBS72-64\testgrp)
groups=1801(BVT-FBS72-64\testgrp)
```

The result of the `id` command exceeds the FreeBSD username length limit.

There are several solutions: set the default domain, change the user name to 16 characters or less, or with Likewise Enterprise use aliases. Keep in mind, though, that aliases will not solve the problem in relation to the Likewise local provider.

14.13. Solaris

14.13.1. Turn On Core Dumps on Solaris 10

If you are investigating a process that is crashing on Solaris 10 or Solaris Sparc 10, but a core dump is not being generated, it's probably because per-process core dumps are turned off. You can use the `coreadm` command to manage the core dumps. The settings are saved in the `/etc/coreadm.conf` file.

A configuration for core dumps with the per-process option turned off looks like this:

```
# coreadm
```

```
global core file pattern:  
global core file content: default  
  init core file pattern: core  
  init core file content: default  
    global core dumps: disabled  
    per-process core dumps: disabled  
  global setid core dumps: disabled  
per-process setid core dumps: disabled  
  global core dump logging: disabled
```

You'll need per-process core dumps, though, to troubleshoot a process that is terminating unexpectedly. To turn on core dumps for a process, execute the following command as root:

coreadm -e process

For more information, see Core Dump Management on the Solaris OS and the man page for `coreadm`.

Chapter 15. Command-Line Reference

This chapter presents an overview of the commands in `/opt/likewise/bin`. Most of the commands are intended to be run as root. Additional troubleshooting information, some of which involves command-line utilities, is in *Troubleshooting the Agent*.

The group policy commands for Likewise Enterprise are not included in this chapter; they are in *Troubleshooting the Group Policy Agent*. The commands for managing the event log are in *Monitoring Events with the Event Log*.

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

15.1. 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 instance, check the status of the services and start or stop them. The service manager is the preferred method for restarting a service because it automatically identifies a service's dependencies and restarts them in the right order. In addition, you can use the service manager to set the logging destination and the log level.

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

`/opt/likewise/bin/lwsmd list`

Example:

```
[root@rhel15d 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, run the following command:

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

15.2. **lwconfig**

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

```
/opt/likewise/bin/lwconfig
```

For more information, see [Modify Settings with the `lwconfig` Tool](#).

15.3. **lwregshell: The Registry Shell**

You can access and modify the Likewise registry by using the registry shell -- `lwregshell`. The shell works in a way that is similar to BASH. You can view a list of the commands that you can execute in the shell by entering `help`:

```
/opt/likewise/bin/lwregshell
\> help
```

You can also manage the registry by executing the registry's commands from the command line. For more information, see [Configuring the Likewise Services with the Registry](#).

15.4. **lw-edit-reg: Export the Registry to Your Editor**

Executing the following command exports the contents of the Likewise registry to the editor specified by your `EDITOR` environment variable. You can use the `lw-edit-reg` command to quickly view the contents of the registry and make changes to the settings. Then, you can launch the registry shell and import the modified file so that your changes take effect.

```
/opt/likewise/bin/lw-edit-reg
```

If you have not set a default editor, the script searches for an available editor in the following order: `gedit`, `vi`, `friends`, `emacs`. On platforms without `gedit`, an error may occur. You can correct the error by setting the `EDITOR` environment variable to an available editor, such as `vi`:

```
export EDITOR=vi
```

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

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

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

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

The log level is changed only until the authentication service (`lsass`) or the computer restarts. Syslog messages are logged through the daemon facility. The default setting is `error`.

15.6. lw-set-machine-name: Change the Hostname in the Local Provider

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

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

15.7. Find a User or a Group

On a Unix or Linux computer that is joined to an Active Directory domain, you can check a domain user's or group's information by either name or ID. These commands can verify that the client can locate the user or group in Active Directory.

Find a User by Name

Execute the following command, replacing `domain\\username` with the full domain user name or the single domain user name of the user that you want to check:

```
/opt/likewise/bin/lw-find-user-by-name domain\\username
```

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

You can optionally specify the level of detail of information that is returned. Example:

```
/opt/likewise/bin/lw-find-user-by-name ---level 2 likewisedemo\\hab
User info (Level-2):
=====
Name:                LIKWISEDEMO\\hab
UPN:                 hab@likewisedemo.com
Uid:                 593495196
Gid:                 593494529
Gecos:               Jorgen Habermas
Shell:               -/bin/sh
Home dir:            -/home/LIKWISEDEMO/hab
LMHash length:      0
NTHash length:      0
Local User:         NO
```



```
Account disabled:          FALSE
Account Expired:          FALSE
Account Locked:           FALSE
Password never expires:   TRUE
Password Expired:         FALSE
Prompt for password change: YES
```

For more information, execute the following command:

```
/opt/likewise/bin/lw-find-user-by-name --help
```

Find a User by UID

To find a user by UID, execute the following command, replacing UID with the user's ID:

```
/opt/likewise/bin/lw-find-user-by-id UID
```

Example:

```
/opt/likewise/bin/lw-find-user-by-id 593495196
```

Find a Group by Name

```
/opt/likewise/bin/lw-find-group-by-name domain\username
```

Example:

```
/opt/likewise/bin/lw-find-group-by-name likewisedemo.com\dnsadmins
```

Find a Group by ID

```
/opt/likewise/bin/lw-find-group-by-id GID
```

Example:

```
[root@rhel14d 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
```

15.8. Find a User by a SID

On a Linux, Unix, or Mac OS X computer that is joined to a domain, you can find a user in Active Directory by his or her security identifier (SID). To find a user by SID, execute the following command as root, replacing SID with the user's security identifier:

```
/opt/likewise/bin/lw-find-by-sid SID
```

Example:

```
[root@rhel4d bin]# /opt/likewise/bin/lw-find-by-sid
S-1-5-21-382349973-3885793314-468868962-1180
User info (Level-0):
=====
Name:      LIKEWISEDEMO\hab
SID:      S-1-5-21-382349973-3885793314-468868962-1180
Uid:      593495196
Gid:      593494529
Gecos:    Jurgen Habermas
Shell:    -/bin/ sh
Home dir: -/home/ LIKEWISEDEMO/ hab
```

Tip: To view the command's options, type the following command:

```
/opt/likewise/bin/lw-find-by-sid --help
```

15.9. List Groups for a User

To find the groups that a user is a member of, execute the following command followed by either the user's name or UID:

```
/opt/likewise/bin/lw-list-groups-for-user
```

Example: `/opt/likewise/bin/lw-list-groups-for-user 593495196`

Here's the command and its result for the user `likewisedemo\hab`:

```
[root@rhel5d bin]# ./lw-list-groups-for-user likewisedemo\hab
Number of groups found for user -'likewisedemo\hab' -: 2
Group[1 of 2] name = LIKEWISEDEMO\enterprise^admins (gid = 593494535)
Group[2 of 2] name = LIKEWISEDEMO\domain^users (gid = 593494529)
```

Tip: To view this command's options, type the following command:

```
/opt/likewise/bin/lw-list-groups-for-user --help
```

15.10. lw-enum-groups: List Groups

On a Linux, Unix, or Mac OS X computer that is joined to a domain, you can enumerate the groups in Active Directory and view their members, GIDs, and SIDs:

```
/opt/likewise/bin/lw-enum-groups --level 1
```

The Likewise agent enumerates groups in the primary domain. Groups in trusted domains and linked cells are not enumerated. NSS membership settings in the registry do not affect the result of the command.

Tip: To view the command's options, type the following command:

```
/opt/likewise/bin/lw-enum-groups --help
```

15.11. lw-enum-users: List Users

On a Linux, Unix, or Mac OS X computer that is joined to a domain, you can enumerate the users in Active Directory and view their members, GIDs, and SIDs:

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

The Likewise agent enumerates users in the primary domain. Users in trusted domains and linked cells are not enumerated. NSS membership settings in the registry do not affect the result of the command.

Tip: To view the command's options, type the following command:

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

To view full information about the users, include the `level` option when you execute the command:

```
/opt/likewise/bin/lw-enum-users --level 2
```

Example result for a one-user batch:

```
User info (Level-2):
=====
Name:                LIKWISEDEMO\sduval
UPN:                 SDUVAL@LIKWISEDEMO.COM
Generated UPN:       NO
Uid:                 593495151
Gid:                 593494529
Gecos:               Shelley Duval
Shell:               -/bin/sh
Home dir:            -/home/LIKWISEDEMO/sduval
LMHash length:      0
NTHash length:      0
Local User:         NO
Account disabled:   FALSE
Account Expired:    FALSE
Account Locked:     FALSE
Password never expires: FALSE
Password Expired:   FALSE
Prompt for password change: NO
```

15.12. lw-get-status: View the Status of the Authentication Providers

Likewise includes two authentication providers:

1. A local provider
2. An Active Directory provider

If the AD provider is offline, you will be unable to log on with your AD credentials. To check the status of the authentication providers, execute the following command as root:

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

A healthy result should look like this:

```
LSA Server Status:
Agent version: 5.4.0
Uptime:        22 days 21 hours 16 minutes 29 seconds
[Authentication provider: lsa-local-provider]
```

```
Status:    Online
Mode:     Local system
[Authentication provider: lsa-activedirectory-provider]
Status:    Online
Mode:     Un-provisioned
Domain:   likewisedemo.com
Forest:   likewisedemo.com
Site:     Default-First-Site-Name
```

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

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

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

To check the status of the daemons, run the following command as root:

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

15.13. Get the Current Domain

This command retrieves the Active Directory domain to which the computer is connected. The command's location is as follows:

```
/opt/likewise/bin/lw-lsa ad-get-machine account
```

15.14. lw-get-dc-list: List Domain Controllers

This command lists the domain controllers for a target domain. You can delimit the list in several ways, including by site. The command's location is as follows:

```
/opt/likewise/bin/lw-get-dc-list
```

Example usage:

```
[root@rhel5d bin]# ./lw-get-dc-list likewisedemo.com
Got 1 DCs:
=====
DC 1: Name = -'steveh-dc.likewisedemo.com', Address
= -'192.168.100.132'
```

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

```
/opt/likewise/bin/lw-get-dc-list --help
```

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

This command displays the name of the current domain controller for the domain you specify. The command can help you select a domain controller. The command's location is as follows:

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

To select a domain controller, run the following command as root until the domain controller you want is displayed. Replace DomainName with the name of your domain:

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

15.16. lw-get-dc-time: Get Domain Controller Time

This command displays the time of the current domain controller for the domain that you specify. The command can help you determine whether there is a Kerberos time-skew error between a Likewise client and a domain controller. The command's location is as follows:

/opt/likewise/bin/lw-get-dc-time

Example:

```
[root@rhel15d bin]# ./lw-get-dc-time likewisedemo.com
DC TIME: 2009-09-08 14:54:18 PDT
```

15.17. lw-get-log-info

This command displays the logging status of the Likewise authentication service. The location of the command is as follows:

/opt/likewise/bin/lw-get-log-info

Example output:

```
[root@rhel15d bin]# ./lw-get-log-info
Current log settings:
=====
LSA Server is logging to syslog
Maximum allowed log level: error
```

15.18. lw-get-metrics

This command displays local security events from the Likewise event log. For information about using the log, see Monitoring Events. The location of the command is as follows:

/opt/likewise/bin/lw-get-metrics

Example output:

```
[root@rhel15d 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
```

15.19. Get Machine Account Information

You can print out the machine account name, machine account password, SID, and other information by running the following command as root.

```
/opt/likewise/bin/lw-lsa ad-get-machine account domainDNSName
```

Example: `/opt/likewise/bin/lw-lsa ad-get-machine account
likewisedemo.com`

15.20. Reload Changes to the Configuration File

After you change a setting in the registry for the Likewise agent, you must force the agent to load the change by executing the following command with super-user privileges:

```
/opt/likewise/bin/lw-refresh-configuration
```

15.21. lw-trace-info: Turn on Trace Markers in Log Messages

This command turns on trace markers in the messages logged by the `lwiod` and `lsassd` daemons. You can use the command to obtain more debugging information than that provided by the log level for debugging.

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

Example usage:

```
/opt/likewise/bin/lw-lsa trace-info --set user-group-  
queries:0,authentication:1 --get user-group-administration
```

To view this command's options, type the following command:

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

15.22. lw-update-dns: Dynamically Update DNS

This command registers an IP address for the computer in DNS. The command is useful when you want to register A and PTR records for your computer and the DHCP server is not registering them.

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

Here's an example of how to use it to register an IP address:

```
/opt/likewise/bin/lw-update-dns --ipaddress 192.168.100.4 --fqdn  
corp.likewisedemo.com
```

If your system has multiple NICs and you are trying to register all their IP addresses in DNS, run the command once with multiple instances of the `ipaddress` option:

```
/opt/likewise/bin/lw-update-dns --fqdn corp.likewisedemo.com --
ipaddress 192.168.100.4 --ipaddress 192.168.100.7 --ipaddress
192.168.100.9
```

To troubleshoot, you can add the `loglevel` option with the `debug` parameter to the command:

```
/opt/likewise/bin/lw-update-dns --loglevel debug --fqdn
corp.likewisedemo.com --ipaddress 192.168.100.4 --ipaddress
192.168.100.7
```

For more information on the command's syntax and arguments, execute the following command:

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

15.23. `lw-ad-cache`: Manage the AD Cache

This command manages the Likewise cache for Active Directory users and groups on Linux and Unix computers. The command's location is as follows:

```
/opt/likewise/bin/lw-ad-cache
```

You can use the command to clear the cache. The command's arguments can delete from the cache a user, a group, or all users and groups. The following example demonstrates how to delete all the users and groups from the cache:

```
/opt/likewise/bin/lw-ad-cache --delete-all
```

Tip: To reclaim disk space from SQLite after you clear the cache when you are using the non-default SQLite caching option, execute the following command as root, replacing `fqdn` with your fully qualified domain name:

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

You can also use the `lw-ad-cache` command to enumerate users in the cache, which may be helpful in troubleshooting. Example:

```
[root@rhel5d bin]# ./lw-ad-cache ---enum-users
TotalNumUsersFound:      0
[root@rhel5d bin]# ssh likewisedemo.com\hab@localhost
Password:
Last login: Tue Aug 11 15:30:05 2009 from rhel5d.likewisedemo.com
[LIKEWISEDEMO\hab@rhel5d ~]$ exit
logout
Connection to localhost closed.
[root@rhel5d bin]# ./lw-ad-cache ---enum-users
User info (Level-0):
=====
Name:      LIKEWISEDEMO\hab
Uid:      593495196
Gid:      593494529
Gecos:    <null>
Shell:    -/bin/bash
Home dir: -/home/LIKEWISEDEMO/hab
```

```
TotalNumUsersFound:      1
[root@rhel5d bin]#
```

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

```
/opt/likewise/bin/lw-ad-cache --help
```

Clear the Cache on a Mac OS X Computer

On a Mac OS X computer, clear the cache by running the following command with superuser privileges in Terminal:

```
dscacheutil -flushcache
```

15.24. domainjoin-cli: Join or Leave a Domain

`domainjoin-cli` is the command-line utility for joining or leaving a domain. For instructions on how to use it, see [Join Active Directory with the Command Line](#).

15.25. lw-ypcat

This command is the Likewise NIS ypcat function for group passwd and netgroup maps.

```
/opt/likewise/bin/lw-ypcat
```

Example usage:

```
/opt/likewise/bin/lw-ypcat -d likewisedemo.com -k map-name
```

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

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

15.26. lw-yptest

This command is the Likewise NIS yptest function for group passwd and netgroup maps.

```
/opt/likewise/bin/lw-yptest
```

Example usage:

```
/opt/likewise/bin/lw-yptest -d likewisedemo.com -k key-name map-name
```

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

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

15.27. lw-adtool: Modify Objects in AD

Likewise Enterprise includes a tool to modify objects in Active Directory from the command line of a Linux, Unix, or Mac OS X computer. Located at `/opt/likewise/bin/lw-adtool`, the tool has two interrelated functions:

- Query and modify objects in Active Directory.
- Find and manage objects in Likewise cells.

You can view a list of these two categories by executing the following command:

```
/opt/likewise/bin/lw-adtool --help -a
```

Here's what the output of the command looks like:

```
[root@rhel5d bin]# ./lw-adtool ---help --a

List of Actions

Generic Active Directory actions:
-----

add-to-group -- add a domain user/group to a security group.
delete-object -- delete an object.
disable-user -- disable a user account in Active Directory.
enable-user -- enable a user account in Active Directory.
lookup-object -- retrieve object attributes.
move-object -- move/rename an object.
new-computer -- create a new computer object.
new-group -- create a new global security group.
new-ou -- create a new organizational unit.
new-user -- create a new user account.
remove-from-group -- remove a user/group from a security group.
reset-user-password -- reset user's password.
search-computer -- search for computer objects, print DNs.
search-group -- search for group objects, print DNs.
search-object -- search for any type of objects using LDAP filter.
search-ou -- search for organizational units, print DNs
search-user -- search for users, print DNs.

Likewise cell management actions:
-----

add-to-cell -- add user/group to a Likewise cell.
delete-cell -- delete a Likewise cell.
edit-cell -- modify Likewise cell properties.
edit-cell-group -- modify properties of a cell's group.
edit-cell-user -- modify properties of a cell's user.
link-cell -- link Likewise cells.
lookup-cell -- retrieve Likewise cell properties.
lookup-cell-group -- retrieve properties of cell's group.
lookup-cell-user -- retrieve properties of cell's user.
new-cell -- create a new Likewise cell.
remove-from-cell -- remove user/group from a Likewise cell.
search-cells -- search for Likewise cells.
unlink-cell -- unlink Likewise cells.
```

To get information about the options for each action, use the following syntax:

```
/opt/likewise/bin/lw-adtool --help -a <ACTION>
```

Here's an example with the information that is returned:

```
/opt/likewise/bin/lw-adtool ---help --a new-user
```

Usage: `lw-adtool [OPTIONS] (-a -|--action) new-user <ARGUMENTS>`

`new-user --` create a new user account.

Acceptable arguments ([X] -- required):

<code>---dn=STRING</code>	DN/RDN of the parent container/ OU containing the
<code>---cn=STRING</code>	user. (use '-' for stdin input) Common name (CN) of the new
<code>---logon-name=STRING</code> (use '-' for stdin	stdin input) Logon name of the new user.
<code>---pre-win-2000-name=STRING</code>	input) [X] Pre Windows-2000 logon name.
<code>---first-name=STRING</code>	First name of the new user.
<code>---last-name=STRING</code>	Last name of the new user.
<code>---description=STRING</code>	Description of the user.
<code>---password=STRING</code> stdin input)	User's password. (use '-' for
<code>---no-password-expires</code> omitted -- user	The password never expires. If must change password on next
logon.	User account will be enabled.
<code>---account-enabled</code> By default it is	disabled on creation

Notes on Using the Tool

Privileges: When you run the tool, you must use an Active Directory account with privileges that allow you to perform the command's action. The level of privileges that you need is set by Microsoft Active Directory and is typically the same as performing the corresponding action in Microsoft Active Directory Users and Computers. For example, to add a user to a security group, you must be a member of a security group, such as the enterprise administrators security group, that has privileges to perform the action.

For more information on Active Directory privileges, permissions, and security groups, see the following references on the Microsoft Technet web site: Active Directory Privileges, Active Directory object permissions, Active Directory Users, Computers, and Groups, Securing Active Directory Administrative Groups and Accounts.

Options There are short and long options. You separate arguments from options with either space or equal sign. If you are not sure about the results of an action you want to execute, run it in read-only mode first (-r). Also it can be useful to set log level to TRACE (-l 5) to see all the execution steps the tool is taking. Authentication SSO by default if the machine is domain-joined. Otherwise, KRB5 via a cached ticket, keytab file, or name/password (unless secure authentication is turned-off (--no-sec)) Name resolution In most cases you can reference objects by FQDN, RDN, UPN, or just names that make sense for a specific action. Use "-" if you want the tool to read values from stdin. This allows you to combine commands via pipes, e.g. search and lookup actions. Multi-forest support You can reference object from a name context (forest) different from the one you are currently connected to, provided that there is a proper trust relation between them. In this way, for instance, you can add a user that lives in one forest to a cell defined in another forest.

Creating a New Cell: When you create a new cell, the tool adds the default primary group (domain users) to the cell. If you are adding a user to the cell and the user has a primary group different from the default group, which is an atypical case, you must add the primary group to the cell, too. The tool does not do it automatically.

Adding Users or Groups Across Domains: If you are adding a user or group to a cell, and the user or group is in a domain different from the one hosting the cell, you must use an account that has write permissions in the cell domain and at least read permissions in the domain hosting the user or group. If, for example, you want to add a user such as CORP\kathy, whose primary group is, say, domain users, to a cell in a domain named CORPQA, two conditions must be met: First, you must be authenticated to the CORPQA domain as a user with administrative rights in the CORPQA domain; second, your user account must exist in the CORP domain with at least read permissions for the CORP domain. Further: Since in this example the primary group of CORP\kathy is CORP\domain users, you must add CORP\domain users to the cell in the CORPQA domain, too.

Automating Commands with a Service Account: To run the tool under a service account, such as a cron job, avoid using krb5 tickets for authentication, especially those cached by the Likewise authentication service in the /tmp directory. The tickets may expire and the tool will not renew them. Instead, it is recommended that you create an entry for the service account in a keytab file and use the keytab file for authentication.

Working with a Default Cell: The tool uses the default cell only when the value of the dn parameter is the root naming context, such as when you use an expression like --dn DC=corp,DC=likewise,DC=com to represent corp.likewise.com.

Options

To view the tool's options and to see examples of how to use them, execute the following command:

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

```
[root@rhel5d bin]# ./lw-adtool ---help
```

```
Usage: lw-adtool [OPTIONS] <ACTION> [ACTION_ARGUMENTS]
```

HELP OPTIONS

```
--u, ---usage           Display brief usage message
--?, ---help           Show this message, help on all
actions (-a), or help on a specific action (-a <ACTION>).
--v, ---version        Print program version and exit.
```

COMMON OPTIONS

```
--l, ---log-level=LOG_LEVEL  Acceptable values: 1 (error),
2(warning), 3(info),
warning).
--q, ---quiet              Suppress printing to stdout. Just
set the return code.
--t, ---print-dn          print-dn option makes an exception.
looked up, modified or   Print DNs of the objects to be
searched for.
--r, ---read-only         Do not actually modify directory
objects when
```

executing actions.

CONNECTION OPTIONS

<code>--s, ---server=STRING</code>	Active Directory server to connect to.
<code>--d, ---domain=STRING</code>	Domain to connect to.
<code>--p, ---port=INT</code>	TCP port number
<code>--m, ---non-schema</code>	Turn off schema mode

AUTHENTICATION OPTIONS

<code>--n, ---logon-as=STRING</code>	User name or UPN.
<code>--x, ---passwd=STRING</code> (use '-' for stdin input)	Password for authentication.
<code>--k, ---keytab=STRING</code> etc/krb5.keytab	Full path of keytab file, e.g. -/etc/krb5.keytab
<code>--c, ---krb5cc=STRING</code> file, e.g.	Full path of krb5 ticket cache file, e.g.

`-/tmp/krb5cc_foo@likewisedemo.com`
Turns off secure authentication.

`--z, ---no-sec`
Simple bind will be

used. Use with caution!

ACTION

<code>--a, ---action[=<ACTION>]</code> a' for a list of	Action to execute. Type <code>'---help --a'</code> for a list of
for information on a	actions, or <code>'---help --a <ACTION>'</code> for information on a
	specific action.

Try `'---help --a'` for a list of actions.

Examples

Here's an example that shows how to use two authentication options `--logon-as` and `passwd` to search Active Directory even though the computer on which the command was executed was not connected to the domain. The account specified in the `logon-as` option is an Active Directory administrative account.

```
root@ubuntu:/opt/likewise/bin# ./lw-adtool -a search-cells --search-base dc=connecticut,dc=com --logon-as=Administrator --passwd=-
```

In this case, the successful result looked like this:

```
Enter password:
CN=$LikewiseIdentityCell,DC=connecticut,DC=com
CN=$LikewiseIdentityCell,OU=mySecureOU,DC=connecticut,DC=com
Total cells: 2
```

Here are a variety of examples. In some of them, the command is broken into two lines and the line break is marked by a back slash (\). In such cases, the back slash is not part of the command.

```
Create OU in a root naming context:
lw-adtool --a new-ou ---dn OU=TestOu
```

Create OU in DC=department,DC=company,DC=com:

```
lw-adtool --a new-ou ---dn OU=TestOu,DC=department,DC=company,DC=com
```

Create Likewise cell in OU TestOU setting the default login shell property to /bin/ksh:

```
lw-adtool --a new-ou ---dn OU=TestOu ---default-login-shell=/bin/ksh
```

Create a new account for user TestUser in OU=Users,OU=TestOu:

```
lw-adtool --a new-user ---dn OU=Users,OU=TestOu ---cn=TestUserCN ---logon-name=TestUser ---password=$PASSWD
```

Enable the user account:

```
lw-adtool --a enable-user ---name=TestUser
```

Reset user's password reading the password from TestUser.pwd file:

```
cat TestUser.pwd -| lw-adtool --a reset-user-password ---name=TestUser ---password=- ---no-password-expires
```

Create a new group in OU=Groups,OU=TestOu:

```
lw-adtool --a new-group ---dn OU=Groups,OU=TestOu ---pre-win-2000-name=TestGroup ---name=TestGroup
```

Look up -"description" attribute of an OU specified by name with a wildcard:

```
lw-adtool --a search-ou ---name='*RootOu' --t -| lw-adtool --a lookup-object ---dn=- ---attr=description
```

Look up -"unixHomeDirectory" attribute of a user with samAccountName TestUser:

```
lw-adtool --a search-user ---name TestUser --t -| lw-adtool --a lookup-object ---dn=- ---attr=unixHomeDirectory
```

Look up -"userAccountControl" attribute of a user with CN TestUserCN:

```
lw-adtool --a search-user ---name CN=TestUserCN --t -| lw-adtool --a lookup-object ---dn=- ---attr=userAccountControl
```

Look up all attributes of an AD object using filter-based search:

```
lw-adtool --a search-object ---filter -'(&(objectClass=person)(displayName=TestUser))' --t -| lw-adtool --a lookup-object
```

Add user TestUser to group TestGroup:

```
lw-adtool --a add-to-group ---user TestUser ---to-group=TestGroup
```

Add group TestGroup2 to group TestGroup:

```
lw-adtool --a add-to-group ---group TestGroup2 ---to-group=TestGroup
```

Remove user TestUser from group TestGroup:

```
lw-adtool --a remove-from-group ---user TestUser ---from-group=TestGroup
```

Rename AD object OU=OldName and move it to a new location:

```
lw-adtool --a move-object ---from  
OU=OldName,DC=department,DC=company,DC=com \
```

```
--to OU=NewName,OU=TestOU,DC=department,DC=company,DC=com
```

Add group TestGroup to Likewise cell in TestOU:

```
lw-adtool --a add-to-cell ---dn
OU=TestOU,DC=department,DC=company,DC=com ---group=TestGroup
```

Remove user TestUser from Likewise cell in TestOU:

```
lw-adtool --a remove-from-cell ---dn
OU=TestOU,DC=department,DC=company,DC=com ---user=TestUser
```

Search for cells in a specific location:

```
lw-adtool --a search-cells ---search-base
OU=department,DC=country,DC=company,DC=com
```

Link cell in OU=TestOU1 to the default cell in DC=country:

```
lw-adtool --a link-cell ---source-dn
OU=TestOU1,DC=department,DC=company,DC=com \
--target-dn DC=country,DC=company,DC=com
```

Unlink cell in OU=TestOU1 from the default cell in DC=country:

```
lw-adtool --a unlink-cell ---source-dn
OU=TestOU1,DC=department,DC=company,DC=com \
--target-dn DC=country,DC=company,DC=com
```

Change the default login shell property of Likewise cell in TestOU:

```
lw-adtool --a edit-cell ---dn OU=TestOU ---default-login-shell=/bin/
csh
```

Find cells linked to Likewise cell in

```
OU=TestOU,DC=department,DC=company,DC=com:
lw-adtool --a lookup-cell ---dn OU=TestOU ---linked-cells
```

Look up login shell property of user TestUser in cell created in TestOU:

```
lw-adtool --a lookup-cell-user ---dn OU=TestOU ---user TestUser ---
login-shell
```

Change login shell property of user TestUser in cell created in TestOU:

```
lw-adtool --a edit-cell-user ---dn OU=TestOU ---user TestUser ---
login-shell=/usr/bin/ksh
```

Delete a cell object and all its children if any (--force):

```
lw-adtool --a delete-object ---dn OU=TestOU ---force
```

Search for Likewise cells in root naming context containing user TestUser:

```
lw-adtool --a search-cells ---user TestUser
```

15.28. lwio: Input-Output Commands

The commands prefaced with `lwio` are included as part of the Likewise-CIFS technology preview. These commands are not covered under your support contract.

15.28.1. `lwio-copy`: Copy Files Across Disparate Operating Systems

The `lwio-copy` command-line utility lets you copy files across computers running different operating systems. You can, for example, copy files from a Linux computer to a Windows computer.

There two prerequisites to use `lwio-copy`: The `lwiiod` 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
```

15.28.2. `lwio-refresh`: Reload the Input-Output Settings After Changes

The `lwio-refresh` command reloads the configuration for the `lwio` daemon, `lwiiod`. 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
```

15.28.3. `lwio-set-log-level`

This command sets the logging status of the Likewise SMB file server to one of six levels: error, warning, info, verbose, debug, or trace.

