DOCUMENTATION

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

PowerBroker Identity Services

Samba Integration Guide

Revision/Update Information: February 2016

Corporate Headquarters
5090 N. 40th Street
Phoenix, AZ 85018
Phone: 1 818-575-4000

COPYRIGHT NOTICE

TRADE SECRET NOTICE

This software and/or documentation, as and when applicable, and the information and know-how they contain constitute the proprietary, confidential and valuable trade secret information of BeyondTrust and/or of the respective manufacturer or author, and may not be disclosed to others without the prior written permission of BeyondTrust. This software and/or documentation, as and when applicable, have been provided pursuant to an agreement that contains prohibitions against and/or restrictions on copying, modification and use.

DISCLAIMER

BeyondTrust makes no representations or warranties with respect to the contents hereof. Other than, any limited warranties expressly provided pursuant to a license agreement, NO OTHER WARRANTY IS EXPRESSED AND NONE SHALL BE IMPLIED, INCLUDING WITHOUT LIMITATION THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR USE OR FOR A PARTICULAR PURPOSE.

LIMITED RIGHTS FARS NOTICE (If Applicable)

If provided pursuant to FARS, this software and/or documentation, as and when applicable, are submitted with limited rights. This software and/or documentation, as and when applicable, may be reproduced and used by the Government with the express limitation that it will not, without the permission of BeyondTrust, be used outside the Government for the following purposes: manufacture, duplication, distribution or disclosure. (FAR 52.227.14(g)(2)(Alternate II))

LIMITED RIGHTS DFARS NOTICE (If Applicable)

If provided pursuant to DFARS, use, duplication, or disclosure of this software and/or documentation by the Government is subject to limited rights and other restrictions, as set forth in the Rights in Technical Data – Noncommercial Items clause at DFARS 252.227-7013.

TRADEMARK NOTICES

PowerBroker, PowerPassword, and PowerKeeper are registered trademarks of BeyondTrust. PowerSeries, PowerADvantage, PowerBroker Password Safe, PowerBroker Directory Integrator, PowerBroker Management Console, PowerBroker Desktops, PowerBroker Virtualization, PowerBroker Express, PowerBroker Databases, PowerBroker Windows Servers, PowerBroker Windows Desktops, and PowerBroker Identity Services are trademarks of BeyondTrust.

ssh® is a registered trademark of SSH Communications Security Corp in the United States and in certain other jurisdictions. The SSH logo, Tectia and tectia logo are trademarks of SSH Communications Security Corp and may be registered in certain jurisdictions.

This application contains software powered by PKAIP®, the leading solution for enabling efficient and secure data storage and transmission. PKAIP® is provided by PKWARE, the inventor and continuing innovator of the ZIP file format. Used with permission.

FICTITIOUS USE OF NAMES

All names of persons mentioned in this document are used fictitiously. Any resemblance to actual persons, living or dead is entirely coincidental.

OTHER NOTICES

If and when applicable the following additional provisions are so noted:

The PowerBroker Identity Services Open software is free to download and use according to the terms of the Limited GPL 2.1 for client libraries and the GPL 2 for daemons. The licenses for PowerBroker Identity Services Enterprise and for PowerBroker Identity Services UID-GID Module are different. For complete information on the software licenses and terms of use for BeyondTrust products, see www.beyondtrust.com.

Contents

Introduction

This document describes how to integrate Samba 3.0.25, 3.2.X, or 3.5.X with PowerBroker Identity Services Enterprise Edition 6 or later or PowerBroker Identity Services Open Edition 6 (or later).

Conventions Used in This Guide

Specific font and linespacing conventions are used in this book to ensure readability and to highlight important information such as commands, syntax, and examples.

Font Conventions

The font conventions used for this document are:

- `Courier New Font` is used for program names, commands, command arguments, directory paths, variable names, text input, text output, configuration file listings, and source code. For example:

  `/etc/powerbroker/product.cfg`

- **`Courier New Bold Font`** is used for information that should be entered into the system exactly as shown. For example:

  `pbcheck -v`

- *`Courier New Italics Font`* is used for input variables that need to be replaced by actual values. In the following example, *`variable-name`*, must be replaced by an actual environment variable name. For example:

  `result = getenv (`*`variable-name`*`);`

- **Bold** is used for Windows buttons. For example:

  Click **OK**.

Linespacing Conventions

The linespacing of commands, syntax, examples, and computer code in this manual may vary from actual Windows and Unix/Linux usage because of space limitations. For example, if the number of characters required for a single line does not fit within the text margins for this book, the text is displayed on two lines with the second line indented as shown in the following sample:

```
result = sprintf ("System administrator Ids: %s %s %s", "Adm1", "Adm2",
   "Adm3");
```

Where to Go Next?

For more information, see the documentation and resources listed in the following sections.

