Red Hat Reference Architecture Series

Deploying a Red Hat Enterprise Linux 6 based Samba Server in a Windows Active Directory Domain

Mark Heslin
Principal Software Engineer

Version 1.1
June 2011

1801 Varsity Drive™
Raleigh NC 27606-2072 USA
Phone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588
Research Triangle Park NC 27709 USA

The information contained herein is subject to change without notice. Red Hat, Inc. shall not be liable for technical or editorial errors or omissions contained herein.

The GPG fingerprint of the security@redhat.com key is:
CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

Send feedback to refarch-feedback@redhat.com

Table of Contents

1 Executive Summary

This paper details how to deploy and integrate Red Hat Enterprise Linux 6 with Samba file sharing and secure shell access into Windows Active Directory domains. Basic concepts, detailed installation, configuration and integration tasks are provided. Solutions to the most commonly encountered issues and errors are also described. The configurations and common use cases demonstrated within this reference architecture, provide a framework that can be customized to meet the requirements of specific computing environments.

Red Hat Enterprise Linux is a high-performing operating system that has delivered outstanding value to IT environments for nearly a decade. As the world's most trusted IT platform, Red Hat Enterprise Linux has been deployed in mission-critical applications at global stock exchanges, financial institutions, leading telcos, and animation studios. It also powers the websites of some of the most recognizable global retail brands.

Samba is the open source application of choice for providing seamless file and print sharing to Windows and CIFS/SMB clients. The Samba software suite provides unified user logon capabilities eliminating the need to manage multiple user accounts across multiple platforms. Users can securely access file shares or logon to the Red Hat Enterprise Linux 6 server using existing Active Directory domain accounts.

Red Hat Enterprise Linux 6 combined with Samba offers unmatched reliability, performance, security, simplified management capabilities and cost savings to organizations looking to integrate into Windows Active Directory domains.

1.1 Audience

This document does not require extensive Red Hat Enterprise Linux experience but the reader is expected to have a working knowledge of Microsoft Windows Server 2008 and Active Directory Domain Services. Detailed steps are provided within this document for configuring Samba, all integration tasks and the most common use cases.

1.2 Deployment and Integration Task Flow

Prior to proceeding with the Active Directory integration, the following components should be fully configured:

- Windows Server 2008 R2 with Active Directory Domain Services
- Windows client with access to both the Red Hat Enterprise Linux 6 (Samba) and Windows Server 2008 R2 file shares
- Red Hat Enterprise Linux 6 Server with Samba file services

Do not proceed with the integration tasks until these components have been fully configured, tested and verified.

As a convenience to the reader, the following summary guides are provided to assist with installation and configuration tasks:

- **Appendix C: Windows Server 2008 R2 – Installation Summary**
- **Appendix D: Active Directory Domain Services – Configuration Summary**
- **Appendix E: Red Hat Enterprise Linux 6 – Installation Summary**

Additional deployment and integration materials are provided in **Appendix F: References**.

Figure 1.2-1: Deployment and Integration Task Flow provides an overview of the order in which installation and integration tasks are completed:

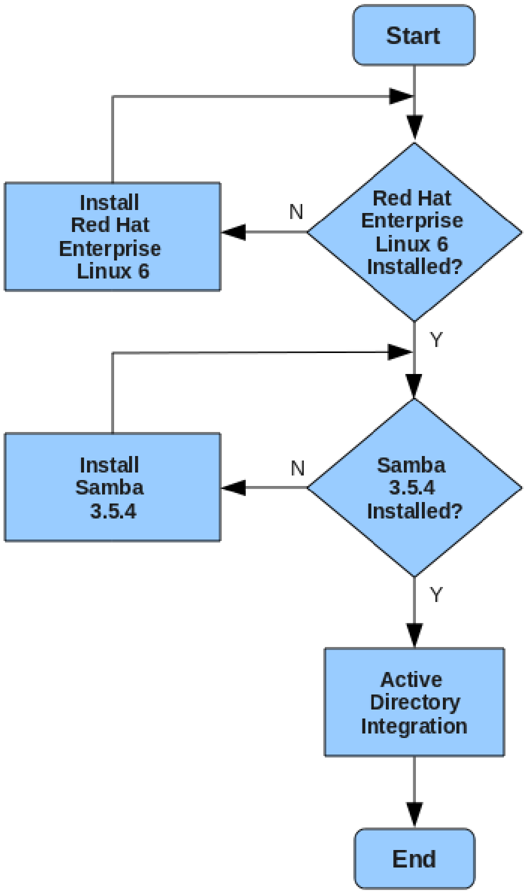

Start
Install Red Hat Enterprise Linux 6
N
Red Hat Enterprise Linux 6 Installed?
Y
Install Samba 3.5.4
N
Samba 3.5.4 Installed?
Y
Active Directory Integration
End

Figure 1.2-1: Deployment and Integration Task Flow

Red Hat Enterprise Linux 6 with Samba and Windows Server 2008 R2 with Active Directory must be fully configured and verified before the integration steps are performed. Administrator account access on the Active Directory domain server is also required.

2 Software Components

The following sections describe each of the software components. Features of particular interest to the integration process are described in further detail below.

2.1 Red Hat Enterprise Linux 6

Red Hat Enterprise Linux 6, the latest release of Red Hat's trusted datacenter platform, delivers advances in application performance, scalability, and security. With Red Hat Enterprise Linux 6, you can deploy physical, virtual, and cloud computing within your datacenter, reducing complexity, increasing efficiency, and minimizing administration overhead while leveraging existing technical skills and operational know-how. Red Hat Enterprise Linux 6 is an ideal platform to translate current and future technology innovations into the best value and scale for IT solutions.

Red Hat Enterprise Linux 6 builds on the previous Red Hat Enterprise Linux releases by introducing significant improvements in the areas of:

Area	Featured Components
Efficiency, scalability and reliability	Scalability, scheduling, reliability, availability and serviceability (RAS), file systems, high availability, power management
Resource Management	System resource allocation, storage, networking
Security	Access control, enforcement and verification of security policies, identity management (IDM)
Application Development and Production	Web infrastructure, Java, development tools/utilities, application tuning, databases, system API/ABI stability
Virtualization	Kernel-based virtualization, kernel features, guest acceleration, security, Microsoft Windows (WHQL) drivers
Enterprise Manageability	Software deployments (installation, updates), task delegation, printing, Windows interoperability

Table 2.1: Red Hat Enterprise 6 Features

Red Hat Enterprise Linux 6 improves Windows Server 2008 R2 interoperability with Samba updates including support for trust relationships, Windows cross-forest, transitive and one-way domain trusts.

2.2 Samba

CIFS (Common Internet File System) is the standard file and print sharing system for Microsoft Windows clients in Windows server environments. CIFS uses the SMB (Server Message Block) protocol to facilitate client to server communications.

Samba is an open-source suite of programs that can be installed on a Red Hat Enterprise Linux 6 server to provide seamless file and print services to Microsoft Windows clients. Like CIFS, Samba uses the SMB protocol for client to server communications.

When combined with the reliability and simplified management capabilities of Red Hat Enterprise Linux 6, Samba is the application of choice for providing file and print sharing to Windows clients. Samba version 3.5 is used in this configuration.

2.3 Windows Server 2008 R2

Windows Server 2008 R2 is Microsoft's enterprise operating system for businesses and provides features for virtualization, power savings, manageability and mobile access.

Windows Server 2008 R2 is available in a number of editions – Foundation, Standard, Enterprise, Datacenter, Web and HPC (High Performance Computing). Windows Server 2008 R2 Enterprise Edition is used for this reference architecture configuration.

2.4 Active Directory Domain Services

Developed by Microsoft and based on Novell's eDirectory, **Active Directory Domain Services** uses customized versions of industry standard network protocols and services including:

- Kerberos authentication
- Domain Name System (DNS)
- Lightweight Directory Access Protocol (LDAP)

Active Directory Domain Services allows Windows system administrators to efficiently manage users, systems, groups, printers, applications and directory objects securely from a centralized location. Directory objects are stored in a hierarchy consisting of nodes, trees, forests and domains.

Prior to Windows Server 2008 R2, Active Directory Domain Services was known as Active Directory. Active Directory Domain Services is included with Windows Server 2008 R2.

2.5 Kerberos

Developed at the Massachusetts Institute of Technology (MIT), **Kerberos** is a network authentication protocol that uses strong cryptography to provide highly secure authentication between client and server applications. Kerberos comes in two versions: Kerberos 4 and Kerberos 5. Kerberos version 4 is no longer supported by MIT and has been deprecated by Kerberos version 5. The configuration described within this paper is based on Kerberos version 5.

Kerberos operates on the basis of “tickets” that are granted by a trusted third-party called a key distribution center (KDC). The KDC maintains a secure database of secret keys that are known only to the KDC itself and the client requesting a ticket. Tickets have a configurable expiration date and must be refreshed by the client on a regular basis.

2.6 Winbind

winbind is a component of the Samba suite of programs that allows for unified user logins. *winbind* uses an implementation of Microsoft RPC (Remote Procedure Calls), PAM (Pluggable Authentication Modules), and Red Hat Enterprise Linux 6 nsswitch (Name Service Switch) to allow Windows Active Directory Domain Services users to appear and operate as local users on a Red Hat Enterprise Linux machine. *Winbind* minimizes the need for administrators to manage separate user accounts on both the Red Hat Enterprise Linux 6 and Windows Server 2008 R2 environments.

winbind provides three separate functions:

- Authentication of user credentials (via PAM). This makes it possible to log onto a Red Hat Enterprise Linux 6 system using Active Directory user and group accounts.
- Identity Resolution via nsswitch. The nsswitch service allows user and system information to be obtained from different database services such as LDAP or NIS.
- ID Mappings. *winbind* maintains a backend database called `winbind_idmap.tdb` which stores mappings between Red Hat Enterprise Linux 6 user (UID), group (GID), and Windows Server 2008 R2 system (SID) IDs. These mappings are only used for users and groups that do not have a local Red Hat Enterprise Linux 6 UID/GID. It stores the Red Hat Enterprise Linux 6 UID/GID allocated from the idmap uid/gid range that it has mapped to the Windows SID.

If the *winbind* daemon (`winbindd`) is not running, smbd utilizes local user and group information from */etc/passwd* and */etc/group* and no dynamic mappings are used.