To troubleshoot connection problems with `lwiiod` and its redirector, set the log level of `lwiiod` 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
```

15.28.4. `lwio-get-log-info`

This command displays the logging status of the Likewise SMB file server. The location of the tool is as follows:

```
/opt/likewise/bin/lwio-get-log-info
```

Example output:

```
[root@rhel5d bin]# ./lwio-get-log-info
Current log settings:
=====
SMB Server is logging to syslog
Maximum allowed log level: error
```

15.29. Commands to Modify Local Accounts

The Likewise local authentication provider for local users and groups includes a full local authentication database. With functionality similar to the local SAM authentication database on every Windows computer, the local authentication provider lets you create, modify, and delete local users and groups on Linux, Unix, and Mac OS X computers by using the following commands.

To execute the commands that modify local accounts, you must use either the root account or an account that has membership in the local administrators group. The account can be an Active Directory account if you manually add it to the local administrators group. For example, you could add the Domain Administrators security group from Active Directory to the local administrators group, and then use an account with membership in the Domain Administrators security group to execute the commands.

15.29.1. `lw-add-user`: Add a Local User by Name or UID

This command adds a user to the local authentication database. The command's location is as follows:

```
/opt/likewise/bin/lw-add-user
```

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

```
/opt/likewise/bin/lw-add-user --help
```

15.29.2. `lw-add-group`: Add a Local Group Member by Name or GID

This command adds a group member to the local authentication database. The command's location is as follows:

```
/opt/likewise/bin/lw-add-group
```

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

```
/opt/likewise/bin/lw-add-group --help
```

15.29.3. `lw-del-user`: Remove a Local User by Name or UID

This command deletes a user from the local authentication database. The command's location is as follows:

```
/opt/likewise/bin/lw-del-user
```

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

```
/opt/likewise/bin/lw-del-user --help
```


15.29.4. `lw-del-group`: Remove a Local Group by Name or GID

This command deletes a group from the local authentication database. The command's location is as follows:

```
/opt/likewise/bin/lw-del-group
```

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

```
/opt/likewise/bin/lw-del-group --help
```

15.29.5. `lw-mod-user`: Modify a Local User by Name or UID

This command modifies a user's account settings in the local authentication database, including an account's expiration date and password. You can also enable a user, disable a user, unlock an account, or remove a user from a group. The command's location is as follows:

```
/opt/likewise/bin/lw-mod-user
```

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

```
/opt/likewise/bin/lw-mod-user --help
```

15.29.6. `lw-mod-group`: Modify a Local Group's Members

This command adds members to or removes members from a group in the local authentication database. The command's location is as follows:

```
/opt/likewise/bin/lw-mod-group
```

Here's an example that demonstrates how to add domain accounts to a local group:

```
/opt/likewise/bin/lw-mod-group --add-members DOMAIN\\Administrator  
BUILTIN\\Administrators
```

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

```
/opt/likewise/bin/lw-mod-group --help
```

15.30. Kerberos Commands

Likewise includes several command-line utilities for working with Kerberos. It is recommended that you use these Kerberos utilities, located in `/opt/likewise/bin`, to manage those aspects of Kerberos authentication that are associated with Likewise. For complete instructions on how to use the Kerberos commands, see the man page for the command.

15.30.1. `kdestroy`: Destroy the Kerberos Ticket Cache

The `kdestroy` utility destroys the user's active Kerberos authorization tickets obtained through Likewise. Destroying the user's tickets can help solve logon problems.

Note: This command destroys only the tickets in the Likewise Kerberos cache of the user account that is used to execute the `kdestroy` command; tickets in other Kerberos caches, including root, are not destroyed. To destroy another user's cache, use the command with its `-c` option.

To destroy a user's Likewise Kerberos tickets, execute the following command with the user's account:

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

Tip: To view this command's options, type the following command:

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

15.30.2. klist: View Kerberos Tickets

On a target Linux or Unix computer, you can see a list of Kerberos tickets by executing the following command:

```
/opt/likewise/bin/klist
```

The command lists the location of the credentials cache, the expiration time of each ticket, and the flags that apply to the tickets. For more information, see the man page for `klist`.

Because Likewise includes its own Kerberos 5 libraries (in `/opt/likewise/lib`), you must use the Likewise `klist` command by either changing directories to `/opt/likewise/bin` or including the path in the command.

Example:

```
-sh-3.00$ -/opt/likewise/bin/klist
Ticket cache: FILE:/tmp/krb5cc_593495191
Default principal: hoenstiv@LIKEWISEDEMO.COM
Valid starting Expires Service principal
07/22/08 16:07:23 07/23/08 02:06:39  krbtgt/
LIKEWISEDEMO.COM@LIKEWISEDEMO.COM
renew until 07/23/08 04:07:23
07/22/08 16:06:39 07/23/08 02:06:39  host/rhel4d.LIKEWISEDEMO.COM@
renew until 07/23/08 04:07:23
07/22/08 16:06:39 07/23/08 02:06:39  host/
rhel4d.LIKEWISEDEMO.COM@LIKEWISEDEMO.COM
renew until 07/23/08 04:07:23
07/22/08 16:06:40 07/23/08 02:06:39  RHEL4D$@LIKEWISEDEMO.COM
renew until 07/23/08 04:07:23
```

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

15.30.3. kinit: Obtain and Cache a TGT

This command obtains and caches an initial ticket-granting ticket for a principal. The command's location is as follows:

```
/opt/likewise/bin/kinit
```

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

```
man kinit
```

15.30.4. kpasswd: Change a Password

The `kpasswd` command changes a Kerberos principal's password on a Linux or Unix computer. (On a Mac computer, use the Mac OS X graphical user interface to change a Kerberos principal's password.) The command's location is as follows:

/opt/likewise/bin/kpasswd

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

```
man kpasswd
```

15.30.5. ktutil: The Keytab File Maintenance Utility

This command invokes a shell from which you can read, write, or edit entries in a Kerberos keytab. The command's location is as follows:

/opt/likewise/bin/ktutil

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

```
man ktutil
```

You can use `ktutil` to add a keytab file to a non-default location. When you join a domain, Likewise initializes a Kerberos keytab by adding the `default_keytab_name` setting to `krb5.conf` and setting it to `/etc/krb5.keytab`. If the keytab file referenced in `krb5.conf` does not exist, the Likewise domain-join utility changes the setting to `/etc/krb5.conf`.

You can set the keytab file to be in a location that is different from the default. To do so, you must pre-create the keytab file in the location you want and set a symlink to it in `/etc/krb5.keytab`. Then, you must set the `default_keytab_name` in `/etc/krb5.conf` to point to either the symlink or the real file. The result is that the keytab file will already exist and the Likewise domain-join utility will not modify its location setting.

The keytab's format does not let you create a keytab file without a keytab, but you can use `ktutil` to manually create one with a place-holder entry. When Likewise adds your computer to the domain, a correct entry will be added to the file.

```
/opt/likewise/bin/ktutil
ktutil: addent --password --p nonexistent@nonexistent --k 1 --e RC4-
HMAC
Password for nonexistent@nonexistent:
ktutil: wkt -/var/OtherPlace/etc/krb5.keytab
ktutil: quit
```

15.30.6. Kvno: Acquire a Service Ticket and Print Key Version Number

This command acquires a service ticket for the specified Kerberos principals and prints out the key version numbers of each. The command's location is as follows:

/opt/likewise/bin/kvno

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

man kvno

15.31. Commands and Scripts Not for Customer Use

The commands and scripts listed in this section are not for end users. It is recommended that you do not use them.

15.31.1. ConfigureLogin

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

15.31.2. dceidl

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

15.31.3. gpccron

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

15.31.4. gpccron.sh

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

15.31.5. gprsrmtmnt.sh

The group policy agent -- gpagentd -- uses this script to restart the automount service after applying automount policy settings. The script applies different commands to restart the automount service on different operating systems, such as AIX, HP-UX, and Linux.

15.31.6. init-base.sh

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

15.32. Likewise Enterprise Tools Installed on Windows Computers

This section covers the command-line tools that are on a Windows computer running Likewise Enterprise. The commands are in C:\Program Files\Likewise\Enterprise. The command-line tools for the Likewise Enterprise database are discussed in the chapter on setting up the database.

15.32.1. Lwopt.exe

Lwopt.exe lets you manage options for Likewise Enterprise from the command-line of a Windows administrative workstation connected to Active Directory. You can, for example, set an option to use sequential IDs instead of hashed IDs. In addition, after you set the option to use sequential IDs, you

can set the initial UID number for a cell. Setting UIDs below 1,000 is ill-advised, as they can result in a security vulnerability.

```
C:\Program Files\Likewise\Enterprise>lwopt
```

```
lwopt -- configures local Windows options for Likewise
```

```
Usage: lwopt OPTIONS
```

```
OPTIONS:
```

```
  ---status          Show current configuration status
  ---narrowsearch    Only search the default cell on the local
domain
  ---widesearch      Search the default cell across all domains and
two-way forest trusts
  ---sequential      Use sequential IDs instead of hashed IDs
  ---hashed          Use hashed IDs
  ---foreignaliases  Allow the use of aliases for users and groups
from other domains.
  ---noforeignaliases Disallow the use of aliases for users and
groups
```

```
  ---usegc          Use the Global Catalog to speed up searches
(default)
```

```
  ---ignoregc       Do not use the Global Catalog to speed up
searches
```

```
  ---startUID=#     Sets the initial UID number for a cell (if ---
sequential)
```

```
  ---startGID=#     Sets the initial GID number for a cell (if ---
sequential)
```

```
  ---minID=#        Sets minimum UID and GID number configurable
through
```

```
  ---cell=LDAPPATH Identifies the cell whose initial IDs (if ---
sequential)
```

```
Example: LDAP://somedc/ou=anou,dc=somecom,dc=com
```

```
  ---enableloginnames Sets the default login names to all the
users enabled
```

```
in all the cells.
```

```
  ---disableloginnames Disable the enable default login names
option to all
```

```
users enabled in all the cells.
```

```
  ---help          Displays this usage information
```

```
If the ---startUID or ---startGID options are set, the ---cell
option must also
be set.
```

Chapter 16. Leaving a Domain and Uninstalling the Agent

16.1. 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/lssasd.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
```

16.2. Uninstall the Domain Join GUI

On a Linux computer, you can uninstall the domain join GUI from the command line by running the following command as root. The command applies only to Linux computers on which you installed the domain-join GUI as a separate component. In Likewise 6.0 or later, the domain-join GUI is included in the main installation for Linux platforms and cannot be uninstalled separately.

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

16.3. Uninstall the Agent on a Linux or Unix Computer

Important: Before uninstalling the agent, you must leave the domain and uninstall the domain-join GUI if you installed it as a separate component. Then execute the `uninstall` command from a directory other than `likewise` so that the uninstall program can delete the `likewise` directory and all its subdirectories -- for example, execute the command from the root directory.

Uninstall Likewise with the Shell Script on Linux or Unix

If you installed the agent on a Linux or Unix computer by using the shell script, you can uninstall the Likewise agent from the command line by using the same shell script with the `uninstall` option. (To uninstall the agent, you must use the shell script with the same version and build number that you used to install it.) For example, on a Linux computer running `glibc`, change directories to the location of Likewise and then run the following command as root, replacing the name of the script with the version you installed:

```
./LikewiseOpen-6.0.0.94-linux-oldlibc-i386-rpm.sh uninstall
```

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

```
./LikewiseOpen-6.0.0.8011-linux-i386-rpm.sh help
```

Uninstall BitRock Installations on Linux or Unix

On a Linux or Unix computer, you can uninstall the Likewise agent from the command line if you originally installed the agent with the BitRock installer, an installer for previous versions of Likewise.

- To uninstall the agent on a Linux computer running Likewise Enterprise, run the following command as root:

```
/opt/likewise/setup/lwise/uninstall
```

- To uninstall the agent on a Linux computer running Likewise Open, run the following command as root:

```
/opt/likewise/setup/lwiso/uninstall
```

16.4. Uninstall the Agent on a Mac

On a Mac OS X computer, you must uninstall the Likewise agent by using Terminal. Before uninstalling the agent, you should leave the domain.

1. Log on the Mac by using a local account with privileges that allow you to use `sudo`.
2. Open a Terminal window: In Finder, on the **Go** menu, click **Utilities**, and then double-click **Terminal**.
3. At the Terminal shell prompt, execute the following command:

```
sudo /opt/likewise/bin/macuninstall.sh
```

Chapter 17. Using Likewise with Smart Cards

17.1. Smart Card Setup

With Likewise Enterprise, you can secure a Linux computer by using a smart card associated with an Active Directory account. The Likewise authentication service links the smart card's cryptography-based identification with an Active Directory domain account to put in place a strong layer of tamper-resistant security for logging on to a Linux computer. The security can be strengthened by setting Likewise group policies to allow logon only with a smart card and to lock the computer when the card is removed.

Here's what you need to get started:

- A Linux platform supported by the Likewise smart card service.
- An Active Directory system configured to manage smart card logons.
- A smart card prepared with Active Directory credentials and a personal identification number to log on to the Linux computer.
- A CCID-compliant smart card reader.
- Likewise Enterprise 6.0 or later. When you install Likewise Enterprise, you must include the `smartcard` option. The installation includes ActivIdentity's ActivClient smart card software for Linux.

Supported Linux Platforms

Likewise's smart card service supports the 32- and 64-bit versions of the following platforms: Red Hat Enterprise Linux 5.3, 5.4, and 5.5.

You can check the version of your Red Hat computer like this:

```
[root@rhel5d ~]# cat /etc/redhat-release
Red Hat Enterprise Linux Client release 5.5 (Tikanga)
```

Prepare Active Directory for Smart Card Logon

To prepare Active Directory for smart card logon, see the Microsoft web site for information and instructions. If you plan to use Microsoft's certification authority to configure smart card logon, see certificate enrollment using smart cards. If you plan to use a third-party certification authority with Active Directory, see guidelines for enabling smart card logon with third-party certification authorities. For an overview of how to implement smart card authentication, see Checklist: Deploying smart cards.

After you configure Active Directory to handle smart cards, you can use an enrollment station, which is typically a Windows administrative workstation connected to Active Directory, to prepare a smart card with Active Directory credentials and a personal identification number (PIN). Again, for more information, see certificate enrollment using smart cards.

Prepare a Linux Computer for Smart Card Logon

To install the Likewise and ActivIdentity components that support smart cards, you must include the `smartcard` option when you run the Likewise Enterprise installer. If Likewise is already installed, simply run the installer again with the `smartcard` option:

```
./LikewiseEnterprise-6.1.0.375-linux-i386-rpm.sh --smartcard
```

To prepare a Red Hat Enterprise Linux computer for smart card logon with Likewise, two pieces must be in place: ActivIdentity's ActivClient software for Linux, version 3.0 or later, and a CCID-compliant smart card reader.

The ActivClient software, manufactured by ActivIdentity (<http://www.actividentity.com/>), is included with Likewise Enterprise 6.0 or later and automatically installed at `/usr/local/ActivIdentity` when you install the Likewise agent on a Linux computer with the installer's `smartcard` option. You can verify installation by checking for the `ActivIdentity` directory like this:

```
[root@rhel5d ~]# ls -/usr/local
ActivIdentity bin etc games include lib libexec sbin share
src
```

You can verify that you are running ActivClient version 3.0 or later as follows:

```
[root@rhel5d ~]# rpm --qa -| grep activ
ai-activclient-scmw-3.0.0-31
ai-activclient-apps-3.0.0-31
```

The ActivClient software depends on the presence of a package, `pcsc-lite`. To make sure it is installed, execute the following command:

```
rpm -q pcsc-lite
```

Here's an example on Red Hat that shows the presence of the package:

```
[root@rhel5d lw]# rpm --q pcsc-lite
pcsc-lite-1.3.1-7
```

Note: Although Likewise includes the ActivClient software, you must contact ActivIdentity to obtain licenses to use their software for anything other than a 30-day trial.

Likewise accepts the smart cards that are supported by ActivClient. The list of supported cards includes PIV-compliant cards and the Common Access Card (CAC) used by the U.S. government. Check the ActivClient documentation to determine whether the type of smart card you plan to use is supported.

You must install a CCID-compliant smart card reader. The readers are available from a variety of manufacturers. Before you buy a reader, you should check with the vendor to make sure it works with your Linux platform and your type of smart card. Follow the setup instructions from the manufacturer of the smart card reader. For information about CCID-compliant smart card readers, see the USB Chip/Smart Card Interface Devices (CCID) Specification.

When all these pieces are in place, you are ready to install Likewise Enterprise on your Linux computer and add the computer to Active Directory. See the chapters on installing the Likewise agent and joining a domain.

17.2. Log On with a Smart Card

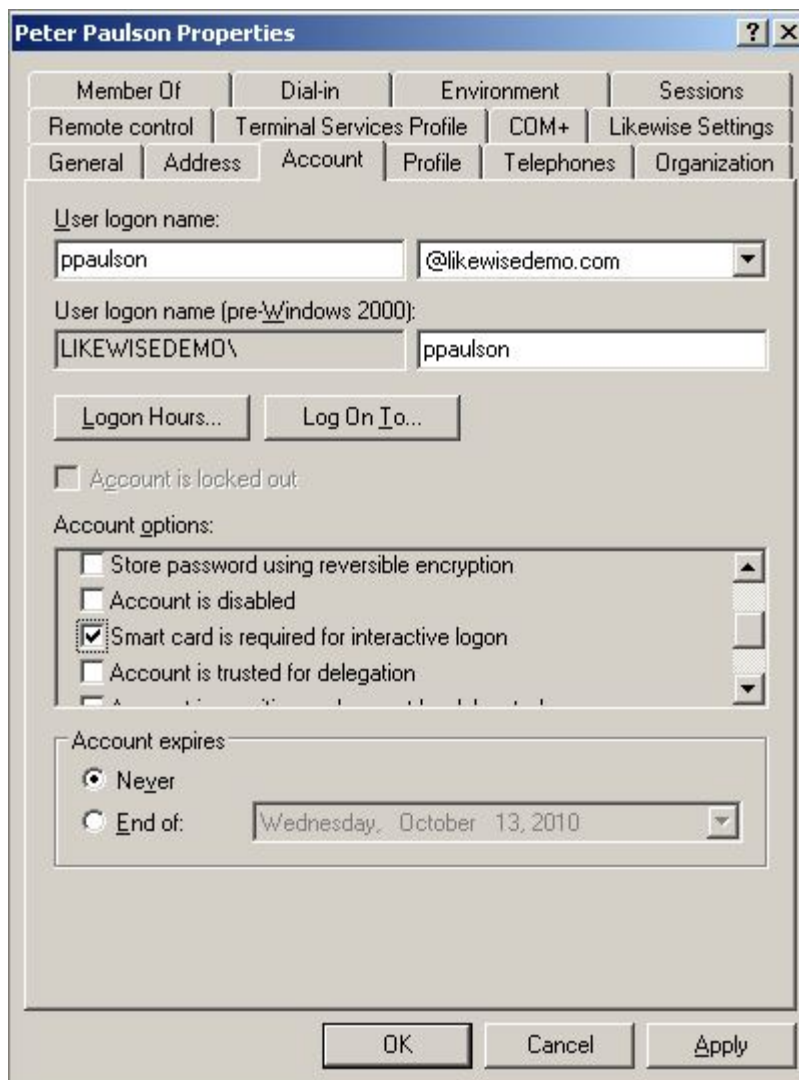
To log on to a computer with a smart card, insert the smart card into the smart card reader. The computer prompts you for your personal identification number (PIN) instead of your domain, user name, and password.

If the PIN you enter is recognized as legitimate, you are logged on to the computer and the domain using the permissions assigned to your user account in Active Directory.

If you enter the incorrect PIN for a smart card several times in a row, you might be unable to log on to the computer with that smart card. The number of allowable invalid logon attempts that can occur before lockout varies by smart card manufacturer and your security policy. If you insert the smart card backward or upside down, the smart card will not be recognized. Smart card logon works only for computers joined to a domain.

Important: With Active Directory, there are two ways to force a user to log on with a smart card:

- On a per-computer basis, by setting a Likewise group policy (which corresponds to a Microsoft group policy with a similar name) to require a smart card to log on to the computers in a Likewise cell. The policy's default is to allow a user to log on with either a smart card and its PIN or a user account and its password. The settings that you choose depend on your IT security policies.
- On a per-user basis, by selecting the option to require a smart card on the Account tab of a user's properties in ADUC, as shown in the following screen shot.



You can generate a log to help troubleshoot problems logging on with a smart card; for more, information, see chapter on troubleshooting the Likewise agent.

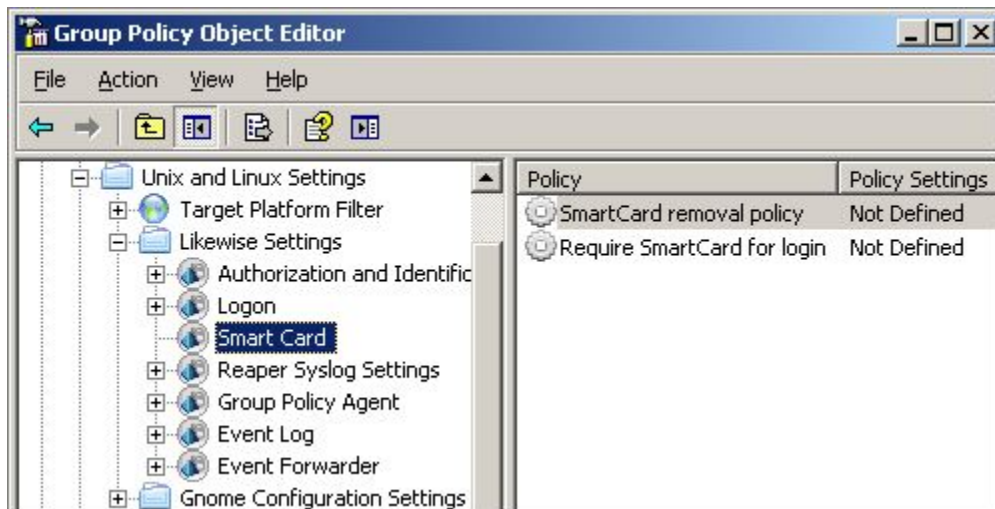
17.3. Smart Card Group Policies

Likewise Enterprise includes the following group policies for managing smart cards on target Linux computers.

Smart Card Group Policy	Description
Require smart card for login	Specifies the requirements for using a smart card to access a target computer. When smart card authentication is enabled, it is possible to log on only with a smart card and its PIN. When this setting is disabled, logon is possible by using either an account user name with a password or a smart card with its PIN.
Smart card removal policy	Specifies the action taken when a smart card is removed from a target computer. When smart card two-factor authentication is used to gain access to a computer, enforcement of logon security can be made stricter if the removal action is set to Lock or Logout. The default setting without this policy is No Action.

Set a Smart Card Group Policy

1. In the Group Policy Management Console, create or edit a group policy for the organization unit that you want, and then open it with the Group Policy Object Editor.
2. In the Group Policy Object Editor, in the console tree under Computer Configuration, expand **Unix and Linux Settings**, expand **Likewise Settings**, and then expand **Smart Card**:



3. In the details pane, double-click the smart card setting that you want, and then select the **Define this Policy Setting** check box.
4. Make the changes that you want:

For This Policy	Do This
Smart card removal policy	In the list, click the option that you want to set.
Require smart card for login	Click Enabled or Disabled .

Chapter 18. Managing Licenses

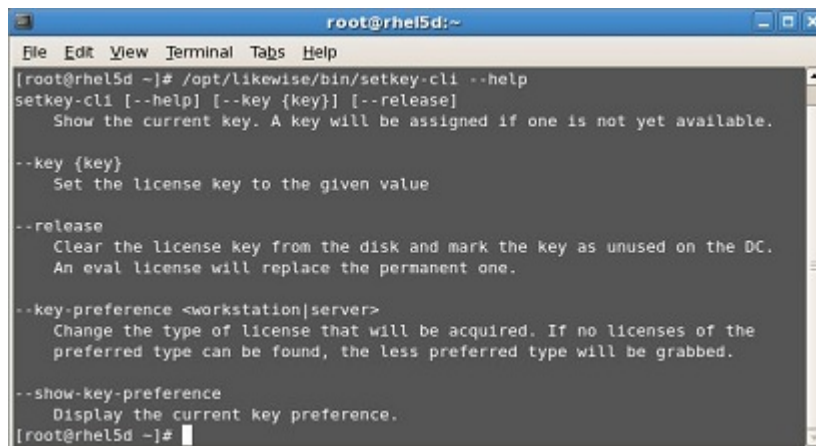
18.1. About Licenses

There are two options to manage the assignment of Likewise licenses:

- Globally, by using the License Management page in the Likewise Management Console on a Windows administrative workstation connected to Microsoft Active Directory. It is recommended that you manage your licenses through the Likewise Management Console.



- Locally, by using a Likewise command-line utility – `setkey-cli --` on a Linux, Unix, or Mac OS X computer.



Evaluation Licenses and Permanent Licenses

When you install the Likewise agent without a permanent license on a Unix or Linux computer, a 30-day product evaluation key is automatically generated. If a permanent license key or an extended evaluation license key is unavailable, Likewise will stop authenticating users and applying group policies after 30 days. The expiration date of an evaluation license applies only to the computer on which the license is installed.

To obtain a permanent license or to convert a trial license to a full license, please contact a Likewise sales representative by sending an email to sales@likewise.com or by calling 1-800-378-1330 in the United States. From outside the United States, call +1-425-378-7887.

You can upgrade an evaluation license to a permanent license by importing the permanent license key into the Likewise Management Console, and applying it to a client computer. If the automatic assignment feature is in use, the Likewise agent will automatically apply a permanent license when you log on a client with an AD account, restart the Likewise authentication service, or run the command-line utility for managing licenses.

Site Licenses and Single-Computer Licenses

Likewise offers site licenses and single-computer licenses. A site license covers all the computers in a domain and its child domains. To determine whether a computer falls under a site license, Likewise checks the last two components of the domain name. If, for example, `likewisedemo.com` is the domain governed by a site license and one of the child domains is named `child.likewisedemo.com`, the child domain is covered by the site license because the last two components of the domain name match.

If there are multiple domains, a different license file is required for each domain, regardless of whether you are using a site license or a set of single-computer licenses. To spread a set of single-computer licenses across two or more domains, you can request Likewise sales to distribute the licenses in two or more license files.

Workstation and Server Licenses

Likewise offers two kinds of licenses: workstation and server. Both single-computer licenses and site licenses distinguish between servers and workstations. When a computer joins a domain, Likewise looks at the version of the operating system to determine whether to assign a workstation or a server license. If a server license is unavailable, a workstation license is automatically used.

A workstation license limits the number of concurrent logins to five discrete user accounts. With a server license, the number of concurrent logins is unlimited. If the computer is a server but is using a workstation license because no server licenses were available, please contact Likewise sales at sales@likewise.com to obtain more server licenses. You can adjust the license type that you want the agent to obtain by using the command-line utility for managing licenses.

The Likewise agent verifies a license when you run the `setkey-cli` utility, when you start the Likewise authentication daemon, and when you log on. To verify a license, the `setkey-cli` utility uses the machine's Active Directory account to search for licenses in the computer's OU hierarchy up to the top of the domain. Other domains in the forest are not searched. If the utility cannot find a license in the OU hierarchy, as a last resort it checks the legacy Likewise container in the `Program Data` container. When the machine's domain controller is down, the utility loads the license from the disk without verifying its assignment in Active Directory.

The Likewise group policy daemon also checks for a license when it refreshes the computer's group policies. If the license is invalid, the daemon ignores the group policy objects. Once the license becomes permanent and valid, the daemon applies the group policy objects when it restarts.

Licenses contain codes that can include or exclude the following features. When a license is displayed in the console, the codes that appear in the Features column indicate the entitlements that the license covers.

License Container: LIKewiseDEMO.COM		
Key	Type	Features ▲
BQNGX-QDV...	Server	SC GP AU AD
ERPYE-PZ5G...	Workstation	SC GP AU AD
FOPWA-PLDZ...	Workstation	SC GP AU AD
HTFMT-5IE4Q...	Workstation	SC GP AU AD
LUWVNZ-JPOS...	Server	SC GP AU AD
NR4QY-R5PO...	Server	SC GP AU AD

The following table describes the meaning of each feature code:

Feature Code	Description
SC	Covers the use of two-factor authentication with a smart card.
GP	Covers the application of group policy objects.
AU	Covers the auditing and reporting components.
AD	Covers the use of the Likewise management tools for Active Directory.

18.2. Creating a License Container

You can install Likewise licenses manually on each Linux, Unix, and Mac OS X computer, or you can install the licenses in Active Directory and manage them from a central location. In Active Directory, you must create a license container before you can import a Likewise license key file.

It is recommended that you manage licenses in Active Directory and that you create your license container in a common location at the highest level of the OU hierarchy to which you have write access. For instance, if you have separate OUs for your Linux and Mac computers, creating the licensing container in a common location above the OUs for the Mac and Linux computers can simplify license management. If you have a default cell, it is recommended that you create the license container at the level of the domain.

Any organizational unit may have a license container. The container need not be in the same OU as a Likewise cell. The Likewise agent searches the OU hierarchy for a licensing container in the same way that it searches for a cell. When a license container is found, the agent stops trying to find a key in another container (even if the container it finds is empty) and checks whether the license is assigned to the computer. When the agent finds a license in Active Directory, it marks it as assigned to the computer.

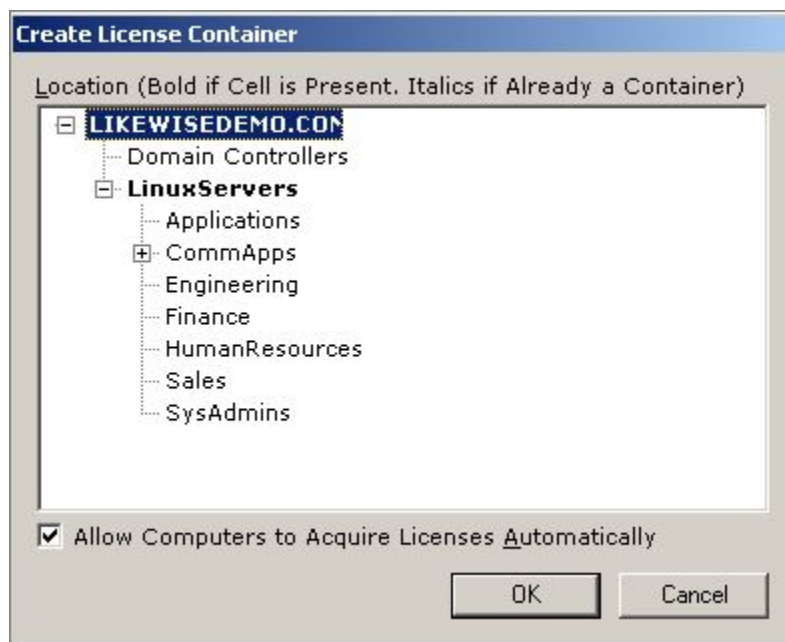
To stop computers from automatically obtaining licenses from the container, you can limit computers' write access to the licensing container on the console's license container creation page by clearing the **Allow Computers to Acquire Licenses Automatically** check box. When the computer cannot automatically obtain a license, you must manually assign a license to it with the console.

If there is no licensing container in Active Directory, the agent verifies the license locally -- a scenario reserved for licenses set with `setkey-cli`.

Create a License Container

Important: To create a license container, you must be a member of the Domain Administrators security group or have privileges sufficient to write data to the location where you want to create the licensing container. It is recommended that you do not create a license container in the Domain Controllers OU.

1. In the Likewise Management Console, right-click the **License Management** node, and then click **Create License Container**.
2. Optionally, to stop a computer from automatically obtaining a license from the license container, clear the **Allow Computers to Acquire Licenses Automatically** check box. If you clear the check box, you must manually assign a license to each computer by using the console.
3. Select the location where you want to create a container and then click OK:



You are now ready to import a license file, which will populate the Likewise licenses container in Active Directory with licenses for your Unix, Linux, and Mac OS X computers.

18.3. Import a License File

Likewise license keys and site licenses are distributed in an XML file. By using the Likewise Management Console on your Windows administrative workstation, you can import a license key file containing licenses. You must create a license container in Active Directory before you can import a license key file.

1. Make sure the XML file containing the licenses is available on your Windows administrative workstation that is running the Likewise Management Console.
2. Under **Enterprise Console**, right-click **License Management**, and then click **Import License File**.
3. Locate the XML file that contains the licenses, and then click **Open**.

18.4. Assign a License to a Computer in AD

By default, Likewise automatically assigns licenses to computers running the Likewise agent when the computers connect to the domain. If a computer cannot automatically obtain a license, however, you can manually assign a license to it by using the Likewise Management Console.

If you turned off the default Likewise setting that lets computers acquire licenses automatically, you can manually assign licenses by using the following procedure.

1. In the console tree, expand **Enterprise Console**, and then click **License Management**.
2. In the list of licenses, right-click the license that you want to assign, and then click **Assign License**.
3. In the **Select Computer** dialog box, click **Locations**, select the location that contains the computer you want, and then click **OK**.
4. In the **Enter the object names to select** box, type the name of one or more computers -- for example, `AppSrvSeattle-1`. Separate multiple entries with semicolons. For a list of examples, click **examples**.
5. Click **Check Names**, and then click **OK**.

Tip: To use additional criteria to search for and select computers, click **Advanced**. Then, to show more information about a computer in the **Search results** box, click **Columns**, and add or remove columns.