Documentation for PBIS

The PBIS documentation includes:

- *PBIS Enterprise Installation Guide*
- *PBIS Enterprise Administration Guide*

- *PBIS Enterprise Linux Administration Guide*
- *PBIS Enterprise Auditing & Reporting Guide*
- *PBIS Open Quick Start Guide Guide*
- *PBIS Enterprise Group Policy Administration Guide*
- *PBIS Enterprise Evaluation Guide*

Contacting Support

For support, go to our Customer Portal then follow the link to the product you need assistance with.

The Customer Portal contains information regarding contacting Technical Support by telephone and chat, along with product downloads, product installers, license management, account, latest product releases, product documentation, webcasts and product demos.

Telephone

Privileged Account Management Support

Within Continental United States: 800.234.9072

Outside Continental United States: 818.575.4040

Vulnerability Management Support

North/South America: 866.529.2201 | 949.333.1997

+ enter access code

All other Regions:

Standard Support: 949.333.1995

+ enter access code

Platinum Support: 949.333.1996

+ enter access code

Online

http://www.beyondtrust.com/Resources/Support/

Getting Started

The following procedures must be performed before you can configure Samba for use with PowerBroker Identity Services.

This guide assumes you are a systems administrator who knows how to manage shared files and folders on Linux, Unix, and Windows computers, including configuring the Linux and Unix file servers to run Samba and 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.

Instructions on how to set up Samba are beyond the scope of this document. For information about installing and configuring Samba, see http://www.samba.org/samba/docs/.

Requirements

The following prerequisites must be in place:

- Root access to the Linux or Unix file server where you want to run Samba and PowerBroker Identity Services.
- PBIS Enterprise 6.0 or later or PBIS Open 6.0 or later, such as 6.1. The build number for PBIS Open 6.0 must be 8330 or later.
- The Linux or Unix computer must be connected to Active Directory with PowerBroker Identity Services. For instructions on how to join a domain, see the *PowerBroker Identity Services Installation Guide*.
- Supported Samba versions:
  - Samba version 3.0.25 or later versions in the 3.0 series
  - Samba 3.2.X
  - Samba 3.4.X
  - Samba 3.5.X

  Download Samba here: http://www.samba.org/samba/download/.
- Winbind must be installed and running when you are using Samba version 3.0.25 or later versions in the 3.0 series.

  If you are using Samba version 3.2.X or 3.5.X, Winbind is **not** required.
- Samba package must support ADS security. PowerBroker Identity Services relies on ADS security in a Samba and PowerBroker Identity Services configuration. For more information, see:

  https://wiki.samba.org/index.php/Setup_Samba_as_an_AD_Domain_Member

Installing Files

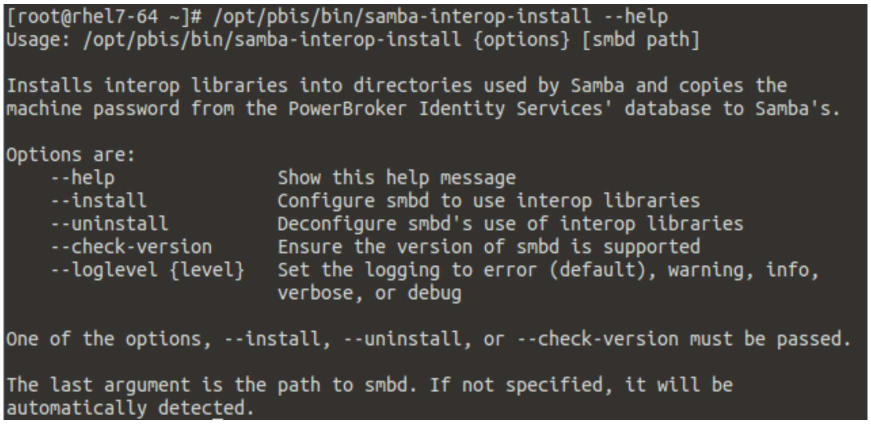
PowerBroker Identity Services includes the following tool to install the files necessary to use Samba:

```
samba-interop-install
```

Located in `/opt/pbis/bin`

To view the tool's options, run the following command:

```
/opt/pbis/bin/samba-interop-install --help
```



```
[root@rhel7-64 ~]# /opt/pbis/bin/samba-interop-install --help
Usage: /opt/pbis/bin/samba-interop-install {options} [smbd path]

Installs interop libraries into directories used by Samba and copies the
machine password from the PowerBroker Identity Services' database to Samba's.

Options are:
    --help              Show this help message
    --install           Configure smbd to use interop libraries
    --uninstall         Deconfigure smbd's use of interop libraries
    --check-version     Ensure the version of smbd is supported
    --loglevel {level}  Set the logging to error (default), warning, info,
                        verbose, or debug

One of the options, --install, --uninstall, or --check-version must be passed.

The last argument is the path to smbd. If not specified, it will be
automatically detected.
```

When you run the tool with the `install` option:

- PowerBroker Identity Services `idmapper` plug-in for Windbind is copied to Samba's `idmap` directory.
- `libwbclient` is replaced with the PowerBroker Identity Services version of the client library. The old `libwbclient` is backed up in `/usr/lib`.
- The machine password from Active Directory is copied into Samba's `secrets.tdb` file. It is synchronized with the machine password in Active Directory.