The relationship between Samba and the Active Directory mappings maintained by the Winbind database are represented in **Figure 2.6-1: Winbind backend (idmap_tdb)** :

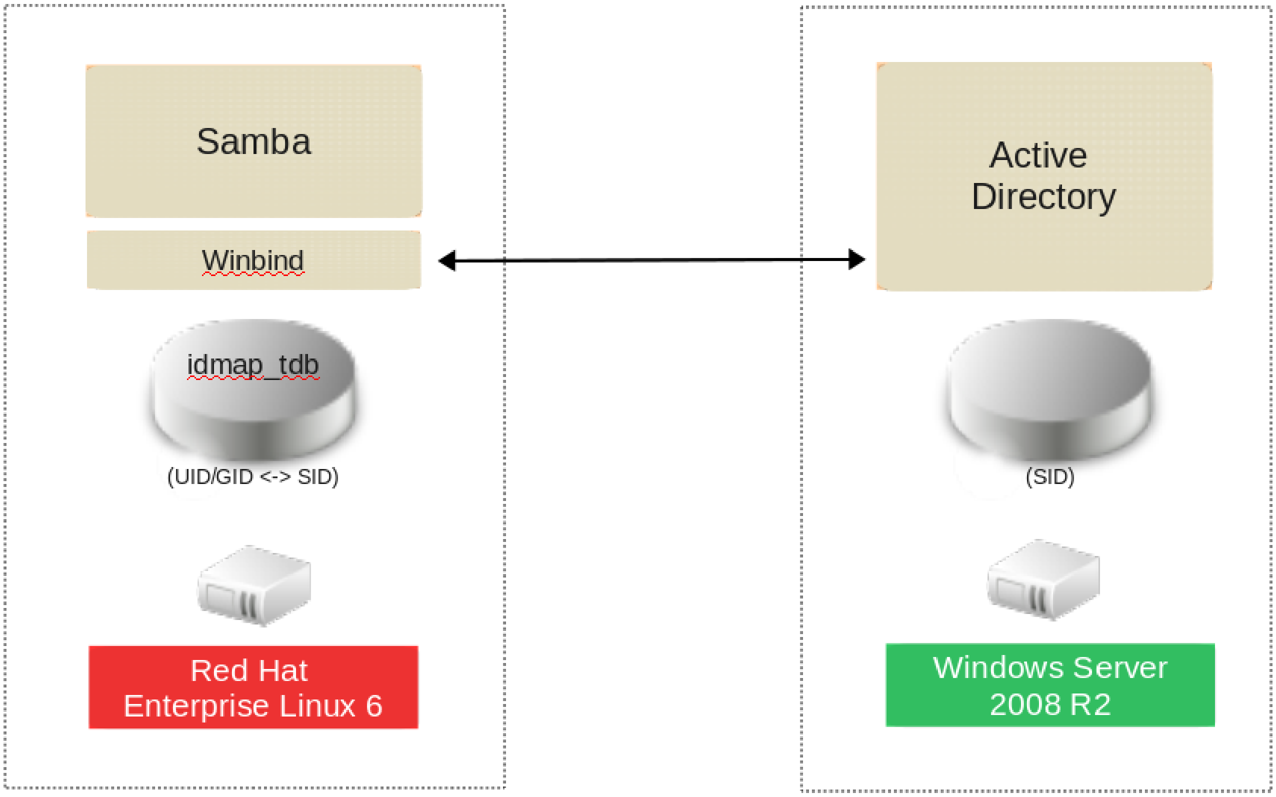


Figure 2.6-1: Winbind backend (idmap_tdb)

The *winbind* backend (idmap_tdb) described within this reference architecture is both the default configuration and the one most commonly implemented by Red Hat customers and partners.

It should be noted that there are a variety of *winbind* backends available for managing account mappings and authorization. The selection made is dependent on factors such as:

- Use of LDAP
- Active Directory schema modification preferences
- Preferred location of mappings
- Number of Red Hat Enterprise Linux 6 servers
- Number of nodes in the Windows Active Directory forest

Each of these criteria will influence the selection of which *winbind* backend to implement. Active Directory environments using LDAP might implement the LDAP (idmap_ldap) backend. Environments without LDAP might prefer to use the Active Directory (idmap_ad) backend. The advantages and disadvantages of each backend are beyond the scope of this document but are described within the corresponding Red Hat Enterprise Linux 6 on-line manual pages and documentation.

2.7 Systems Overview

Figure 2.7-1 provides an overview of the systems, applications and services as configured within this reference architecture. The deployment and integration sections of this paper provide further detail on each of these components.

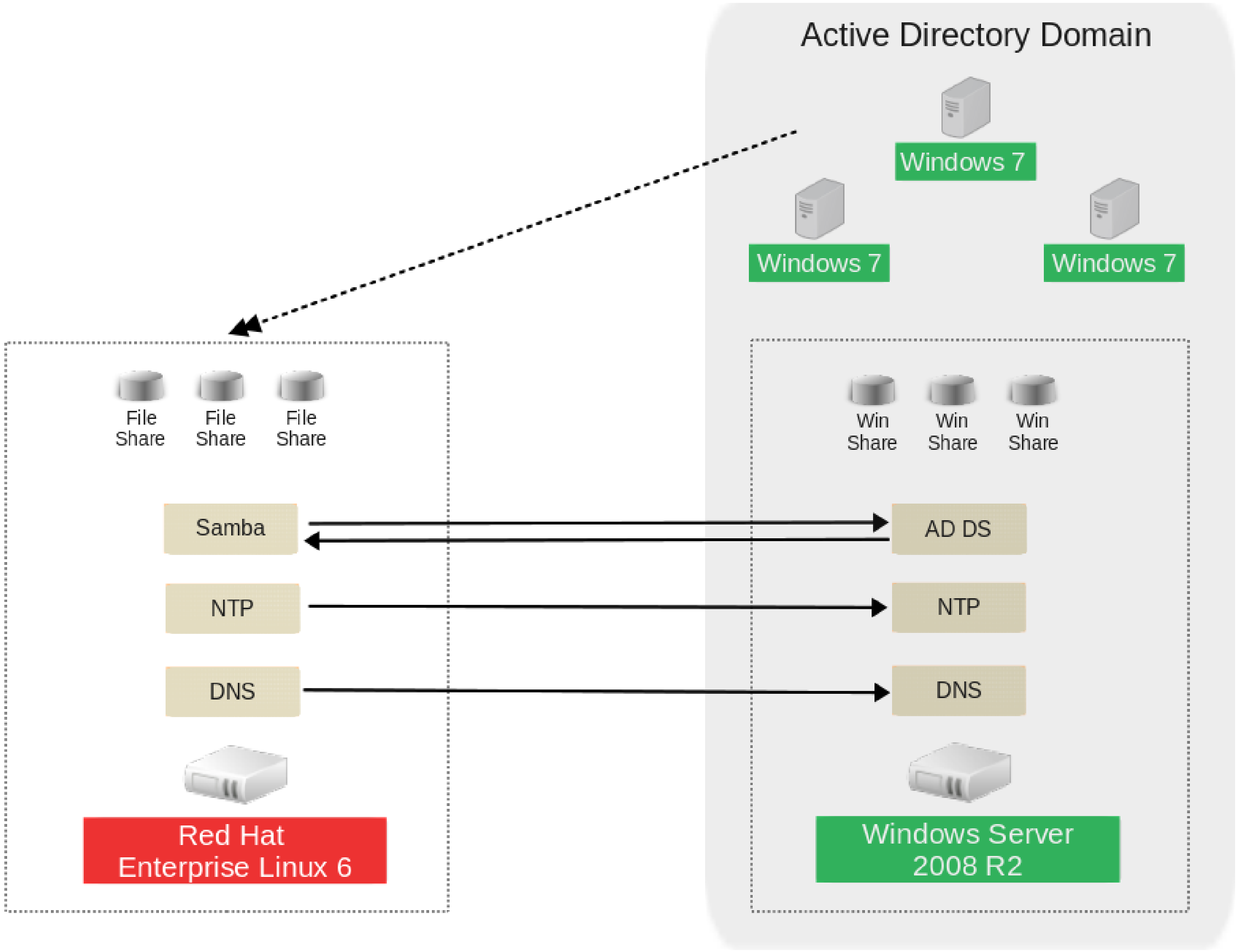


Figure 2.7-1

During integration, the time service (NTP) is synchronized to the Windows AD server to avoid Kerberos authentication failures due to clock skew. Domain Name System (DNS) lookups are also configured to resolve from the Windows AD server. No changes are made to the Windows clients.

3 System Configurations

3.1 Red Hat Enterprise Linux 6 Server

Component	Detail
Hostname	RHEL6-srv
Operating System	Red Hat Enterprise Linux 6 (64-bit) (2.6.32-71.14.1 kernel)
Samba	3.5 (3.5.4-68.el6_0.2)
Kerberos	5
System Type	HP ProLiant DL580 G5
Processor	Quad Socket, Quad Core (16 cores) Intel® Xeon® CPU X5550 @2.93GHz
Memory	64 GB
Storage	4 x 146 GB SATA internal disk drive (RAID 1)
Network	2 x Broadcom BCM5708C NetXtreme II GigE

Table 3.1: Red Hat Enterprise Linux 6 Configuration

3.2 Windows 2008 Server R2

Component	Detail
Hostname	Win2008-srv
Operating System	Windows 2008 Server R2 – Enterprise Edition (64-bit) Version 6.1 (Build 7601: Service Pack 1)
Active Directory Domain Services	Schema Version 47
System Type	HP ProLiant DL580 G5
Processor	Quad Socket, Quad Core (16 cores) Intel® Xeon® CPU W5550 @2.93GHz
Memory	64 GB
Storage	4 x 146 GB SATA internal disk drive (RAID 1)
Network	2 x Broadcom BCM5708C NetXtreme II GigE 1 x HP NC110T PCIe Gigabit Server Adapter

Table 3.2: Windows 2008 Server R2 Configuration

3.3 Windows Client

Component	Detail
Hostname	Win7-up
Operating System	Windows 7 – Ultimate Edition (64-bit) Version 6.1 (Build 7601: Service Pack 1)
System Type	HP ProLiant DL370 G6
Processor	Dual Socket, Quad Core (8 cores) Intel® Xeon® CPU W5580 @3.20GHz
Memory	48 GB
Storage	6 x 146 GB SATA internal disk drive (500GB, RAID 50)
Network	1 x Intel Pro/1000 PT

Table 3.3: Windows Client Configuration

4 Installing Red Hat Enterprise Linux 6

The Red Hat Enterprise Linux 6 Installation Guide provides complete details on the installation of Red Hat Enterprise Linux 6 for Intel, AMD, and IBM architectures.

A Red Hat Enterprise Linux 6 installation involves the following series of stages:

1. Install Red Hat Enterprise Linux 6
2. FirstBoot
3. Apply updates

After the operating system has been installed the system reboots and enters what is referred to as FirstBoot. During FirstBoot, administrators are guided through the process of setting date and time, configuring software updates, initial user account creation and options for Kernel (Kdump) dumps. The system then reboots to activate the changes. After login has been completed under the newly created user account, updates to the system are applied to bring the Red Hat Enterprise Linux 6 server to the latest versions of all software.

The Red Hat Enterprise Linux 6 Installation Guide provides complete instructions on each of these stages. Please consult the guide for further installation details.