18.5. Manage a License Key on a Likewise Client

From the command line of a Likewise client, you can check the computer's license, set a license key, release a license, and adjust the type of license that you want the computer to obtain. For more information, run the following command:

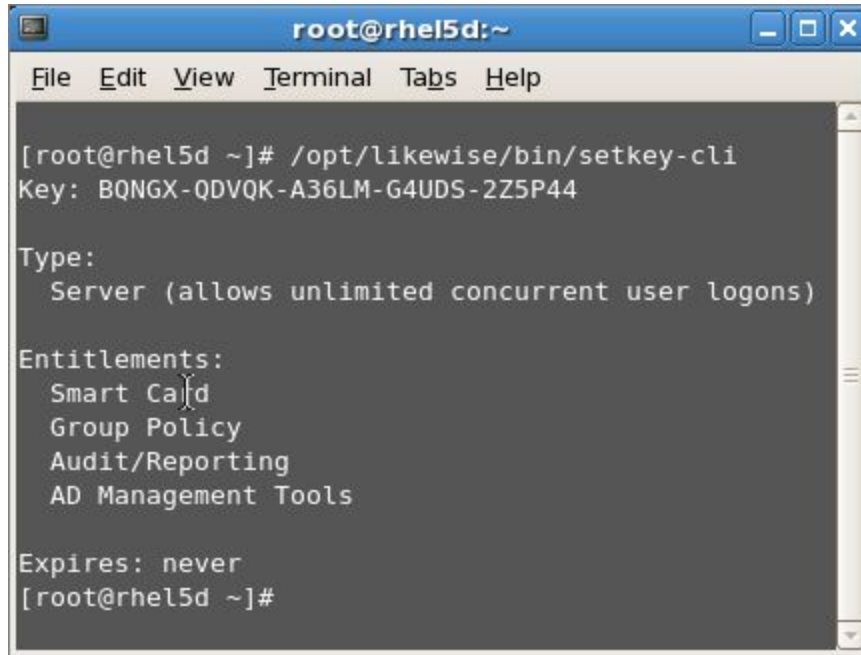
```
/opt/likewise/bin/setkey-cli --help
```

Check the License Key

To view the license key that is installed on a Unix, Linux, or Mac OS X computer, execute the following command at the shell prompt:

```
/opt/likewise/bin/setkey-cli
```

Here's an example:

A terminal window titled 'root@rhel5d:~' with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the command `/opt/likewise/bin/setkey-cli` being executed. The output is: `Key: BQNGX-QDVQK-A36LM-G4UDS-2Z5P44`, `Type: Server (allows unlimited concurrent user logons)`, `Entitlements: Smart Call, Group Policy, Audit/Reporting, AD Management Tools`, and `Expires: never`. The prompt `[root@rhel5d ~]#` is visible at the end.

```
root@rhel5d:~  
File Edit View Terminal Tabs Help  
[root@rhel5d ~]# /opt/likewise/bin/setkey-cli  
Key: BQNGX-QDVQK-A36LM-G4UDS-2Z5P44  
Type:  
  Server (allows unlimited concurrent user logons)  
Entitlements:  
  Smart Call  
  Group Policy  
  Audit/Reporting  
  AD Management Tools  
Expires: never  
[root@rhel5d ~]#
```

Set a License Key

You can set a license key for the Likewise agent by using the command line. You should, however, use this method of setting a key only when there is no licensing container in Active Directory and you want the agent to verify the license locally.

To set a license key, run the following command as root, replacing `LicenseKeyNumber` with a valid license key number:

```
/opt/likewise/bin/setkey-cli --key LicenseKeyNumber
```

Note: If there is a license container in Active Directory, you cannot use the command to apply an additional license or to select a license from the license container; instead, assign the license from Active Directory.

Release a License Key

When you decommission a computer, you can release a computer's license so it can be used by another computer. When you release a permanent license key, it is replaced by a temporary evaluation license. You can also release a license so you can apply a different permanent license to the computer.

```
/opt/likewise/bin/setkey-cli --release
```

Change the Type of License

You can change the type of license that the computer obtains when it connects to Active Directory by executing the following command as root, replacing `typeOfLicense` with either `workstation` or `server`. If a license of the type you specify is unavailable, however, the non-preferred type is obtained.

```
/opt/likewise/bin/setkey-cli --key-preference typeOfLicense
```

18.6. Delete a License

When you rename or remove a domain from Active Directory, you might also need to delete Likewise license keys from Active Directory. If you rename an Active Directory domain, you must obtain new license keys from Likewise Software. Licenses are provided on a per-domain basis; domain licenses apply only to the fully qualified domain name or child domain to which they were issued.

1. In the console tree, expand **Enterprise Console**, and then click **License Management**.
2. In the list of licenses, under **Key**, right-click the license that you want to delete and then click **Delete**.

Tip: If you inadvertently delete a license, you can restore it by importing the license file that contains it.

18.7. Revoke a License

1. In the console tree, expand **Enterprise Console**, and then click **License Management**.
2. In the list of licenses, under **Key**, right-click the license that you want to revoke, and then click **Revoke License**.

Chapter 19. Setting Up the Likewise Reporting Database

19.1. Introduction

To use the Likewise Enterprise reporting components, you must set up a database server named `LikewiseEnterprise` with either SQL Server or MySQL. You must also install the Likewise data collectors on a server to forward events to the database. The following Likewise Enterprise reporting components depend on the use of the database and the data collectors:

- Audit and Access Reporting
- Operations Dashboard
- Enterprise Database Management

This chapter describes how to set up the Likewise database and its event collectors so you can generate access reports, audit your network, archive records, and monitor security events.

19.2. Overview

The Likewise reporting system comprises the following components: a SQL Server or MySQL database set up on a dedicated database server; a dedicated data collection server set up on a Windows computer; and two Likewise data collectors that run on the data collection server.

When you install the Likewise Enterprise database utilities package (`LikewiseDBUtilities.exe`) on your data collection server, the following Likewise data collectors are installed and started automatically:

- `LWCollector`. It contains Likewise's RPC server code to enable the Likewise agent's forwarding daemon, `eventfwdd`, to upload events to the Likewise database server by using secure, authenticated transport protocols. `LWCollector` runs as a Windows auto-start service and can be managed from the command line.
- `LWEventDBReaper`. It copies events from the collector server to the central Likewise database. The process runs as a Windows auto-start service and can be managed from the command line. `LWEventDBReaper` depends on `LWCollector` to function properly: If `LWCollector` is not running, `LWEventDBReaper` will fail.

For these components to work together so that you can monitor events and generate reports, you must use the Likewise Management Console's Enterprise Database Management plug-in to connect to the database server and you must set your Linux, Unix, and Mac OS X computers to forward events to the data collector. This chapter includes instructions on how to connect the console to database and how to set computers to forward events to the collector.

Thus, the process of setting up the Likewise database and the other reporting components typically proceeds in the following order:

1. Set up the database instance and name it `LikewiseEnterprise`.
2. Run the Likewise database creation script to format the database for Likewise.
3. Install the Likewise DB Utilities package, which contains the collectors, on a server dedicated to data collection.

4. Use the Likewise Management Console's Enterprise Database Management plug-in to connect to the database server.
5. Configure the database and its accounts to meet your security policies.
6. Set your Linux, Unix, and Mac OS X computers to forward events to the data collector either by setting a Likewise group policy or by modifying a local setting.
7. Optionally, configure the collectors to meet the needs of your environment if the default settings don't work for you.

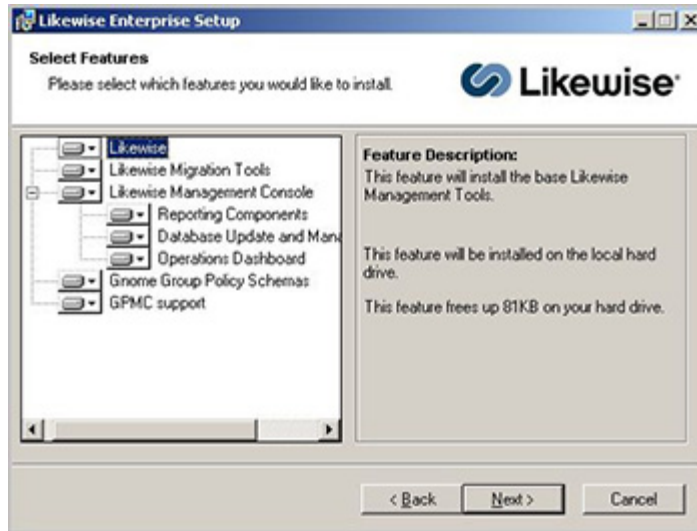
19.3. Requirements

- A database named `LikewiseEnterprise` running on Microsoft SQL Server 2005 or later, SQL Server Express 2005 or later, or MySQL 4.0 or later. SQL Server Express 2005 and MySQL are available for free from Microsoft and Sun Microsystems respectively.
- For MySQL, you must also install the MySQL Connector/Net version 6.0 -- MySQL's fully managed ADO.Net provider. You must use version 6.0. It is available for free at <http://dev.mysql.com/downloads/connector/net/6.0.html>.
- For SQL Server, you must also install the free SQL Server Management Studio Express package so you can create the Likewise database and set security options.
- The Likewise collector requires .Net Framework version 2.0.
- The Likewise collector requires a 32-bit version of Microsoft Vista, Microsoft Windows Server 2003, or Microsoft Windows Server 2008 to act as a server for the event collector server.
- The Microsoft Report Viewer 8.0 (ReportViewer.exe) must be installed. To download the Report Viewer, go to <http://www.microsoft.com/downloads/details.aspx?FamilyID=82833F27-081D-4B72-83EF-2836360A904D&displaylang=en>.
- The requirements to run the collector in an enterprise are as follows. The requirements might vary with the size of your network. It is suggested that you use a separate collector for every 1,000 computers that are forwarding events to a collector.

Item	Requirement
Memory	2Gb
Disk space	10Gb free disk space (for local event storage before copying to the central database). The size you require might vary depending on the number of events, the number of systems, and other factors.
Processor	2GHz dual core
Network	1Gb Ethernet (at least, to database server)

- The Likewise Management Console and its reporting components must be installed. The requirements to install the Likewise Management Console are in [Installing and Using the Console](#).

When you install Likewise Enterprise on your Windows administrative workstation, you must install the following components of the Likewise Management Console, or you must run the installer again and select these components for installation: Reporting Components, Database Update and Management Tools, Operations Dashboard.



19.4. Setting Up SQL Server

This section demonstrates how to set up SQL Server Express 2008 on Windows Server 2003 by specifying a basic configuration of a single database instance for Likewise Enterprise. The procedure is similar on other versions of Windows and with other versions of SQL Server, but the vendor's requirements for those products might differ. If you are setting up the Likewise reporting components to test and preview the features, you might find it easier to use SQL Server 2005 Express Edition.

Important: This section assumes you are a database administrator who knows how to set up and administer SQL Server, including configuring the database to comply with your IT security policy. There are numerous configuration options. You are responsible for tailoring the settings to meet your networking and security requirements. The *example setup* and brief discussion of security issues below serve only as a primer: Your actual setup and configuration will depend on the intricacies of your mixed network and your organization's security policies.

Depending on your system and its configuration, you might need the following prerequisites for SQL Server 2008, listed here for your convenience.

Important: For a full list of prerequisites, see Microsoft's listing of SQL Server 2008 requirements at <http://msdn.microsoft.com/en-us/library/ms143506.aspx>.

- Microsoft Windows Installer 4.5 for Windows Server 2003 (also known as Hotfix for Windows Server 2003 (WindowsServer2003-KB942288-v4-x86.exe)).
- Microsoft PowerShell 1.0 for Windows Server 2003, which is needed by SQL Server Management Studio (WindowsServer2003-KB926139-v2-x86-ENU.exe).
- Microsoft .NET Framework 3.5 SP1. It includes .NET Framework 2.0 SP2, which is required by SQL Server 2008.

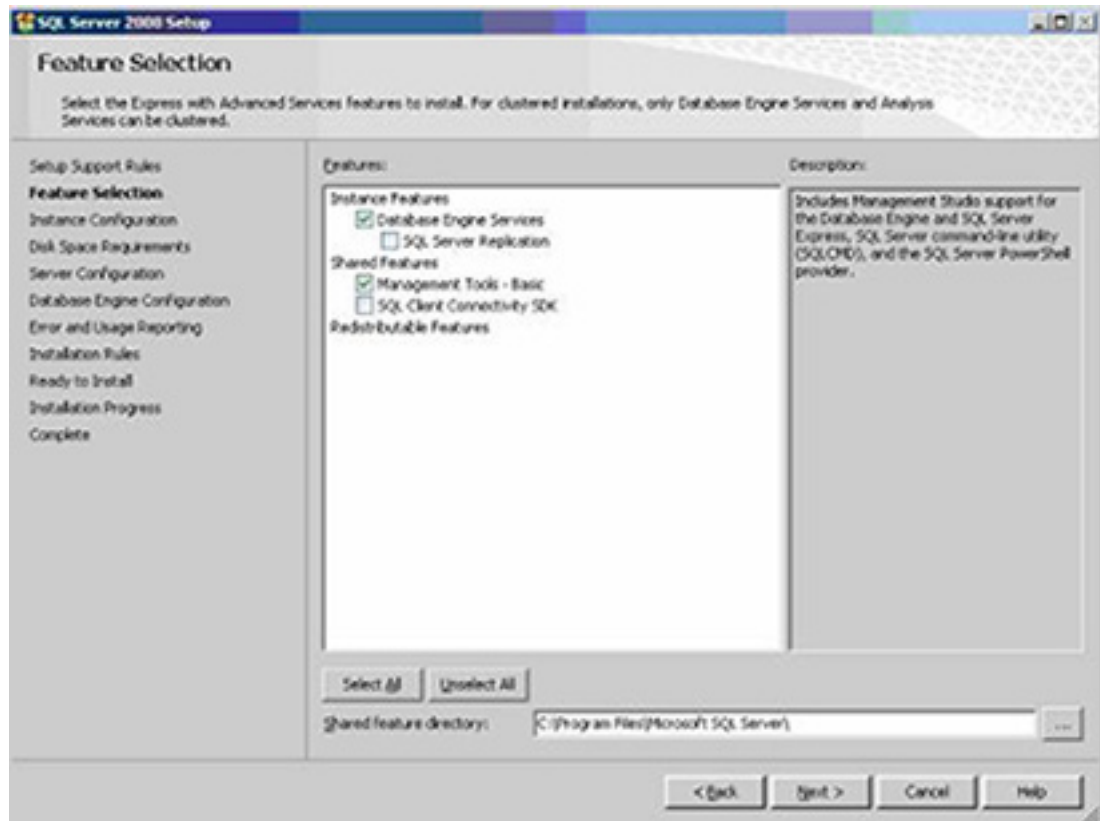
19.4.1. Install and Configure SQL Server

A database server must first be set up and running. You can use either Microsoft SQL Server or MySQL. This section covers Microsoft SQL Server; if you want to use MySQL, see [Setting Up MySQL](#) below. It is recommended that you set up the database on a new server.

Setting Up the Likewise Reporting Database

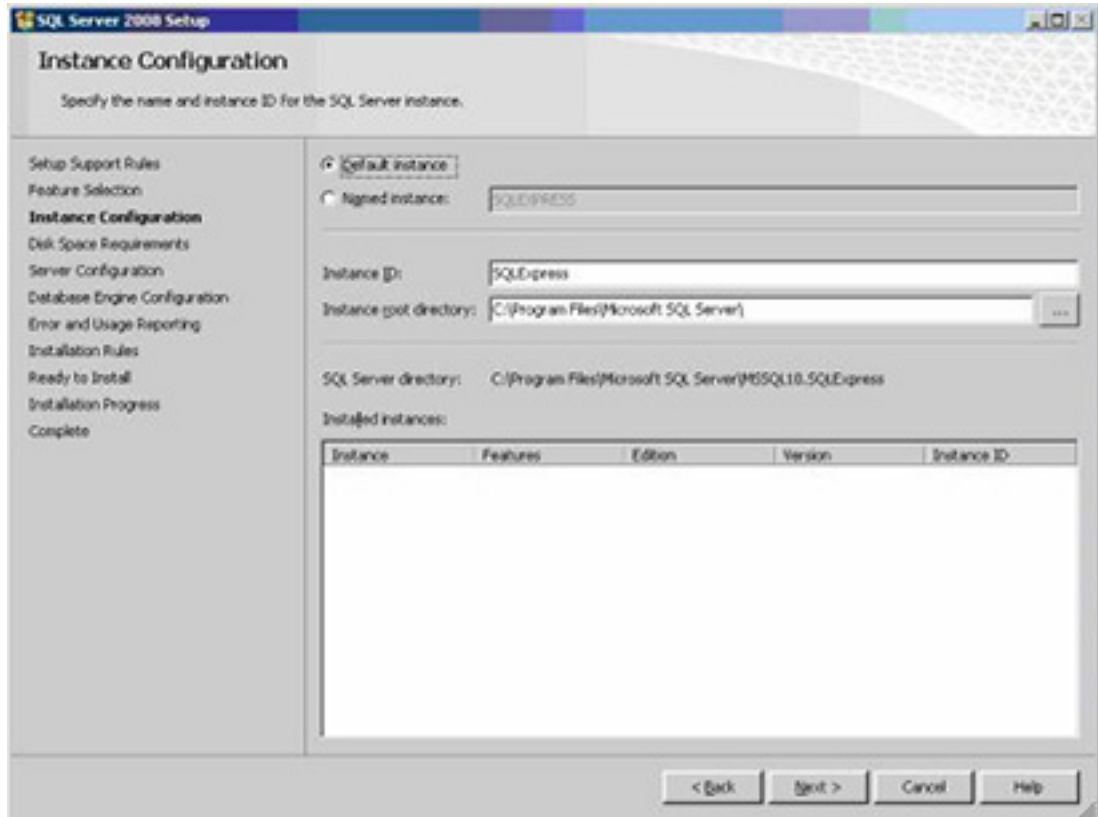
Important: *The following steps, including the screenshots, are intended only to orient you to setting up SQL Server in the context of configuring the Likewise reporting components. The instructions for setting up SQL Server are in the Microsoft SQL Server documentation at <http://www.microsoft.com>.*

1. Obtain SQL Server Express 2008 from <http://www.microsoft.com/express/sql/download/> and install it on your Windows Server 2003 computer.
2. During the SQL Server Express setup, under **Feature Selection**, select the following features:



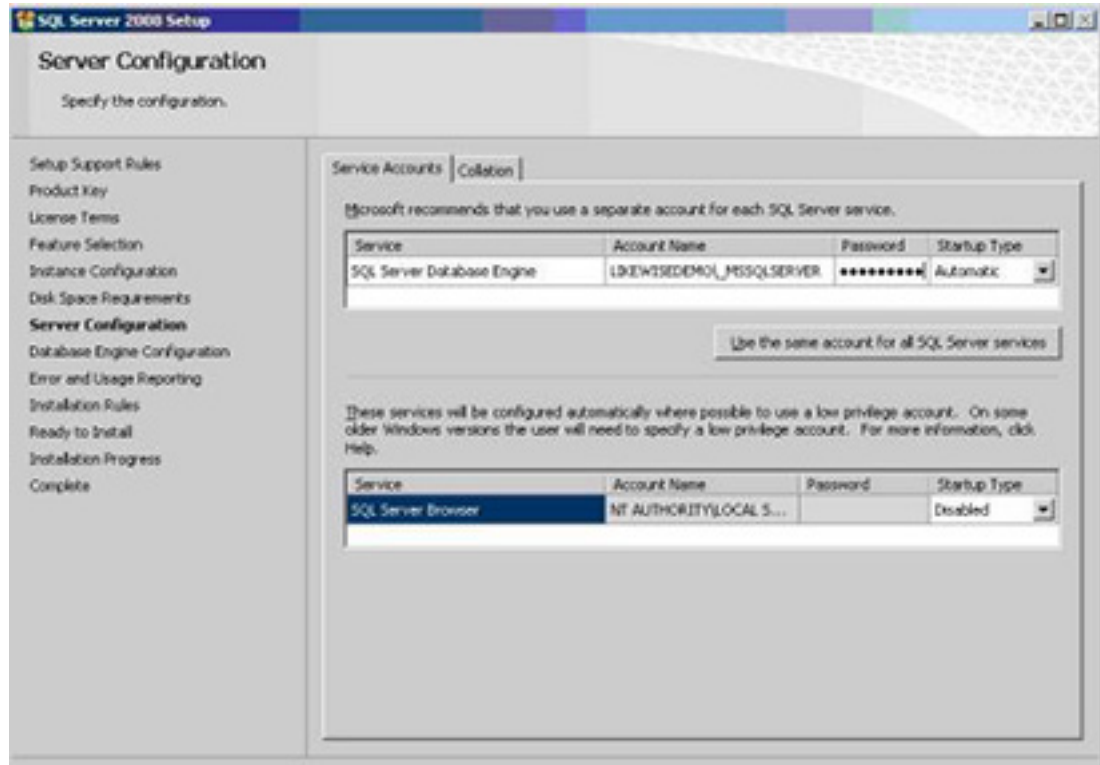
3. Under **Instance Configuration**, select **Default instance**. If there is more than one database instance on the computer, select a **Named Instance**. Remember the name of your instance; you'll need it later.

Setting Up the Likewise Reporting Database



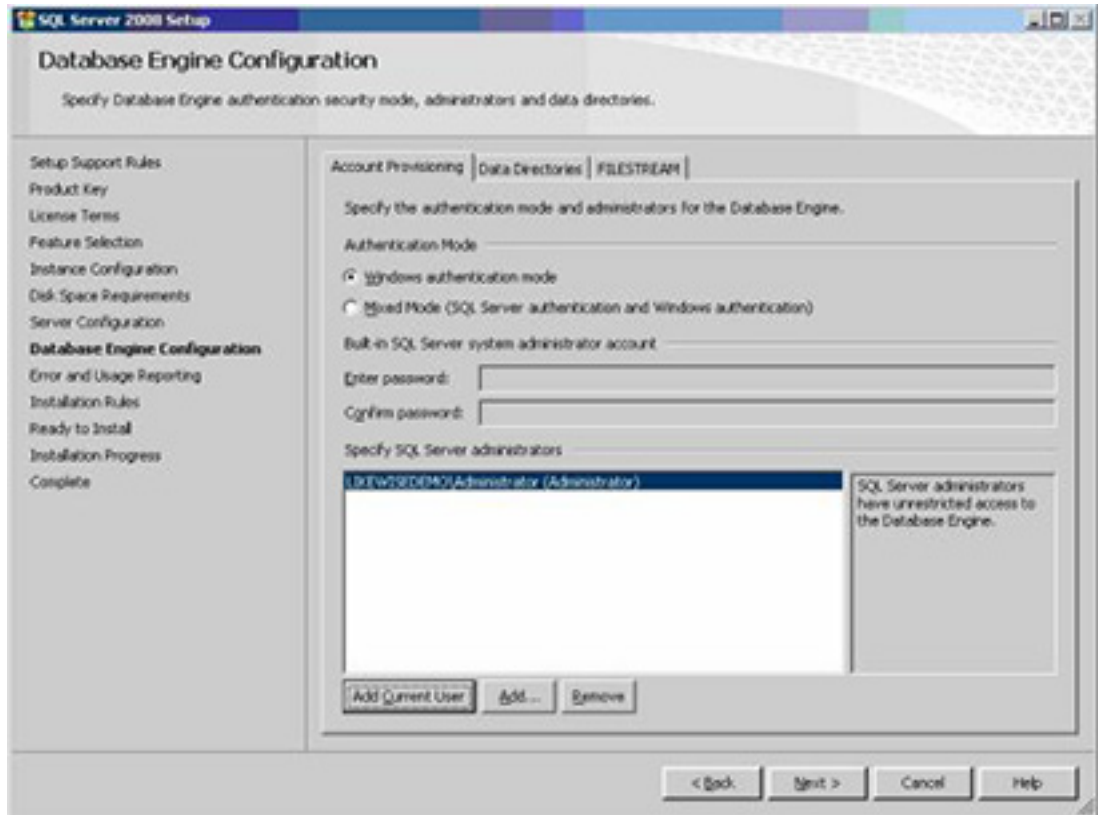
4. Under **Server Configuration**, on the **Service Accounts** tab, create a service account. The service accounts that you create and configure will depend on a range of factors, including your environment and your IT security policy. For more information, see your SQL Server documentation and the section below titled SQL Server Database Security Notes.
5. Under **Server Configuration**, on the **Service Accounts** tab, enable the **Sequel Server Browser** service.

Setting Up the Likewise Reporting Database



6. Under **Database Engine Configuration**, on the **Account Provisioning** tab, select **Windows authentication mode**.
7. Under **Specify SQL Server administrators**, add your administrator account.

Setting Up the Likewise Reporting Database

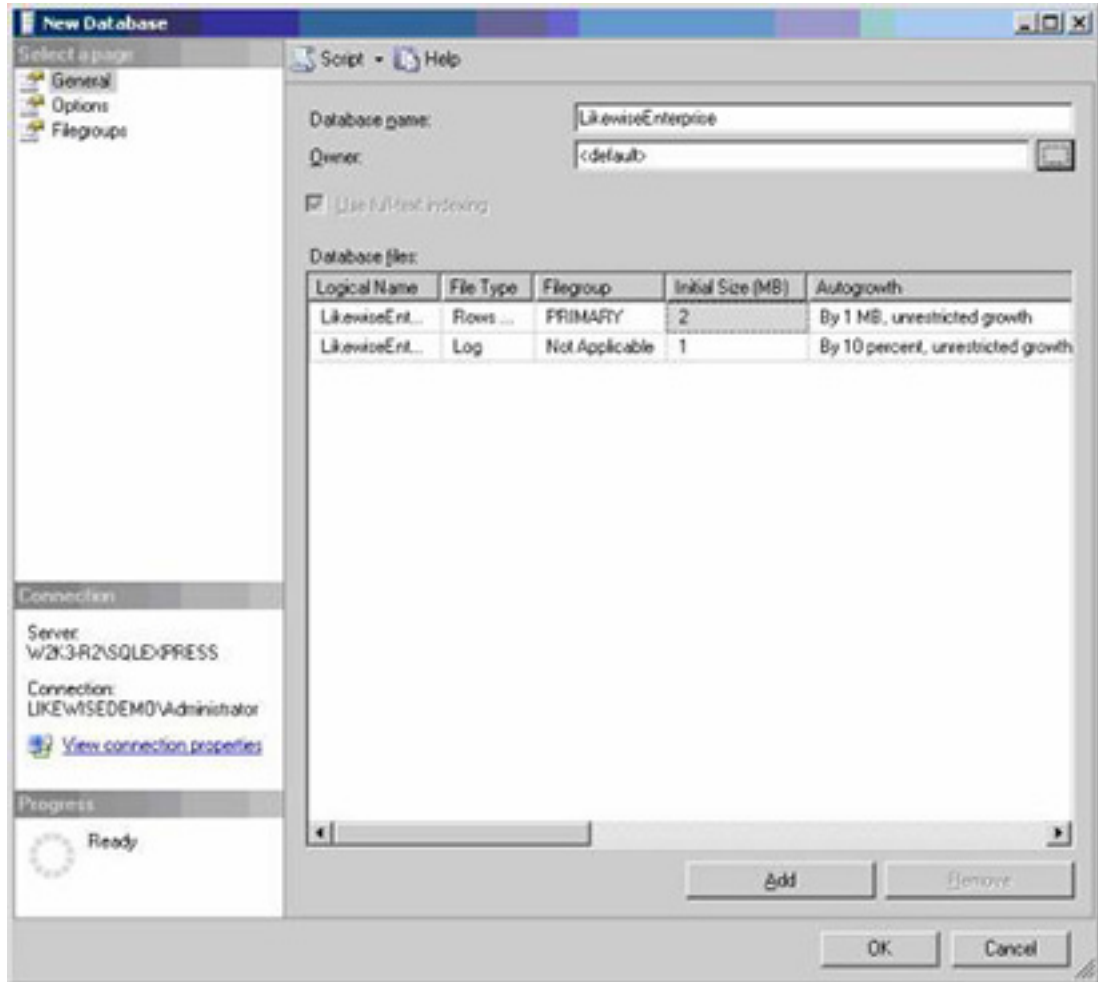


8. Click **Next** and follow the instructions in the SQL Server 2008 Setup wizard.
9. Using SQL Server Configuration Manager, set the SQL Server Network Configuration protocols to allow external connections with named pipes:



19.4.2. Create a Database Named LikewiseEnterprise

1. Start Microsoft SQL Server Management Studio and connect to the database engine.
2. Create a database named LikewiseEnterprise.



19.4.3. Run the Likewise Database Creation Script

1. Copy the SQL Server database creation script from the installation media – `CreateLikewiseEnterpriseDatabase.sql` -- to a location accessible from SQL Server.
2. In SQL Server Management Studio Express, on the **File** menu, click **Open** and load the Likewise Enterprise database creation script for SQL Server:

```
CreateLikewiseEnterpriseDatabase.sql
```

Warning: Make sure that you connect to the newly created `LikewiseEnterprise` database. Failure to connect to the correct database might create tables and views in the wrong database, possibly rendering it unusable.

3. After making sure that you are connected to the `LikewiseEnterprise` database, execute the script.

If the script executes with errors, try running it again.

You can now use SQL Server Management Studio Express to explore the structure of the `LikewiseEnterprise` database.

19.4.4. Install the Likewise DB Utilities

The Likewise DB Utilities executable installs the collectors. It is recommended that you install the collectors on a dedicated server. In a network with only a few computers or for testing, you can install the collectors on the same server as the Likewise database.

1. Install the collector software by running the Likewise Database Utilities installer program (typically, `LikewiseDBUtilities-6.1.375.exe` in `C:\Program Files\Likewise\Enterprise` or on your Likewise installation media). Follow the instructions in the installer. Install all the database tools listed in the installer.

2. In the **Database Provider Library** box, enter the following string:

```
System.Data.SqlClient
```

3. In the **Connection String** box, enter the following string, where `DBSERVERNAME` is the name of the server running SQL Server and containing the Enterprise database. The `Initial Catalog` clause identifies the database to be used while `Integrated Security=True` specifies that Windows authentication should be used when connecting to the database server.

```
Data Source=DBSERVERNAME;Initial  
Catalog=LikewiseEnterprise;Integrated Security=True
```

Example:

```
Data Source=W2K3-R2\SQLEXPRESS;Initial  
Catalog=LikewiseEnterprise;Integrated Security=True
```

4. Click Next.
5. Click Install.

19.4.4.1. Set the Start Order for Collector Processes

If the collectors are installed on the same machine as the database, the collector services – `LWCollector` and `LWEventDBReaper` -- must start after the Microsoft SQL Engine. In addition, `LWCollector` should start before `LWEventDBReaper`. For information about setting dependencies for system services, see MSDN. For an example of how to create a service dependency, see this article on delaying startup services.

19.4.5. SQL Server Database Security Notes

Although the SQL Server database will contain no user passwords or other highly confidential information, it will contain a list of user accounts, information about what users are allowed to access what resources, and other information that could be used for nefarious purposes. In considering the security of the database, you should ask yourself several questions:

1. Who will be allowed to write to the database?
2. Who will be allowed to read from the database?
3. What accounts will be used to access the database?

Data is written to the database in several cases:

Setting Up the Likewise Reporting Database

- a. When a collector copies events to the database.
- b. When the `LDBUpdate` process writes information from Active Directory to the database.
- c. When administrators perform maintenance operations on the database (for example, creating or restoring event archives).