Note the following depending on the Samba version:

- Samba 3.0.25 - The PowerBroker Identity Services `idmapper` maps SIDs to UIDs and GIDs for the PowerBroker Identity Services authentication service (lsass).
- Samba 3.0.25 - The PowerBroker Identity Services version of `libwbclient` is not loaded or used.
- Samba 3.2.X or later - The PowerBroker Identity Services version of `libwbclient` communicates directly with the PowerBroker Identity Services authentication service instead of Winbind.

Configuring Samba for Use With PBIS

Note: There are differences in how you set up Samba for use with PowerBroker Identity Services that depend on the version of Samba you are using. In the following procedure, pay close attention to the version numbers.

The following example setup took place on a Red Hat Enterprise Linux 5 desktop computer running Samba server version 3.0.33.

1. Make sure your Samba version is supported by PowerBroker Identity Services by running the following command as root:

   ```
   /opt/pbis/bin/samba-interop-install --check-version
   ```

2. On your Linux or Unix computer that is running Samba, add the following settings—which are required to authenticate users with Active Directory with all the versions of Samba that PowerBroker Identity Services supports—to the global section of the Samba configuration file, `smb.conf`, typically located in the `/etc/samba` directory.

   The `ADS` value for the `security` setting is required. Replace the values of `workgroup` and `realm` with the values for your network. The `workgroup` is your computer's NetBIOS domain name. The `realm` is your computer's Active Directory domain. Here is an example:

   ```
   [global]
      security = ADS
      workgroup = TESTER
      realm = TESTER.PBISDEMO.COM
      machine password timeout = 0
   ```

   Note: If you fail to add the `machine password timeout` option to `smb.conf` and set it to 0, Samba will change the machine account password without notifying the PowerBroker Identity Services authentication service, leaving PowerBroker Identity Services unable to connect to the domain.

   If an alternate hostname is used, then set that hostname as the NetBIOS name:

   ```
   [global]
      security = ADS
      workgroup = TESTER
      realm = TESTER.PBISDEMO.COM
      netbios name = CENTOS-TEST
   ```

3. If you are using Samba 3.0.25 or later versions in the 3.0 series, you must also add the following settings and values to the global section of `smb.conf`. (These settings are not required for Samba 3.2 or later; using them might result in a warning or an error.)

   ```
   idmap domains = ALL
   idmap config ALL:backend = lwicompat_v4
   idmap config ALL:default = yes
   idmap config ALL:readonly = yes
   idmap uid = 10000-33554431 idmap gid = 10000-33554431
   ```

   The range of the values for `idmap uid` and `idmap gid` will depend on the UID and GID ranges that you have established for your users and groups in Active Directory.

4. In `smb.conf`, create a new section to define a shared resource (named `testshare` in the example below) or use your own predefined section that specifies a shared resource, known as a share, and configure it with the Samba parameters that you want. For more information, see the Samba documentation or the Samba man page.
   In this example, the value of the `valid users` setting is an Active Directory account. Leaving the value of `valid users` blank allows all AD users to access the share; defining a list of AD users constrains access to those in the list. For more information, see the Samba documentation.

   ```
   [testshare]
      comment = This is a test share
      path = /share
      browseable = yes
      read only = no
      valid users = DEMO\Administrator
      writeable = yes
      guest ok = yes
   ```

5. As root, run the `testparm` command to make sure `smb.conf` contains no syntax errors:

   ```
   testparm /etc/samba/smb.conf
   ```

6. If you created a share like the example above, execute the following commands as root to create a corresponding directory for the share and set its permissions and ownership:

   ```
   mkdir /share
   chmod a+rx /share
   chown pbisdemo\\administrator /share/
   ```

7. As root, run the PowerBroker Identity Services-Samba interoperability installer to copy the PowerBroker Identity Services files to the Samba directory and write the machine password in `secrets.tdb`:

   ```
   /opt/pbis/bin/samba-interop-install --install
   ```

   If your Samba daemon is installed in a location other than `/usr/sbin` or another standard location, you must specify the path to its location. For example:

   ```
   /opt/pbis/bin/samba-interop-install --install /etc/apps/samba/bin
   ```

8. Restart Samba:

   ```
   /etc/init.d/smb restart
   ```

9. With Samba version 3.0.25 or later versions in the 3.0 series, you must also restart Winbind unless you are running a distribution on which Winbind is automatically restarted by the smb process:

   ```
   /etc/init.d/winbind restart
   ```

You are now ready to access the share from a Windows computer and log on with an AD account. (In the example configuration above, it would be `DEMO\administrator`.) If you cannot access the share or log on with your AD account, see "Troubleshooting PBIS-Samba Integration," page 10.