5 Deploying Samba

The following sections describe how to install, configure and verify a Samba file share on a Red Hat Enterprise Linux 6 standalone server. A basic Samba file share called *samba-demo* is created and the firewall configured to allow secure Samba client connections to the file share. Access to the *samba-demo* file share is verified from both Red Hat Enterprise Linux 6 and a Windows 7 client.

Deploying Samba on Red Hat Enterprise Linux 6 involves the following series of steps.

1. Samba Installation
2. Samba Configuration
3. Configure SELinux Security Parameters
4. Configure Red Hat Enterprise Linux 6 Firewall
5. Samba Verification

During the integration stage a separate file share (*ad-demo*) will be created for the actual Active Directory integration process. The file share created during the Samba Deployment stage (*samba-demo*) is for the purpose of verifying Samba file sharing functionality.

The next sections provide a step-by-step guide to the Samba deployment process.

5.1 Install Samba

Verify whether or not Samba is installed:

```
# yum list installed | grep samba
samba.x86_64                      3.5.4-68.el6_0.2         @rhel-x86_64-
server-6
samba-client.x86_64               3.5.4-68.el6_0.2         @rhel-x86_64-
server-6
samba-common.x86_64               3.5.4-68.el6_0.2         @rhel-x86_64-
server-6
samba-winbind.x86_64              3.5.4-68.el6_0.2         @rhel-x86_64-
server-6
samba-winbind-clients.x86_64      3.5.4-68.el6_0.2         @rhel-x86_64-
server-6
#
```

If Samba or any of the Samba packages are not installed, use *yum* to install them:

```
# yum -y install samba samba-client samba-common samba-winbind \
samba-winbind-clients
Loaded plugins: refresh-packagekit, rhnplugin
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package samba.x86_64 0:3.5.4-68.el6_0.2 set to be updated
---> Package samba-client.x86_64 0:3.5.4-68.el6_0.2 set to be updated
---> Package samba-common.x86_64 0:3.5.4-68.el6_0.2 set to be updated
---> Package samba-winbind.x86_64 0:3.5.4-68.el6_0.2 set to be updated
---> Package samba-winbind-clients.x86_64 0:3.5.4-68.el6_0.2 set to be
updated
--> Finished Dependency Resolution

                        ...output abbreviated...

Running Transaction
  Installing     : samba-winbind-clients-3.5.4-68.el6_0.2.x86_64   1/5
  Installing     : samba-common-3.5.4-68.el6_0.2.x86_64            2/5
  Installing     : samba-client-3.5.4-68.el6_0.2.x86_64            3/5
  Installing     : samba-3.5.4-68.el6_0.2.x86_64                   4/5
  Installing     : samba-winbind-3.5.4-68.el6_0.2.x86_64           5/5

Installed:
  samba.x86_64 0:3.5.4-68.el6_0.2
  samba-client.x86_64 0:3.5.4-68.el6_0.2
  samba-common.x86_64 0:3.5.4-68.el6_0.2
  samba-winbind.x86_64 0:3.5.4-68.el6_0.2
  samba-winbind-clients.x86_64 0:3.5.4-68.el6_0.2
#
```

Start and verify Samba services are running for use in subsequent steps:

```
# service smb start
Starting SMB services:                                     [  OK  ]
# service smb status
smbd (pid  2733) is running...
# ps -aef | grep smb
root      2733     1  0 12:31 ?        00:00:00 smbd -D
root      2735  2733  0 12:31 ?        00:00:00 smbd -D
root      2747  1733  0 12:31 pts/0    00:00:00 grep smb
#
```

A base installation of Samba with no file shares configured runs two instances of the Samba (*smbd)* daemon. The smbd daemon handles all connection requests and spawns a new process for each client connection made. It not unusual for many processes to be seen if there are many clients mapping shares.

5.2 Configure Samba

Make a safety copy of original configuration file:

```
# cp -p /etc/samba/smb.conf /etc/samba/smb.conf.orig
# ls -la /etc/samba/smb.*
-rw-r--r--. 1 root root 9778 Feb 18 12:43 smb.conf
-rw-r--r--. 1 root root 9778 Feb 18 12:43 smb.conf.orig
#
```

Using the editor of your choice, define a file share called *samba-demo* with access limited to the user *samba-user* by making the following changes to the configuration file.

In the [global] section set the workgroup parameter:

```
workgroup = RA-DEMO
```

add the following to the end of the file then save it:

```
[samba-demo]
       comment = RHEL6-Windows Demo Share
       path=/samba-demo
       writeable = yes
       browseable = yes
       valid users = samba-user
```

Next, create a Samba group, user and home directory for the *samba-demo* file share:

```
# groupadd -g 1234 samba-users
# adduser -d /samba-demo -m -u 1234 -g 1234 -c "Samba demo user accnt" \
samba-user
# ls -ld /samba-demo
drwx------.  4 samba-user samba-users 4096 Apr  5 12:49 /samba-demo
#
```

The option flag (-m) creates the *samba-user* home directory (*/samba-demo*) if it does not already exist. The user ID (-u) and group ID (-g) option flag values specified here are set for demonstration purposes only and can be adjusted as needed.

Populate the demo share area with a test file (used in later steps) to verify the share:

```
# echo “This file was placed in the /samba-demo file share area on the
RHEL6 server” > /samba-demo/This_is_the_RHEL6_server

# chown samba-user:samba-users /samba-demo/This_is_the_RHEL6_server
# ls -l /samba-demo
total 8
-rw-r--r--.  1 samba-user samba-users   79 Apr  5 12:52
This_is_the_RHEL6_server
#
```

Add the newly created user (*samba-user*) to the Samba password file:

```
# smbpasswd -a samba-user
New SMB password:
Retype new SMB password:
Added user demo.
#
```

Test the new configuration file using the Samba `testparm` utility.

```
# testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[samba-demo]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions

[global]
        workgroup = RA-DEMO
        server string = Samba Server Version %v
        log file = /var/log/samba/log.%m
        max log size = 50
        cups options = raw
[homes]
        comment = Home Directories
        read only = No
        browseable = No

[printers]
        comment = All Printers
        path = /var/spool/samba
        printable = Yes
        browseable = No

[samba-demo]
        comment = RHEL6-Windows Demo Share
        path = /samba-demo
        valid users = samba-user
        read only = No
#
```

Re-start Samba to activate the new Samba configuration:

```
# service smb restart
Shutting down SMB services:                                [  OK  ]
Starting SMB services:                                     [  OK  ]
# service smb status
smbd (pid  2902) is running...
#
```

Configure the Samba daemon to start on server boot:

```
# chkconfig smb on
# chkconfig --list smb
smb             0:off   1:off   2:on    3:on    4:on    5:on    6:off
#
```

5.3 Configure SELinux Security Parameters

By default, SELinux is enabled during the Red Hat Enterprise Linux 6 installation process. For maximum security, Red Hat recommends running Red Hat Enterprise Linux 6 with SELinux enabled. In this section, verification is done to ensure that SELinux is enabled and the file context set correctly.

Verify whether or not SELinux is enabled using the `getenforce` utlity:

```
# getenforce
Enforcing
#
```

If getenforce returns “Permissive” then set to “Enforcing” and verify:

```
# getenforce
Permissive
# setenforce 1
# getenforce
Enforcing
#
```

Edit the file */etc/selinux/config* and set SELinux to be persistent across reboots:

```
SELINUX=enforcing
```

Add (-a) the file context (fcontext) for type (-t) Samba share to the directory */samba-demo* and all contents within it. This will make the changes permanent:

```
# semanage fcontext -a -t samba_share_t "/samba-demo(/.*)?"
#
```

Note: If the `semanage` (*/usr/sbin/semanage*) utility is not available, install the core policy utilities kit:

```
# yum -y install policycoreutils-python
Loaded plugins: refresh-packagekit, rhnplugin
Setting up Install Process
Resolving Dependencies

                        ...output abbreviated...

Installed:
  policycoreutils-python.x86_64 0:2.0.83-19.8.el6_0
```

```
Dependency Installed:
  audit-libs-python.x86_64 0:2.0.4-1.el6          libsemanage-
python.x86_64 0:2.0.43-4.el6
  setools-libs.x86_64 0:3.3.7-4.el6               setools-libs-
python.x86_64 0:3.3.7-4.el6

Complete!
# semanage fcontext -a -t samba_share_t "/samba-demo(/.*)?"
#
```

View the current security policy file context:

```
# ls -ldZ /samba-demo
drwx------. samba-user samba-users system_u:object_r:etc_runtime_t:s0
/samba-demo
#
```

Run the `restorecon` command to apply the changes and view updated the file context:

```
# restorecon -R -v /samba-demo
restorecon reset /samba-demo context system_u:object_r:etc_runtime_t:s0-
>system_u:object_r:samba_share_t:s0 /samba-demo

# ls -ldZ /samba-demo
drwx------. samba-user samba-users system_u:object_r:samba_share_t:s0
/samba-demo
#
```

5.4 Configure Red Hat Enterprise Linux 6 Firewall

Red Hat Enterprise Linux 6 firewall settings can be configured with the iptables command line utility or from the *Firewall Configuration* graphical tool. The example screen shots that follow use the 'Firewall Configuration' tool. This tool supports both graphical and text (terminal) modes.

Run the *Firewall Configuration* tool by selecting *System -> Administration -> Firewall* from the desktop or from the command line:

```
# system-config-firewall
```