In general, to minimize security risks, you should define and use privileged accounts in as narrow a fashion as possible. One possible set of answers to the above questions that meets these security criteria is as follows:

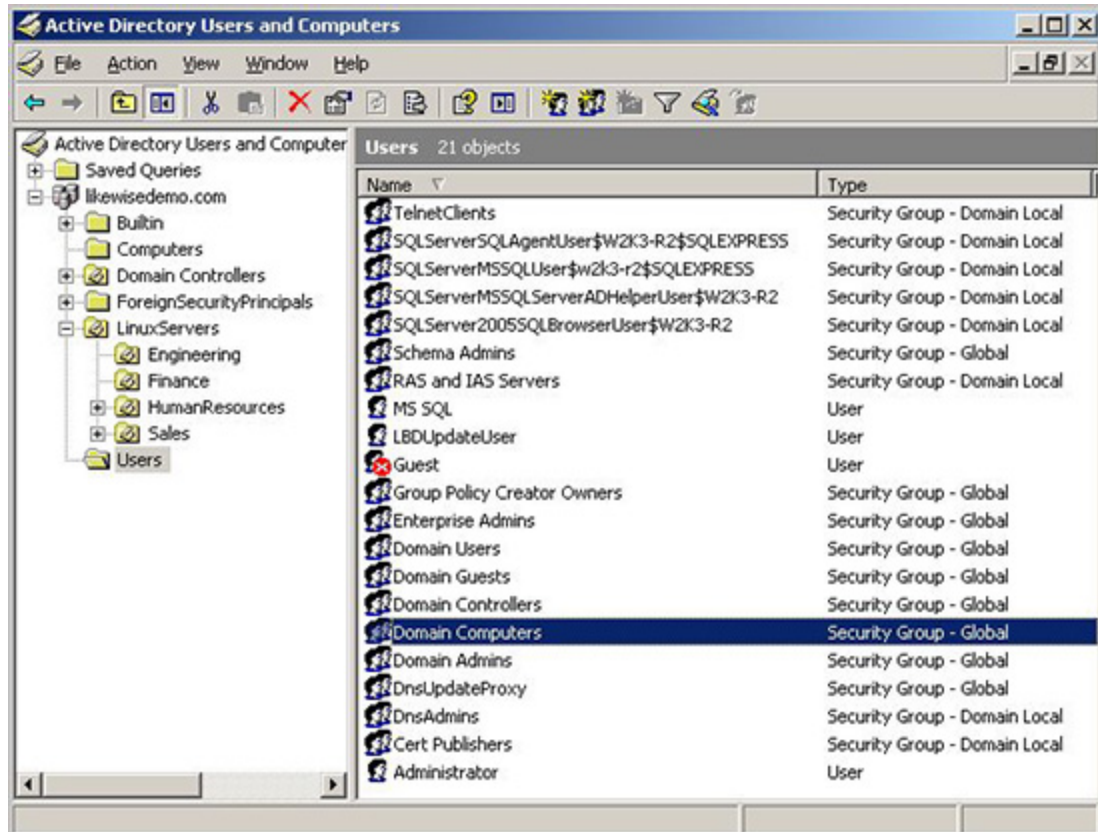
1. The collector computers need to be able to write to the database. To allow this while maintaining stringent security, we will create a security group in AD called `LikewiseCollectors`. The collector computer accounts will be made members of the group. The group will be given read-write access to the events, collectors, and `CollectorStats` tables in the database.
2. The `LDBUpdate` process needs to write to many tables in the database. To allow this, we will create an AD user called `LDBUpdateUser`. We will give this user read-write access to all tables in the database but we will not allow this user to log on interactively on any machine. We will create a Windows scheduled task to periodically run `LDBUpdate` using `LDBUpdateUser`. We will set `LDBUpdateUser`'s password to `never expires` or our administrators will manually update the account password and update scheduled tasks with the new password as necessary.
3. Interactive database administration will be allowed only by certain administrators. A new security group, `LikewiseArchiveAdministrators`, will be created and given read access to all tables and write access to the archives and events.
4. Reporting will be allowed only by trained administrators. To secure this, we will create a new security group called `LikewiseAdministrators`. We will give this group and the `LikewiseArchiveAdministrators` read access to all of the tables in the database.
5. If we are to allow users to manually run `LDBUpdate` from the Likewise Management Console, these users must have the same rights as the `LDBUpdateUser` described above.

The following table summarizes the suggestions above:

AD Group	Read Access	Write Access
<code>LikewiseCollectors</code> group	collectors, <code>CollectorStats</code> , Events tables	collectors, <code>CollectorStats</code> , Events tables
<code>LDBUpdateUser</code> user	All tables	All tables
<code>LikewiseArchiveAdministrators</code> group	All tables	Archives, collectors, Events tables
<code>LikewiseAdministrators</code> group	All tables	None

These suggestions are all based on using Windows authentication rather than SQL Server authentication. Windows Authentication greatly simplifies the implementation of database security. If you want to use SQL Server authentication, you must embed user names and passwords in the collector servers and in the Likewise Management Console -- a practice that is not recommended. If you nevertheless want to take this approach, consult the MySQL Security Notes; much of the MySQL security information applies to using SQL Server with SQL Server Authentication.

Here's an example of SQL Server accounts in ADUC:



19.5. Setting Up MySQL

A database server must first be set up and running. You can use either MySQL or Microsoft SQL Server. This section covers MySQL; if you want to use SQL Server, see Setting Up SQL Server.

The following example demonstrates how to set up MySQL Server 5.1 on Windows Server 2003 by using the MySQL command-line utility to specify a basic configuration of a single database instance for Likewise Enterprise. The procedure is similar on other operating systems, including Linux. For information about installing and using the utility or MySQL Server, see the MySQL documentation. MySQL has its own set of requirements -- again, see the vendor's documentation. It is recommended that you set up the database on a new server.

Important: This section assumes you are a database administrator who knows how to set up and administer MySQL, including configuring the database to comply with your IT security policy. There are numerous configuration options. You are responsible for tailoring the settings to meet your networking and security requirements. The example setup and brief discussion of security issues below serve only as a primer: Your actual setup and configuration will depend on the intricacies of your mixed network and your organization's security policies.

19.5.1. Create a Database Named LikewiseEnterprise

1. After you have installed MySQL, create a database named LikewiseEnterprise:

```
C:\Program Files\Support Tools>mysql ---user=root ---  
password=password  
Welcome to the MySQL monitor. Commands end with -; or \g.
```

```
Your MySQL connection id is 8
Server version: 5.1.36-community MySQL Community Server (GPL)
```

```
Type -'help;' or -'\h' for help. Type -'\c' to clear the current
input statement.
```

```
mysql> create database LikewiseEnterprise;
Query OK, 1 row affected (0.14 sec)
```

2. In the MySQL utility, set the database to use LikewiseEnterprise:

```
mysql>use LikewiseEnterprise;
Database changed
```

19.5.2. Allow the Database To Accept External Connections from Account

You must configure the MySQL database to allow external database connections for the account that connects to the database -- your database definer account. The code block below configures the MySQL root account to connect to the database with local or external connections.

The accounts that you use to connect to the database and the permissions that you grant those accounts will depend on your environment and your security policy; see the section below on MySQL Security Notes.

```
mysql> GRANT ALL PRIVILEGES ON *.* TO -'root'@'localhost' WITH GRANT
OPTION;
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> CREATE USER -'root'@'%' IDENTIFIED BY -'password';
Query OK, 0 rows affected (0.02 sec)
```

```
mysql> GRANT ALL PRIVILEGES ON *.* TO -'root'@'%' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)
```

19.5.3. Run the Likewise Database Creation Script

1. Copy the MySQL database creation script from the installation media to a location accessible from the MySQL server.
2. Run the Likewise Enterprise database creation script for MySQL:

```
mysql>source CreateLikewiseEnterpriseDatabase.msql;
```

If the script executes with errors, try running it again.

19.5.4. Install the Likewise DB Utilities

1. Install the collector software by running the Likewise Database Utilities installer program (typically, `LikewiseDBUtilities-6.1.375.exe` in `C:\Program Files\Likewise\Enterprise` or on your Likewise installation media). Follow the instructions in the installer. Install all the database tools listed in the installer.
2. In the **Database Provider Library** box, enter the following string:


```
MySQL.Data.MySqlClient
```

3. In the **Connection String** box, enter the following string, where *dbUserAccount* is your database definer account for your MySQL LikewiseEnterprise database and *dbUserAccountPassword* is the account's password. The account must be granted all privileges for local and external connections. Remember the name and password of this account -- you must enter it later to connect to the database from the Likewise Management Console.

```
server=yourDBserverInstanceName;database=LikewiseEnterprise;user  
id=dbUserAccount;password=dbUserAccountPassword;
```

Example:

```
server=steveh-dc;database=LikewiseEnterprise;user  
id=root;password=password;
```

4. Click Next.
5. Click Install.

19.5.5. Customize Your MySQL Security Settings

Because MySQL does not support integrated Windows Authentication, you must include an explicit user name and password in the database connection strings that Likewise components use to connect to the database.

MySQL does, however, support security restrictions based on IP addresses. The following are the recommended best practices for using MySQL with Likewise Enterprise:

1. Create a MySQL user called LwCollector@hostname for each collector server, where hostname is the name of the collector server. This practice will restrict the use of LwCollector to the collector machines.
2. Grant the LwCollector read and write access to the database tables as shown in the table below.
3. Create an LwDbUpdate@hostname user, where hostname is the name of the computer on which the LDBUpdate scheduled task will be run.
4. Grant this user read and write access as shown in the table below.
5. Create a LwArchiveAdmin user.
6. Grant this user read and write access to tables as shown in the table below.
7. Create a LwAdmin user.
8. Grant this user read and write access to tables as shown in the table below.

The result should be as follows:

MySQL User	Read Access	Write Access
LwCollector@hostname	collectors, CollectorStats, Events tables	collectors, CollectorStats, Events tables
LwDbUpdate	All tables	All tables
LwArchiveAdmin	All tables	Archives, Events tables

LwAdmin	All tables	None
---------	------------	------

All these users should get different passwords. The user names and passwords must be specified in the database connection strings used when configuring Likewise collectors, reporting components, and the Operations Dashboard.

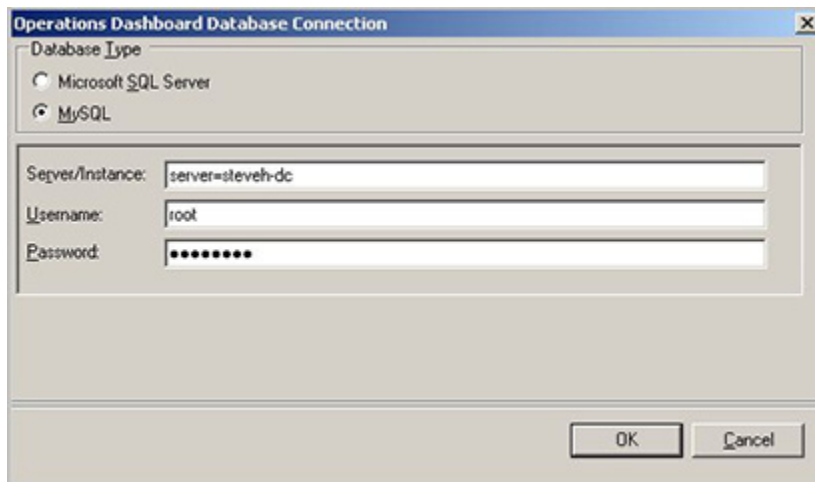
19.6. Connecting the Likewise Console to the Database

This section assumes the Likewise Management Console and the following Likewise reporting components are installed on your Windows administrative workstation: Reporting Components, Database Update and Management Tools, Operations Dashboard.

19.6.1. Connect the Likewise Console to the Database

In the Likewise Management Console, load the Enterprise Database Management plug-in and connect to the database server instance (which is typically but not necessarily your server's machine name).

1. In the console, on the **File** menu, click **Add/Remove Plug-in**.
2. Click **Add**.
3. Click **Enterprise Database Management**, and then click **Add**.
4. Click **Close**, and then click **OK**.
5. In the console tree, right-click the **Enterprise Database Management** node and then click **Connect to database**.
6. Click **Change**. Under **Database Type**, select **MySQL**, and then enter the name of your database server instance in the **Server/Instance** box.
7. In the **Username** and **Password** boxes, enter the credentials of your database definer account.



19.6.2. Make Sure the Collector Processes Are Running

Although `LWCollector` and `LWEventDBReaper` are typically started automatically, you should take a moment to check whether they are running.

1. Make sure `LWCollector` is running by executing the following command on the command line of the Windows computer running the collector:

```
C:\Program Files\Likewise\Enterprise>sc query LWCollector
```

```
SERVICE_NAME: LWCollector
        TYPE               -: 10   WIN32_OWN_PROCESS
        STATE                -: 4    RUNNING
                                (STOPPABLE, NOT_PAUSABLE,
IGNORES_SHUTDOWN))
        WIN32_EXIT_CODE      -: 0    (0x0)
        SERVICE_EXIT_CODE   -: 0    (0x0)
        CHECKPOINT           -: 0x0
        WAIT_HINT            -: 0x0
```

2. If it is not running, start it by executing the following command on the command-line:

```
C:\Program Files\Likewise\Enterprise>sc start lwcollector
```

3. Make sure `LWEventDBReaper` is running:

```
C:\Program Files\Likewise\Enterprise>sc query lweventdbreaper
```

```
SERVICE_NAME: lweventdbreaper
        TYPE               -: 10   WIN32_OWN_PROCESS
        STATE                -: 4    RUNNING
                                (STOPPABLE, NOT_PAUSABLE,
ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE      -: 0    (0x0)
        SERVICE_EXIT_CODE   -: 0    (0x0)
        CHECKPOINT           -: 0x0
        WAIT_HINT            -: 0x0
```

4. If it is not running, start it by executing the following command:

```
C:\Program Files\Likewise\Enterprise>sc start lweventdbreaper
```

19.6.3. Run the DB Update Script

The `LDBUpdate` script is a batch program for Windows that reads information from Active Directory and writes it to the Likewise database so you can generate reports about computers and users in Active Directory. You can run the update script on demand from the Likewise Management Console, or you can set it up as a scheduled task.

If the information in Active Directory has changed since you last ran the script and if you want those changes included in your reports, you should run the script before you generate your reports.

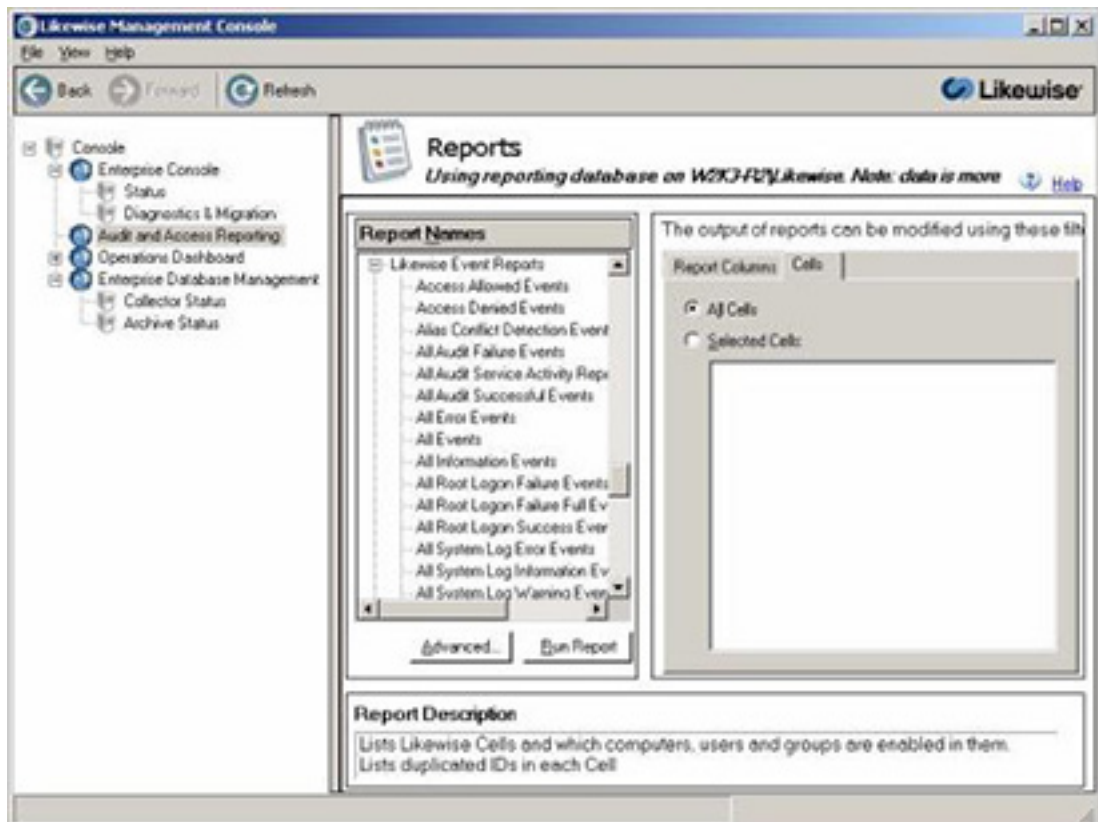
To access Active Directory, the `LDBUpdate` script uses the LDAP and RPC ports.

The Update DB button will only be enabled if the update utility is available on the current machine. The Likewise Enterprise installer allows you to select whether the utility is installed on a machine. To be able to run the utility, the current user must have privileges to read and write to any table in the Enterprise database.

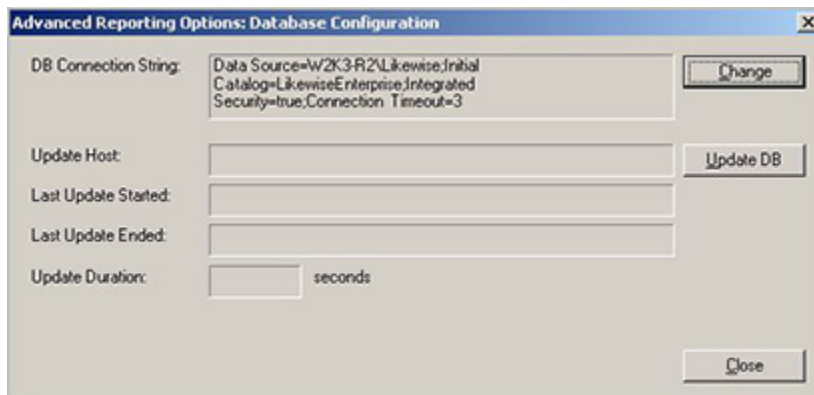
Setting Up the Likewise Reporting Database

Important: The Windows administrative workstation on which you run the script must be connected to Active Directory. In addition, the user account with which you execute the script must have at least read permission for objects and child objects in Active Directory.

1. In the Likewise Management Console, on the **File** menu, click **Add/Remove Plug-in**.
2. Click **Add**.
3. Click **Audit and Access Reporting**, and then click **Add**.
4. Click **Close**, and then click **OK**.
5. In the console tree, click the **Audit and Access Reporting** node and then click **Advanced**.



6. Click **Update DB**, and then click **OK**.



19.6.4. Run the `ldbupdate.exe` from the Command Line

The `LDBUpdate` script reads information from Active Directory and writes it to the Likewise database so you can generate reports about computers and users in Active Directory. You can manage the update script on demand from the shell prompt of your Windows administrative workstation running Likewise Enterprise.

The Windows administrative workstation on which you run the script must be connected to Active Directory. To use the shell commands, the current user must have privileges to read and write to any table in the Enterprise database. In addition, the user account with which you execute the script must have at least read permission for objects and child objects in Active Directory.

```
C:\Program Files\Likewise\Enterprise>ldbupdate.exe -/?
```

```
Usage:  LDBUpdate OPTIONS
```

Where `OPTIONS` include:

```
--f LDAPPATH      Path of the forest to synchronize; required
--d FQDN          Domain (in forest or in trusts) to process; can
repeat
--o FILE          Send output to FILE
--p PROVIDER      Use PROVIDER as the database type
                  (default: System.Data.SqlClient)
--c STRING        Use STRING as the database connection parameter
--nogpo          Don't analyze GPOs (faster)
--v              Display verbose output
---force         Ignore the database status and perform update even
if
                  marked as busy
---debug         Display debug level output
---help          Display this help output
```

If the `--d` option is not specified, all the domains in the forest and in any trusted forests will be processed.

Here's an example of how to use the command-line utility to set the provider and the connection string for a SQL Server database:

```
ldbupdate.exe -f dc=likewisedemo,dc=com -p System.Data.SqlClient
-c "Data Source=RVLN-BUILD; Initial Catalog=LikewiseEnterprise;
Integrated Security=True" --force
```

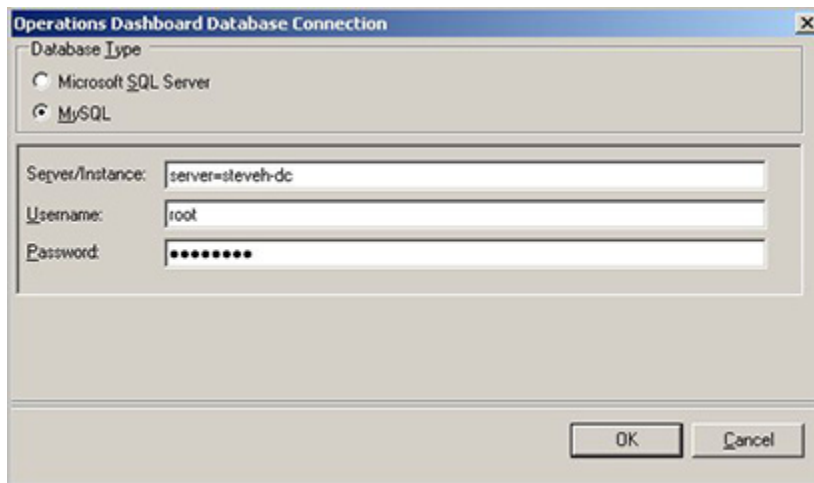
19.7. Connecting the Likewise Console to the Database

This section assumes the Likewise Management Console and the following Likewise reporting components are installed on your Windows administrative workstation: Reporting Components, Database Update and Management Tools, Operations Dashboard.

19.7.1. Connect the Likewise Console to the Database

In the Likewise Management Console, load the Enterprise Database Management plug-in and connect to the database server instance (which is typically but not necessarily your server's machine name).

1. In the console, on the **File** menu, click **Add/Remove Plug-in**.
2. Click **Add**.
3. Click **Enterprise Database Management**, and then click **Add**.
4. Click **Close**, and then click **OK**.
5. In the console tree, right-click the **Enterprise Database Management** node and then click **Connect to database**.
6. Click **Change**. Under **Database Type**, select **MySQL**, and then enter the name of your database server instance in the **Server/Instance** box.
7. In the **Username** and **Password** boxes, enter the credentials of your database definer account.



19.7.2. Make Sure the Collector Processes Are Running

Although `LWCollector` and `LWEventDBReaper` are typically started automatically, you should take a moment to check whether they are running.

1. Make sure `LWCollector` is running by executing the following command on the command line of the Windows computer running the collector:

```
C:\Program Files\Likewise\Enterprise>sc query LWCollector
```

```
SERVICE_NAME: LWCollector
        TYPE               -: 10   WIN32_OWN_PROCESS
        STATE                -: 4    RUNNING
                                (STOPPABLE, NOT_PAUSABLE,
        IGNORES_SHUTDOWN))
        WIN32_EXIT_CODE      -: 0    (0x0)
        SERVICE_EXIT_CODE   -: 0    (0x0)
        CHECKPOINT          -: 0x0
        WAIT_HINT           -: 0x0
```

2. If it is not running, start it by executing the following command on the command-line:

```
C:\Program Files\Likewise\Enterprise>sc start lwcollector
```

3. Make sure `LWEventDBReaper` is running:

```
C:\Program Files\Likewise\Enterprise>sc query lweventdbreaper
```

```
SERVICE_NAME: lweventdbreaper
        TYPE                -: 10   WIN32_OWN_PROCESS
        STATE                 -: 4    RUNNING
                                (STOPPABLE, NOT_PAUSABLE,
ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       -: 0    (0x0)
        SERVICE_EXIT_CODE    -: 0    (0x0)
        CHECKPOINT           -: 0x0
        WAIT_HINT            -: 0x0
```

4. If it is not running, start it by executing the following command:

```
C:\Program Files\Likewise\Enterprise>sc start lweventdbreaper
```

19.8. Setting Computers to Forward Events to LWCollector

You can set computers to forward events to LWCollector in two ways: globally by setting a Likewise group policy to modify the configuration for the event forwarding daemon on target computers or locally by editing the Likewise registry.

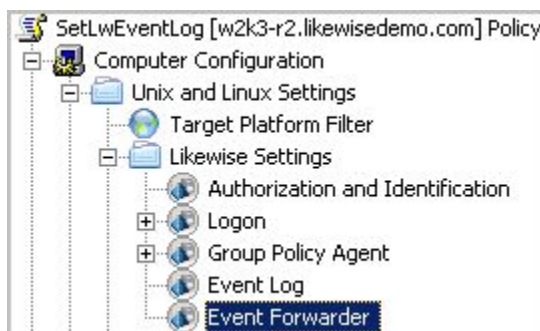
You can also cull events from syslog.

19.8.1. Set Event Forwarding with a GPO

This group policy modifies the settings in the Likewise registry to forward events from target Linux, Unix, and Mac OS X computers to the Likewise database collector service, LWCollector, on a Windows computer. You can use this policy to improve security monitoring by logging authentication and authorization events and viewing them in the Likewise Operations Dashboard.

Important: To use this policy, you must first enable the event log; see Turn on Event Logging with a GPO. Depending on your network configuration, you might also have to set a group policy to specify the service principal of the collector.

1. In Active Directory Users and Computers or in the Group Policy Management Console, create or edit a group policy for the organizational unit that you want, and then open it with the Group Policy Object Editor.
2. In the console tree under **Computer Configuration**, expand **Unix and Linux Settings**, expand **Likewise Settings**, and then click **Event Forwarder**:



3. In the details pane, double-click **Event log collector**, and then select the **Define this policy setting** check box.
4. In the **Name** or **Address** box, enter the host name of the computer running LWCollector.
Example: `w2k3-r2.likewisedemo.com`

19.8.2. Forward Events by Changing Your Local Settings

Important: Before you can forward events, you must turn on the event log; see Turn on Event Logging. The following procedure assumes you know how to edit the Likewise registry. For instructions on how to modify the registry, see the chapter on configuring the Likewise services with the registry.

1. On the target Linux, Unix, or Mac OS X computer, edit the registry to set the value of the following line to the host name of the computer running LWCollector.

```
[HKEY_THIS_MACHINE\Services\eventfwd\Parameters]
"Collector"=""
```

Example: `"Collector"="w2k3-r2.likewisedemo.com"`

2. Or, you can specify an IP address for the collector. If you do so, you must also specify the service principal of the collector on the following line:

```
[HKEY_THIS_MACHINE\Services\eventfwd\Parameters]
"CollectorPrincipal"=""
```

After you change the service's settings in the registry, you must force the service to load the change by restarting, with super-user privileges, `eventfwd`:

```
/opt/likewise/bin/lwsm restart eventfwd
```

19.8.3. Cull Events from Syslog

To collect sudo events and other system events that appear in syslog, you must configure syslog to write data to a location where the Likewise `reapsysld` daemon can find it and copy it to the local event log.

Note: You can set a Likewise group policy to modify `/etc/syslog.conf` on target computers.

The `reapsysld` daemon creates three named pipes and picks up the syslog information written to them:

```
/var/lib/likewise/syslog-reaper/error
/var/lib/likewise/syslog-reaper/warning
/var/lib/likewise/syslog-reaper/information
```

To configure syslog to write to the pipes, add the following lines to `/etc/syslog.conf`:

```
*.err /var/lib/likewise/syslog-reaper/error
*.warning /var/lib/likewise/syslog-reaper/warning
*.debug /var/lib/likewise/syslog-reaper/information
```

The last entry is not analogous to the first two. Some versions of syslog require a tab character instead of spaces to separate the two components of each line; for more information, see your syslog documentation.

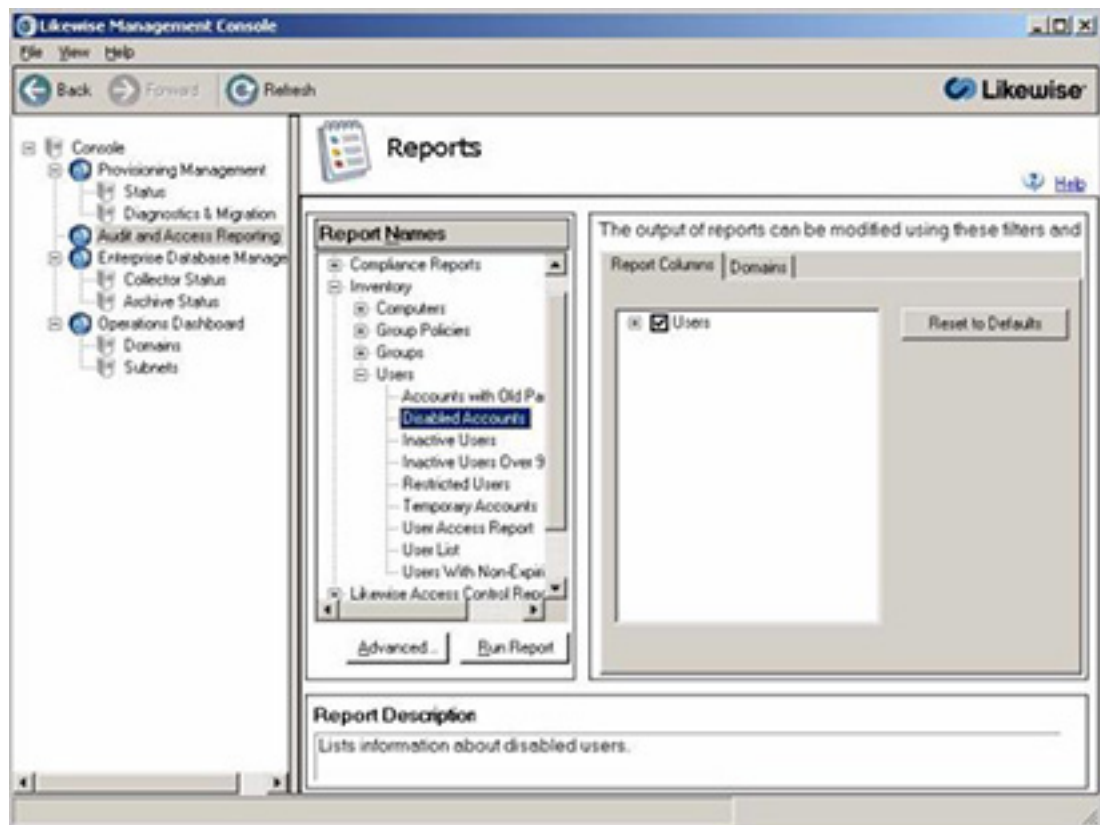
After you modify `syslog.conf`, you must restart the syslog service for the changes to take effect:


```
/etc/init.d/syslog restart
```

19.9. Generate a Sample Report

You can generate reports by using the Audit and Access Reporting plug-in for the Likewise Management Console. The following procedure demonstrates, as an example, how to create an inventory report of users with disabled accounts. The procedure to run compliance reports, access reports, and event reports is similar.

1. In the Likewise Management Console tree, click the **Audit and Access Reporting** node.
2. Under **Report Names**, expand **Inventory**, expand **Users**, and then click **Disabled Accounts**.