Troubleshooting PBIS-Samba Integration

You can troubleshoot PowerBroker Identity Services-Samba interoperability by executing the following sequence of steps.

Run the commands as root.

1. To help troubleshoot, turn on Samba logging by adding the following settings to the global section of the Samba configuration file, `smb.conf`.

```
[global]
   ...
   #Debugging settings:
   log level = 10
   debug pid = true
   log file = /var/log/samba/smbd.log
```

2. Verify that you can look up a domain user through Samba and that the user's UID is the same as the UID that PowerBroker Identity Services returns. With Samba 3.0.X, only password synchronization and UID mapping is provided. If UID mapping is broken, the user will show up, but with a different UID.

```
wbinfo -i demo\\administrator
demo\administrator:x:239600116:239600129:(null):/home/local/DEMO
```

   Make sure the UID matches the PowerBroker Identity Services UID for the same user by executing the following command:

```
/opt/pbis/bin/find-user-by-name demo\\administrator
User info (Level-0):
====================
Name: DEMO\administrator
SID:               S-1-5-21-3447809367-3151979076-456401374-500
Uid:               239600116
Gid: 239600129
Gecos:             <null>
Shell:             /bin/sh
Home dir:          /home/local/DEMO/administrator
Logon restriction: NO
```

   If the user's UIDs do not match, make sure the symlinks are in place to link Samba to the PowerBroker Identity Services library.

   Note: With Samba version 3.0.25 or later versions in the 3.0 series, fields other than the UID might not match because they are beyond the control of PowerBroker Identity Services. If the aliased user name, home directory, shell, or fields other than the UID do not match, no action is required.

3. Verify that the password is accepted through Samba, replacing `password` in the following command with the password for your account:

```
wbinfo -a demo\\administrator%password
plaintext password authentication succeeded
challenge/response password authentication succeeded
```

If the password fails, check the Samba log files to try to identify the reason. Also, check whether PowerBroker Identity Services can authenticate the user.

Keep in mind that with Samba 3.2.X, the `wbinfo` command could succeed with a bad machine password and you could access the share through NTLM. Kerberos authentication to the share, however, would fail. With Samba 3.0.X, nothing will work if the machine password is wrong.

If the output of the `wbinfo -a` command says that challenge-response authenticate failed, as in the following example, see "Turn on NTLMv2 If Challenge/Response Password Authentication Failed," page 13.

```
[root@rhel5d ~]# wbinfo -a demo\\administrator%password
plaintext password authentication failed
Could not authenticate user demo\administrator%password with plaintext
   password
could not obtain winbind separator!
challenge/response password authentication failed
Could not authenticate user demo\administrator with challenge/response
```

4. Verify that the machine password is up to date and that the password in `secrets.tdb` is correct by running the `net ads testjoin` command. The location of `secrets.tdb` varies across the Linux distributions and Samba versions. It might, for instance, appear in `/var/lib/samba/private` or in `/etc/samba`.

   ```
   net ads testjoin
   ```

   The result should look like this: `Join is OK`.

   If the result of the command is invalid, see "Net ADS Testjoin Failed," page 17.

5. Compare the machine password that is stored in `secrets.tdb` with the machine password that is stored in Active Directory. The passwords must match.

First, use the `tdbtool` to check the machine password in `secrets.tdb`.

```
[root@rhel5d lib]# locate secrets.tdb
/etc/samba/secrets.tdb
[root@rhel5d lib]# cd /etc/samba/
[root@rhel5d samba]# ls
lmhosts secrets.tdb smb.conf smb.conf~ smbpasswd smbusers
[root@rhel5d samba]# tdbtool
tdb> open secrets.tdb
tdb> dump

key 45 bytes
SECRETS/MACHINE_SEC_CHANNEL_TYPE/DEMO
data 4 bytes
[000] 02 00 00 00 ...

key 18 bytes
SECRETS/SID/RHEL5D
data 68 bytes
[000] 01 04 00 00 00 00 00 05 15 00 00 00 F3 EA C4 27 ........ .......'
[010] 41 FB C3 06 AC 5E 04 4D 00 00 00 00 00 00 00 00 A....^.M .......
[020] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....... .......
[030] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....... .......
[040] 00 00 00 00                                     ...

key 24 bytes
SECRETS/SID/DEMO
data 68 bytes
[000] 01 04 00 00 00 00 00 05 15 00 00 00 62 2D 2C BE ........ ....b-,.
[010] D9 D3 09 54 F0 BF 13 D0 00 00 00 00 00 00 00 00 ...T.... .......
[020] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....... .......
[030] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....... .......
[040] 00 00 00 00                                    ...
key 37 bytes
SECRETS/MACHINE_PASSWORD/DEMO
data 17 bytes
[000] 69 28 32 48 32 65 34 31 46 37 74 48 4E 32 37 35 i(2H2e41 F7tHN275
[010] 00

key 45 bytes
SECRETS/MACHINE_LAST_CHANGE_TIME/DEMO
data 4 bytes
[000] F3 0B 3A 4D ..:M
tdb>
```

