



IN THIS DOCUMENT

- Integrating Samba file sharing from Linux and Unix servers with Likewise.
- Replacing the authentication backend and native Samba 3 idmapper with that provided by Likewise.

Samba 3 Integration Guide For Likewise 5.0 or Later

Abstract

This document describes how to integrate Samba file sharing from Linux and Unix servers with Likewise Enterprise 5 or Likewise Open 5, build 3928 or later, so that these shares provide controlled access for Windows clients that are authenticated by Active Directory. The guide also discusses the configuration of home directories and roaming profiles.

The Samba 3.0 integration guide is intended to provide the system administrator with deployment guidance when integrating Samba 3.0 with Likewise to provide secure, interoperable enterprise solutions for Windows file and print sharing on Linux and Unix operating systems. This guide provides a step-by-step instruction on replacing the authentication backend and native Samba 3.0 idmapper with that provided by Likewise.

[This document describes how to integrate Likewise Enterprise 5.0 or later with Samba.](#)

About Likewise

By joining Linux, Unix, and Mac computers to Active Directory – a secure, scalable, stable, and proven identity management system – Likewise gives you the power to manage all your users' identities in one place, use the highly secure Kerberos 5 protocol to authenticate users in the same way on all your systems, apply granular access controls to sensitive resources, and centrally administer Linux, Unix, Mac, and Windows computers with group policies. Likewise includes reporting and auditing capabilities that can help improve regulatory compliance. The result: lower operating costs, better security, enhanced compliance.

The information contained in this document 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.

© 2008 Likewise Software. All rights reserved.

Likewise and the Likewise logo 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



Table of Contents

INTRODUCTION.....	4
Key Benefits of Combining Samba and Likewise.....	4
Consolidation of User Account Management	4
Simplified Installation and Configuration.....	4
SID-TO-UID MAPPING IN AD	4
SIMPLE FILE SHARING.....	5
Prerequisites	5
Setup	6
Verification	8
SAMBA SUPPORT FOR AD INTEGRATION.....	9
How to I determine if your version of Samba supports Active Directory integration?	9
Samba Resources.....	9
TROUBLESHOOTING FAQ	9

Introduction

Samba is the one the most popular and widely available programs used to integrate Unix and Linux servers with Windows clients. Although originally written to facilitate the sharing of files and printers, Samba can also be configured to allow the a Unix server to act as an NT4 equivalent Domain Controller, a master browser, a WINS server, and AD domain member, and more. Samba services beyond simple file sharing and authentication are beyond the scope of this document. For more information about Samba, visit the Samba project website at <http://www.samba.org>.

Key Benefits of Combining Samba and Likewise

Consolidation of User Account Management

Samba, by default, will maintain its own database of users and passwords. These credentials are in addition to those required by the Unix server itself and by your Windows environment, and must be managed separately.

Likewise allows you to consolidate all these identities in a single AD account, simplifying management.

Simplified Installation and Configuration

Likewise provides an easy-to-use installer and configuration tool. This tool simplifies the Samba manual process of Active Directory integration through the following process:

- Configuring hostname and DNS, including Active Directory integrated Secure Dynamic DNS support
- Installation and configuration of authentication components to match multi-forest, multi-domain Active Directory expectations
- Joining an Active Directory domain

SID-to-UID Mapping in AD

Microsoft Windows distinguishes one user from another using a security ID (SID). The SID is not recognized by Unix-based systems, however, which use a simple number (the user ID, or UID) to each user in the

environment. In order for a single security principle (user) to exist in both realms, it must be mapped to both of these types of identifiers.

The `idmapper` is the part of Samba that maps Active Directory SIDs to Unix UIDs and GIDs. The `idmap backend` refers to the name of the module used by idmap to store the name space information. Other parameters are available for idmap configuration of allowed UID and GID ranges, cache time, etc.

Simple File Sharing

Likewise contains a compatibility idmap plugin for Samba 3.0.0 - 3.0.X. This section describes integration of a vendor's version of Samba to integrate with the Likewise authentication daemon. Be aware that older versions of Samba may contain bugs that will alter the behavior from what is described below.