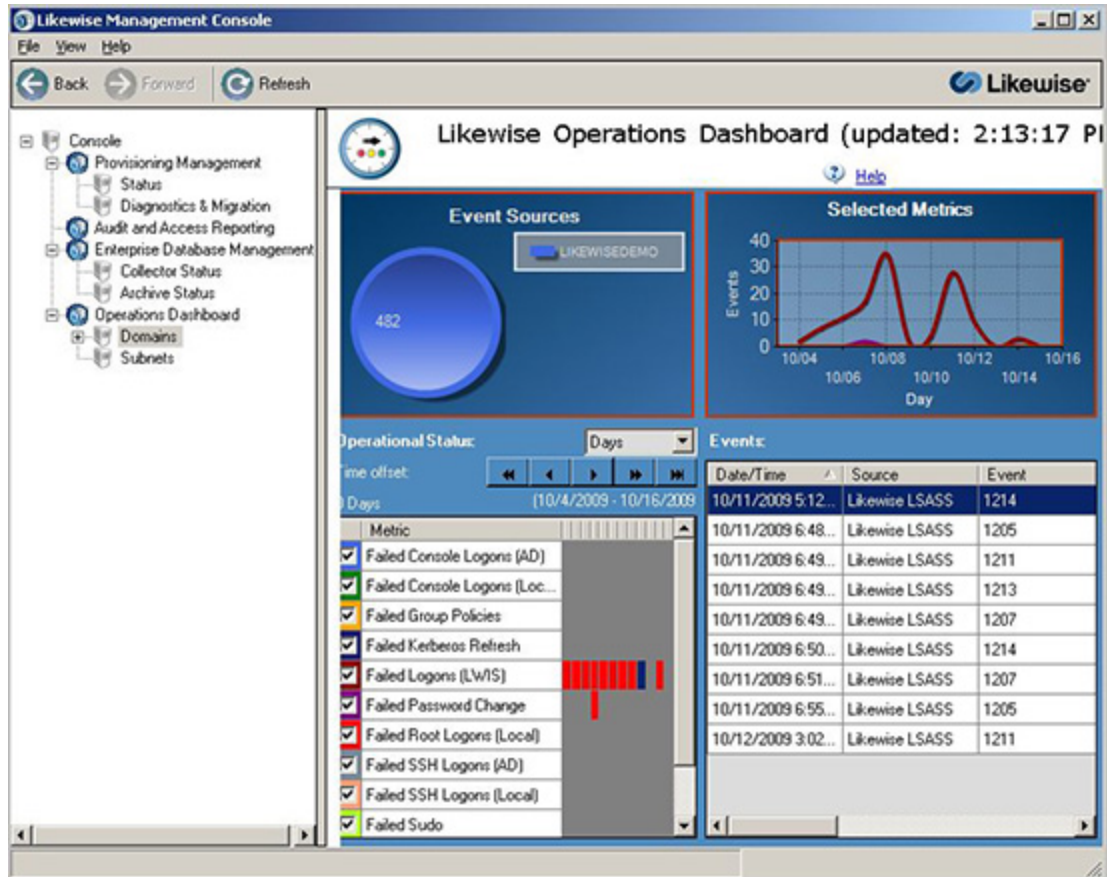


3. Click **Run Report**.

19.10. Monitoring Events with the Operations Dashboard

The Likewise Operations Dashboard is a management application, or plug-in, for the Likewise Management Console. The dashboard runs on a Windows administrative workstation connected to the Likewise Reporting Database and an Active Directory domain controller. The dashboard retrieves information from the Likewise database to display authentication transactions, authorization requests, network events, and other security events that take place 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 dashboard looks like this:

Setting Up the Likewise Reporting Database



Here's a partial list of the kind of events the dashboard can display. You can also create custom events and monitor them:

- All Success Audit Events
- All System Log Error Events
- Console Logons (AD or Local)
- Domain Joins
- Domain Leaves
- Failed Console Logons (AD or Local)
- Failed Group Policies
- Failed Kerberos Refresh
- Failed Password Change
- Failed Root Logons (Local)
- Failed SSH Logons (AD or Local)
- Failed Sudo
- Likewise Services Failures
- Network Offline Warning
- Root Account Logons (Local)
- SSH Logons (AD or Local)
- Sudo

19.10.1. Start the Operations Dashboard

You can run the Operations Dashboard either as a stand-alone console or in the Likewise Management Console.

19.10.1.1. Run the Dashboard

- On the desktop of your Windows administrative workstation, double-click the Likewise Operations



Dashboard Console

- Or, on the desktop of your Windows administrative workstation, click **Start**, click **All Programs**, point to **Likewise**, and then click **Likewise Operations Dashboard Console**.

19.10.1.2. Add the Dashboard to the Management Console

1. On your Windows administrative workstation, in the Likewise Management Console, on the **File** menu, click **Add/Remove Plug-in**.
2. Click **Add**.
3. Click **Operations Dashboard**, click **Add**, and then click **Close**.
4. Click **OK**.

19.10.2. Connect to a Database

You can connect to a database or change your database connection.

1. In the console tree, click **Operations Dashboard**.
2. Right-click **Operations Dashboard** and then click **Connect to**.
3. Click **Change**.
4. Under **Database Type**, select the kind of database you want to connect to.
5. In the **Server/Instance** box, click the drop-down list and select the instance that you want, or type the name of your server/instance.

19.10.3. Change the Refresh Rate

1. In the console tree, click **Operations Dashboard**.
2. Right-click **Operations Dashboard** and then click **Metric settings**.
3. Under **Options**, in the **Refresh Interval** box, enter the number of minutes .
4. Under **Database Type**, select the kind of database you want to connect to.
5. In the **Server/Instance** box, click the drop-down list and select the instance that you want, or type the name of your server/instance.

19.11. Configuring the Likewise Data Collectors

You can manage the Likewise data collectors, `LWCollector` and `LWEventDBReaper`, in two ways: by using the shell prompt or by using the Likewise Enterprise Database plug-in for the management console. This section describes how to configure the collectors with the shell prompt. The next section shows you how to manage the collectors with the plug-in.

19.11.1. LWCollector

A provider name and a connection string are the only required parameters to run the LWCollector, which is auto-started as a Windows process at `c:\program files\likewise\enterprise`. Unless you change the optional parameters, the collector uses its defaults. You can change the defaults from the Likewise Management Console by using the Enterprise Database Management plug-in or the command line.

To view the arguments of LWCollector, execute the following command at the shell prompt:

```
C:\Program Files\Likewise\Enterprise>lwcollector /?
```

The options of LWCollector are as follows:

Option	Description
/? or /h	Displays help.
/b	Controls how many events are sent per batch.
/p	Controls the maximum number of events that an endpoint sends to the collector during each period.
/s	Shows the settings.
/t	Controls how often the endpoint is to connect to the collector to forward events.
/a	Specifies the access-control list (ACL) of the machines allowed to communicate with the collector.

The service includes `/b`, `/p`, and `/s` options, each of which is discussed in this section. The options configure the size and time period for the data that the endpoints on the computers running the Likewise agent send to the collector. You configure the collector with parameters for the endpoints. The endpoints query the collector for their communication parameters.

The `/t` parameter controls how often the endpoint is to connect to the collector to forward events. The parameter sets the forwarding period in seconds. If the forwarding period is set to 300 seconds, for example, the endpoint event forwarder daemon sends events to a collector once every 5 minutes. The smaller the number is, the more frequently endpoints communicate with collectors and the smaller the latency between the time when an event is generated and when it appears in the database. If the number is too small, however, it can result in excessive load on the endpoints and in excessive network traffic.

The `/p` parameter controls the maximum number of events that an endpoint sends to the collector during each period. This number, in combination with the `/t` parameter, can be set to control the load on endpoints imposed by the event forwarding daemon (`eventfwdd`) sending events to collectors. If this number is large, the event forwarder might consume excessive CPU time and network bandwidth. If the number is small, however, the endpoint might fall behind with the incoming event rate and end up with a large backlog of uncollected events.

The `/b` parameter controls how many events are sent per batch. The collector sends events in batches until the number of sent events reaches the value that you set (or until there are no more left to send, whichever number is smaller). If the `/b` parameter is set too high, the network transaction might fail because of a connection that times out. If the parameter is set too low, the event forwarding daemon might consume too much CPU time and bandwidth because there are more network transactions.

The final LWCollector parameter, `/a`, specifies the access-control list (ACL) of the machines allowed to communicate with the collector. The parameter sets configuration information that affects the collector

itself rather than the endpoints that communicate with it. By default, the ACL for the collector's RPC port is set to allow computers in the Active Directory Domain Computers group to write to the collector. This is the permission set by the long SDDL formatted string shown in the usage information for the /a parameter. In the case of collectors that are servicing multiple domains, however, this ACL is insufficient as it allows only endpoints joined to the same domain as the collector to write to it. In such cases, you can use the /a parameter to specify a more inclusive ACL.

The /s parameter shows the default settings:

```
C:\Program Files\Likewise\Enterprise>lwcollector -/s
Current settings:
Records per period      10000
Records per batch      100
Seconds in a period    10
Database location C:\Program Files\Likewise\Enterprise\LWCollector.db
Remote access security descriptor O:LSG:BAD:P(A;;CC;;;DC)(A;;CC;;;DA)
(A;;RP;;;DA)(A;;DC;;;DA)(A;;CC;;;BA)(A;;RP;;;BA)(A;;DC;;;BA)
(A;;CC;;;S-1-5-21-418081286-1191099226-2202501032-515)
```

The remote access security descriptor shown in the above output is the default. It provides the following group accounts with these permissions:

- Domain Computers are allowed to create children (add events)
- Domain Administrators are allowed to create children (add events)
- Domain Administrators are allowed to read properties (read events)
- Domain Administrators are allowed to delete children (delete events)
- Built-in Likewise Administrators are allowed to create children (add events)
- Built-in Likewise Administrators are allowed to read properties (read events)
- Built-in Likewise Administrators are allowed to delete children (delete events)

The ACL is stored in the Windows registry of the collector server. The Likewise console writes the ACL to the Likewise Enterprise database. The `LWEventDBReaper` service pulls it from the database and writes it to the registry.

19.11.2. LWEventDBReaper

The other collector service, `LWEventDBReaper`, takes events from a collector (forwarded by endpoints) and writes these events to the database. `LWCollector` stores incoming events in a local, intermediate, database while `LWEventDBReaper` takes these events and writes them to the central database. To view the arguments of `LWEventDBReaper`, execute the following command:

```
C:\Program Files\Likewise\Enterprise>lweventdbreaper /?

LWEventDBReaper -- Likewise Event Reaper agent for Windows. Copies
events from a Likewise Event Collector server to the central
Likewise SQL Server database. This program is run as a Windows
service,
but can be run from the command line to set up parameters for the
service.
```

Usage:

Setting Up the Likewise
Reporting Database

LWEventDBReaper OPTIONS

Options:

-/?	Shows this help
-/gui not	Shows graphical database configuration form (do not specify -/d or -/c if using this option).
-/d PROVIDER Specify	Specifies the database provider to be used. System.Data.SqlClient for SQL Server (default) or MySql.Data.MySqlClient for MySQL.
-/c DBSTRING	Specifies the database connection string to be used to talk to the Likewise database.
-/f NUMBER	Specifies the earliest record id that should be copied when the agent runs. USE WITH CAUTION!
-/r	Refreshes the agent with new registry settings.
-/s	Shows the current status

The /d and /c parameters are used to set the database provider and connection strings for the service. Or, you can run the following command to open the dialog box for changing the database provider and connection strings:

```
C:\Program Files\Likewise\Enterprise>lweventdbreaper /gui
```

The /f parameter is used to control the point at which the first event in the local collector database is written to the central Likewise database. Under normal circumstances, it should not be necessary to set this parameter.

Any parameters set from the command line will take effect the next time that LWEventDBReaper runs. If you want the service to immediately make use of the new parameters, you can run LWEventDBReaper with the /r command-line argument.

The /s is used to display the current configuration settings for the service:

```
C:\Program Files\Likewise\Enterprise>lweventdbreaper -/s
```

Current settings:

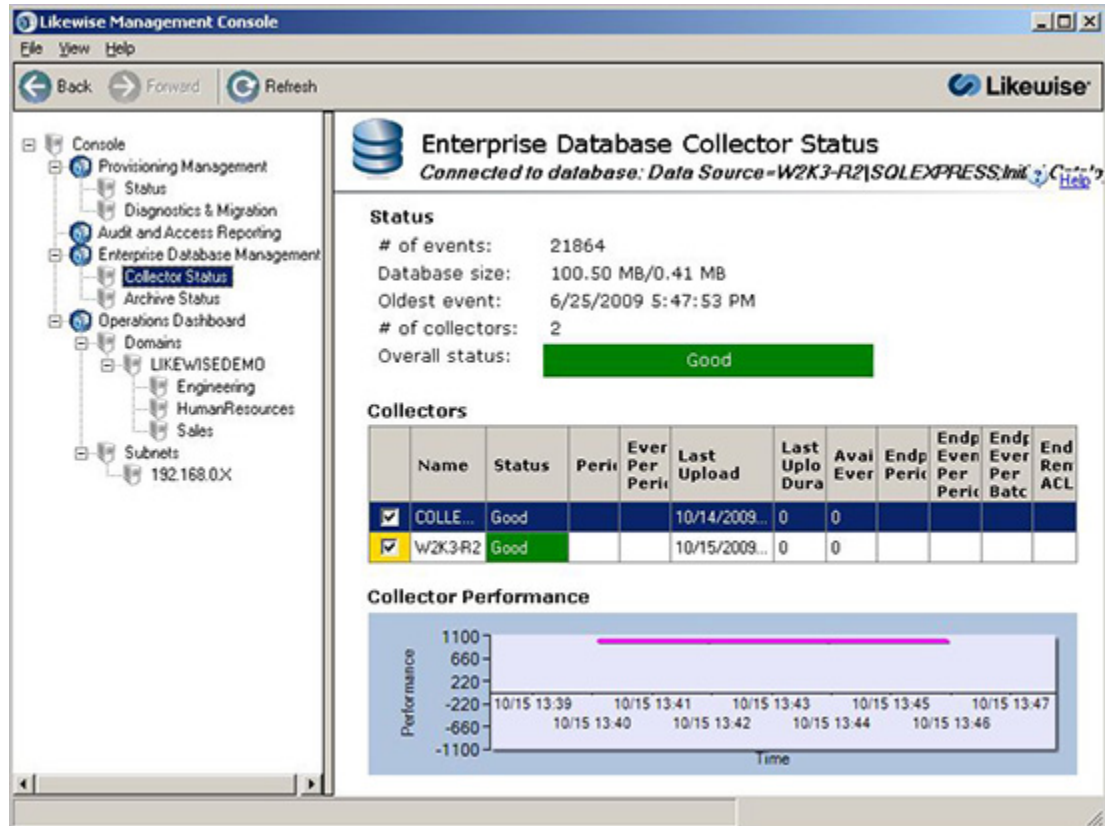
```
Database provider:      System.Data.SqlClient
Connection string:     Data Source=RVLN-BUILD;
                       Initial Catalog=LikewiseEnterprise;
                       Integrated Security=True
Record id last copied: 1794
Records per period:    300
Seconds in a period:   1200
```

Although the settings include records per period and seconds in a period, the parameters cannot be configured from the command-line. The default values can be changed through the Enterprise Database Management plug-in in the Likewise Management Console.

19.12. Working with the Enterprise Database Management Plug-In

You can use the Enterprise Database Management plug-in for the Likewise Management Console to monitor and configure the Likewise Enterprise database and to manipulate archived event information. You add the plug-in to the console in the same way that you add other plug-ins; for an example, see Add the Dashboard to the Management Console.

The plug-in looks like this:



19.12.1. Connect to a Database

You can connect to a database or change your database connection.

1. In the console tree, right-click **Enterprise Database Management** and then click **Connect to**.
2. Click **Change**.
3. Under **Database Type**, select the kind of database you want to connect to.
4. In the **Server/Instance** box, click the drop-down list and select the instance that you want, or type the name of your server/instance.

19.12.2. Change the Parameters of the Collectors

You can use the Enterprise Database Management plug-in to set parameters for the collectors.

1. In the console tree, expand **Enterprise Database Management**.
2. Click **Collector Status**, and then right-click **Collector Status**.
3. Click **Set collector parameters**.

Or, in the list of collectors, right-click the name of the collector that you want to modify.

4. Enter the parameters that you want.

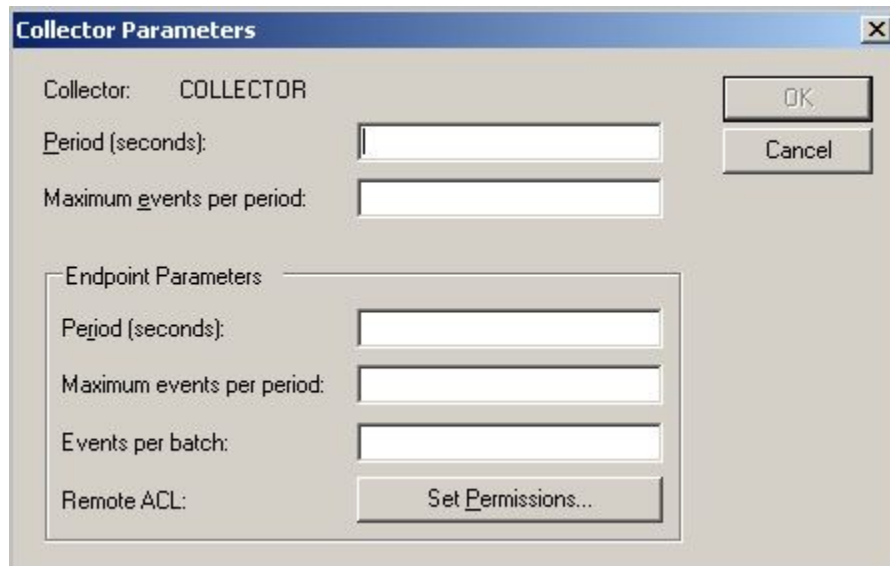
19.12.3. Set the ACL for RPC Access

You can set the access control list for the remote procedure calls that take place between the collector and its endpoints.

1. In the console tree, expand **Enterprise Database Management**.
2. Click **Collector Status**, and then right-click **Collector Status**.
3. Click **Set collector parameters**.

Or, in the list of collectors, right-click the name of the collector that you want to modify.

4. Click **Set Permissions**:



5. In the same way that you set permissions with Active Directory Users and Computers, set the permissions that you want.

19.13. Archiving Events

You can archive events in two ways: either with the Enterprise Database Management plug-in or with the command line.

The Likewise event-archiving utility – `LWArchive` -- combines events older than one year into compressed archives and stores them in a separate database table. A separate archive is created for

each month of old event data. After events are archived, they are deleted. The event-archiving utility is intended to be run according to a monthly schedule.

Archive Events with the Console

1. In the console tree, expand **Enterprise Database Management**.
2. Click **Archive Status**, and then right-click **Archive Status**.
3. Click **Create archive**, and then follow the instructions in the wizard.

Archive Events with the Command Line

To view the arguments of LWArchive, execute the following command at the shell prompt on a Windows computer running the Likewise collectors:

```
C:\Program Files\Likewise\Enterprise>lwarchive /?
```

The `-p` and `-c` options identify the database type and connection string of the central Likewise Enterprise database. The connection string is the same as the one that you used when you configured the connection the database. With SQL Server, for example, you enter a string like this:

```
Data Source=DBSERVERNAME;Initial Catalog=LikewiseEnterprise;Integrated Security=True
```

Here's an example:

```
Data Source=W2K3-R2\SQLEXPRESS;Initial Catalog=LikewiseEnterprise;Integrated Security=True
```

With MySQL, you enter a string like this:

```
server=yourDBserverInstanceName;database=LikewiseEnterprise;userid=dbUserAccount;password=dbUserAccountPassword;
```

Here's an example:

```
server=steveh-dc;database=LikewiseEnterprise;userid=root;password=password;
```

The `-a` and `-t` options are used to control the archive time unit and the date threshold for archiving. It is suggested that these options not be used and that the program use its default settings, which are `-a monthly` and `-t 12`. These defaults create monthly archives for data older than 12 months.

The `-o` option is used to control where the log output of LWArchive is written. By default, the output is written to the console.

19.14. Troubleshooting

If the information in your reports or the events displayed in the Operations Dashboard seem incomplete, perform the following series of diagnostic tests sequentially. The series of tests begins with the endpoints -- your Linux, Unix, and Mac OS X computers that log events and send them to the collector

server. The tests then move on to the collector server -- the server that processes events from the Likewise clients and forwards them to the database. The final series of tests examines the database.

19.14.1. Check the Endpoints

1. Log on to a computer that you suspect might have a problematic endpoint and check whether events are being logged in the local event database by executing the following command as root or as an AD user with administrator privileges:

```
/opt/likewise/bin/lw-eventlog-cli -s - localhost
```

2. If no recent events are displayed or if the command returns errors, make sure that the `eventlog` service is running:

```
/opt/likewise/bin/lwsm status eventlog
```

3. If it is not running, check `/var/log/messages` to find out why and report the information to Likewise support. Then, restart the service:

```
/opt/likewise/bin/lwsm start eventlog
```

Note: On HP-UX, Likewise uses HP's `rpcd` daemon instead of `dcerpcd`. If the HP-UX `rpcd` daemon does not allow `eventlogd` to register an RPC endpoint, restart the `rpcd` daemon and then restart `eventlogd`.

4. If recent events are present but are not being forwarded, make sure that the event forwarding service is running:

```
/opt/likewise/bin/lwsm status eventfwd
```

5. If it is not running, check `/var/log/messages` to try to identify the cause and report the information to Likewise support. Then, restart the service:

```
/opt/likewise/bin/lwsm start eventfwd
```

6. Next, check the event forwarding service's configuration in the Likewise registry to make sure that it properly identifies a collector server and, if the collector server is identified by its IP address, its `collector-principal`. If you modify the settings of the `eventfwd` service, you must restart the service for the changes to take effect.

Example of a configuration that uses the host name of its collector:

```
[HKEY_THIS_MACHINE\Services\eventfwd\Parameters]  
- "Collector"="w2k3-r2.likewisedemo.com"
```

7. Make sure the collector can be resolved:

```
[root@rhel15d bin]# nslookup w2k3-r2.likewisedemo.com  
Server:          192.168.92.20  
Address:         192.168.92.20#53  
Name:   w2k3-r2.likewisedemo.com  
Address: 192.168.92.20
```

8. Make sure the collector server can be reached:

```
[root@rhel15d bin]# ping w2k3-r2.likewisedemo.com  
PING w2k3-r2.likewisedemo.com (192.168.92.20) 56(84) bytes of data.
```

```
64 bytes from 192.168.92.20: icmp_seq=1 ttl=128 time=1.40 ms
```

9. If the collector is identified by IP address, make sure the collector-principal is properly set. For example, if the collector server is at IP address 10.100.1.100 and has a Kerberos machine name of EventCollector in the AD domain mycorp.com, the collector-principal parameter would be:

```
collector-principal = host/EventCollector@MYCORP.COM
```

10. Check /var/log/messages for errors.

11. Stop the eventfwdd service and then run it from the command line to display error information about the event forwarder's communication with the collector server:

```
/opt/likewise/bin/lwsm stop eventfwd
```

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

After you run eventfwdd from the command line, stop it with CTRL-C and then restart it:

```
/opt/likewise/bin/lwsm start eventfwd
```

After you have verified that the endpoint is properly receiving events and forwarding them to a collector server, check the collector. If there are recent events, make a note of the last event's time stamp, event category, and event description. In the next section, you check whether the collector received the event.

19.14.2. Check the Collector

1. Make sure LWCollector is running by executing the following command at the shell prompt of the Windows computer running the collector:

```
C:\Program Files\Likewise\Enterprise>sc query LWCollector
```

```
SERVICE_NAME: LWCollector
                TYPE                -: 10   WIN32_OWN_PROCESS
                STATE                 -: 4    RUNNING
```

2. If the process is stopped, use eventvwr.exe to check the Windows event log for information about why the service failed.

Note: If there are unusual RPC errors in the Windows event log, make sure you have not installed the LikewiseDBUtilities on a Windows XP machine. The collector server must be running Windows 2003 or Windows 2008. Windows XP, by default, restricts the incoming TCP-based RPC used by lwcollector.

3. If the process is not running, start it by executing the following command:

```
C:\Program Files\Likewise\Enterprise>sc start lwcollector
```

4. Verify that the service is receiving forwarded events by viewing the contents of the collector's local SQLite database. To execute the following command, the lwcollector process must be running and you must have read privileges in the access control list:

```
C:\Program Files\Likewise\Enterprise>lwcollector-cli -s - localhost
```

The command should return a list of the events collected from the endpoints. If there is no data, it is likely that your endpoints are improperly configured (see the previous section). If the event that you

noted when checked the event forwarder in the previous section is among the results, make sure the `lweventdbreaper` service is functioning properly.

5. Verify that `lweventdbreaper` is running:

```
C:>sc query lweventdbreaper
```

6. If the process is stopped, use `eventvwr.exe` to check the Windows event log for information about why the service failed. Restart the service with:

```
C:>sc start lweventdbreaper
```

7. Check the database connection string and the service's other execution parameters:

```
C:\Program Files\Likewise\Enterprise>lweventdbreaper /s
```

The results should look something like this:

```
Database provider:      System.Data.SqlClient
Connection string:      Data Source=SomeCollector;Initial
Catalog=LikewiseEnterprise;Integrated Security=yes
Record id last copied: 487
Records per period:     120
Seconds in a period:    10000
```

If the database server (`Data Source=` for SQL Server or `Server=` for MySQL) is identified by name (as in the example), verify that the name can be resolved to an address by using `nslookup` and verify that the address is reachable from the collector server by using `ping`.

8. Use `eventvwr.exe` to check the Windows event log for messages. If `lweventdbreaper` is failing to write to the central Likewise Enterprise database and if you are using SQL Server with integrated security, make sure that the collector server's machine account has sufficient privileges to write to the Likewise Enterprise database.

19.14.3. Check the Database

1. Check the Likewise Enterprise database on the database server to check whether the table containing events is complete. If necessary, write a manual query to view recent events or to look for an event. For example, with MySQL you can use the MySQL command-line utility to open the LikewiseEnterprise database and run the following command to display all the events in the table named `Events`:

```
select * from Events;
```

2. If you have a problem opening or reading the database, you might not have sufficient privileges to access it -- which can result in problems when you run reports in the Likewise Console or use the Operations Dashboard.
3. If you are using SQL Server and the `Events` table is empty, use the SQL Server Configuration Manager to make sure that the name-pipe client protocol is enabled. If it is not and you have to enable it, you must restart the SQL Server service for the changes to take effect.
4. If you find events in the `Events` table, check whether the events are also present in the `EventsViewWithOUnName` view. If an event appears in the `Events` table but not in the `EventsWithOUnName` view, it is because the database cannot associate your event with a computer

in Active Directory. Run the `ldbupdate.exe` script and then check whether the event now appears in both views.

19.14.4. Troubleshooting Checklists

The checklists in this section can help you troubleshoot problems with the reporting components.

Endpoints

Item to Check
eventlogd running
eventfwdd running
reapsysld running
eventfwd service properly configured
Collector name resolvable; address reachable
Collector principal properly set
/etc/syslog.conf properly configured
Events present in local event log (test with <code>lw-eventlog-cli</code>)
eventfwdd seems to forwarding messages properly (run from command-line to test)
Firewall not blocking RPC access of collector server

Collector Servers

Item to Check
lwcollector service running
lweventdbreaper service running
Events present in local collector database (test with <code>lwcollector-cli</code>)
lweventdbreaper properly configured (test with <code>lweventdbreaper /s</code>)
Database provider and connection string properly set
Collector ACL allows endpoints to write to it (set with Event Management Console)
Collector machine account has sufficient privileges to write to database
No unusual errors in Windows event log (run <code>eventvwr.exe</code>)
Firewall not blocking incoming RPC connections or outgoing database connections

Database

Item to Check
Can connect to it with SQL Server Management Studio or MySQL utility
Events table contains events
EventsWithOUName view contains events
Database security set to allow writing by collector servers, by <code>ldbupdate</code> user, and by administrators
<code>ldbupdate</code> utility recently run to account for new endpoints joined to AD
Named-pipe client access enabled in SQL Server

Firewall not blocking incoming database connection

Windows Reporting Components

Item to Check
Database connection strings set properly
User has sufficient privileges to access database
Firewall not blocking database connections

19.14.5. Switching Between Databases

To send events to a different database, you must change the database connection string in at least two places: the reaper service for the database (`lweventdbreaper`) and the Enterprise Database Management page in the Likewise Management Console. Changing the setting on the Enterprise Database Management page automatically changes the same setting on the console's Audit and Access Reporting page and the Operations Dashboard.

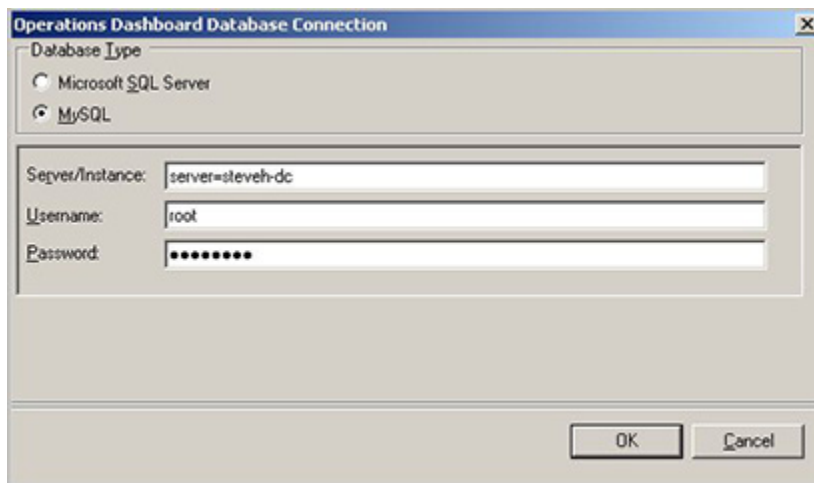
If, however, you have installed different plug-ins of the Likewise Management Console on different computers -- for example, to run the Operations Dashboard on a separate machine -- you must change the database connection string on each machine and you might have to change it in the following additional locations, especially if the computer's Likewise console does not include the Enterprise Database Management plug-in: the Audit and Access Reporting page and the Operations Dashboard page.

After making the changes, you must reset the reaper service so it begins sending events to the new database.

1. In the Likewise console tree on your Windows administrative workstation, right-click the **Enterprise Database Management** node and then click **Connect to database**.

Click **Change**. Under **Database Type**, select **MySQL** or **Microsoft SQL Server**, and then enter the name of the database server instance in the **Server/Instance** box.

In the **Username** and **Password** boxes, enter the credentials of the database definer account if required for the authentication type that you selected, and then click **OK**.



2. In the console tree, right-click the **Operations Dashboard** node and then click **Connect to**.

Click **Change**. Make the changes that you want, and then click **OK**.

3. In the console tree, right-click the **Audit and Access Reporting** node, and then click **Advanced**.

Click **Change**. Make the changes that you want, and then click **OK**.

4. Open a command prompt window as an administrator and then change directories to C:\Program Files\Likewise\Enterprise, and then run the following command:

```
lweventdbreaper /gui
```

Make the changes that you want, and then click **OK**.

5. Finally, you must reset the eventdbreaper to 0 and then refresh its settings to prompt it to send the events to the new database. To do so, from the C:\Program Files\Likewise\Enterprise directory, run the following commands as an administrator:

```
lweventdbreaper -/f 0  
lweventdbreaper -/r
```

Chapter 20. Monitoring Events with the Event Log

20.1. 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.

20.2. View the Local Event Log

On a Linux, Unix, or Mac OS X computer, you view the local Likewise Event Log by using the `eventlog` command-line utility with the root account:

```
/opt/likewise/bin/lw-eventlog-cli
```

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

```
/opt/likewise/bin/lw-eventlog-cli -h
```


You can gain access to the event log by using either localhost or the virtual loopback interface of the computer, which is typically assigned to the address 127.0.0.1.