Second, use the
`/opt/pbis/bin/lsa ad-get-machine password`
command to check the password that is stored in Active Directory. Make sure it matches the machine password stored in `secrets.tdb`.

```
[root@rhel5d samba]# /opt/pbis/bin/lsa ad-get-machine password
Machine Password Info:
  DNS Domain Name: DEMO.COM
  NetBIOS Domain Name: DEMO
  Domain SID: S-1-5-21-3190566242-1409930201-3490955248
  SAM Account Name: RHEL5D$
  FQDN: rhel5d.demo.com
  Join Type: 1
  Key Version: 0
     Last Change Time: 129401233790000000
  Password: i(2H2e41F7tHN275
[root@rhel5d samba]#
```

In the above examples, the two passwords match. But if they do not, you can resolve the mismatch by rerunning the PowerBroker Identity Services Samba interop tool. Because the PowerBroker Identity Services tool resychronizes the machine password in `secrets.tdb` with the machine password in Active Directory, you must restart both Samba and Winbind for the change to take effect.

6. The PowerBroker Identity Services Samba interop tool tries to locate the `secrets.tdb` file based on the `PRIVATE_DIR` and `STATEDIR` options returned by `smbd -b`. You can view the location that the tool found by running the following command to check registry:

   ```
   /opt/pbis/bin/lwregshell ls '[HKEY_THIS_MACHINE\
       Services\lsass\Parameters\Providers\ActiveDirectory\
       Pstore\Plugins\Samba\]'
   ```

   If the location specified in the registry is different from the actual location of the `secrets.tdb` file, you could, as a workaround, create a symbolic link from the location that PowerBroker Identity Services found to Samba's location.

7. Make sure that at least the following ports are open for use by Samba (for more information, see the Samba information on server security at http://www.samba.org/samba/docs/server_security.html):

   ```
   UDP/137 - used by nmbd
   UDP/138 - used by nmbd
   TCP/139 - used by smbd
   TCP/445 - used by smbd
   ```

Turn on NTLMv2 If Challenge/Response Password Authentication Failed

With Samba version 3.0.25 or later versions in the 3.0 series as well as Samba 3.2.X or 3.5.X, you must configure NTLMv2 authentication for both your Samba file server and the Windows computer that you plan to use to connect to the file server if the output of the `wbinfo -a` command shows that challenge-response authenticate failed, as in the following result:

```
[root@rhel5d ~]# wbinfo -a demo\\administrator%password
plaintext password authentication failed
```

```
Could not authenticate user demo\administrator%password with plaintext
   password
could not obtain winbind separator!
challenge/response password authentication failed
Could not authenticate user demo\administrator with challenge/response
```

With Samba 3.2.X or 3.5.X, you do not need to change your Samba configuration file. Instead, you must run the `wbinfo` command with the `ntlmv2` option. You still must configure your Windows computer for NTLMv2 authentication.

When you try to access the Samba file server with AD credentials from the Windows computer, the symptom is that you are repeatedly prompted to enter your user name and password.

The solution is twofold:

- Turn on client NTLMv2 authentication in the Samba configuration file
- Modify the Windows computer to send an NTLMv2 response either by changing the local security setting or by applying a group policy to change the setting.

Samba File Server

The following procedure shows how to turn on NTLMv2 authentication on a Linux computer that is running Samba.

1. On your Linux or Unix computer that is running Samba, add the following setting as root to the global section of the Samba configuration file, `smb.conf`, typically located in the `/etc/samba` directory:

   ```
   [global]
   client ntlmv2 auth = yes
   ```

   With Samba 3.2.X or 3.5.X, do not add the `client ntlmv2 auth` to the configuration file; instead, run the `wbinfo` command with the `ntlmv2` option, like this:

   ```
   wbinfo --ntlmv2 -a pbisdemo\\administrator%password
   ```

   For information about the setting and the option, see the Samba documentation at http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html.