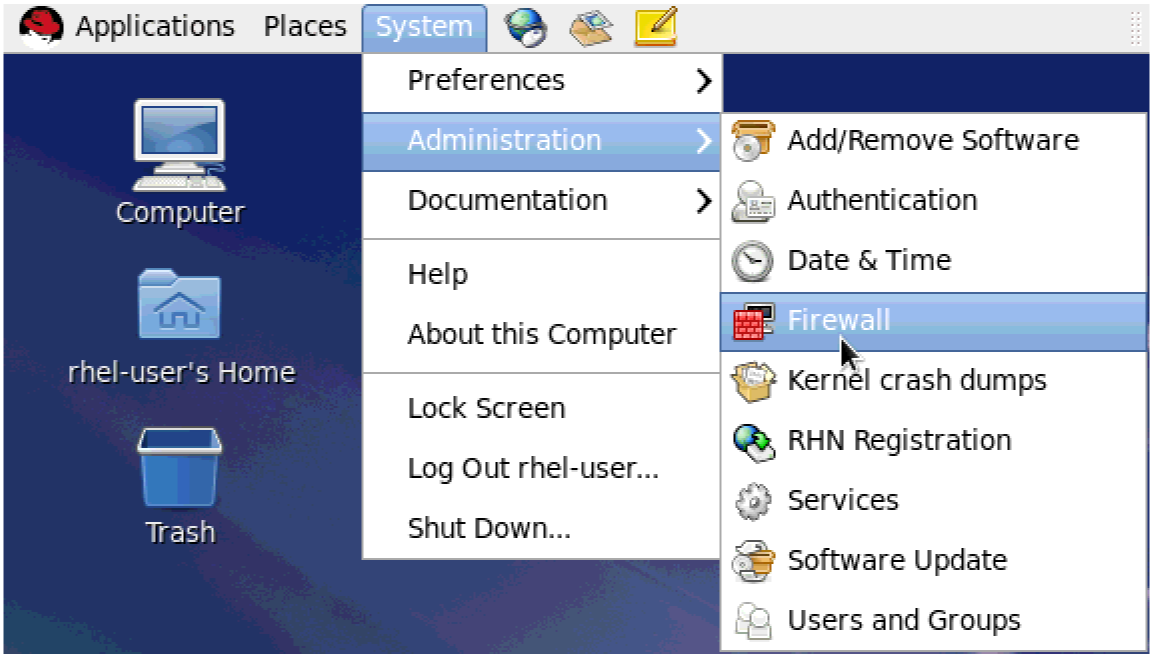
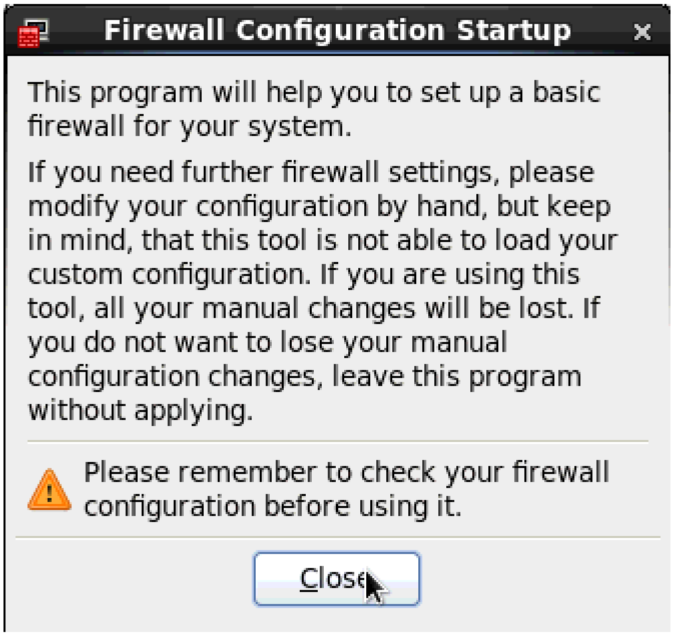


Figure 5.4-1

The tool notifies you that any prior manual changes that have been made but not saved may be lost. Select “Close” to continue:



Firewall Configuration Startup

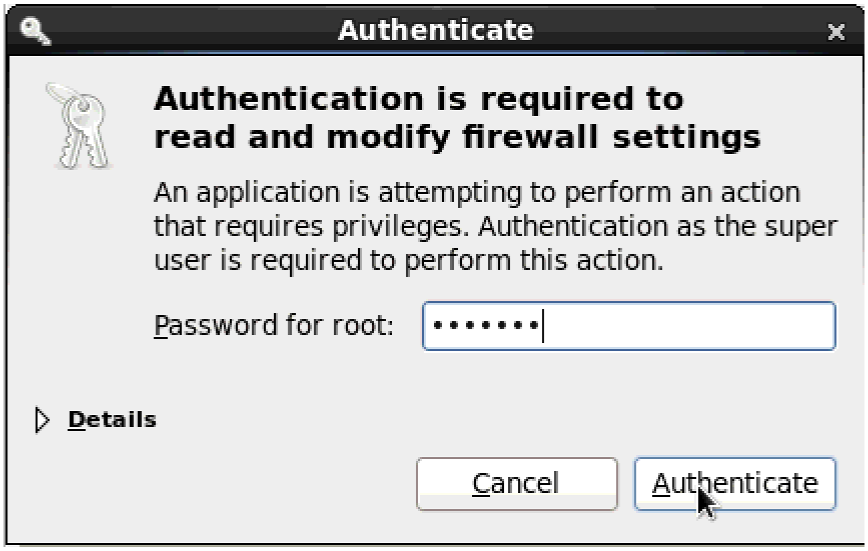
This program will help you to set up a basic firewall for your system.

If you need further firewall settings, please modify your configuration by hand, but keep in mind, that this tool is not able to load your custom configuration. If you are using this tool, all your manual changes will be lost. If you do not want to lose your manual configuration changes, leave this program without applying.

Please remember to check your firewall configuration before using it.

Figure 5.4-2

The *Firewall Configuration* tool requires root access. Enter the password for root then select “Authenticate” to continue:



Authenticate

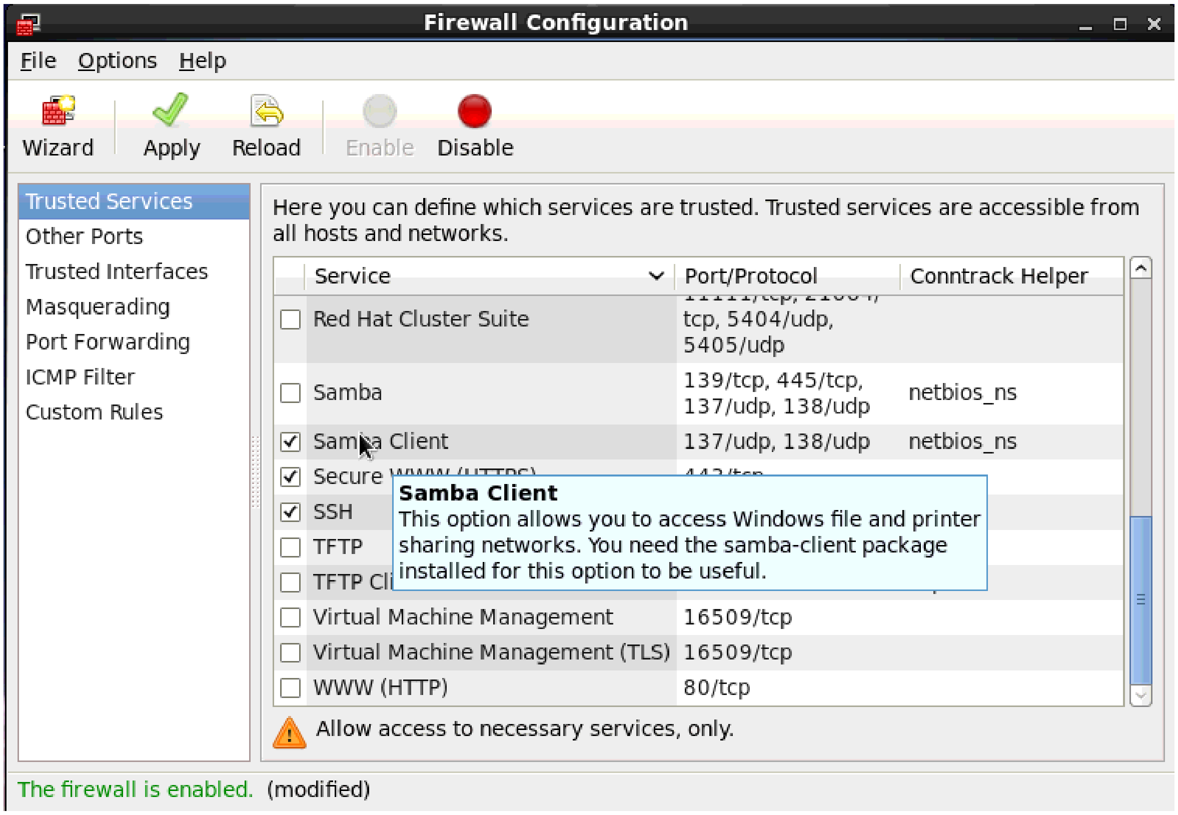
Authentication is required to read and modify firewall settings

An application is attempting to perform an action that requires privileges. Authentication as the super user is required to perform this action.

Password for root: •••••••

Figure 5.4-3

Scroll down through the list of *Trusted Services*, select both 'Samba' and 'Samba-client':



Here you can define which services are trusted. Trusted services are accessible from all hosts and networks.

	Service	Port/Protocol	Conntrack Helper
□	Red Hat Cluster Suite	tcp, 5404/udp, 5405/udp	
□	Samba	139/tcp, 445/tcp, 137/udp, 138/udp	netbios_ns
☑	Samba Client	137/udp, 138/udp	netbios_ns
☑	Secure		
☑	SSH		
□	TFTP		
□	TFTP Cl		
□	Virtual Machine Management	16509/tcp	
□	Virtual Machine Management (TLS)	16509/tcp	
□	WWW (HTTP)	80/tcp	

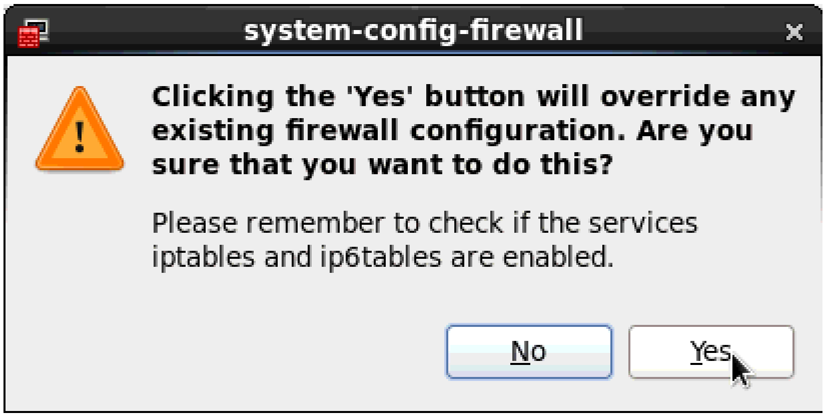
Samba Client
This option allows you to access Windows file and printer sharing networks. You need the samba-client package installed for this option to be useful.

Allow access to necessary services, only.

The firewall is enabled. (modified)

Figure 5.4-4

Select “Apply” to activate the changes then “Yes” to update the firewall configuration. At this point the firewall configuration has been updated to allow Samba connections. Select “File” then “Quit” to leave the firewall configuration tool.



Clicking the 'Yes' button will override any existing firewall configuration. Are you sure that you want to do this?

Please remember to check if the services iptables and ip6tables are enabled.