To view a summary of events, execute the following command with the root account:

```
/opt/likewise/bin/lw-eventlog-cli -s - localhost
```

Example output:

```
=====
Event Record: (392/396) (392 total)
=====
Event Record ID..... 392
Event Table Category.... System
Event Type..... Information
Event Date..... 2010-02-16
Event Time..... 07:37:58 AM
Event Source..... Likewise LSASS
Event Category..... Service
Event Source ID..... 1004
Event User..... SYSTEM
Event Computer..... glennc-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]
=====

```

20.3. 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"

```

20.4. The Event Source

The Event Source is typically one of the following values: Likewise LSASS, Likewise GPAGENT, Likewise DomainJoin, Likewise NETLOGON, System Log.

20.5. 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

```

Monitoring Events with the Event Log

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_ENCOUNTERED 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 21. Using Likewise for Single Sign-On

21.1. About Single Sign-On

When you log on a Linux, Unix, or Mac OS X computer by using your Active Directory domain credentials, Likewise initializes and maintains a Kerberos ticket granting ticket (TGT). The TGT lets you log on other computers joined to Active Directory or applications provisioned with a service principal name and be automatically authenticated with Kerberos and authorized for access through Active Directory. In a transparent process, the underlying Generic Security Services (GSS) system requests a Kerberos service ticket for the Kerberos-enabled application or server. The result: single sign-on.

To gain access to another computer, you can use various protocols and applications:

- SSH (how to configure single sign-on for SSH)
- rlogin
- rsh
- Telnet
- FTP
- Firefox (for browsing of intranet sites)
- LDAP queries against Active Directory
- HTTP with an Apache HTTP Server

How Likewise Makes SSO Happen

Since Microsoft Windows 2000 was released, Active Directory's primary authentication protocol has been Kerberos. When a user logs on to a Windows computer that is joined to a domain, the operating system uses the Kerberos protocol to establish a key and to request a ticket for the user. Active Directory serves as the Kerberos key distribution center, or KDC.

Likewise configures Linux and Unix computers to interact with Active Directory in a similar way. When a user logs on a Linux and Unix computer joined to a domain, Likewise requests a ticket for the user. The ticket can then be used to implement SSO with other applications.

Likewise fosters the use of the highly secure Kerberos 5 protocol by automating its configuration on Linux and Unix computers. To ensure that the Kerberos authentication service is properly configured, Likewise does the following:

- Ensures that DNS is properly configured to resolve names associated with Active Directory (AD).
- Performs secure, dynamic DNS updates to ensure that Linux and Unix computer names can be resolved with AD-integrated DNS servers.
- Configures Kerberos. In an environment with multiple KDCs, Likewise makes sure that Kerberos selects the right server.

- Configures SSHD to support SSO through Kerberos by using GSSAPI.
- Creates a keytab for the computer in the following way: When you join a Linux or Unix computer to AD, Likewise creates a machine account for the computer. Likewise then automatically creates a keytab for the SPN and places it in the standard system location (typically `/etc/krb5.keytab`).
- Creates a keytab for the user during logon. On most systems, the user keytab is placed in the `/tmp` directory and named `krb5cc_UID`, where `UID` is the numeric user ID assigned by the system.

Overview of How to Implement SSO with Likewise

When you install Likewise on a Linux, Unix, or Mac OS X computer and join it to Active Directory, Likewise prepares it for single sign-on by creating a keytab for the computer. However, when you use Likewise to implement SSO with other applications or services, you will likely have to configure the application to use GSSAPI and Kerberos 5 authentication and you will likely have to provision each application user for external Kerberos authentication. At the very least, you will have to provision your application with a service principal name in Active Directory. A service principal name, or SPN, is the name with which a client uniquely identifies an instance of a service. Kerberos then uses the SPN to authenticate a service.

Note: Configuring an external application for SSO with Kerberos is beyond the scope of the Likewise documentation; for more information, see the vendor's manual for your application.

The following process outlines the steps for setting up an application or service to use Likewise for single sign-on. For a detailed example of how to configure an application for SSO, see [Configure Apache for SSO](#). For examples of how to create a service account in AD, register an SPN for the service account, and create a keytab for the SPN, see [creating a Kerberos service principal and keytab file for SSO on the IBM web site](#).

1. Create a service account for the application in Active Directory.
2. Associate a service principal name, or SPN, with the service account in Active Directory; see the overview of `setspn.exe` on Microsoft TechNet.
3. Create a keytab for the SPN with the `ktpass` utility.
4. Place the keytab in the appropriate location on the Linux or Unix computer.
5. Configure the authentication module to get its Kerberos key from the generated keytab.
6. Configure the authentication module to determine appropriate roles by examining Active Directory group membership.
7. Configure an application to restrict access to Active Directory authenticated users in certain roles.
8. Test SSO by accessing restricted web sites from a Windows client running Microsoft Internet Explorer or Mozilla Firefox. Repeat this step on Linux and Unix using Firefox.

21.2. 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#

```

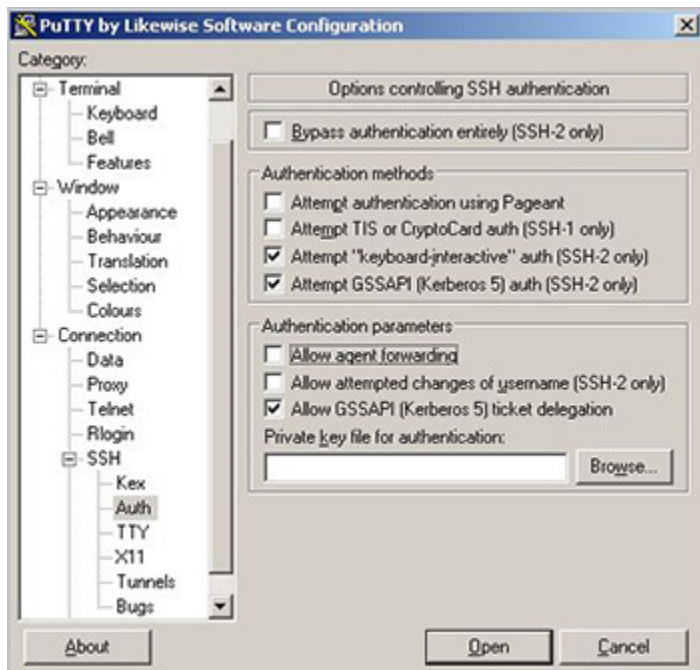
21.3. Configure PuTTY for Windows-Based SSO

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**.

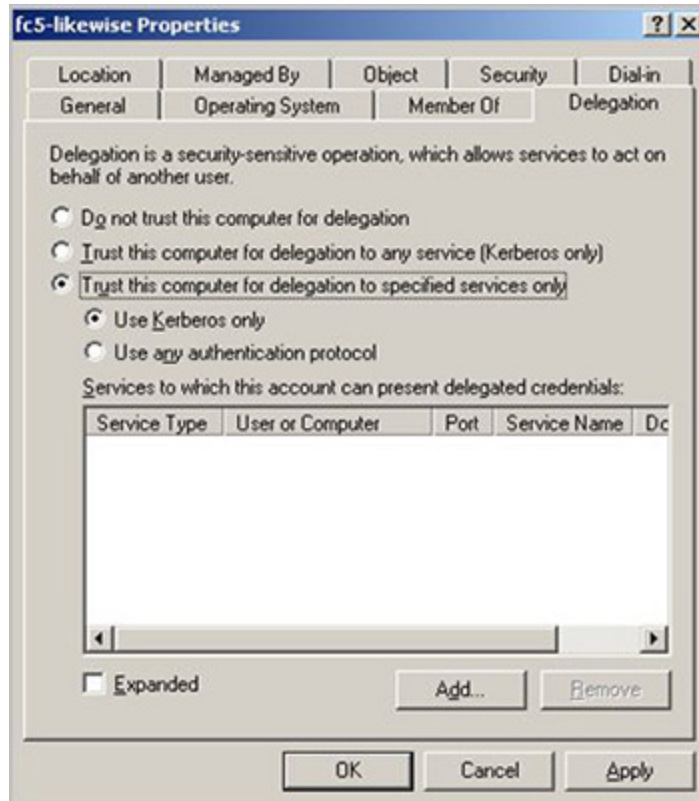


Configure the Base Linux Computer in Active Directory

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

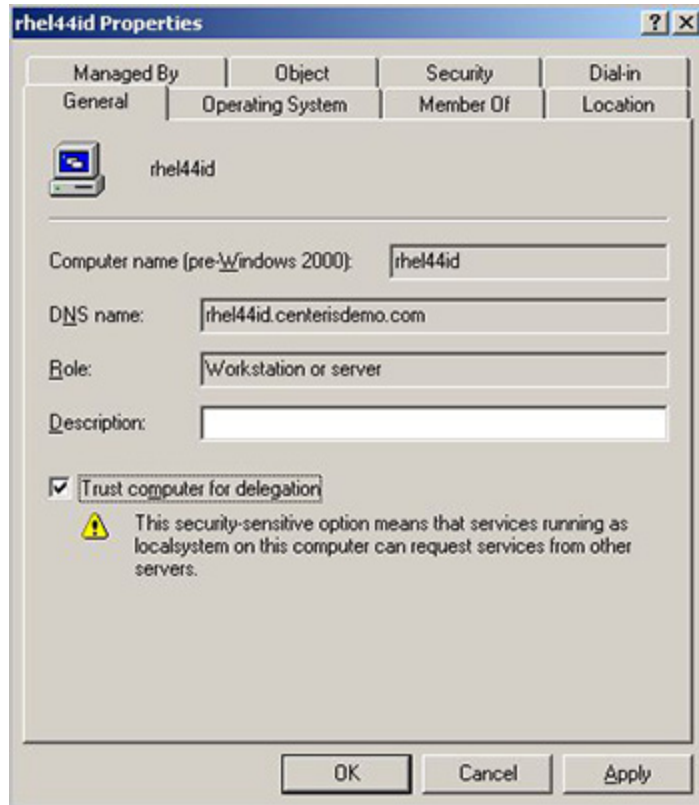
1. In Active Directory Users and Computers, in the console tree, click **Computers**.
2. In the details pane, right-click the computer that you want, and then click **Properties**.
3. On the **Delegation** tab, click **Trust this computer for delegation to specified services only**:



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**:



21.4. Configure Apache for SSO

This section describes how to configure Likewise and the Apache HTTP Server to provide single sign-on authentication through Active Directory with Kerberos 5. The instructions assume that you know how to administer Active Directory, the Apache HTTP Server, and computers running Linux.

Single sign-on for the Apache HTTP server uses the Simple and Protected GSS-API Negotiation Mechanism, or SPNEGO, to negotiate authentication with Kerberos. SPNEGO is an Internet standard documented in RFC 2478 and is commonly referred to as the negotiate authentication protocol. The Likewise `mod_auth_kerb` module lets an Apache web server running on a Linux or Unix system authenticate and authorize users based on their Active Directory domain credentials.

Important: This topic assumes that you have installed either Likewise Open 5.0 or later or Likewise Enterprise 5.0 or later, build **3946** or later, on the Linux computer running your Apache HTTP Server and that you have joined the server to Active Directory. With build 3946, Likewise 5.0 began to include the Apache `mod_auth_kerb` module in `/opt/likewise/apache`; the Likewise version of the `mod_auth_kerb` module is required to set up your Apache HTTP Server for single sign-on. Later versions of Likewise, such as 6.1, package the module independently: It is in the application integration installer, which you can obtain for free from the Likewise web site by registering to download Likewise Open. (The name of the application integration package looks like this: `LikewiseAppIntegration-6.1.0.8656-linux-i386-rpm.sh`.)

To check whether your build of Likewise Enterprise or Likewise Open includes `mod_auth_kerb`, confirm that the following components exist:

```
/opt/likewise/apache/2.0/mod_auth_kerb.a
```

```
/opt/likewise/apache/2.0/mod_auth_kerb.so  
/opt/likewise/apache/2.2/mod_auth_kerb.a  
/opt/likewise/apache/2.2/mod_auth_kerb.so
```

Requirements

- Likewise Open 5.0 or later or Likewise Enterprise 5.0 or later, build 3946 or later. Later versions of Likewise, such as 6.1, also require the application integration package (LikewiseAppIntegration-6.1.0.8656-linux-i386-rpm.sh).
- The Linux or Unix computer that is hosting the Apache web server is joined to Active Directory.
- An Apache HTTP Server 2.0 or 2.2 that supports dynamically loaded modules. To check whether your Apache web server supports dynamically loaded modules, execute the following command and verify that `mod_so.c` appears in the list of compiled modules:

```
httpd -l
```

```
Compiled in modules:  
  core.c  
  prefork.c  
  http_core.c  
  mod_so.c
```

For Apache installations that are compiled from the source code, make sure that `--enable-module=so` is specified when `./configure` is executed:

```
./configure --enable-module=so
```

- Your Kerberos libraries must support SPNEGO. For example, MIT Kerberos libraries that are version 1.5 and later support SPNEGO; earlier versions do not. Make sure your Kerberos libraries support SPNEGO by running `ldd`:

```
which httpd  
/usr/sbin/httpd  
ldd -/usr/sbin/httpd
```

In the results, find the line that references `libgssapi`:

```
libgssapi_krb5.so.2 => /usr/lib/libgssapi_krb5.so.2 (0x00231000)
```

Finally, query the version number of the library and make sure it is **1.5 or later**:

```
rpm -qif /usr/lib/libgssapi_krb5.so.2
```

```
Name           -: krb5-libs           Relocations: (not  
relocatable)  
Version        -: 1.5                 Vendor: Red Hat, Inc.  
Release        -: 17                 Build Date: Tue 16 Jan  
2007 10:01:00 AM PST  
Install Date:  Fri 14 Dec 2007 09:09:44 AM PST      Build Host: ls20-  
bc1-13.build.redhat.com  
Group          -: System Environment/Libraries   Source RPM:  
krb5-1.5-17.src.rpm
```

```

Size          -: 1333337                               License: MIT, freely
distributable.
Signature     -: DSA/SHA1, Wed 17 Jan 2007 10:57:33 AM PST, Key ID
5326810137017186
Packager      -: Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
URL           -: http://web.mit.edu/kerberos/www/
Summary       -: The shared libraries used by Kerberos 5.
Description   -:
Kerberos is a network authentication system. The krb5-libs package
contains the shared libraries needed by Kerberos 5. If you are using
Kerberos, you need to install this package.
[root@rhel5d sbin]#

```

Configure Apache HTTP Server 2.2 for SSO on RHEL 5

The following instructions demonstrate how to configure Likewise and Apache for SSO on a Red Hat Enterprise Linux 5 computer. The steps vary by operating system and by Apache version. Ubuntu, in particular, uses `apache2` instead of `httpd` for commands, the name of the daemon, the configuration directory, the name of the configuration file, and so forth.

Important: Configuring web servers is complex. Before you deploy your configuration to a production web server, implement and test it in a test environment. More: Before you change your web server's configuration, read and understand the Apache HTTP Server documentation at <http://httpd.apache.org/docs/> and the `mod_auth_kerb` documentation at <http://modauthkerb.sourceforge.net/configure.html>. Before you change a file, make a backup copy of it.

1. Determine whether your Apache server is 2.0 or 2.2 by running the following command:

```

httpd -v

Server version: Apache/2.2.3
Server built:   Nov 29 2006 06:33:19

```

2. Edit your Apache configuration file `-- /etc/httpd/conf/httpd.conf --` to add a directive to load the Likewise `auth_kerb_module` for your version of Apache. Since my Red Hat computer is running Apache 2.2.3, I have added the 2.2 version of the module to the list after the other `auth` modules (which were already listed in the file):

```

LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule auth_kerb_module  -/opt/likewise/apache/2.2/
mod_auth_kerb.so

```

3. In `/etc/httpd/conf/httpd.conf`, configure authentication for a directory and then restart the web server; example:

```

<Directory -"/var/www/html/secure">
Options Indexes MultiViews FollowSymLinks
AllowOverride None
Order deny,allow
Deny from all
Allow from 127.0.0.0/255.0.0.0 -::1/128
AuthType Kerberos
AuthName -"Kerberos Login"
KrbAuthRealms LIKewiseDEMO.COM

```

```
Krb5Keytab -/etc/apache2/http.ktb
Require valid-user
</Directory>
```

Tip: You can require that a user be a member of a security group to access the Apache web server by replacing `Require valid-user` with `Require group name-of-your-group`, as shown in the example below. To control group access by requiring group membership, however, you must first install and load `mod_auth_pam`; for instructions on how to set up `mod_auth_pam`, see http://pam.sourceforge.net/mod_auth_pam/install.html. (Because `mod_auth_pam` is no longer maintained, you should consider using `mod_authz_unixgroup` instead; see the instructions later in this section.)

```
<Directory -"/var/www/html/secure">
Options Indexes MultiViews FollowSymLinks
AllowOverride None
Order deny,allow
Deny from all
Allow from 127.0.0.0/255.0.0.0 -::1/128
AuthType Kerberos
AuthName -"Kerberos Login"
KrbAuthRealms LIKEWISEDEMO.COM
Krb5Keytab -/etc/apache2/http.ktb
Require group linuxfulladmins
</Directory>
```

4. Configure your web server for Secure Socket Layer (SSL). For instructions, see the Apache HTTP Server documentation.

Important: If SSO fails and you have not turned on SSL, your server will prompt you for an ID and password -- which will be sent in clear text. SSL encrypts all data that passes between the client browser and the web server. SSL can also perform Basic Authentication in a secure fashion, providing a fallback mechanism in the event that Kerberos authentication fails. Using SSL is especially important if the protected web site also needs to be accessible from outside the corporate network. For more information, see <http://modauthkerb.sourceforge.net/configure.html>.

5. In Active Directory, create a user account for the Apache web server in the same OU (or, with Likewise Enterprise, cell) to which the Linux computer hosting the web server is joined. Set the password of the user account to never expire. In the examples that follow, the user account for my Apache web server is named `httpUser`.
6. On the domain controller, create an RC4-HMAC keytab for the Apache web server by using Microsoft's `ktpass` utility. For information on `ktpass`, see <http://technet.microsoft.com/en-us/library/cc776746.aspx>. The keytab that you must create can vary by Windows version.

Example:

```
C:\>ktpass -/out keytabfile -/princ HTTP/
rhel5d.likewisedemo.com@LIKEWISEDEMO.COM -/pass SkiAlta2008 -/
mapuser likewisedemo\httpUser -/ptype KRB5_NT_PRINCIPAL
Targeting domain controller: steveh-dc.likewisedemo.com
Using legacy password setting method
Successfully mapped HTTP/rhel5d.likewisedemo.com to httpUser.
Key created.
Output keytab to keytabfile:
Keytab version: 0x502
```

```
keysize 80 HTTP/rhel5d.likewisedemo.com@LIKEWISEDEMO.COM ptype
0 (KRB5_NT_UNKNOWN) vno 3 etype 0x17 (RC4-HMAC) keylength 16
(0x2998807dc299940e2c6c81a08315c596)
```

Note: On Windows 2000, do not specify the domain name as part of the `/mapuser` parameter; just enter the name of the user.

7. Use secure FTP or another method to transfer the keytab file to the Linux computer that hosts your Apache web server and place the file in the location specified in your `<Directory>` configuration in `httpd.conf`. For example, using the configuration shown in Step 3 above, the keytab file would be placed in `/etc/apache2/http.ktb`.
8. Set the permissions of the keytab file to be readable by the ID under which the Apache web server runs and no one else.

Important: The Kerberos keytab file is necessary to authenticate incoming requests. It contains an encrypted, local copy of the host's key and, if compromised, might allow unrestricted access to the host computer. It is therefore crucial to protect it with file-access permissions.

Control Group Access with `mod_authz_unixgroup`

Instead of using the `mod_auth_pam`, which is no longer maintained, you can require that a user be a member of a security group to access the Apache web server by using `mod_authz_unixgroup`. First, install `mod_authz_unixgroup`:

```
yum install httpd-devel
wget http://mod-auth-external.googlecode.com/files/
mod_authz_unixgroup-1.0.2.tar.gz
tar --xzvf mod_authz_unixgroup-1.0.2.tar.gz
cd mod_authz_unixgroup-1.0.2
apxs --c mod_authz_unixgroup.c
apxs --i --a mod_authz_unixgroup.la
```

Then, in `/etc/httpd/conf/httpd.conf`, replace `Require valid-user` with `AuthzUnixgroup on` and `Require group name-of-your-group`:

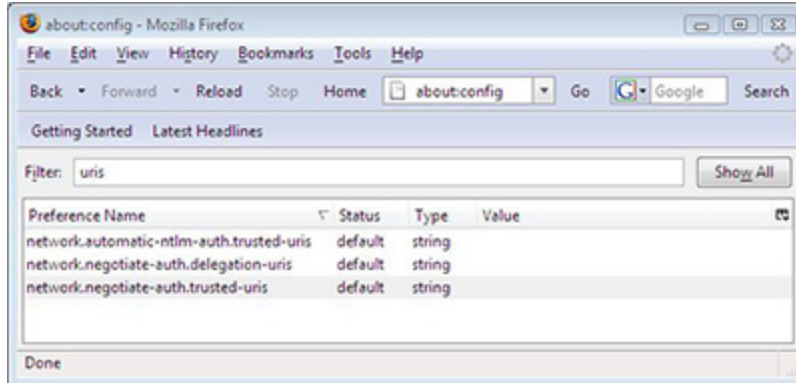
```
<Directory -"/var/www/html/secure">
...
KrbAuthRealms LIKEWISEDEMO.COM
Krb5Keytab -/etc/apache2/http.ktb
AuthzUnixgroup on
Require group linuxfulladmins
</Directory>
```

For more information, see the documentation for `mod_authz_unixgroup`.

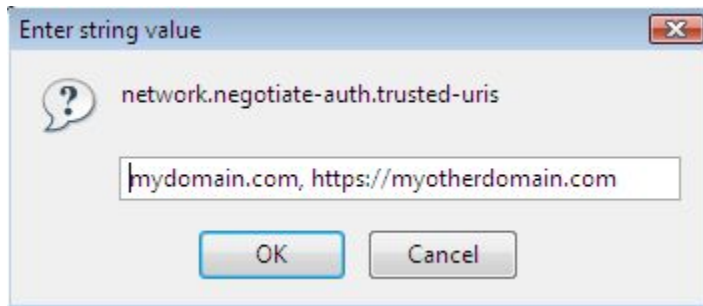
Configure Firefox for SSO

To set up Firefox for single sign-on, you must turn on the Simple and Protected GSS-API Negotiation Mechanism, or SPNEGO, to negotiate authentication with Kerberos.

1. Open Firefox.
2. In the **Go** box, type `about:config`, and then click **Go**.
3. In the **Filter** box, type `uris`.



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:

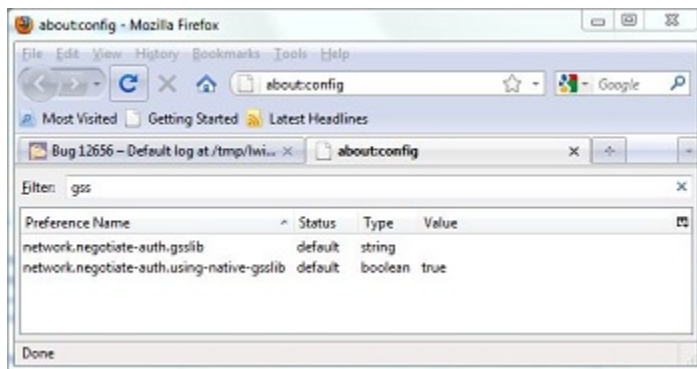


5. Double-click **network.negotiate-auth.delegation-uris**, enter a comma-separated list of the sites for which the browser may delegate user authorization to the server, and then click **OK**.

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

6. To negotiate with your web server through the GSSAPI by using NTLM as the preferred authentication protocol on a Mac OS X computer, you must also modify the GSS preferences as follows. To find the preferences, type `gss` into Firefox's filter box:

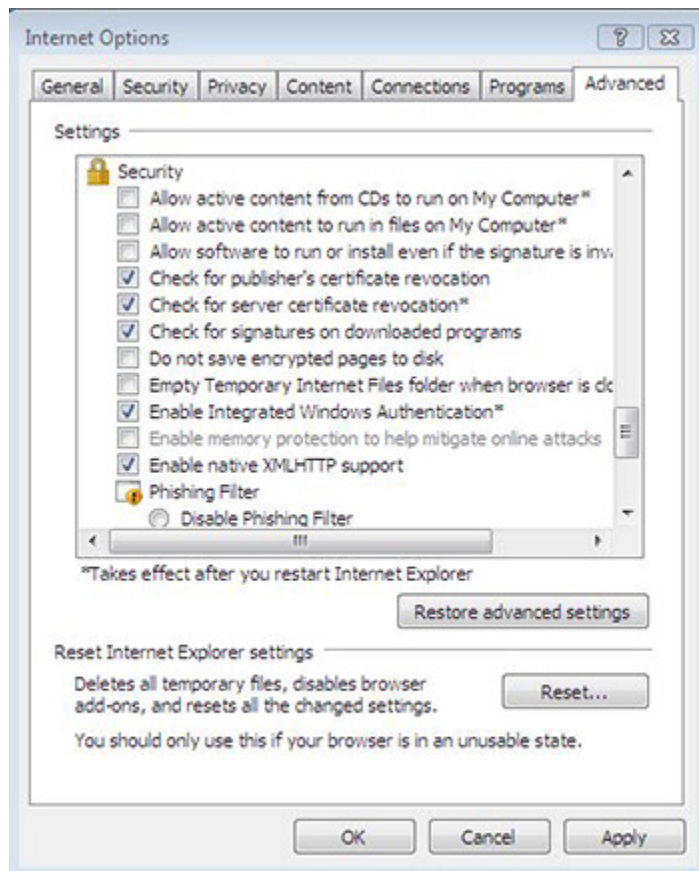
```
network.negotiate-auth.gsslib user set string -/opt/likewise/lib/
libgssapi_krb5.2.2.dylib
network.negotiate-auth.using-native-gsslib user set boolean
false
```



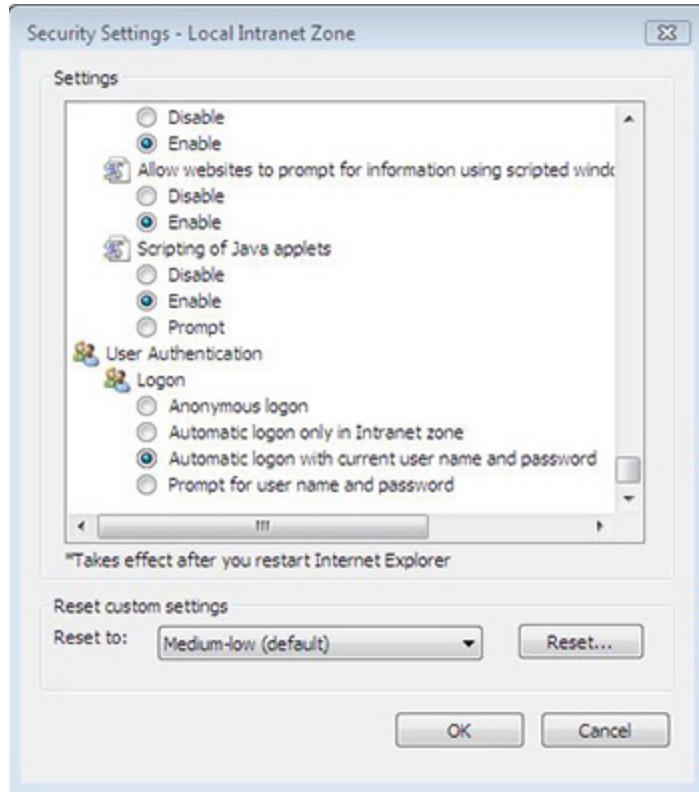
Configure Internet Explorer for SSO

Here's how to configure Internet Explorer 7.0 to use SPNEGO and Kerberos. The settings for other versions of IE might vary; see your browser's documentation for more information.

1. Start Internet Explorer 7.0.
2. On the **Tools** menu, click **Internet Options**.
3. Click the **Advanced** tab and make sure that the **Enable Integrated Windows Authentication** box is selected:



4. Click the **Security** tab.
5. Select a zone -- for example, **Local intranet** -- and then click **Custom level**.
6. In the **Settings** list, under **User Authentication**, click **Automatic logon with current user name and password** for a trusted site, or **Automatic logon only in Intranet zone** for a site you added to IE's list of Intranet sites. For more information, see your browser's documentation.



7. Return to the **Security** tab for **Internet Options** and set your web server as a trusted site.
8. Restart Internet Explorer.

Troubleshooting

The following tools can help diagnose problems with Kerberos authentication.

Apache Log File

The location of the Apache error logs is specified in the Apache configuration file under the `ErrorLog` directive. Here's an example directive from `/etc/httpd/conf/httpd.conf` on RHEL 5:

```
ErrorLog logs/error_log
```

The Microsoft Kerbtray Utility

The Microsoft `Kerbtray.exe` utility, part of the Windows 2000 Resource Kit, can verify whether Internet Explorer obtained a Kerberos ticket for your web server. You can download the utility at the following URL:

<http://www.microsoft.com/downloads/details.aspx?familyid=4E3A58BE-29F6-49F6-85BE-E866AF8E7A88&displaylang=en>

Klist

You can use the `klist` utility in `/opt/likewise/bin/klist` to check the Kerberos keytab file on a Linux or Unix computer. The command shows all the service principal tickets contained in the

keytab file so you can verify that the correct service principal names appear. Confirm that HTTP/myserver@MYDOMAIN.COM and HTTP/myserver.mydomain.com@MYDOMAIN.COM appear in the list. It is normal to see multiple entries for the same name.

Example:

```
klist --k krb5_myserver.keytab
```

```
Keytab name: FILE:krb5_myserver.keytab
```

```
KVNO Principal
```

```
-----
 6 HTTP/myserver@MYDOMAIN.COM
 6 HTTP/myserver@MYDOMAIN.COM
 6 HTTP/myserver@MYDOMAIN.COM
 6 HTTP/myserver.mydomain.com@MYDOMAIN.COM
 6 HTTP/myserver.mydomain.com@MYDOMAIN.COM
 6 HTTP/myserver.mydomain.com@MYDOMAIN.COM
```

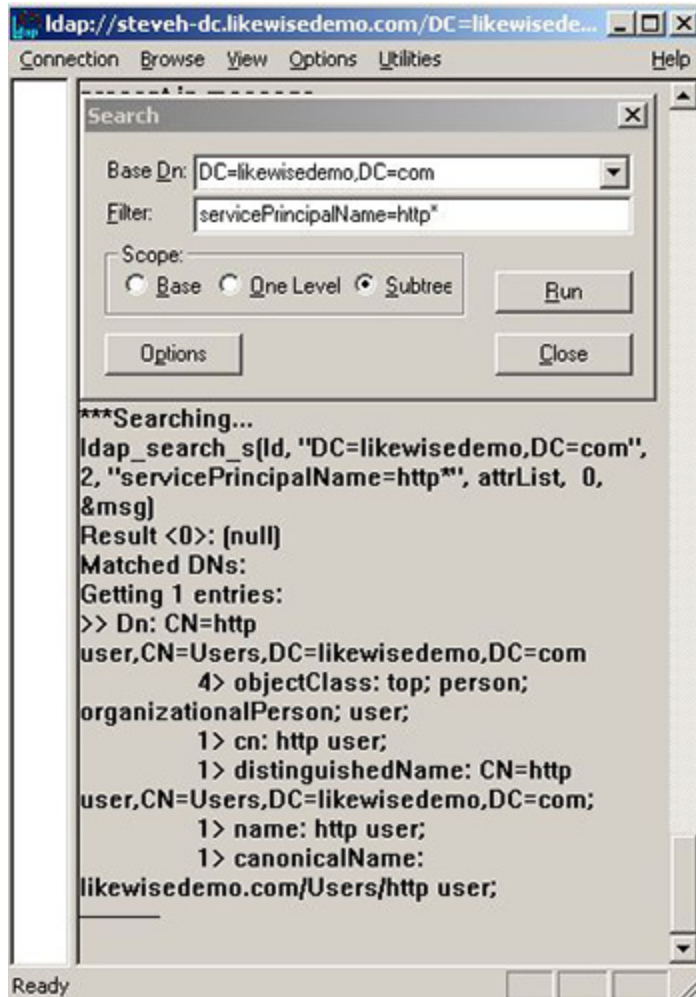
If your service principal names are incorrect, generate a new Kerberos keytab file.

Common Problems

Authentication problems can be difficult to diagnose. First, check all the configuration parameters, including the validity of the keytab file. Second, make sure none of the common problems listed in the following table are sabotaging authentication.

Problem	Solution
The system's clock is out of sync.	The Kerberos standard requires that system clocks be no more than 5 minutes apart. Make sure that the system clocks on the Active Directory domain controller, the Linux or Unix web server, and the client are synchronized.
The user accessing the web site is not on the require list	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: access to / failed, reason: user MYDOMAIN\user not allowed access Add the user to the require user directive or add the user's group to the require group directive.
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 <code>on</code>, or was not specified and thus defaults to <code>on</code>, the user will be prompted for credentials. 2. If <code>KrbMethodK5Passwd</code> is set to <code>off</code>, authentication will fail and the <code>Authorization Required</code> page will be displayed.
<p>Internet Explorer does not consider the URL to be part of the Local Intranet zone or the Trusted sites.</p>	<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>
<p>The service principal name of the web site is mapped to more than one object in the Active Directory.</p>	<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> <pre>There are multiple accounts with name HTTP/myserver.mydomain.com of type DS_SERVICE_PRINCIPAL_NAME.</pre> <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 “HTTP/myserver.mydomain.com” 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 HTTP by using Ldp:</p>



21.4.1. Kerberos Library Mismatch

Problem: Because some operating systems, such as the 64-bit version of Red Hat Enterprise Linux 5, use an outdated version of `/lib/libcom_err.so`, the Likewise authentication agent cannot locate the proper system library, leading to an error that looks like this:

```

httpd: Syntax error on line 202 of /etc/httpd/conf/httpd.conf:
Cannot load /opt/likewise/apache/2.2/mod_auth_kerb.so into server:
/opt/likewise/lib/libcom_err.so.3: symbol krb5int_strncpy, version
krb5support_0_MIT not defined in file libkrb5support.so.0
with link time reference
  
```

Solution: Force the `httpd` daemon to use the Likewise `krb5` libraries by opening the startup script for the Apache HTTP Server -- `/etc/init.d/httpd` -- and adding the path to the Likewise Kerberos libraries on the line that starts Apache. The line that starts the daemon can vary by operating system. Example on a 64-bit system:

```

LD_LIBRARY_PATH=/opt/likewise/lib64 LANG=$HTTPD_LANG daemon $httpd
$OPTIONS
  
```

On a 32-bit system, the path would look like this:

```
/opt/likewise/lib
```

Note: This modification changes the version of the Kerberos libraries that are used by the Apache HTTP Server. The change might result in compatibility issues with other modules of Apache that use Kerberos.

21.5. Configure a Java Application Server for SSO

This section describes how to set up Likewise and a Java web server to provide secure single sign-on through Active Directory with Integrated Windows Authentication. The instructions use Apache Tomcat as an example to demonstrate how to implement single sign-on with servlet authentication filters. Because servlet authentication filters are a generic Java technology common to most Java application servers, the procedure is similar for other Java application servers, such as JBoss. The instructions assume that you know how to configure Active Directory, Tomcat, and computers running Linux.

Before you can integrate Likewise 6.1 with a Java application servers, you must install a separate application integration package, which you can download for free from the Likewise web site by registering to download Likewise Open. (The name of the application integration package looks like this: `LikewiseAppIntegration-6.1.0.8656-linux-i386-rpm.sh`.)

Once you have installed the application integration package, here's how to configure your Tomcat server for SSO with Likewise. This section assumes you have installed Likewise 6.1 or later on the computer running the Java application server and have joined the server to an Active Directory domain.

Requirements

- Root access to the Linux or Unix computer.
- The Linux or Unix computer is joined to Active Directory with Likewise 6.1.
- The Linux or Unix computer is running Apache Tomcat Server version 5.5 or 6.0.
- The server is running JRE 1.5.0 or higher.
- The Likewise application integration package is installed.

Important: Configuring Java application servers is complex. Before you deploy your configuration to a production web server, implement and test it in a test environment. More: Before you change your application server's configuration, read and understand the Apache Tomcat documentation. Before you change a file, make a backup copy of it.

Components

The following Likewise components relevant to Apache integration are installed at `/opt/likewise/{lib, lib64}`:

Component name	Description
<code>lwjplatform.jar</code>	Likewise Platform Library
<code>lwservlets.jar</code>	Likewise authentication modules, including Servlet Filter and JAAS Module.
<code>lwtomcat.jar</code>	Likewise authentication modules specific to implementing the Tomcat authentication valve.

jna.jar	Java Native Access Library patched for UCS-2 support.
commons-codec-1.4.jar	Base64 and other encoding routines
commons-net-2.2.jar	Network utilities

Install the Authentication Components

The components from the integration package must be installed. Typically, an Apache Tomcat installation uses the following environment variables:

Environment Variable	Value
CATALINA_HOME_DIR	/usr/share/tomcat5 or /usr/share/tomcat6
CATALINA_BASE_DIR	/var/lib/tomcat5 or /var/lib/tomcat6

For the servlet filter and the required JAAS module, you must install the following components in `${CATALINA_HOME_DIR}/webapps/<web application>/lib`:

```
lwservlets.jar, lwjplatform.jar, jna.jar,
commons-codec-1.4.jar, commons-net-2.2.jar
```

Symbolic links can be created to these jar files from the target directory.

Generate Kerberos Keytab File

The Kerberos keytab file is necessary to authenticate incoming requests. It contains an encrypted, local copy of the host's key. If compromised may allow unrestricted access to the host computer. It is therefore important to protect it with file access permissions. The file must be readable by the user group under which the Apache Tomcat server is running, typically `tomcat` on most Linux systems.

Next, you must get the server name of the web site that will require authentication. If you don't know the server name, try doing a reverse DNS name lookup on the IP address of the host or just use the `hostname` of the Linux or Unix system.

You will also need to know the full domain name of the domain to which the Linux or Unix system is joined.

Finally, you will need to figure out where to save the generated keytab file.

The steps below use a sample Apache user account name named `tomcat`, a sample server name of `myserver`, a sample full domain name of `MYDOMAIN.COM`, and a sample Kerberos keytab file named `/etc/krb5_myserver.keytab`. You must substitute the correct names from your system and configuration.

1. Set the `KRB5_KTNAME` environment variable to point to the Kerberos keytab file to be generated. This can be set in the `tomcat` init script at `/etc/init.d/tomcat`:

```
# export KRB5_KTNAME=FILE:/etc/krb5_myserver.keytab
```

2. Select a user in Active Directory. If you create a user, make sure to set the password for the user account to never expire. Also make sure "Use DES Encryption types for this account" is not checked in the user account properties in Active Directory. In this example, we are using the following user: `MYDOMAIN\tomcat`

3. Generate keytab entry on your Windows domain controller for the default HTTP service principal:

```
# ktpass
  -/out          c:\krb5_myserver.keytab
  -/pType       KRB5_NT_PRINCIPAL
  -/crypto      RC4-HMAC-NT
  -/princ       HTTP/myserver.mydomain.com@MYDOMAIN.COM
  -/mapuser     tomcat@MYDOMAIN.COM
  -/mapop       set
  -/pass        *
```

4. Change the group ownership of the keytab file:

```
# chown tomcat:tomcat /etc/krb5_myserver.keytab
```

5. Set appropriate file permissions of the keytab file:

```
# chmod 600 /etc/krb5_myserver.keytab
```

6. If you choose not to create a separate keytab and the Tomcat server process is running in the context of the local tomcat user, you must provide read access to the default keytab file (typically at `/etc/krb5.keytab`) to the local tomcat user:

```
# chgrp tomcat -/etc/krb5.keytab
# chmod g+r -/etc/krb5.keytab
```

Modify the Web Application Configuration File

The only configuration that remains is to modify the Apache Tomcat configuration file -- `web.xml` -- by adding directives in each application container that is to be protected. Remember to replace `/etc/krb5_myserver.keytab` with your own keytab file name and replace `MYDOMAIN` with your short domain name. Servlet filters can be applied only to specific web applications.

Include the following configuration in the `web.xml` for the web application requiring authorization:

```
<filter>
  <filter-name>LikewiseAuth</filter-name>
  <filter-
class>com.likewise.auth.filter.spnego.LikewiseNegotiateFilter</filter-
class>
  <init-param>
    <param-name>deny-role</param-name>
    <param-value>MYDOMAIN\guests</param-value>
  </init-param>
  <init-param>
    <param-name>allow-role</param-name>
    <param-value>MYDOMAIN\domain^users</param-value>
  </init-param>
  <init-param>
    <param-name>remote-address-accept-filter</param-name>
    <param-value>10.100.0.0/24</param-value>
  </init-param>
  <init-param>
    <param-name>remote-address-accept-filter</param-name>
    <param-value>10.100.1.0,255.255.255.0</param-value>
  </init-param>
</filter>
```



```
<filter-mapping>
<filter-name>LikewiseAuth</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>
```

The configuration above ensures that only users who are in the `MYDOMAIN\domain^users` group can access the web pages from this application. Users who belong to the `MYDOMAIN\guests` group will be denied access. It is possible to configure multiple deny and allow roles. The user is checked for membership in the deny roles before being checked in the allow roles.

The `remote-address-accept-filter` configuration parameter can be used to specify IP addresses in the CIDR format or by using an IP Address, Subnet mask format. If this configuration is specified, the servlet performs authentication only on requests whose remote IP Address is in the range of one of the permitted addresses.

Protect the Web Pages

When trying to protect the web pages in a web application, the corresponding `web.xml` file should include the following configuration to protect all the web pages so they are accessible only to users who belong to the `MYDOMAIN\domain^users` group.

```
<security-role>
  <role-name>MYDOMAIN\domain^users</role-name>
</security-role>

<security-constraint>
  <display-name>Likewise Security Constraint</display-name>
  <web-resource-collection>
    <web-resource-name>Protected Area</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>MYDOMAIN\domain^users</role-name>
  </auth-constraint>
</security-constraint>
```

Likewise supports programmatic security. In addition, Likewise extends the standard `Principal` class. Once a request has been authenticated, you can get access to the additional principal information like this:

```
Principal p = request.getUserPrincipal();
If(p != null)
  LikewiseUser lwUser = (LikewiseUser) p;
```

Configure the JAAS Module

Likewise depends on the JAAS module: To integrate Likewise with a your servlet filters, the JAAS module is required. Here's how to set up the JAAS module to complete the integration of your Java application server with Likewise.

1. Create a file named `/opt/likewise/share/config/jaas.policy` and add the following lines to it:

```
grant Principal * * {
```

```

        permission java.security.AllPermission -"/**";
    -};

```

Create a file name `/opt/likewise/share/config/login.conf` and add the following lines to it:

```

        Jaas {
            com.likewise.auth.jaas.LikewiseLoginModule
sufficient;
        -};

```

2. Include the above files in your Tomcat startup environment, using the following variables as part of `CATALINA_OPTS`:

```

        --Djava.security.auth.login.config=/opt/likewise/share/
config/login.conf
        --Djava.security.auth.policy=/opt/likewise/share/config/
jaas.policy

```

3. Add the following configuration to `${CATALINA_BASE_DIR}/webapps/<web application>/WEB-INF/web.xml`:

```

<login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>Jaas</realm-name>
</login-config>

<security-role>
    <role-name>MYDOMAIN\domain^users</role-name>
</security-role>

<security-constraint>
    <display-name>Likewise Security Constraint</display-
name>
    <web-resource-collection>
        <web-resource-name>Protected Area</web-resource-
name>
        <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <role-name>MYDOMAIN\domain^users</role-name>
    </auth-constraint>
</security-constraint>

```

4. Add the following configuration to `${CATALINA_BASE_DIR}/webapps/<web application>/META-INF/context.xml` to add a realm named Jaas and to protect all the pages accessible by AD domain users:

```

<Context>
    <Realm className="org.apache.catalina.realm.JAASRealm"
        appName="Jaas"
        userClassNames="com.likewise.auth.LikewiseUser"
        roleClassNames="com.likewise.auth.LikewiseGroup"

```

```
        useContextClassLoader="false"  
        debug="true" -/>  
</Context>
```

Restart the Tomcat Server

Finally, restart the Tomcat server:

```
/etc/init.d/tomcat restart
```

Set Up Firefox and Internet Explorer for SSO

Follow the directions in the following sections and then you're ready to use your Java web application for SSO with Likewise:

Configure Firefox for SSO

Configure Internet Explorer for SSO

Troubleshooting

In the case of an authentication failure, the Apache Tomcat log file may contain information to help solve the problem. The Tomcat logs are typically located under `${CATALINA_HOME_DIR}/logs`. It is possible to set the “`java.security.debug`” variable in the Tomcat environment to elevate the log level and to help check for security issues.

```
$SU -- $TOMCAT_USER --c -"KRB5_KTNAME=/etc/keytab.likewise  
CATALINA_OPTS=-Djava.security.debug=access,failure  
$TOMCAT_SCRIPT start" >> $TOMCAT_LOG 2>&1
```

21.6. Examples

To view sample code that shows you how to use Likewise for single sign-on with protocols such as FTP and Telnet, see [Single Sign-On Examples](#).

Chapter 22. Configuring the Likewise Services with the Registry

22.1. About the Registry

The Likewise registry is a hierarchical database that stores configuration information for Likewise daemons, authentication providers, drivers, and other services. On Linux, Unix, and Mac computers, the Likewise services continually access the registry to obtain settings for their parameters. The Likewise authentication service, for example, queries the registry to determine which log level to use or which home directory template to apply to a user. In Likewise 5.4 or later, the registry replaces the text-based configuration files like `lsassd.conf` that were used in Likewise 5.3 or earlier.

When you install the Likewise agent on a Linux, Unix, or Mac computer but do not install Likewise Enterprise on a Windows administrative workstation connected to Active Directory, you cannot configure local Likewise settings with group policies. Instead, you must edit the local Likewise registry. You can access the registry and modify its settings by using the Likewise registry shell `-- lwregshell -- in /opt/likewise/bin/`.

This chapter describes the structure of the registry, demonstrates how to change a value in it, and lists the local Likewise configuration options.

Most of the registry settings can be centrally managed with group policies when you use Likewise Enterprise; see [About Group Policies in the Group Policy Administration Guide](#). If you modify a setting in the registry that is managed by a group policy, the change will not persist: It will be overwritten by the setting in the policy as soon as the group policy object is updated, which typically takes place once every 30 minutes. Likewise Open does not apply group policies.

22.1.1. 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\svsvsc]
```

Each of the services corresponds to a Likewise daemon, driver, or other service. The subkeys within each service contain value entries. A value specifies the setting for an entry, often presented under the `parameters` key. The following output illustrates the hierarchy of keys, subkeys, and their value entries for the upper levels of the `lsass` service.

```
[HKEY_THIS_MACHINE\Services\lsass\] ❶
  -"Arguments"      REG_SZ          -"/opt/likewise/sbin/lsassd ---
syslog" ❷
  -"Dependencies"  REG_SZ          -"netlogon lwio lwreg rdr npfs" ❸
  -"Description"   REG_SZ          -"Likewise Security and
Authentication Subsystem"
  -"Path"          REG_SZ          -"/opt/likewise/sbin/lsassd" ❹
  -"Type"          REG_DWORD       0x00000001 (1) ❺
```

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters] ❻
```

```
HKEY_THIS_MACHINE\Services\lsass> cd Parameters
HKEY_THIS_MACHINE\Services\lsass\Parameters> ls
```

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\]
  -"EnableEventlog"      REG_DWORD       0x00000000 (0) ❼
  -"LogLevel"            REG_SZ          -"error"
  -"LogNetworkConnectionEvents" REG_DWORD       0x00000001 (1)
```

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\NTLM] ❽
[HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM]
[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers]
[HKEY_THIS_MACHINE\Services\lsass\Parameters\RPCServers]
```

- ❶ The key for the `lsass` service. `lsass` is the Likewise authentication and security subsystem.
- ❷ The value entry for the command that is run to start the service, including command-line arguments. For the `lsass` daemon, the default argument routes messages to `syslog`.
- ❸ Other services that the service depends on. The Likewise Service Manager starts the dependencies before it starts the `lsassd` service. It is recommended that you do not change a service's list of dependencies or start order.
- ❹ The system path to the `lsassd` daemon. It is recommended that you do not change the path to a daemon or other service.
- ❺ The data type of the daemon. Its boolean value is set to the hexadecimal representation of 1, for true: It is turned on. Data types are discussed below.
- ❻ The branch for the service's parameters.
- ❼ The value entry for `EnableEventlog`. By default, this entry is set to 0, for false: It is turned off.
- ❽ The branch for the NTLM subkey.

The lsass service is the primary location for configurations targeted at system administrators and end users. It contains nearly all the configuration options for the Likewise authentication and security service.

22.1.1.1. 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\srvsvc]
"Dependencies"="dcerpc lwio srv npfs"
"Description"="Likewise Server Service"
"Path"="/opt/likewise/sbin/srsvcd"
```

22.1.2. 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).

22.2. Modify Settings with the `lwconfig` Tool

To quickly change an end-user setting in the registry that is not managed by a group policy, you can run the `lwconfig` command-line tool as root:

```
/opt/likewise/bin/lwconfig
```

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

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

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

```
[root@rhel5d bin]# ./lwconfig ---detail AssumeDefaultDomain ❶
Name: AssumeDefaultDomain
```

Description: Apply domain name prefix to account name at logon
Type: boolean
Current Value: false
Accepted Values: true, false
Current Value is determined by local policy.

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

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

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

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

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

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

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

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

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

Another Example

Here's another example of how to use `lwconfig` to find a setting and change it. Let's say you want to view the available trust settings because you know there are inaccessible trusts in your Active Directory network and you want to set Likewise to ignore all the trusts before you try to join a domain.

To do so, use `grep` with the `list` option:

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

The results will look something like this:

```
DomainManagerIgnoreAllTrusts  
DomainManagerIncludeTrustsList  
DomainManagerExcludeTrustsList
```


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

```
[root@rhel15d bin]# ./lwconfig ---details DomainManagerIgnoreAllTrusts
Name: DomainManagerIgnoreAllTrusts
Description: When true, ignore all trusts during domain enumeration.
Type: boolean
Current Value: false
Accepted Values: true, false
Current Value is determined by local policy.
```

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

```
[root@rhel15d bin]# ./lwconfig DomainManagerIgnoreAllTrusts true
```

Finally, check to make sure the change took effect:

```
[root@rhel15d bin]# ./lwconfig ---show DomainManagerIgnoreAllTrusts
boolean
true
local policy
```

In the example output that shows the setting's current values, `local policy` is listed -- meaning that the policy is managed locally through `lwconfig` because a Likewise Enterprise group policy is not managing the setting. You cannot locally modify a setting that is managed by a group policy.

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

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

22.3. Gain Access to the Registry

You can access and modify the registry by using the registry shell -- `lwregshell` -- in `/opt/likewise/bin`. The shell works in a way that is similar to `BASH`. You can navigate the registry's hierarchy with the following commands:

```
cd
ls
pwd
```

You can view a list of commands that you can execute in the shell by entering `help`:

```
/opt/likewise/bin/lwregshell
\> help
usage: regshell [--file -| --f] command_file.txt
       add_key [[KeyName]]
       list_keys [[keyName]]
       delete_key [KeyName]
       delete_tree [KeyName]
       cd [KeyName]
       pwd
       add_value [[KeyName]] -"ValueName" Type -"Value" ["Value2"]
[...]
       set_value [[KeyName]] -"ValueName" -"Value" ["Value2"] [...]
       list_values [[keyName]]
```

```
delete_value [[KeyName]] -"ValueName"  
set_hive HIVE_NAME  
import file.reg  
export [[keyName]] file.reg  
upgrade file.reg  
exit -| quit -| ^D  
  
Type: REG_SZ -| REG_DWORD -| REG_BINARY -| REG_MULTI_SZ  
REG_DWORD and REG_BINARY values are hexadecimal  
Note: cd and pwd only function in interactive mode  
Note: HKEY_THIS_MACHINE is the only supported hive  
  
\>
```

Note: In the unlikely event that you want to restore all the registry's default values, you must leave the domain, stop all the Likewise services, manually delete `/var/lib/likewise/db/registry.db`, and then reinstall Likewise.

22.4. Change the Value of an Entry with the Shell

You can change a value in the registry by executing the `set_value` command with the shell. The following procedure demonstrates how to change the value of the PAM key's `LogLevel` entry. The procedure to change other keys is similar. After you modify a registry setting for a Likewise service, you must refresh the corresponding service with the Likewise Service Manager for the changes to take effect.

1. With the root account, start `lwregshell`:

```
/opt/likewise/bin/lwregshell
```

2. Change directories to the location of the PAM key and list its current settings:

```
[root@rhel5d bin]# ./lwregshell  
\> cd HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM  
HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM> ls  
  
[HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM\  
- "DisplayMotd"          REG_DWORD          0x00000001 (1)  
- "LogLevel"            REG_SZ             -"error"  
- "UserNotAllowedError" REG_SZ             -"Access denied"
```

3. Execute the `set_value` command with the name of the value as the first argument and the new value as the second argument:

```
HKEY_THIS_MACHINE\services\lsass\Parameters\PAM> set_value  
LogLevel debug
```

4. List the key's value entries to confirm that the value was changed:

```
HKEY_THIS_MACHINE\services\lsass\Parameters\PAM> ls  
  
[HKEY_THIS_MACHINE\services\lsass\Parameters\PAM\  
- "DisplayMotd"          REG_DWORD          0x00000001 (1)  
- "LogLevel"            REG_SZ             -"debug"
```

```
-"UserNotAllowedError" REG_SZ          -"Access denied"
```

5. Exit the shell:

```
HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM> quit
```

6. After you change a setting in the registry, you must use the Likewise Service Manager -- lwsn -- 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/lwsn refresh lsass
```

22.4.1. Set Common Options with the Registry Shell

This section shows you how to modify several common Likewise settings by using the registry shell: the default domain, the home directory, and the shell.

1. As root or with sudo, start the registry shell:

```
/opt/likewise/bin/lwregshell
```

2. Change directories to the following location:

```
cd HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers  
\ActiveDirectory
```

3. Change the shell to, for example, bash:

```
set_value LoginShellTemplate /bin/bash
```

For more information, see [Set the Home Directory and Shell for Domain Users](#).

4. Set the option to use the default domain:

```
set_value AssumeDefaultDomain 1
```

5. Leave the shell:

```
quit
```

6. After you change a setting in the registry, you must use the Likewise Service Manager -- lwsn -- 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/lwsn refresh lsass
```

Here's how the string of commands looks in the registry shell:

```
[root@rhel5d docs]# -/opt/likewise/bin/lwregshell  
> cd HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers  
\ActiveDirectory  
HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers  
\ActiveDirectory> set_value AssumeDefaultDomain 1  
HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers  
\ActiveDirectory> set_value LoginShellTemplate -/bin/bash  
HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers  
\ActiveDirectory> quit
```

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

22.5. Change the Value of an Entry from the Command Line

You can also change a value in the registry by executing the `set_value` command from the command line. The following code block demonstrates how to change the value of the PAM key's `LogLevel` entry without using the shell. After you modify a registry setting for a Likewise service, you must refresh the corresponding service with the Likewise Service Manager for the changes to take effect.

```
/opt/likewise/bin/lwregshell ls -'[HKEY_THIS_MACHINE\Services\lsass
\Parameters\PAM\]'
```

[HKEY_THIS_MACHINE\\Services\lsass\Parameters\PAM]
- "DisplayMotd" REG_DWORD 0x00000001 (1)
- "LogLevel" REG_SZ -"error"
- "UserNotAllowedError" REG_SZ -"Access denied"

```
/opt/likewise/bin/lwregshell set_value -'[HKEY_THIS_MACHINE\Services
\lsass\Parameters\PAM\]' LogLevel debug
```

```
/opt/likewise/bin/lwregshell ls -'[HKEY_THIS_MACHINE\Services\lsass
\Parameters\PAM\]'
```

[HKEY_THIS_MACHINE\\Services\lsass\Parameters\PAM]
- "DisplayMotd" REG_DWORD 0x00000001 (1)
- "LogLevel" REG_SZ -"debug"
- "UserNotAllowedError" REG_SZ -"Access denied"

22.6. Find a Value Entry

When you're unsure where to find a setting that you want to change, you can export the registry's structure to a file and then search the file for the value entry's location.

Important: You must export the registry as root.

1. With the root account, start `lwregshell`:

```
/opt/likewise/bin/lwregshell
```

2. In the shell, execute the `export` command with the root key as the first argument and a target file as the second argument:

```
export HKEY_THIS_MACHINE\ lwregistry.reg
```

The file is exported to your current directory unless you specify a path.

In a text editor such as `vi`, open the file to which you exported the registry and search for the entry that you are want to find.

22.7. Settings in the Lsass Branch

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

22.7.1. Log Level Value Entries

There is a `LogLevel` value entry under several keys, including `lsass/Parameters` and `PAM`. Although the default value is typically `error`, you can change it to any of the following values: `disabled`, `error`, `warning`, `info`, `verbose`.

Locations

[HKEY_THIS_MACHINE\Services\lsass\Parameters]

[HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM]

Value Entry

`LogLevel`

Example with default value:

```
"LogLevel"="error"
```

22.7.2. Turn On Event Logging

You can capture information about authentication transactions, authorization requests, and other security events by turning on event logging. For information about managing and viewing events, see [Monitoring Events with the Event Log](#).

Note: With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see [Turn on Event Logging with a GPO](#).

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters]

Value Entry

`EnableEventlog`

Example with default value:

```
"EnableEventlog"=dword:00000000
```

22.7.3. Turn Off Network Event Logging

After you turn on event logging, network connection events are logged by default. On laptop computers, computers with a wireless connection, or other computers whose network status might be in flux, you can turn off event logging so that the event log is not inundated with connectivity events.

Note: With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see [Turn Off Logging of Network Events](#).

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters]

Value Entry

LogNetworkConnectionEvents

Example with default value:

```
"LogNetworkConnectionEvents"=dword:00000001
```

22.7.4. Restrict Logon Rights

With Likewise Open and Likewise Enterprise, you can require that a user be a member of a group to log on a computer, or you can limit logon to only the users that you specify. With Likewise Enterprise, you can also restrict logon rights with a Likewise group policy; see Allow Logon Rights in the Group Policy Administrators Guide. Likewise checks `require_membership_of` information in both the authentication phase and the account phase.

Location

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

Value Entry

RequireMembershipOf

Notes

Add each user or group to the value entry by using an NT4-style name (the short domain name with the group name) or an Active Directory security identifier (SID). Aliases are not supported. The entries must be in the form of a list of quoted entries: Each entry must be enclosed in quotation marks. A slash character must be escaped by being preceded by a slash. Example:

```
"RequireMembershipOf"="likewisedemo\\support"  
"likewisedemo\\domain^admins" "likewisedemo\\joe"  
"S-1-5-21-3447809367-3151979076-456401374-513"
```

Only the users that you specify and the users who are members of the groups that you specify are allowed to log on the computer.

22.7.5. Display an Error to Users Without Access Rights

You can set Likewise to display an error message when a user attempts to log on a computer without the right to access it. With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see Display a Message of the Day at Logon in the Likewise Enterprise guide.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM]

Value Entry

UserNotAllowedError

Notes

Add the text of the error message that you want to display to the value of the entry. Example with default value:

```
"UserNotAllowedError"="Access denied"
```

22.7.6. Display an MOTD

You can set Likewise to display a message of the day. It appears after a user logs on but before the logon script executes to give users information about a computer. The message can, for instance, remind users of the next scheduled maintenance window.

With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see Display a Message of the Day at Logon in the Likewise Enterprise guide.

Location in registry:

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM]
```

Value Entry

DisplayMotd

Example with the value set to 1, or true, to display a message:

```
"DisplayMotd"=dword:00000001
```

22.7.7. Change the Domain Separator Character

The default domain separator character is set to `\.` So, by default, the Active Directory group `DOMAIN\Administrators` appears as `DOMAIN\administrators` on target Linux and Unix computers. The Likewise authentication daemon renders all names of Active Directory users and groups lowercase.

You can, however, replace the slash that acts as the separator between an Active Directory domain name and the SAM account name with a character that you choose by modifying the `DomainSeparator` value entry in the registry.

The following characters cannot be used as the separator:

- alphanumeric characters -- letters and digits
- @
- #
- And not the character that you used for the `space-replacement` setting; for more information, see [Change the Replacement Character for Spaces](#).

Location

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters]
```

Value Entry

DomainSeparator

Example entry with default value:

```
"DomainSeparator"="\\"
```

Notes

In the default value, the slash character is escaped by the slash that precedes it.

22.7.8. Change the Replacement Character for Spaces

The default replacement character is set to `^`. So, by default, the Active Directory group `DOMAIN\Domain Users` appears as `DOMAIN\domain^users` on target Linux and Unix computers. You can, however, replace the spaces in Active Directory user and group names with a character that you choose by editing the `SpaceReplacement` value entry in the registry.

With Likewise Enterprise, you can manage this setting with a Likewise group policy; see [Replace Spaces in Names with a Character in the Likewise Enterprise guide](#).

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters]

Value Entry

SpaceReplacement

Example with default value:

```
"SpaceReplacement" = "^"
```

Notes

The following characters cannot be used as the separator:

- whitespace -- spaces and tabs
- alphanumeric characters -- letters and digits
- @
- \
- #

The Likewise authentication daemon renders all names of Active Directory users and groups lowercase.

22.7.9. Turn Off System Time Synchronization

With Likewise Open and Likewise Enterprise, you can specify whether a joined computer synchronizes its time with that of the domain controller. By default, when a computer is joined to a domain without using the `notimesync` command-line option, the computer's time is synchronized with the domain controller's when there is a difference of more than 60 seconds but less than the maximum clock skew, which is typically 5 minutes. With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see [Turn Off System Time Synchronization with a GPO in the Likewise Enterprise guide](#).

Location

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

Value Entry

SyncSystemTime

Example with default value:

```
"SyncSystemTime"=dword:00000001
```

22.7.10. Set the Default Domain

If your Active Directory environment has only one domain, you can set Likewise to assume the default domain, liberating users from typing the domain name before their user or group name each time they log on a computer or switch users. With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see Prepend Domain Name for AD Users and Groups in the Likewise Enterprise guide.

Location

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

Value Entry

```
AssumeDefaultDomain
```

Example with default value:

```
"AssumeDefaultDomain"=dword:00000000
```

22.7.11. Set the Home Directory and Shell for Domain Users

When you install Likewise on a Linux, Unix, or Mac computer but not on Active Directory, you cannot associate a Likewise cell with an organizational unit, and thus you have no way to define a home directory or shell in Active Directory for users who log on the computer with their domain credentials. To set the home directory and shell for a Linux, Unix, or Mac computer that is using Likewise Open or Likewise Enterprise without cell, edit the value entry in registry.