2. As root, run the `testparm` command to make sure you did not introduce a syntax error when you edited `smb.conf`:

   ```
   testparm /etc/samba/smb.conf
   ```

3. Restart Samba:

   ```
   /etc/init.d/smb restart
   ```

4. With Samba version 3.0.25 or later versions in the 3.0 series, you must also restart Winbind:

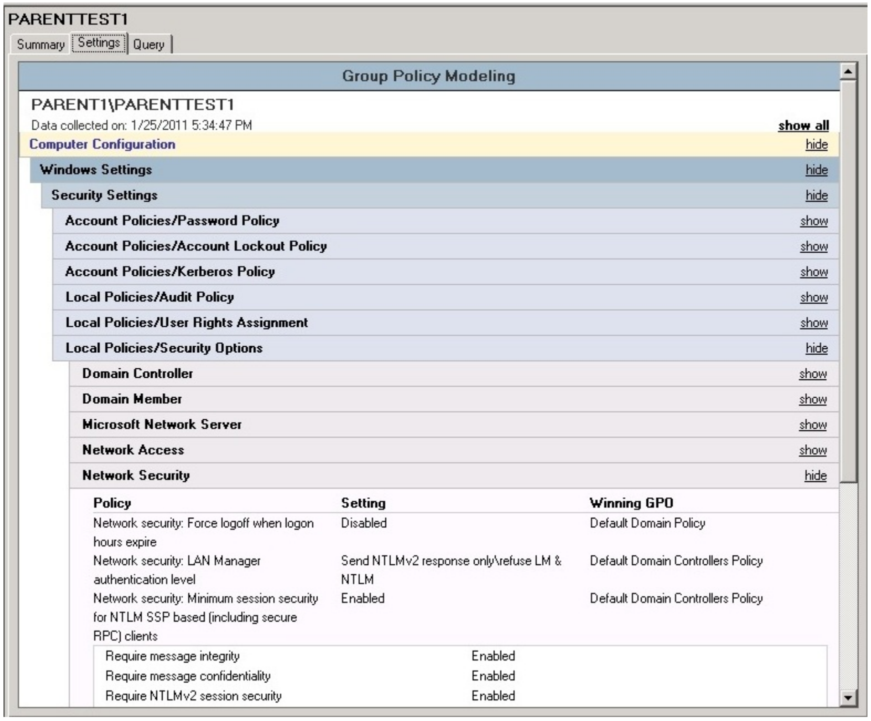
   ```
   /etc/init.d/winbind restart
   ```

Fix the Windows computer that you are using to access the Samba file server to send NTLMv2 response only by following the instructions below to modify the local LAN manager security setting or by following the Microsoft documentation to set a group policy to override the LAN manager setting.

Windows

On a Windows administrative workstation connected to your Active Directory domain controller, use group policy modeling in GPMC to determine which policy is applying a setting to refuse NTMLv2 on the Windows computer that is trying to access the Samba file server. For more information and instructions, see the Microsoft TechNet web site at http://technet.microsoft.com/en-us/library/cc781242(WS.10).aspx.

When you perform the modeling, do it for any user (that is, do not specify a user).



PARENT1\PARENTTEST1

Data collected on: 1/25/2011 5:34:47 PM

Computer Configuration

Windows Settings

Security Settings

Account Policies/Password Policy

Account Policies/Account Lockout Policy

Account Policies/Kerberos Policy

Local Policies/Audit Policy

Local Policies/User Rights Assignment

Local Policies/Security Options

Domain Controller

Domain Member

Microsoft Network Server

Network Access

Network Security

Policy	Setting	Winning GPO
Network security: Force logoff when logon hours expire	Disabled	Default Domain Policy
Network security: LAN Manager authentication level	Send NTLMv2 response only\refuse LM & NTLM	Default Domain Controllers Policy
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Enabled	Default Domain Controllers Policy
Require message integrity	Enabled	
Require message confidentiality	Enabled	
Require NTLMv2 session security	Enabled	

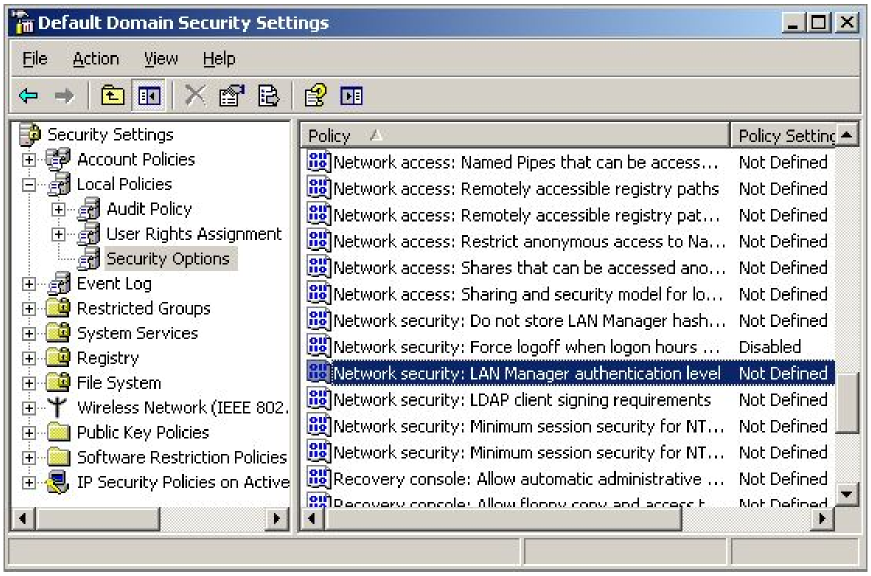
You can override the setting in two ways:

The first method is to override the setting by using a group policy to set the Windows computer to send NTLMv2 response only; the policy must take precedence over other group policy objects that want to impose the same setting. (For more information, see http://technet.microsoft.com/en-us/library/cc738867(WS.10).aspx.) That is, the policy that you set must be the winning GPO. For more information and instructions, see the Microsoft documentation for your version of Windows; for example, http://support.microsoft.com/kb/932461.