Prerequisites

1. Make sure the Likewise NNS library and not Samba's is configured for user and group ID lookups. For example, the `/etc/nsswitch.conf` `passwd` and `group` entries for Linux should be as follows:

```
passwd:      files lsass
group:       files lsass
```

2. In `/etc/krb5.conf`, include maps to variations of the AD domain name. Example:

```
.example.com = EXAMPLE.COM
example.com = ROVING.COM
```

3. Winbind must be installed, running, and responding to ID mapping requests. Check it like this:

```
$ /etc/init.d/winbind restart
#Test trust:
$ wbinfo -t
#List domain users:
$ wbinfo -u
#Find by SID:
$ wbinfo -S [user_SID]
$ wbinfo -Y [group_SID]
```

Setup

This procedure assumes that **Likewise 5.0 or later** has been installed on your Linux or Unix server and that the system has been joined to Active Directory. You might need to update to the latest version of Likewise; the libraries for Samba integration were added in build 3928 to Likewise Open 5.0 and Likewise Enterprise 5.0. Also: The vendor's version of Samba must be installed and functional on the Linux or Unix system.

Tip: After you locate the `smbd` file, you can find the paths where Samba has been installed by typing the following command: `smbd -b`

1. Create a directory named 'idmap' under `/usr/lib/samba`, if necessary (**`/usr/lib64/samba`** for 64-bit servers). Create a symbolic link from **`/usr/lib/samba/idmap/lwicompat_v2.so`** to point to **`/opt/likewise/lib/lwicompat_v2.so`**. Repeat for **`lwicompat_v3`** and **`lwicompat_v4`**.

```
# cd /usr/lib/samba
# mkdir idmap
# cd idmap
# ln -s /opt/likewise/lib/lwicompat_v2.so /usr/lib/samba/idmap/lwicompat_v2.so
# ln -s /opt/likewise/lib/lwicompat_v3.so /usr/lib/samba/idmap/lwicompat_v3.so
# ln -s /opt/likewise/lib/lwicompat_v4.so /usr/lib/samba/idmap/lwicompat_v4.so
```

On a 64-bit server, the path is slightly different:

```
# cd /usr/lib64/samba
# mkdir idmap
# cd idmap
# ln -s /opt/likewise/lib64/lwicompat_v2.so /usr/lib64/samba/idmap/lwicompat_v2.so
# ln -s /opt/likewise/lib64/lwicompat_v3.so /usr/lib64/samba/idmap/lwicompat_v3.so
# ln -s /opt/likewise/lib64/lwicompat_v4.so /usr/lib64/samba/idmap/lwicompat_v4.so
```

2. Confirm the version of Samba that you have installed and edit the Samba configuration file accordingly.

```
# smb -V
Version 3.0.26a-1478
```

Now that you know the version number, edit the Samba configuration file **`/etc/samba/smb.conf`** to set the following parameters to the listed values. If the parameters are not included in the **`smb.conf`** file, add a new line for them in the **[global]** section. Here are the compatibility plugins to use by Samba version:

`lwicompat_v2` for Samba 3.0.0 - 3.0.22



lwicompat_v3 for Samba 3.0.23 - 3.0.24

lwicompat_v4 for Samba 3.0.25 and later 3.0 releases.

Here is how to edit your smb.conf file for lwicompat_v2 or lwicompat_v3:

```
security = ads
workgroup = <enter NETBIOS name from /opt/likewise/bin/lw-get-status>
realm = <enter realm from /etc/krb5.conf>
# idmap backend = lwicompat_v2
idmap backend = lwicompat_v3
idmap uid = 50-9999999999
idmap gid = 50-9999999999
```

The configuration for Samba 3.0.25 and later 3.0 releases is different. Here is how to edit your smb.conf file for lwicompat_v4 for Samba version 3.0.25 and later 3.0 releases:

```
security = ads
workgroup = <enter NETBIOS name from /opt/likewise/bin/lw-get-status>
realm = <enter realm from /etc/krb5.conf>
idmap domains = ALL
idmap config ALL:backend = lwicompat_v4
idmap config ALL:default = yes
idmap config ALL:readonly = yes
```

3. Print out the machine account information by running the following command as root to retrieve the machine account password from the Likewise authentication system and provide it to the Samba server's authentication system:

```
/opt/likewise/bin/lw-dump-machine-acct <dns domain>
DomainSID = S-1-5-21-aaaa-bbbb-cccc-dddd
DomainName = AD
Domain DNS Name = AD.PLAINJOE.ORG
HostName = srv3
Machine Account Name = srv3$
Machine Account Password = EncryptedStringPassword
```

4. Set the domain SID in Samba's database by using the Samba net command:

```
net setdomainsid S-1-5-21-aaaa-bbbb-cccc-dddd
```

5. Store the machine account password by using the `net` command. You can copy the encrypted machine account password from the output of the `/opt/likewise/bin/lw-dump-machine-acct <dns domain>` that you executed in a previous step.