5.5 Verify Samba

List the shares available from the Red Hat Enterprise Linux 6 Samba server:

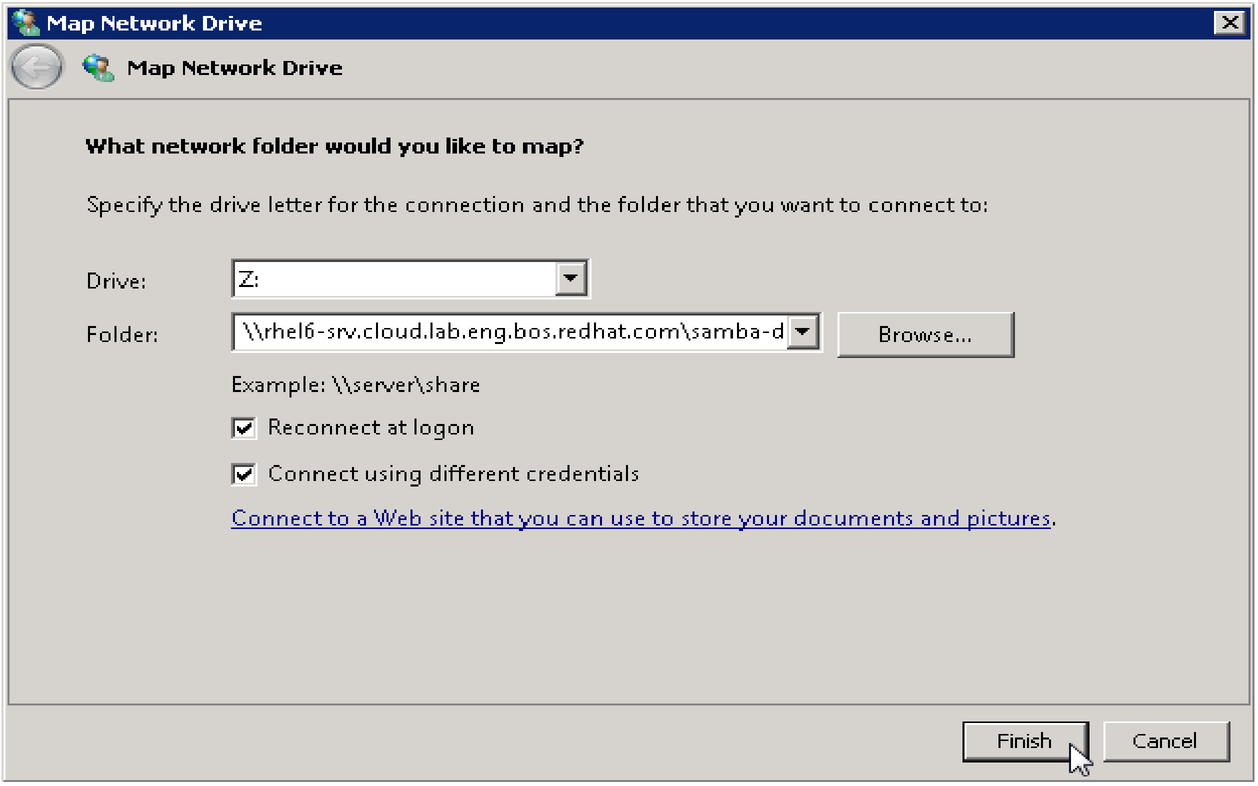
```
$ smbclient -L RHEL6-srv -U samba-user
Enter samba-user's password: 
Domain=[RA-DEMO] OS=[Unix] Server=[Samba 3.5.4-68.el6_0.2]

             Sharename       Type      Comment
             ---------       ----      -------
             samba-demo      Disk      RHEL6-Windows Demo Share
             IPC$            IPC       IPC Service (Samba Server Version 
3.5.4-68.el6_0.2)
             samba-user      Disk      Home Directories
Domain=[RA-DEMO] OS=[Unix] Server=[Samba 3.5.4-68.el6_0.2]

             Server               Comment
             ---------            -------

             Workgroup            Master
             ---------            -------
$
```

Connect to the share from a Linux client:

```
$ smbclient //RHEL6-srv/samba-demo -U samba-user
Enter samba-user's password: 
Domain=[RA-DEMO] OS=[Unix] Server=[Samba 3.5.4-68.el6_0.2]
smb: \> ls
  .                             D        0  Tue Apr  5 12:52:12 2011
  ..                           DR        0  Tue Apr  5 12:49:12 2011
  This_is_the_RHEL6_server              79  Tue Apr  5 12:52:39 2011
  .bash_profile                 H      176  Tue Jun 22 11:49:51 2010
  .gnome2                      DH        0  Wed Jul 14 11:55:40 2010
  .bash_logout                  H       18  Tue Jun 22 11:49:51 2010
  .mozilla                     DH        0  Mon Apr  4 19:10:31 2011
  .bashrc                       H      124  Tue Jun 22 11:49:51 2010

                50396 blocks of size 1048576. 44533 blocks available
smb: \> q
$
```

Connect to the share from a Windows Client (*Method 1 - Windows Explorer*)

Open the “Map Network Drive” tool by selecting Start, right-click on Computer and select Map network drive:



Map Network Drive

Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\rhel6-srv.cloud.lab.eng.bos.redhat.com\samba-d

Example: \\server\share

☑ Reconnect at logon

☑ Connect using different credentials

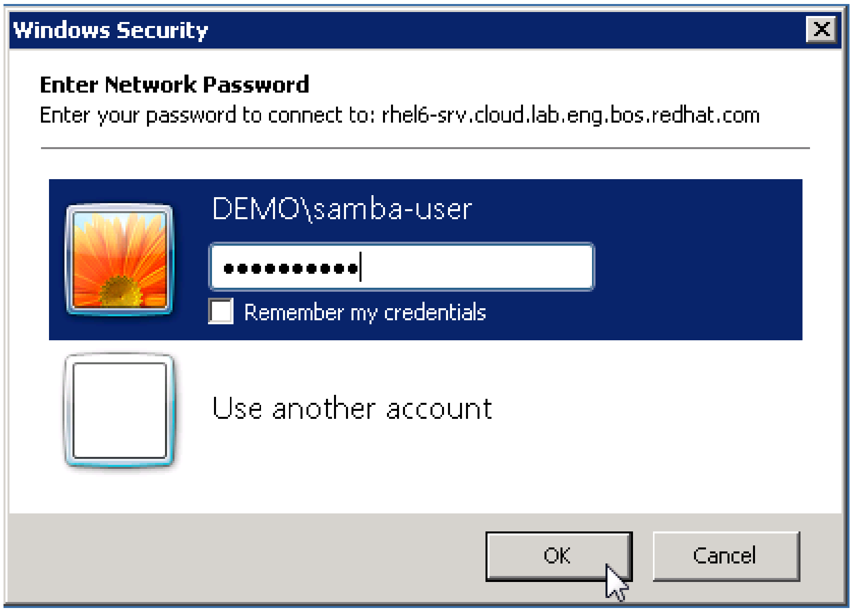
Connect to a Web site that you can use to store your documents and pictures.

Figure 5.5-1

Specify a drive letter and the full path to the file share. Be sure to check the option “Connect using different credentials”. In most cases the option “Reconnect at logon” would also be selected.

Note: If there is no response, check to make sure the SMB service is running on the Red Hat Enterprise Linux 6 server with `service smb status` or `smbstatus`. If necessary restart it with `service smb restart`. If drive mapping continues to fail then see **Section 5.3 Configure SELinux Security Parameters** and **Section 5.4 Configure Red Hat Enterprise Linux 6 Firewall** to verify the security policies and firewall have been correctly configured.

Specify the account 'samba-user' and password. The option 'Remember my credentials' may be specified. Select “OK” to continue:



Windows Security

Enter Network Password

Enter your password to connect to: rhel6-srv.cloud.lab.eng.bos.redhat.com

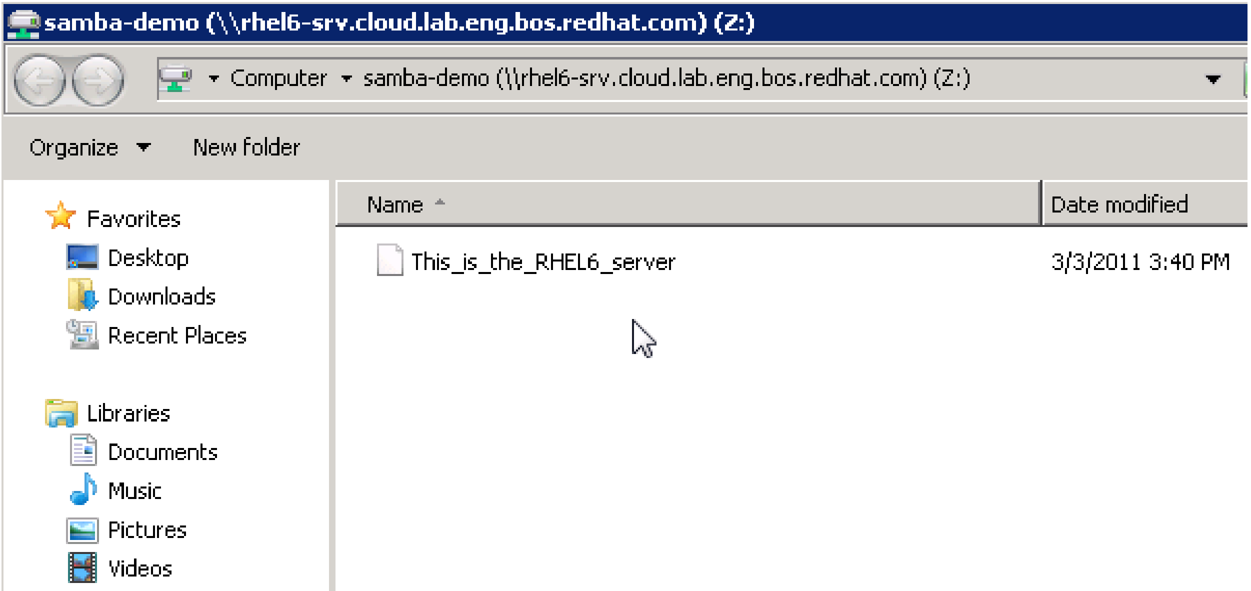
DEMO\samba-user

●●●●●●●●●●●

☐ Remember my credentials

Figure 5.5-2

Windows explorer opens and displays the contents of the share:



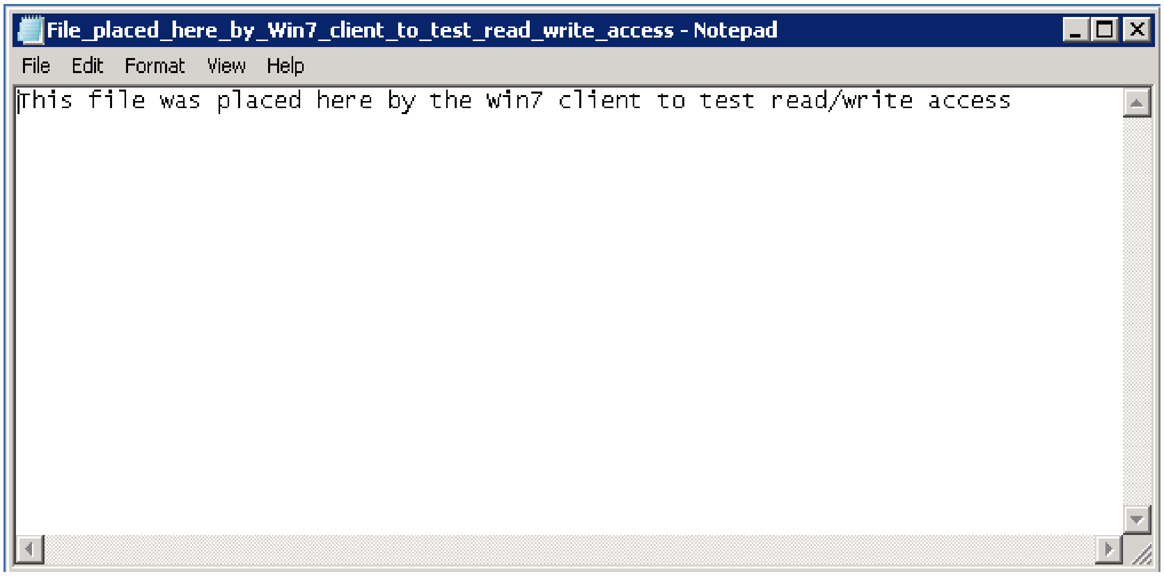
samba-demo (\\rhel6-srv.cloud.lab.eng.bos.redhat.com) (Z:)