If you use Likewise Enterprise to set the shell and home directory both in Active Directory and in the registry, the settings in Active Directory take precedence.

After you change the home directory or shell in the registry, you must clear the Likewise authentication cache, log off, and then log on before your changes will take effect.

In the lsass branch, there are two keys that contain value entries for the home directory and shell. One is for the local provider, the other is for the Active Directory provider. Locations:

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

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\Local]
```

The following value entries for the home directory and shell, shown with their default settings, appear under both the Active Directory and Local provider keys:

```
"LoginShellTemplate"="/bin/sh"  
"HomeDirTemplate"="%H/local/%D/%U"  
"HomeDirPrefix"="/home"  
"CreateHomeDir"=dword:00000001
```

Set the Shell

Under the key for a provider, modify the value of the following entry to set the shell that you want:

LoginShellTemplate

Example with default value:

```
"LoginShellTemplate"="/bin/sh"
```

Note: /bin/bash might not be available on all systems.

Set the Home Directory

You can modify the HomeDirTemplate value entry to set the home directory that you want by using these variables:

Variable	Description
%U	The default user name. It is required.
%D	The default domain name. It is optional.
%H	The default home directory. It is optional. If used, it must be set as an absolute path. This value, if used, is typically the first variable in the sequence.
%L	The hostname of the computer. It is optional.

Here's an example with all four variables set: %H/%L/%D/%U

Example with default value:

```
"HomeDirTemplate"="%H/local/%D/%U"
```

In the example above, the HomeDirTemplate is using the %H variable for the HomeDirPrefix to set the user's home directory. In the example, the HomeDirPrefix is not preceded by a slash because the slash is included in the default HomeDirPrefix to ensure that the path is absolute. By default, the %H variable automatically changes to be compatible with the operating system to generate a home directory path. On Solaris, for example, the %H variable maps to /export/home. On Mac OS X it maps to /Users; on Linux, it maps to /home.

Optionally, you can set the HomeDirPrefix by changing the prefix to the path that you want. However, the HomeDirPrefix must be an absolute path -- so you must precede it with a slash.

Example with default value:

```
"HomeDirPrefix"="/home"
```

You must use the default user name variable (%U). You may specify the default domain name by using the domain name variable (%D), but it is not required.

All the users who log on the computer by using their Active Directory domain credentials will have the shell and home directory that you set under the Providers\ActiveDirectory key. All the users who log on the computer by using their local Likewise provider credentials will have the shell and home directory that you set under the Providers\Local key.

Important: On Solaris, you cannot create a local home directory in /home, because /home is used by autofs, Sun's automatic mounting service. The standard on Solaris is to create local home directories in /export/home.

On Mac OS X, to mount a remote home directory, you must first create the directory on the remote server as well as the folders for music, movies, and so forth. See [Use the createhomedir Command to Create Home Directories](#) and other information on Apple's web site.

Turn Off Home Directories

By default, a user's home directory is created upon logon. 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](#)

22.7.12. Set the Umask for Home Directories

Likewise presets the umask for the home directory and all the files in it to 022. With a umask value of 022, the default file permissions for your AD user account are as follows: Read-write access for files and read-write-search for directories you own. All others have read access only to your files and read-search access to your directories. You can, however, set the umask for home directories by modifying its value entry in the registry.

With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see [Set Permissions with a File Creation Mask in the Likewise Enterprise guide](#).

Locations

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

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\Local]
```

Value Entry

HomeDirUmask

Example with default value:

```
"HomeDirUmask"="022"
```

22.7.13. Set the Skeleton Directory

By default, Likewise adds the contents of `/etc/skel` to the home directory created for a new user account on Linux and Unix computers. Using `/etc/skel` or a directory that you designate ensures that all users begin with the same settings or environment.

On Mac OS X computers, the default skeleton directory is as follows:

```
System/Library/User Template/Non_localized,  
/System/Library/User Template/English.lproj
```

Note: With Likewise Enterprise, you can manage this setting by using a Likewise group policy.

Locations

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

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

Value Entry

SkeletonDirs

Example with default value:

```
"SkeletonDirs"="/etc/skel"
```

Notes

Add the skeleton directory that you want to set to the entry. You can add multiple entries, but each entry must be enclosed in quotation marks and separated by a space.

22.7.14. Force Likewise Enterprise to Work Without Cell Information

To use the Likewise Enterprise agent to join a Linux, Unix, or Mac OS X computer to a domain that has not been configured with cell information, you must change the value of `CellSupport` to `unprovisioned`. This setting, which applies only to Likewise Enterprise, forces the authentication service to ignore the following Unix information even though it is set in Active Directory:

- Home directory
- UID
- GID
- Unix shell

Instead of using the information from Active Directory, the `unprovisioned` value sets the authentication service to hash the user's security identifier and use local settings for the Unix shell and the home directory.

Location

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

Value Entry

CellSupport

Notes

The value must be set as one of the following: `no-unprovisioned`, `full` or `unprovisioned`.

The default is `no-unprovisioned`, a setting that requires you to create a cell in Active Directory before you join a Likewise client to it. If you are using Likewise Enterprise with cells and you want to

use the Unix settings in AD, it is recommended that you leave `cell-support` set to its default value of `no-unprovisioned`:

```
"CellSupport"="no-unprovisioned"
```

Here's an example with the value set to `unprovisioned` to force Likewise Enterprise to ignore Unix settings and other cell information in AD:

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

Setting the value to `full` configures the Likewise Enterprise agent to use cell information when it appears in AD and local settings when no cells are in AD:

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

22.7.15. Refresh User Credentials

By default, Likewise automatically refreshes user credentials, but you can turn off automatic refreshes by modifying the configuration of the Likewise authentication daemon.

Location

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

Value Entry

```
RefreshUserCredentials
```

Example with default setting:

```
"RefreshUserCredentials"=dword:00000001
```

22.7.16. Turn Off K5Logon File Creation

By default, Likewise creates a `.k5login` file in the home directory of an Active Directory user who is authenticated by Kerberos when logging on a Linux, Unix, or Mac OS X computer. You can, however, stop the creation of a `.k5login` file.

The `.k5login` file contains the user's Kerberos principal, which uniquely identifies the user within the Kerberos authentication protocol. Kerberos can use the `.k5login` file to check whether a principal is allowed to log on as a user. A `.k5login` file is useful when your computers and your users are in different Kerberos realms or different Active Directory domains, which can occur when you use Active Directory trusts.

With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see [Create a .k5login File in a User's Home Directory in the Likewise Enterprise guide](#).

Location

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

Value Entry

```
CreateK5Login
```

Example with default value:

```
"CreateK5Login"=dword:00000001
```

22.7.17. Change the Duration of the Machine Password

You can set the machine account password's expiration time. The expiration time specifies when a machine account password is reset in Active Directory if the account is not used. The default is 30 days.

Active Directory handles machine accounts for Linux, Unix, and Mac in the same way as those for Windows computers; for more information, see the Microsoft Active Directory documentation.

With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see [Set the Machine Account Password Expiration Time](#) in the Likewise Enterprise guide.

Location

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

Value Entry

MachinePasswordLifespan

Example with default value, which is shown as seconds in hexadecimal format:

```
"MachinePasswordLifespan"=dword:000927c0
```

Notes

Setting the value to 0 disables expiration. The minimum value is 1 hour, expressed in seconds, and the maximum is 60 days, expressed in seconds. To avoid issues with Kerberos key tables and single sign-on, the `MachinePasswordLifespan` must be at least twice the maximum lifetime for user tickets, plus a little more time to account for the permitted clock skew. The expiration time for a user ticket is set by using an Active Directory group policy called **Maximum lifetime for user ticket**. The default user ticket lifetime is 10 hours; the default Likewise machine password lifetime is 30 days.

Check the Maximum Lifetime for a User Ticket in the Group Policy Object Editor

1. Open the default domain policy in the Group Policy Object Editor.
2. In the console tree under **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Account Policies**, and then click **Kerberos policy**.



3. In the details pane, double-click **Maximum lifetime for user ticket**.

4. In the **Ticket expires in** box, make sure that the number of hours is no more than half that of the `MachinePasswordLifespan` you set in the registry.

See Also

Fix a Key Table Entry-Ticket Mismatch

22.7.18. Sign and Seal LDAP Traffic

You can sign and seal LDAP traffic to certify it and to encrypt it so that others cannot see your LDAP traffic on your network. This setting can help improve network security.

Location

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

Value Entry

LdapSignAndSeal

Example with default value:

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

22.7.19. NTLM Value Entries

There are a number of NTLM settings that system administrators can use to manage NTLM sessions.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\Local]

Value Entry with Default Values

```
"AcceptNTLMv1"=dword:00000001
```

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\NTLM]

Value Entries with Default Values

```
"SendNTLMv2"=dword:00000000  
"Support128bit"=dword:00000001  
"Support56bit"=dword:00000001  
"SupportKeyExchange"=dword:00000001  
"SupportNTLM2SessionSecurity"=dword:00000001  
"SupportUnicode"=dword:00000001
```

Each NTLM value entry is described in the following table. For additional information, see Microsoft's description of the LAN Manager authentication levels.

Value Entry	Description
AcceptNTLMv1	Controls whether the Likewise local provider accepts the older and less secure NTLM protocol

	for authentication in addition to NTLMv2. This setting does not apply to the Active Directory provider because it passes off NTLM and NTLMv2 authentication to a domain controller through schannel; it is the domain controller's settings that determine which versions of NTLM are allowed.
SendNTLMv2	Forces lsassd to use NTLMv2 rather than the older and less secure NTLM when lsassd acts as a client. (Lsassd typically serves as an NTLM client in relation to domain controllers.)
Support128bit and Support56bit	Control the length of the encryption key. They are intended to serve as a mechanism for debugging NTLM sessions. There are no corresponding settings in Windows.
SupportKeyExchange	Allows the protocol to exchange a session key -- Kerberos has a similar feature. During authentication, an alternate key is exchanged for subsequent encryption to reduce the risk of exposing a password. It is recommended that you use the default setting.
SupportNTLM2SessionSecurity	Permits the client to use a more secure variation of the protocol if the client discovers that the server supports it. Corresponds to a similar setting in Windows.
SupportUnicode	Sets NTLM to represent text according to the Unicode industry standard. It is recommended that you use the default setting -- which is to support Unicode.

22.7.20. Additional Subkeys

There are additional subkeys in the lsass branch that the lsass service uses to store information for the Likewise application. It is recommended that you do not change these subkeys or their value entries.

- [HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin\YourDNSdomainName\DomainTrust]

Stores information about domain trusts.

- [HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin\YourDNSdomainName\ProviderData]

Stores data used by the Active Directory authentication provider.

- [HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin\YourDNSdomainName\Pstore]

Caches information about the computer and the user's Active Directory account, including the machine password. The machine password is visible only to root users when they view or export the registry.

- [HKEY_THIS_MACHINE\Services\lsass\Parameters\RPCServers]

Stores information that the system uses to execute remote procedure calls.

22.7.21. Add Domain Groups To Local Groups

This value entry controls whether the domain-join process adds domain groups to the local Likewise groups and whether the domain-leave process removes domain groups from the local Likewise groups. The default setting is 0, for disabled -- no domain groups are added to local groups.

When the setting is enabled, the AD group `Domain Admins` is added to `BUILTIN\Administrators`, and `Domain Users` is added to `BUILTIN\Users`.

After joining or leaving a domain, you can verify that the domain groups were added to or removed from the local groups by running the `lw-lsa enum-members` command for the `BUILTIN\Administrators` group and the `BUILTIN\Users` group.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

AddDomainToLocalGroupsEnabled

22.7.22. Control Trust Enumeration

Likewise includes the following settings for controlling how the domain manager component of the authentication service enumerates trusts. The settings can help improve performance of the authentication service in an extended AD topology. With Likewise Enterprise, you can manage these settings with their corresponding group policies.

Important: The setting that specifies an include list is dependent on defining the setting for ignoring all trusts: To use the include list, you must first enable the setting to ignore all trusts. The include-list setting must explicitly contain every domain that you want to enumerate. It is insufficient to include only the forests that contain the domains.

For a domain that is added to the include list, Likewise tries to discover its trust. If some of the domains are not included in the space-separated list, the resulting trust relationships might run counter to your intentions: The Likewise agent might process the trust as a one-way forest child trust when it is not.

Changes to the trust enumeration settings take effect when you restart either the computer or the Likewise authentication service (`lsass`).

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entries

Value Entry	Description
DomainManagerIgnoreAllTrusts	Determines whether the authentication service discovers domain trusts. In the default configuration of disabled, the service enumerates all the parent and child domains as

	<p>well as forest trusts to other domains. For each domain, the service establishes a preferred domain controller by checking for site affinity and testing server responsiveness, a process that can be slowed by WAN links, subnet firewall blocks, stale AD site topology data, or invalid DNS information.</p> <p>When it is unnecessary to enumerate all the trusts -- because, for example, the intended users of the target computer are only from the forest that the computer is joined to -- turning on this setting can improve startup times of the authentication service.</p>
DomainManagerIncludeTrustsList	<p>When the setting <code>DomainManagerIgnoreAllTrusts</code> is turned on, only the domain names in the space-separated include list are enumerated for trusts and checked for server availability. Each item in the list must be separated by a space.</p>
DomainManagerExcludeTrustsList	<p>When the setting <code>DomainManagerIgnoreAllTrusts</code> is turned off (its default setting), the domain names in the space-separated exclude list are not enumerated for trusts and not checked for server availability. Each item in the list must be separated by a space.</p>

22.7.23. Modify Smart Card Settings

The following settings are available only with Likewise Enterprise.

Location in registry:

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\PAM]
```

Value Entries

SmartCardPromptGecos

SmartCardServices

22.7.24. Set the Interval for Checking the Status of a Domain

This value entry determines how frequently the Likewise domain manager checks whether a domain is online. The default is 5 minutes.

Location

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]
```

Value Entry

DomainManagerCheckDomainOnlineInterval

Example with default value:

```
"DomainManagerCheckDomainOnlineInterval"=dword:0000012c
```

22.7.25. Set the Interval for Caching an Unknown Domain

This value entry determines how long the Likewise domain manager caches an unknown domain as unknown. The default is 1 hour.

Location

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]
```

Value Entry

```
DomainManagerUnknownDomainCacheTimeout
```

Example with default value:

```
"DomainManagerUnknownDomainCacheTimeout"=dword:00000e10
```

22.8. Cache Settings in the Lsass Branch

Many of the following cache settings can be managed by the group policies of Likewise Enterprise. For more information, see the Likewise Enterprise Group Policy Administration Guide.

22.8.1. Set the Cache Type

By default, the Lsass service uses SQLite to cache information about users, groups, and the state of the computer. You can, however, change the cache to store the information in memory, which might improve the performance of your system.

Location

```
[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]
```

Value Entry

```
CacheType
```

Example with default value:

```
"CacheType"="sqlite"
```

Notes

To use the memory cache, change the value to memory. Example:

```
"CacheType"="memory"
```

22.8.2. Cap the Size of the Memory Cache

By default, the Lsass service caches information about users, groups, and the state of the computer in a SQLite database. If, however, you change the cache to store the data in memory, you can limit the size of the cache to prevent it from consuming too much memory. It is suggested that the size of the cache be

between 1 MB and 10 MB, but the size limit that you choose will depend on your environment. Groups with many members call for a larger memory cache to enumerate all the users.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

MemoryCacheSizeCap

Example with default value:

```
"MemoryCacheSizeCap"=dword:00000000
```

Notes

To limit the memory cache to a maximum value, change the value to the byte count that you want. When the total cache size exceeds the limit, old data is purged. The default value is 0: no limit is set.

22.8.3. Change the Duration of Cached Credentials

You can specify how long the Likewise agent caches information about an Active Directory user's home directory, logon shell, and the mapping between the user or group and its security identifier (SID). This setting can improve the performance of your system by increasing the expiration time of the cache.

Note: With Likewise Enterprise, you can manage this setting by using a Likewise group policy; see Set the Cache Expiration Time in the Likewise Enterprise guide.

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entry

CacheEntryExpiry

Example with default value:

```
"CacheEntryExpiry"=dword:00003840
```

Notes

Set the value to an interval, in seconds. The minimum entry is 0 seconds and the maximum is 1 day, expressed in seconds.

22.8.4. Change NSS Membership and NSS Cache Settings

To customize Likewise to meet the performance needs of your network, you can specify how the Likewise agent parses and caches group and user membership information with the following value entries in the registry:

Location

[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory]

Value Entries

Here are the value entries with their default values:

```
"TrimUserMembership"=dword:00000001
"NssGroupMembersQueryCacheOnly"=dword:00000001
"NssUserMembershipQueryCacheOnly"=dword:00000000
"NssEnumerationEnabled"=dword:00000000
```

Each setting is described in the table that follows.

Setting	Description
TrimUserMembership	<p>Specifies whether to discard cached information from a Privilege Attribute Certificate (PAC) entry when it conflicts with new information retrieved through LDAP. Otherwise, PAC information, which does not expire, is updated the next time the user logs on.</p> <p>The default setting is 1: It is turned on.</p>
NssGroupMembersQueryCacheOnly	<p>Specifies whether to return only cached information for the members of a group when queried through nsswitch. More specifically, the setting determines whether nsswitch-based group APIs obtain group membership information exclusively from the cache, or whether they search for additional group membership data through LDAP.</p> <p>This setting is made available because, with large amounts of data, the LDAP enumeration can be slow and can affect performance. To improve performance for groups with more than 10,000 users, set this option to <i>yes</i>. Without the LDAP enumeration, only when a user logs on can that user's complete group membership be retrieved based on the PAC.</p> <p>The default setting is 1: It is turned on.</p>
NssUserMembershipQueryCacheOnly	<p>When set to <i>yes</i>, enumerates the groups to which a user belongs using information based solely on the cache. When set to <i>no</i>, it checks the cache and searches for more information over LDAP.</p> <p>The default setting is 0: It is turned off.</p>
NssEnumerationEnabled	<p>Controls whether all users or all groups can be incrementally listed through NSS. On Linux computers and Unix computers other than Mac, the default setting is 0, or turned off. On Mac OS X computers, the default setting is 1, or turned on.</p> <p>To allow third-party software show Active Directory users and groups in lists, you can</p>

change this setting to 1, but performance might be affected.

Note: When you run the `id` command for an Active Directory user other than the current user on some Linux systems, such as SLES 10 and SLED 10, the command returns only that user's primary group. The command enumerates all the groups and searches for the user in the groups' membership. To properly find another user's membership with the `id` command on SLES 10 and SLED 10, you must turn on NSS enumeration.

22.9. Settings in the eventlog Branch

This section lists value entries in the registry's eventlog branch.

22.9.1. Allow Users and Groups to Delete Events

This entry specifies the Active Directory users and groups who can delete events from the Likewise event log.

Location

[HKEY_THIS_MACHINE\Services\eventlog\Parameters]

Value Entry

AllowDeleteTo

Notes

Add the users and groups, separated by commas, to the value entry by using NT4-style names (the short domain name with the group name), the user's or group's alias, or an Active Directory security identifier (SID). The comma-separated list must be enclosed in quotation marks. Example:

```
AllowDeleteTo="likewisedemo\support, likewisedemo\domain^admins,  
likewisedemo\joe, jane, S-1-5-21-3447809367-3151979076-456401374-513,  
sales^admins"
```

22.9.2. Allow Users and Groups to Read Events

This value entry specifies the Active Directory users and groups who can read events in the Likewise event log.

Location

[HKEY_THIS_MACHINE\Services\eventlog\Parameters]

Value Entry

AllowReadTo

Notes

Add the users and groups, separated by commas, to the value entry by using NT4-style names (the short domain name with the group name), the user's or group's alias, or an Active Directory security identifier (SID). The comma-separated list must be enclosed in quotation marks. Example:

```
AllowReadTo="likewisedemo\support, likewisedemo\domain^admins,  
likewisedemo\joe, jane, S-1-5-21-3447809367-3151979076-456401374-513,  
sales^admins"
```

22.9.3. Allow Users and Groups to Write Events

This value entry specifies the Active Directory users and groups who can write events in the Likewise event log.

Location

```
[HKEY_THIS_MACHINE\Services\eventlog\Parameters]
```

Value Entry

```
AllowWriteTo
```

Notes

Add the users and groups, separated by commas, to the value entry by using NT4-style names (the short domain name with the group name), the user's or group's alias, or an Active Directory security identifier (SID). The comma-separated list must be enclosed in quotation marks. Example:

```
AllowWriteTo="likewisedemo\support, likewisedemo\domain^admins,  
likewisedemo\joe, jane, S-1-5-21-3447809367-3151979076-456401374-513,  
sales^admins"
```

22.9.4. Set the Maximum Disk Size

This value entry specifies the maximum size of the event log. The default is 512 KB. The minimum size is 64 KB. The maximum is 419424 KB.

Location

```
[HKEY_THIS_MACHINE\Services\eventlog\Parameters]
```

Value Entry

```
MaxDiskUsage
```

Example with default value:

```
"MaxDiskUsage"=dword:06400000
```

22.9.5. Set the Maximum Number of Events

This value entry defines the maximum number of events that can reside in the event log. The default is 100,000. The minimum number is 100. The maximum is 2,000,000.

Location

```
[HKEY_THIS_MACHINE\Services\eventlog\Parameters]
```

Value Entry

MaxNumEvents

Example with default value:

```
"MaxNumEvents"=dword:000186a0
```

22.9.6. Set the Maximum Event Timespan

This value entry defines maximum length of time, in days, that events can remain in the event log. Events older than the specified time span are removed. The default is 90 days. The maximum is 365 days.

Location

```
[HKEY_THIS_MACHINE\Services\eventlog\Parameters]
```

Value Entry

MaxEventLifespan

Example with the default value of 90 days:

```
"MaxEventLifespan"=dword:0000005a
```

22.9.7. Change the Purge Interval

This value entry defines the number of days after which to purge the database of events. The default is 1 day.

Location

```
[HKEY_THIS_MACHINE\Services\eventlog\Parameters]
```

Value Entry

EventDbPurgeInterval

Example with default value of 1 day:

```
"EventDbPurgeInterval"=dword:00000001
```

22.10. Settings in the netlogon Branch

The `netlogon` branch contains value entries for setting the expiration of the cache that holds information for the site affinity service, including the optimal domain controller and global catalog. The `netlogon` service generates the value entries under the `[HKEY_THIS_MACHINE\Services\netlogon\cachedb]` subkey to cache information about your domain controllers and global catalog. It is recommended that you do not change the values of entries under the `cachedb` subkey. Only the value entries under the `Parameters` subkey are documented in this section.

```
[HKEY_THIS_MACHINE\Services\netlogon]
"Arguments"="/opt/likewise/sbin/netlogond ---syslog"
"Dependencies"="lwreg"
```



```
"Description"="Likewise Site Affinity Service"  
"Path"="/opt/likewise/sbin/netlogond"  
"Type"=dword:00000001
```

```
[HKEY_THIS_MACHINE\Services\netlogon\cachedb]
```

```
[HKEY_THIS_MACHINE\Services\netlogon\Parameters]  
"NegativeCacheTimeout"=dword:0000003c  
"PingAgainTimeout"=dword:00000384  
"WritableRediscoveryTimeout"=dword:00000708  
"WritableTimestampMinimumChange"=dword:00000000
```

22.10.1. Set the Negative Cache Timeout

This setting is reserved for internal use only.

Location

```
[HKEY_THIS_MACHINE\Services\netlogon\Parameters]
```

Value Entry

NegativeCacheTimeout

Example with default value:

```
"NegativeCacheTimeout"=dword:0000003c
```

22.10.2. Set the Ping Again Timeout

The netlogon service periodically tests whether cached domain controllers are available. This setting controls how often it does so.

Location

```
[HKEY_THIS_MACHINE\Services\netlogon\Parameters]
```

Value Entry

PingAgainTimeout

Example with default value:

```
"PingAgainTimeout"=dword:00000384
```

22.10.3. Set the Writable Rediscovery Timeout

When a service requests a writable domain controller and one does not exist in the local site, this setting controls how long the service stays affinitized to the writable domain controller before reaffinitizing to a closer read-only domain controller.

Location

```
[HKEY_THIS_MACHINE\Services\netlogon\Parameters]
```

Value Entry

WritableRediscoveryTimeout

Example with default value:

```
"WritableRediscoveryTimeout"=dword:00000708
```

22.10.4. Set the Writable Timestamp Minimum Change

Netlogon 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
```

22.10.5. Set CLdap Options

The netlogon service uses multiple asynchronous CLDAP searches in a single thread to find servers that act as domain controllers and global catalogs. To improve performance in the context of your unique network, you can adjust the following settings for the Connection-less Lightweight Directory Access Protocol.

Location

[HKEY_THIS_MACHINE\Services\netlogon\Parameters]

Value Entries

`CLdapMaximumConnections` is the maximum number of servers that will be pinged simultaneously. The default is 100.

`CLdapSearchTimeout` is the timeout for the entire search (in seconds). The default is 15 seconds.

`CLdapSingleConnectionTimeout` is the timeout for pingging a single server (in seconds). The default is 15 seconds.

22.11. Settings in the Lwio Branch

The `lwio` branch contains value entries for the input-output service, `lwio`, that plays a fundamental role in the operation of the CIFS file server.

The value entries under the `shares` subkey define shared folders and the security descriptors that control access to them. It is recommended that you do not directly change the values under the `shares` subkey while the `lwiod` service is running.

22.11.1. Sign Messages If Supported

Although signing messages is turned off by default, you can set the input-output service to sign messages. Doing so, however, can degrade performance. When signing is turned off, the input-output service will reject clients that require signing.

Location

[HKEY_THIS_MACHINE\Services\lwo\Parameters\Drivers\rdr]

Value Entry

SignMessagesIfSupported

Example with default value:

```
"SignMessagesIfSupported"=dword:00000000
```

22.11.2. Enable Security Signatures

This value entry, which is turned on by default, sets the CIFS file server to sign responses when it receives signed messages from a client.

Location

[HKEY_THIS_MACHINE\Services\lwo\Parameters\Drivers\srv]

Value Entry

EnableSecuritySignatures

Example with default value:

```
"EnableSecuritySignatures"=dword:00000001
```

22.11.3. Require Security Signatures

This value entry determines whether the CIFS file server will reject clients that do not support signing.

Location

[HKEY_THIS_MACHINE\Services\lwo\Parameters\Drivers\srv]

Value Entry

RequireSecuritySignatures

Example with default value:

```
"RequireSecuritySignatures"=dword:00000001
```

22.11.4. Set Support for SMB2

This value entry determines whether the CIFS file server will engage the SMB2 protocol module. When the setting is turned off, the server will not negotiate with SMB2.

Location

[HKEY_THIS_MACHINE\Services\lwo\Parameters\Drivers\srv]

Value Entry

SupportSmb2

Example with default value:

"SupportSmb2"=dword:00000000

22.12. Settings in the Lwedsplugin Branch for Mac Computers

The Likewise registry includes the following settings to manage the directory services plugin on a Mac OS X computer. Each of these settings can be managed by a corresponding Likewise Enterprise group policy; for more information, see the Group Policy Administration Guide. Here's an example configuration in the registry:

```
[HKEY_THIS_MACHINE\Services\lwedsplugin\Parameters\]
- "AllowAdministrationBy"          REG_SZ          - "CORP\
\EnterpriseTeam"
- "EnableForceHomedirOnStartupDisk" REG_DWORD       0x00000001 (1)
- "EnableMergeAdmins"             REG_DWORD       0x00000001 (1)
- "UncProtocolForHomeLocation"    REG_SZ          - "smb"
- "UseADUncForHomeLocation"       REG_DWORD       0x00000001 (1)
```

Each setting is described in the following table.

DS Plugin Setting in the Registry	Description
Allow administration by	Specifies the administrators included the local admin group (GID: 80) on the computer. The setting can specify Active Directory users or groups. Local entries are overwritten unless you also set the parameter to merge administrators who are defined locally.
Force home directory on startup disk	Sets a computer to use a local home directory path. When a user with a home folder connection defined in Active Directory logs on, the connection is created in the dock under / Network/Servers/homeFolderName.
Merge Administrators	Preserves members of the admin group who are defined locally but are not specified in the allow administration by policy.
Set the UNC Protocol for the Home Location	Sets the protocol for the home location.
Use UNC path from Active Directory to create home location	Sets the computer to connect to the network share defined in the Active Directory user account. The UNC path is converted to SMB when the target share is running Windows or AFP when the target is running Mac OS X.

If the setting for forcing the home directory on the startup disk is enabled, the UNC path is used to create a folder in the user's dock and the home directory is set to the user's local home directory path.

To set the path for the home directory, go to the **Profile** tab of the user's properties in ADUC and under **Home folder** select **Connect**, choose a drive letter (which is ignored by a Mac OS X computer), and then in the **To** box type the UNC path that you want.

Here's the form the path takes: \\server
\share\folder

Here's an example of a path: \
\lwdemo01\homes\fanthony

Chapter 23. Contacting Technical Support

23.1. 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**.

23.2. Provide Diagnostic Information to Technical Support

When you work with Likewise technical support staff to troubleshoot a problem, it is useful to provide a set of information to help solve the problem. The list below outlines the information that, as a best practice, you should collect and provide to Likewise technical support staff.

Information for All Problems

1. Operating system version.
2. Likewise version and build number. See Check the Version and Build Number.

Problem: Segmentation Faults

1. Core dump of the Likewise application:

```
ulimit - c unlimited
```
2. Exact patch level or exact versions of all installed packages. See Check the Version and Build Number.

Problem: Program Freezes

1. Debug logs.
2. `tcpdump`.
3. An `strace` of the program.

Problem: Domain Join Errors

1. Debug logs. See [Generate a Domain-Join Log](#) or grab the log file from `/var/log/likewise-join.log`.

2. `tcpdump`.

See [Solve Domain-Join Problems](#).

Problem: All Active Directory Users Are Missing

1. Run `/opt/likewise/bin/lw-get-status`

See [Get the Status of the Authentication Providers](#).

2. Contents of `nsswitch.conf`.

See [Solve Logon Problems on Linux or Unix](#).

Problem: All Active Directory Users Cannot Log On

1. Output of `id <user>`

2. Output of `su -c 'su <user>' <user>`

3. Lsass debug logs. See [Generate an Authentication Agent Debug Log](#).

4. Contents of `pam.d/pam.conf`.

5. The `sshd` and `ssh` debug logs and `syslog`.

Problem: AD Users or Groups Are Missing

1. The debug logs for `lsass`.

2. Output for `getent passwd` or `getent group` for the missing object.

3. Output for `id <user>` if user.

4. `tcpdump`.

5. Copy of `lsass` cache file. For the file name and location of the cache files, see [About the Likewise Agent](#).

Problem: Poor Performance When Logging On or Looking Up Users

1. Output of `id <user>`

2. The lsass debug log.
3. Copy of lsass cache file. For the file name and location of the cache files, see [About the Likewise Agent](#).
4. tcpdump.

Chapter 24. Legal Disclaimer and Copyright Notice

The information contained in these documents represents the current view of Likewise Software on the issues discussed as of the date of publication. Because Likewise Software must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Likewise, and Likewise Software cannot guarantee the accuracy of any information presented after the date of publication.

These documents are for informational purposes only. LIKewise SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form, by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Likewise Software.

Likewise may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Likewise, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. For complete information on the software licenses and terms of use for Likewise products, see www.likewise.com.

Likewise and the Likewise logos are either registered trademarks or trademarks of Likewise Software in the United States and/or other countries. All other trademarks are property of their respective owners.

Likewise Software
15395 SE 30th Place, Suite 140
Bellevue, WA 98007
USA

Terms of Use.

For more information, contact info@likewise.com or visit www.Likewise.com.

Copyright © 2011 Likewise Software. All rights reserved.