In the second method, if the setting is from the default domain controllers policy and is not being managed by a group policy, you can override it locally by changing the Windows security setting on the computer. The following procedure demonstrates how to do so on a Windows Server 2003 computer. Some of the settings might vary with other versions of Windows; see your Microsoft documentation for instructions.

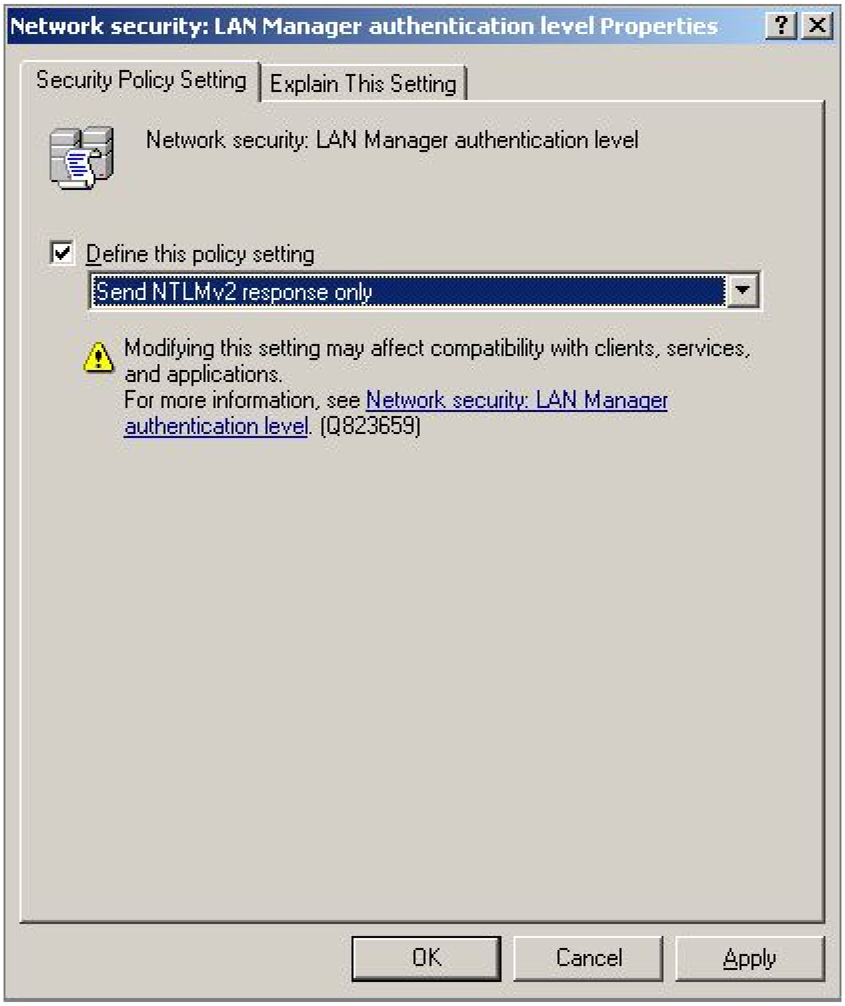
Caution! Client, service, and program incompatibilities might occur when you change the LAN manager security settings; see http://support.microsoft.com/kb/823659.

1. As an administrator, locate the following local security setting on the Windows computer that you will use to access the Samba file server: **Network security: LAN Manager authentication level**. For example:



Policy	Policy Settinc
Network access: Named Pipes that can be access…	Not Defined
Network access: Remotely accessible registry paths	Not Defined
Network access: Remotely accessible registry pat…	Not Defined
Network access: Restrict anonymous access to Na…	Not Defined
Network access: Shares that can be accessed ano…	Not Defined
Network access: Sharing and security model for lo…	Not Defined
Network security: Do not store LAN Manager hash…	Not Defined
Network security: Force logoff when logon hours …	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Not Defined
Network security: Minimum session security for NT…	Not Defined
Network security: Minimum session security for NT…	Not Defined
Recovery console: Allow automatic administrative …	Not Defined
Recovery console: Allow floppy copy and access t	Not Defined

2. Select the **Define this policy setting** check box and then, from the list, select **Send NTLMv2 response only**. Click **Apply**.