Computer ▸ samba-demo (\\rhel6-srv.cloud.lab.eng.bos.redhat.com) (Z:)

Name	Date modified
This_is_the_RHEL6_server	3/3/2011 3:40 PM

Figure 5.5-3

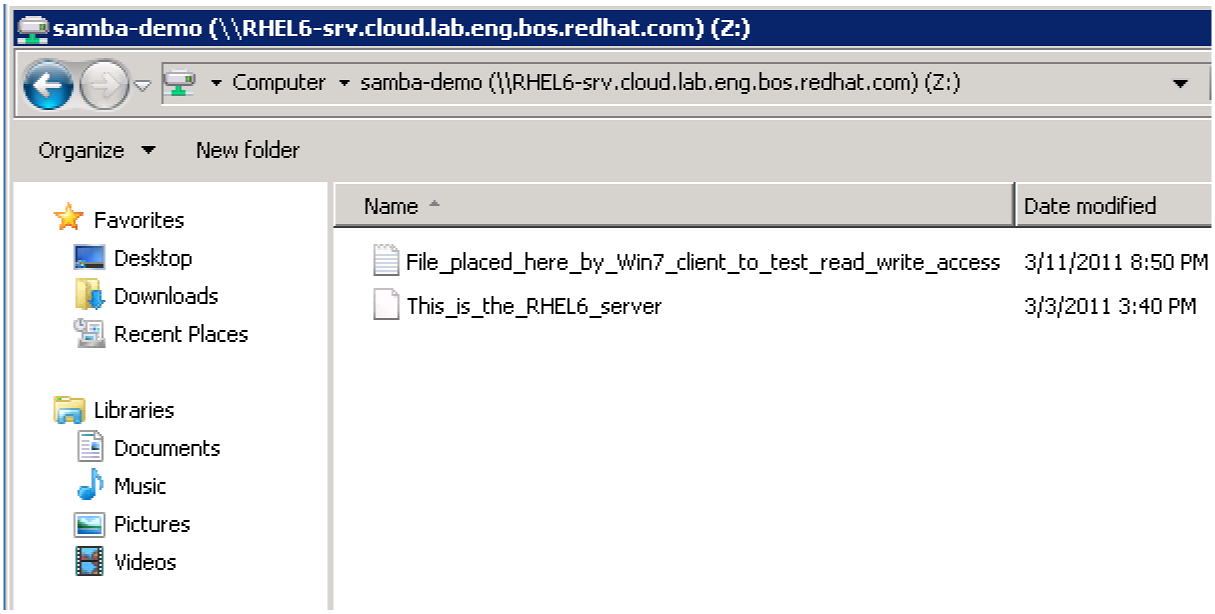
Verify the share can be written to by creating a text file (using Notepad or WordPad):


File_placed_here_by_Win7_client_to_test_read_write_access - Notepad
File
Edit
Format
View
Help

```
This file was placed here by the Win7 client to test read/write access
```

Figure 5.5-4

Then save it on the share:


samba-demo (\\RHEL6-srv.cloud.lab.eng.bos.redhat.com) (Z:)
Computer
samba-demo (\\RHEL6-srv.cloud.lab.eng.bos.redhat.com) (Z:)
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos

Name	Date modified
File_placed_here_by_Win7_client_to_test_read_write_access	3/11/2011 8:50 PM
This_is_the_RHEL6_server	3/3/2011 3:40 PM

Figure 5.5-5

Disconnect from the drive by selecting Start, right-click on Computer and select 'Disconnect network drive'. At this point the installation and configuration of Samba is complete. Proceed to **Section 6 Integrating Active Directory** to begin the process of integrating Red Hat Enterprise Linux 6 with Samba into Active Directory Domain Services.

Connect to the share from a Windows Client (*Method 2 – Command Prompt*)

Open a Command Prompt: *Start-> All Programs -> Accessories -> Command Prompt:*

```
C:\Users\win7-user> net use Z: \\RHEL6-srv.cloud.lab.eng.bos.redhat.com
\samba-demo /user:samba-user
Enter the password for 'samba-user' to connect to 'RHEL6-
srv.cloud.lab.eng.bos.redhat.com':
The command completed successfully.


C:\Users\win7-user> dir Z:
 Volume in drive Z is samba-demo
 Volume Serial Number is 5756-0262

 Directory of Z:\

04/05/2011  01:40 PM    <DIR>          .
04/05/2011  12:49 PM    <DIR>          ..
04/05/2011  12:52 PM                72 This_is_the_RHEL6_server
03/11/2011  08:50 PM                70 File_placed_here_by_Win7_client_
to_test_read_write_access.txt
               2 File(s)            149 bytes
               2 Dir(s)  46,696,873,984 bytes free

C:\Users\win7-user>
```

Disconnect from a Windows Client:

```
C:\Users\win7-user> net use Z: /delete
Z: was deleted successfully.
C:\Users\win7-user> dir Z:
The system cannot find the path specified.
C:\Users\win7-user>
```

Active Samba connections can be viewed from the Red Hat Enterprise Linux 6 Samba as follows:

```
# smbstatus

Samba version 3.5.4-68.el6_0.2
PID     Username      Group         Machine
-------------------------------------------------------------------
16205   samba-user    samba-users   win7-up      (::ffff:10.16.143.164)

Service      pid     machine       Connected at
-------------------------------------------------------
samba-demo   16205   win7-up       Fri Mar 11 14:58:11 2011

No locked files

#
```

In the above example the remote client machine (*win7-up*) is connected to the file service (*samba-demo*).

5.6 Common Samba Deployment Issues/Errors

In general, the best place to start troubleshooting Samba issues are the log files located under */var/log/samba*. One log file exists for the Samba server itself (e.g. - *log.rhel6-srv*) and each client (e.g. - *log.win7-up*) that connects to the server. The logs files are useful for troubleshooting everyday administration issues.

Below are some of the most common issues/error conditions that may be encountered while deploying Samba. For other issues, please consult "**How to Install and Test SAMBA"** and "**The Samba Checklist**".

Parameter file check (testparm) error – rlimit_max below minimum Windows limit

Symptom

```
# testparm smb.conf
Load smb config files from smb.conf
rlimit_max: rlimit_max (1024) below minimum Windows limit (16384)

                          ...output abbreviated...

#
```

Explanation

This is a common warning caused by the default value for the maximum number of open files being lower than the default Windows limit. Correct it by adding the entry:

```
* - nofile 16384
```

to the file */etc/security/limits.conf.* The change is activated immediately for all new SMB sessions. Existing sessions do not utilize the change until users logout and login again to the Red Hat Enterprise Linux 6 server.

Large Number of smbd Processes

Symptom

```
# ps -aef | grep smbd
root      8495     1  0 Feb24 ?        00:00:00 smbd -D
root      8497  8495  0 Feb24 ?        00:00:00 smbd -D
root      8552  8495  0 Mar03 ?        00:00:00 smbd -D
root      8581  8495  0 Mar03 ?        00:00:00 smbd -D
root      8627  8495  0 Mar04 ?        00:00:00 smbd -D
root      8639  8495  0 Mar04 ?        00:00:00 smbd -D
root      8644  8495  0 Mar04 ?        00:00:00 smbd -D
root      8878  8495  0 Mar06 ?        00:00:00 smbd -D
 .         .     .    .  .    .          .  .    .    .
 .         .     .    .  .    .          .  .    .    .
 .         .     .    .  .    .          .  .    .    .

                        ...output abbreviated...
 .         .     .    .  .    .          .  .    .    .
 .         .     .    .  .    .          .  .    .    .
 .         .     .    .  .    .          .  .    .    .
root      9181  8495  0 Apr13 ?        00:00:00 smbd -D
root      9272  8495  0 Apr14 ?        00:00:00 smbd -D
root      9639  8495  0 May04 ?        00:00:00 smbd -D
root      9664  8495  0 May04 ?        00:00:00 smbd -D
root      9778  8495  0 May06 ?        00:00:00 smbd -D
#
```

Explanation

This is expected behavior. The `smbd` daemon handles all connection requests and spawns a new process for each client connection made. Alternatively, `smbstatus` may be used to display active connections. No corrective actions are required.

Network Connectivity Issue – Network Unreachable

Windows clients will manifest the issue as a drive mapping failure.

Symptom

```
$ smbclient -L RHEL6-srv -U samba-user
Enter samba-user's password:
Connection to RHEL6-srv failed (Error NT_STATUS_NETWORK_UNREACHABLE)
$
```

Explanation

The client is not able to connect to the Samba server. The server may still be reachable via ping (ICMP) from the client (Windows, Linux):

Windows Client:

```
C:\>ping RHEL6-srv

Pinging RHEL6-srv [10.16.143.162] with 32 bytes of
data:
Reply from 10.16.143.162: bytes=32 time<1ms TTL=64
Reply from 10.16.143.162: bytes=32 time<1ms TTL=64

Ping statistics for 10.16.143.162:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\>
```

Linux Client:

```
$ ping -c3 RHEL6-srv
PING RHEL6-srv (10.16.143.162) 56(84) bytes of data.
64 bytes from RHEL6-srv (10.16.143.162): icmp_seq=1 ttl=64 time=0.051 ms
64 bytes from RHEL6-srv (10.16.143.162): icmp_seq=2 ttl=64 time=0.013 ms
64 bytes from RHEL6-srv (10.16.143.162): icmp_seq=3 ttl=64 time=0.022 ms
^C
--- RHEL6-srv ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2359ms
rtt min/avg/max/mdev = 0.013/0.028/0.051/0.017 ms
$
```

From the Red Hat Enterprise Linux 6 server, try to ping itself:

```
# ping -c3 RHEL6-srv
PING RHEL6-srv (127.0.0.1) 56(84) bytes of data.

--- RHEL6-srv ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 11999ms

#
```