Important: Your machine account password expires, according to your default AD domain policy, after 40 days. Therefore, you must repeat these steps every time your machine account password expires. However, you can set up a cron job to automate this operation, but doing so is beyond the scope of this document.

```
net changesecretpw -f
Enter password: <EncryptedStringPassword>
```

6. For Samba 3.0.0 through 3.0.22, you must add the `userPrincipalName` attribute for the machine account in Active Directory, by using either `adsiedit` or LDIF. The machine's distinguished name, or DN, can be obtained from the output of the Likewise `domainjoin-cli query` command:

```
/opt/likewise/bin/domainjoin-cli query
Name = srv3
Domain = CORP.LIKEWISE.COM
Distinguished Name = CN=SRV3,OU=Engineering,DC=corp,DC=likewise,DC=com
```

The following LDIF excerpt shows the settings necessary to add the `userPrincipalName` attribute to this account. Replace the `<MACHINE>` value with the computer's hostname in upper case and the `<REALM>` with the AD domain name in upper case.

```
dn: CN=SRV3,OU=Engineering,DC=corp,DC=likewise,DC=com
changetype: modify
add: userPrincipalName
userPrincipalName: host/<MACHINE>@<REALM>
```

Note: Ubuntu and Debian store `secrets.tdb` in `/var/lib/samba`, so you must create a symlink back to `/etc/samba/secrets.tdb`.

```
mv /var/lib/samba/secrets.tdb /var/lib/samba/secrets.tdb.orig
ln -s /etc/samba/secrets.tdb /var/lib/samba/secrets.tdb
```

Verification

You can verify that the previous steps were a success by running the following command, which should report that "Join is OK":



```
net ads testjoin
Join is OK
```

Samba Support for AD Integration

How to I determine if your version of Samba supports Active Directory integration?

In order to determine whether your version of Samba supports Active Directory integration run, examine the build options for the WITH_ADS option. You can execute the Samba daemon with the build options '-b' argument and search for the WITH_ADS 'build' and 'with' option with grep, e.g.:

```
$ /usr/sbin/smbd -b | grep WITH_ADS

WITH_ADS
WITH_ADS
```

Samba Resources

Samba documentation and resources can be found at the Samba website:
<http://www.samba.org>.

Troubleshooting FAQ

Q. Samba 3.0.10 (FC3 and RHEL4) fails to allow a user to connect.

A. This and possibly other versions of Samba's winbindd have a bug that causes a connection to fail if the getgroups() call fails to resolve the first group SID in a user's list to a gid. The bug shows up as a NT_STATUS_NO_SUCH_USER error in the Samba log files. An alternative method of testing this is to run "wbinfo -r DOMAIN\User". This should return a list of gids (at least one). The workaround is to enable all the user's groups for Unix access in the cell or forest.

Q. How do I use the non-sAMAccount Likewise Enterprise aliases (usernames) and Samba?

A. You must inform Samba of the alias by including a username map. Add "username map = /etc/samba/users.map" to the [global] section of /etc/samba/smb.conf. The create the /etc/samba/users.map file and add an entry for each aliases user in the form "!alias = DOMAIN\user".

To alias AD groups, use the form "!alias = @DOMAIN\group".



Note: The exclamation mark causes Samba to stop processing on the first matching alias. This prevents issues with multiple alias matches caused by the use of wildcards.

ABOUT LIKEWISE

Likewise Software is an open source company that provides audit and authentication solutions designed to improve security, reduce operational costs and help demonstrate regulatory compliance in mixed network environments. Likewise Open allows large organizations to securely authenticate Linux, Unix and Mac systems with a unified directory such as Microsoft Active Directory. Additionally, Likewise Enterprise includes world-class group policy, audit and reporting modules.

Likewise Software is a Bellevue, WA-based software company funded by leading venture capital firms Ignition Partners, Intel Capital, and Trinity Ventures. Likewise has experienced management and engineering teams in place and is led by senior executives from leading technology companies such as Microsoft, F5 Networks, EMC and Mercury.