Network security: LAN Manager authentication level Properties
?
Security Policy Setting
Explain This Setting
OK
Cancel
Apply

Network security: LAN Manager authentication level

☑ Define this policy setting

Send NTLMv2 response only

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: LAN Manager authentication level. (Q823659)

3. Try again to verify that the password is authenticated through Samba, replacing `password` in the following command with the password for your account:
   ```
   wbinfo -a demo\\administrator%password
   ```

If you have properly configured both the Windows client and the Samba file server to use NTLMv2 authentication, the result should look like this:

```
plaintext password authentication succeeded
challenge/response password authentication succeeded
```

If there is still an error, recheck the Windows computer to make sure that its winning policy is to send an NTLMv2 response only.

Net ADS Testjoin Failed

If the `net ads testjoin` command fails or returns an invalid result, make sure that the SAM account name exactly matches the first component of the UPN used by the `net ads testjoin` command, as shown in bold in the following examples.

First, check the SAM account name by running the `lsa ad-get-machine password` command:

```
bvt-sld11p1-64g:~ # /opt/pbis/bin/lsa ad-get-machine password
Machine Password Info:
  DNS Domain Name: PARENT1.DEMO.COM
  NetBIOS Domain Name: PARENT1
   Domain SID: S-1-5-21-2320699617-2498519213-3481626681
  SAM Account Name: BVTF-SLD-INTM8WB$
  FQDN: parent1.pbisdemo.com
   Account Flags: 0x00000001 (1)
  Key Version: 0
  Last Change Time: 129434110220000000
  Password: 2cleT*3h;(A1+DCF
```

Second, compare the SAM account name with the first component of the UPN used by the `net ads testjoin` command:

```
bvt-sld11p1-64g:~ # net ads testjoin
[2011/02/28 16:17:36, 0, pid=22649] libads/kerberos.c:332(ads_kinit_password)
kerberos_kinit_password BVTF-SLD11P1-64G$@PARENT1.DEMO.COM failed: Preauthentication failed
[2011/02/28 16:17:36, 0, pid=22649] libads/kerberos.c:332(ads_kinit_password)
   kerberos_kinit_password BVTF-SLD11P1-64G$@PARENT1.DEMO.COM failed: Preauthentication failed
Join to domain is not valid: Logon failure
```

If the SAM account name and the first component of the UPN do not match, you must resolve the mismatch by doing the following:

1. Make sure the host name is 15 characters or less.
2. Make sure there are no computer accounts in AD that have the same SAM account name but a different DNS suffix.
3. Leave the domain.
4. Manually delete the machine account in Active Directory.
5. Rejoin the domain.

Another option is to manually change the host name to match the SAM account name, but such an approach is not recommended. For one thing, the hashed SAM account name could change in the future.

Fix a Netbios Name Mismatch

If you encounter the mismatch issue and believe that the length of the name is not at issue, you can use the `netbios name` parameter in `smb.conf` to set the SAM account name. Do not include the trailing dollar sign ($):

```
[global]
security = ADS
   workgroup = TESTER
  realm = TESTER.DEMO.COM
  netbios name = WEBSERV1-X1BG54
```

Fix Error Code 40022: Failed to Refresh Machine TGT

If you get an error in the log that looks something like the following entries (the time stamps and the machine name have been removed), you must add the `machine password timeout` option to the global section of `smb.conf` and set it to **0** to integrate PowerBroker Identity Serviceswith Samba:

```
lsassd[1722]: 0x7fafc3ff7700:Error:
Failed to refresh machine TGT [Error code: 40022]
lsassd[1722]: 0x7fafc3ff7700:Error:
Failed to refresh machine TGT [Error code: 40022]
```

Without the `machine password timeout` option set to **0**, Samba changes the machine account password without notifying the PowerBroker Identity Services authentication service, leaving PowerBroker Identity Services unable to connect to the domain. The result is that PowerBroker Identity Services cannot refresh the machine TGT and you cannot access your Samba file share with your Active Directory credentials.

The solution is to make sure that the global section of `smb.conf` contains the `machine password timeout` option and that it is set to **0**, like this:

```
[global]
security = ADS
  ...
   machine password timeout = 0
```

After you add the line to the Samba configuration file, run the `testparm` command as root to make sure `smb.conf` contains no syntax errors:

```
testparm /etc/samba/smb.conf
```

Tips and Tricks

Use a Username Map for Aliases

With Samba 3.0.25, you can use the non-SAM account aliases of PowerBroker Identity Services Enterprise by including a user name map:

- Add `username map = /etc/samba/users.map` to the global section of `smb.conf`
- Create an `/etc/samba/users.map` file
- In the `users.map` file, add an entry for each aliased user in the following form: `!alias = DOMAIN\user`.

To make an alias for an Active Directory group, use the form `!alias = @DOMAIN\group`. The exclamation point triggers Samba to stop processing on the first matching alias, preventing issues with multiple alias matches from wildcards. See the Samba documentation for more information about how to add users to a user name map.