If the ping fails, then make sure the `loopback` (lo) on the Red Hat Enterprise Linux 6 server is up. If not, bring it up then try connecting again:

```
# ip link show lo
1: lo: <LOOPBACK> mtu 16436 qdisc noqueue state DOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

# ip link set up lo
# ip link show lo
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

# ping -c3 RHEL6-srv
PING RHEL6-srv (10.16.143.162) 56(84) bytes of data.
64 bytes from RHEL6-srv (10.16.143.162): icmp_seq=1 ttl=64 time=0.051 ms
64 bytes from RHEL6-srv (10.16.143.162): icmp_seq=2 ttl=64 time=0.013 ms
64 bytes from RHEL6-srv (10.16.143.162): icmp_seq=3 ttl=64 time=0.022 ms

--- RHEL6-srv ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2359ms
rtt min/avg/max/mdev = 0.013/0.028/0.051/0.017 ms

#
```

Network Connectivity Issue – Host Unreachable

Symptom

```
$ smbclient -L RHEL6-srv -U samba-user
Enter samba-users's password:
Connection to RHEL6-srv failed (Error NT_STATUS_HOST_UNREACHABLE)

$
```

Explanation

The client is not able to connect to the Samba server. The server may still be reachable via ping (ICMP):

```
$ ping -c3 RHEL6-srv
PING RHEL6-srv (10.16.143.162) 56(84) bytes of data.
64 bytes from RHEL6-srv (10.16.143.162): icmp_seq=1 ttl=63 time=0.272 ms
64 bytes from RHEL6-srv (10.16.143.162): icmp_seq=2 ttl=63 time=0.189 ms
64 bytes from RHEL6-srv (10.16.143.162): icmp_seq=3 ttl=63 time=0.205 ms
--- RHEL6-srv ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.189/0.222/0.272/0.035 ms

$
```

but Samba (SMB) sessions may be blocked due to network (firewall, router) filtering. Ensure any network devices permit SMB traffic to pass through to ports 445/tcp and 445/udp. Also be sure the firewall on the Red Hat Enterprise Linux 6 server is allowing traffic on these ports as well. When troubleshooting potential firewall issues be aware of the following session characteristics:

1. Windows clients running NetBIOS over TCP/IP try to connect to the SMB server at both port 139 and port 445 simultaneously. If the server responds on port 445, it sends a reset to port 139, and the SMB session is established on port 445. If the server does not respond on port 445, the client SMB session is established on port 139. If there is no response from either of the ports, the session terminates.
2. Clients not running NetBIOS over TCP/IP try to connect to the SMB server at port 445 only. If the server responds on port 445, the session is established. If not, the SMB session terminates.
3. Servers running NetBIOS over TCP/IP listen on UDP ports 137, 138, and on TCP ports 139, 445. If NetBIOS over TCP/IP is not running, the server listens on TCP port 445 only.

Network Logon Failure

Symptom

```
# smbclient -L RHEL6-srv
Enter root's password:
session setup failed: NT_STATUS_LOGON_FAILURE
#
```

Explanation

The client is not able to logon to the Samba server due to an incorrect password or logon account being specified. Verify the account and password are correct:

```
# smbclient -L RHEL6-srv -U samba-user
Enter samba-user's password:
Domain=[RA-DEMO] OS=[Unix] Server=[Samba 3.5.4-68.el6_0.1]

Sharename   Type    Comment
----------  -----   -------------
samba-demo  Disk    RHEL6-Windows Demo Share
IPC$        IPC     IPC Service (Samba Server Version 3.5.4-68.el6_0.1)
samba-user  Disk    Home Directories

Domain=[RA-DEMO] OS=[Unix] Server=[Samba 3.5.4-68.el6_0.1]

Server           Comment
---------        ---------

Workgroup        Master
---------        ---------
#
```

Network Access Denied

Symptom

```
$ smbclient //rhel6-srv/samba-demo -U samba-user
Enter samba-user's password:
Domain=[RA-DEMO] OS=[Unix] Server=[Samba 3.5.4-68.el6_0.2]
tree connect failed: NT_STATUS_ACCESS_DENIED
$
```

Explanation

The client is not able to logon to the Samba server due to an invalid user being specified in the */etc/samba/smb.conf* file:

Before:

```
[samba-demo]
                comment = RHEL6-Windows Demo Share
                path=/samba-demo
                writeable = yes
                browseable = yes
                valid users = samba-users     # This is a problem !!!
```

After:

```
[samba-demo]
                comment = RHEL6-Windows Demo Share
                path=/samba-demo
                writeable = yes
                browseable = yes
                valid users = samba-user      # This is correct !!!
```

After correcting the error and restarting Samba, connect to the share to verify access. In this example the Samba `smbclient` utlity is used to login to the account and display the share contents:

```
# service smb restart
Shutting down SMB services:                            [  OK  ]
Starting SMB services:                                 [  OK  ]
# smbclient //rhel6-srv/samba-demo -U samba-user
Enter samba-user's password:
Domain=[RA-DEMO] OS=[Unix] Server=[Samba 3.5.4-68.el6_0.2]
smb: \> ls
.                                   D        0  Fri Mar 11 15:02:31 2011
..                                 DR        0  Wed Mar 16 16:01:13 2011
.bash_history                       H      275  Wed Mar 16 16:13:21 2011
.gnome2                            DH        0  Wed Jul 14 11:55:40 2010
This_is_the_RHEL6_server                    72  Thu Mar  3 15:40:43 2011
.mozilla                           DH        0  Wed Feb 16 13:59:00 2011
```

```
.bash_profile                     H      176  Tue Jun 22 11:49:51 2010
.bashrc                           H      124  Tue Jun 22 11:49:51 2010
File_placed_here_by_Win7_client_to_test_read_write_access.txt
                                  A       70  Fri Mar 11 20:50:41 2011
.bash_logout                      H       18  Tue Jun 22 11:49:51 2010

                                50396 blocks of size 1048576. 44479
blocks available
smb: \> q
#
```

6 Integrating Active Directory

In this section, the process of integrating Samba file services with an Active Directory domain is performed. At this point the following components should be fully configured:

- Windows Server 2008 R2 with Active Directory Domain Services
- Windows client with access to both the Red Hat Enterprise Linux 6 (Samba) and Windows Server 2008 R2 file shares
- Red Hat Enterprise Linux 6 Server with Samba file services

Do not proceed with the integration tasks until the prior components have been fully configured, tested and verified. As a convenience, the following guides are provided to assist with Windows Server and Active Directory installation and configuration:

- **Appendix C: Windows Server 2008 R2 – Installation Summary**
- **Appendix D: Active Directory Domain Services – Configuration Summary**

Integrating Red Hat Enterprise Linux 6 with Samba into an Active Directory domain involves the following series of steps.

1. Synchronize Time Servers
2. Configure DNS
3. Install Kerberos (*optional*)
4. Configuration/Test Kerberos (*optional*)
5. Configure Authentication
6. Verify/Test Active Directory
7. Modify Samba Configuration

The following sections provide a step-by-step guide to the Active Directory integration process.

6.1 Synchronize Time Servers

It is essential that the time service on the Red Hat Enterprise Linux 6 Samba server and Active Directory (Windows 2008) server are synchronized, otherwise Kerberos authentication may fail due to clock skew. Best practice is to configure the Red Hat Enterprise Linux 6 server to synchronize time from the Windows Server 2008 R2 server.

Edit the file */etc/ntp.conf* so that the Red Hat Enterprise Linux 6 server time is synchronized from the Windows Active Directory server:

```
# Enable writing of statistics records.
#statistics clockstats cryptostats loopstats peerstats
server 10.16.143.163
```

Activate the change on the Red Hat Enterprise Linux 6 server by stopping the `ntp` daemon, updating the time, then starting the `ntp` daemon. Verify the change on both servers.

Red Hat Enterprise Linux 6 server:

```
# service ntpd stop
Shutting down ntpd:                                        [  OK  ]

# ntpdate 10.16.143.163
 5 Apr 18:03:30 ntpdate[4134]: adjust time server 10.16.143.163 offset
-0.002382 sec
# service ntpd start
Starting ntpd:                                             [  OK  ]
#
```

Windows Server 2008 R2 server:

```
C:\Users\Administrator> w32tm /query /status | find "Source"
Source: ns1.bos.redhat.com

C:\Users\Administrator> w32tm /query /status | find "source"
ReferenceId: 0x0A10FF02 (source IP:  10.16.255.2)
```

The Windows Server 2008 R2 server is synchronizing time from a remote time source (IP address 10.16.255.2). This can be seen from the Red Hat Enterprise Linux 6 server:

```
# ntpq -p
  remote       refid        st t when poll reach delay  offset  jitter
=======================================================================
 Win2008-srv   10.16.255.2  3  u 25   64   1     0.263  1.794   0.000
#
```

Configure the ntpd daemon to start on server boot:

```
# chkconfig ntpd on
# chkconfig --list ntpd
smb             0:off   1:off   2:on   3:on   4:on   5:on   6:off
#
```

6.2 Configure DNS

Best practice is to configure the Red Hat Enterprise Linux 6 server to perform DNS lookups from the Windows Server 2008 R2 Active Directory server. Edit the file */etc/resolv.conf* so that the fully qualified domain name (FQDN) of the Windows Active Directory server is specified:

```
domain cloud.lab.eng.bos.redhat.com
search cloud.lab.eng.bos.redhat.com
nameserver 10.16.143.163
```

Similarly, the hostname of the Red Hat Enterprise Linux 6 server should be set to the FQDN. Edit the file */etc/sysconfig/network* and set the hostname to use the FQDN:

```
HOSTNAME=RHEL6-srv.cloud.lab.eng.bos.redhat.com
```

6.3 Install Kerberos

Best practice is to install and configure the Kerberos client (`krb5-workstation`) to insure Kerberos is able to properly authenticate to Active Directory on the Windows Server 2008 R2 server. This step is optional but highly recommended as it is useful for troubleshooting Kerberos authentication issues.

Verify the Kerberos client is installed:

```
# yum list installed | grep krb5
krb5-libs.x86_64                  1.8.2-3.el6_0.6          @rhel-x86_64-
server-6
krb5-server.x86_64                1.8.2-3.el6_0.6          @rhel-x86_64-
server-6
krb5-workstation.x86_64           1.8.2-3.el6_0.6          @rhel-x86_64-
server-6
pam_krb5.x86_64                   2.3.11-1.el6             @anaconda-
RedHatEnterpriseLinux-201009221801.x86_64/6.0
#
```

If not, install it as follows:

```
# yum -y install krb5-workstation

Loaded plugins: refresh-packagekit, rhnplugin
Setting up Install Process
```

```
Resolving Dependencies
--> Running transaction check
---> Package krb5-workstation.x86_64 0:1.8.2-3.el6_0.6 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

                        ...output abbreviated...

Installed:
  krb5-workstation.x86_64 0:1.8.2-3.el6_0.6

Complete!
#
```

6.4 Configure/Test Kerberos

Modify the Kerberos configuration file (*/etc/krb5.conf*) by adding entries for the new Kerberos and Active Directory realms. Note the differences in the Kerberos `[realm]` and Active Directory `[domain_realm]` realm entries. Alternatively, the kdc server may be specified by IP address. The entries for PAM authentication are added to automate the process of ticket renewals.

Create a safety copy of the Kerberos configuration file:

```
# cp -p /etc/krb5.conf /etc/krb5.conf.orig
```

Edit the file */etc/krb5.conf* as follows – changes are highlighted bold:

```
[logging]
  default = FILE:/var/log/krb5libs.log
  kdc = FILE:/var/log/krb5kdc.log
  admin_server = FILE:/var/log/kadmind.log

[libdefaults]
  default_realm = DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
  dns_lookup_realm = true
  dns_lookup_kdc = true
  ticket_lifetime = 24h
  renew_lifetime = 7d
  forwardable = false

[realms]
  DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM  = {
    kdc = WIN2008-SRV.DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
    admin_server = WIN2008-SRV.DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
 }

[domain_realm]
  .demo = DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
  demo  = DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
```

Under Kerberos, [realms] is set to the Kerberos server definitions and [domain_realm] defines the Active Directory server. Both are in the Active Directory DEMO domain.

Verify the Kerberos configuration. First, clear out any existing tickets:

```
# kdestroy
# klist
klist: No credentials cache found (ticket cache FILE:/tmp/krb5cc_0)
# kinit
kinit: Client not found in Kerberos database while getting initial
credentials
#
```

Obtain a new Kerberos ticket:

```
# kinit administrator@DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
Password for administrator@DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM:
#
```

Verify a new Kerberos ticket was granted:

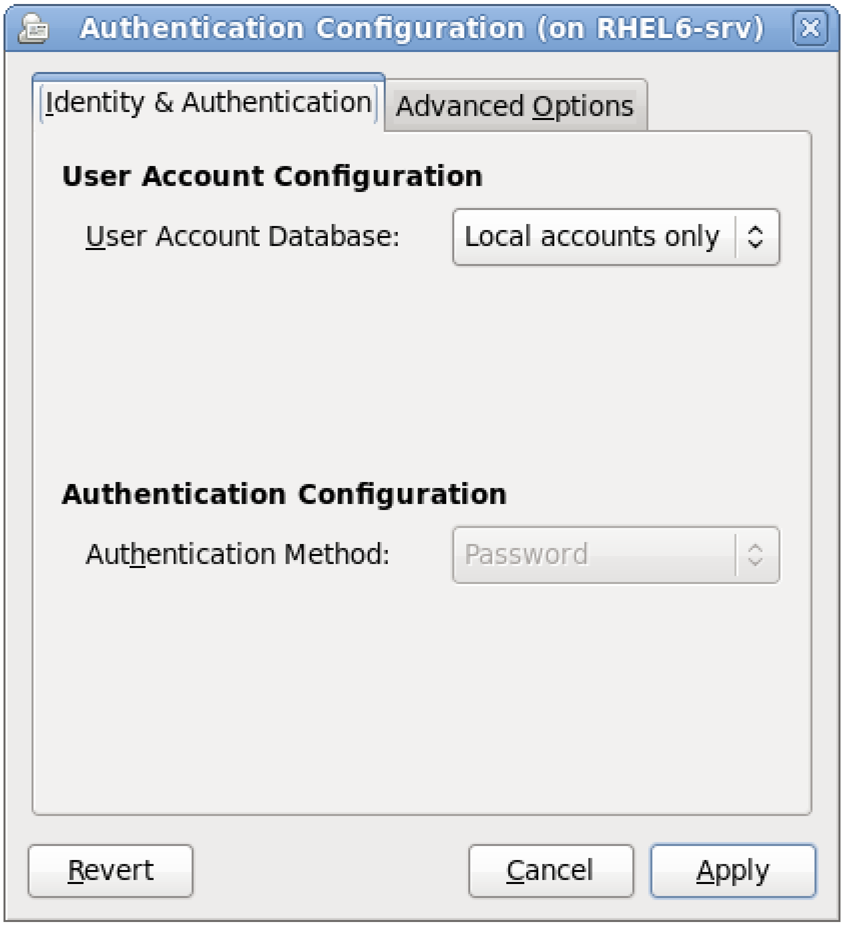
```
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM

Valid starting     Expires            Service principal
04/05/11 18:54:38  04/06/11 04:54:44
krbtgt/DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM@DEMO.CLOUD.LAB.ENG.BOS.REDHAT.C
OM
                                      renew until 04/12/11 18:54:38
#
```

At this point Kerberos is fully functional and the client utilities (*kinit, klist, kdestroy*) can be used for testing and verifying Kerberos functionality.

6.5 Configure Authentication

The `system-config-authentication` tool simplifies configuring the Samba, Kerberos, security and authentication files for Active Directory access. Running the tool as a background process in a subshell is recommended for viewing any configuration errors or warnings on the underlying command line window. Invoke the tool as follows:

```
# system-config-authentication &
```



Authentication Configuration (on RHEL6-srv)

User Account Configuration

User Account Database: Local accounts only

Authentication Configuration

Authentication Method: Password

Figure 6.5-1

On the "Identity & Authentication" tab, select the "User Account Database" drop-down and select "Winbind".

A new set of fields is displayed. Selecting the “Winbind” option configures the system to connect to a Windows Active Directory domain. User information from a domain can then be accessed, and the following server authentication options can be configured:

- **Winbind Domain**: Windows Active Directory domain
- **Security Model**: The Samba client mode of operation. The drop-down list allows selection of the following options:

  ads - This mode instructs Samba to act as a domain member in an Active Directory Server (ADS) realm. To operate in this mode, the `krb5-server` package must be installed, and Kerberos must be configured properly.

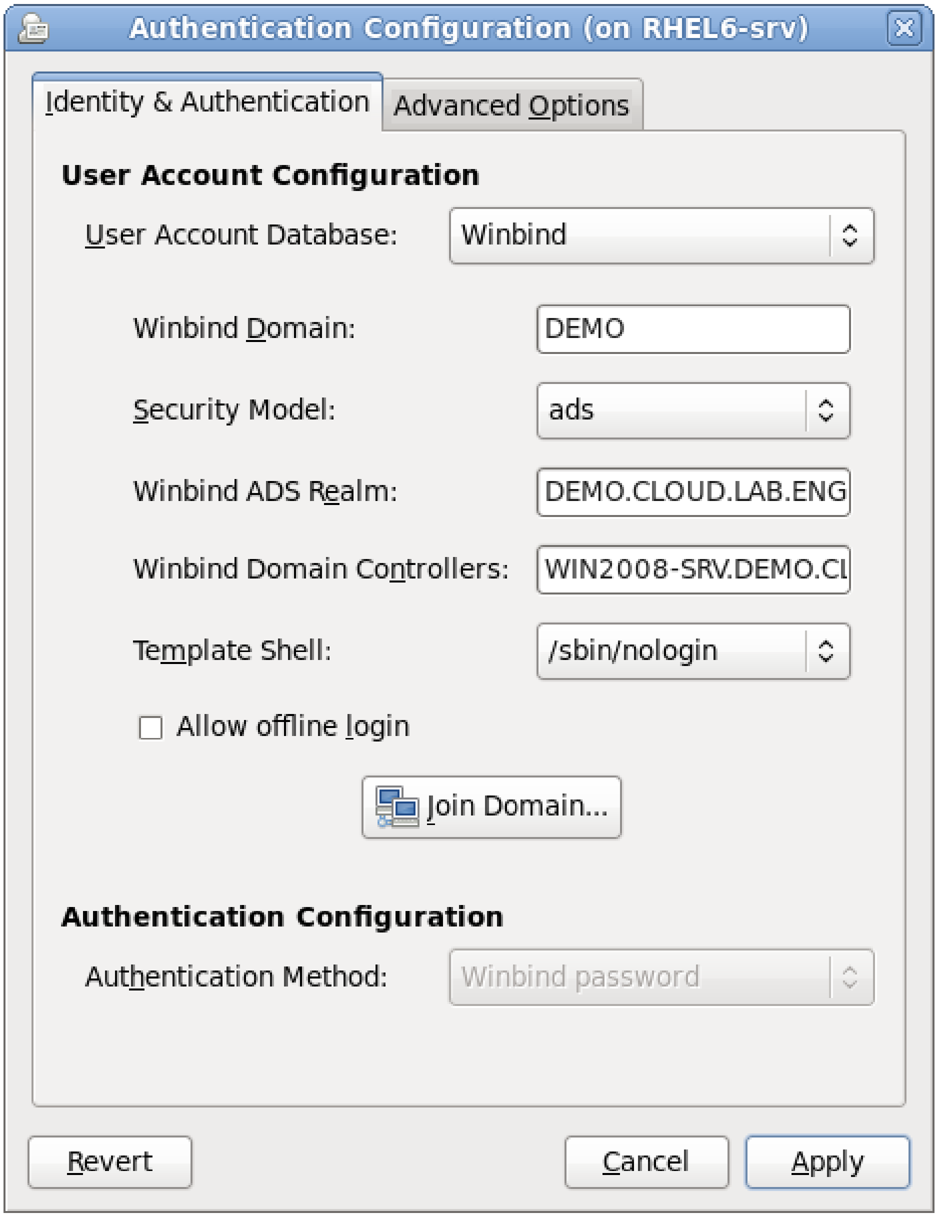
  domain - In this mode, Samba will attempt to validate the username/password by authenticating it through a Windows Active Directory domain server, similar to how a Windows Server would.

  server - In this mode, Samba will attempt to validate the username/password by authenticating it through another SMB server. If the attempt fails, the user mode will take effect instead.

  user - This is the default mode. With this level of security, a client must first log in with a valid username and password. Encrypted passwords can also be used in this security mode.
- **Winbind ADS Realm**: When the ads Security Model is selected, this allows you to specify the ADS Realm the Samba server should act as a domain member of.
- **Winbind Domain Controllers**: Use this option to specify which domain server winbind should use.
- **Template Shell**: When filling out the user information for a Windows user, the `winbindd` daemon uses the value chosen here to specify the login shell for that user.
- **Allow offline login**: By checking this option, authentication information is stored in a local cache (provided by SSSD). This information is then used when a user attempts to authenticate while offline.

Populate the fields as follows:

User Account Database:	**Winbind**
Winbind Domain:	**DEMO**
Security Model:	**ads**
Winbind ADS Realm:	**DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM**
Winbind Domain Controllers:	**WIN2008-SRV.DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM**
Template Shell:	***/sbin/nologin***



Authentication Configuration (on RHEL6-srv)

Identity & Authentication | Advanced Options

User Account Configuration

User Account Database: Winbind

Winbind Domain: DEMO

Security Model: ads

Winbind ADS Realm: DEMO.CLOUD.LAB.ENG

Winbind Domain Controllers: WIN2008-SRV.DEMO.CL

Template Shell: /sbin/nologin

□ Allow offline login

Join Domain...

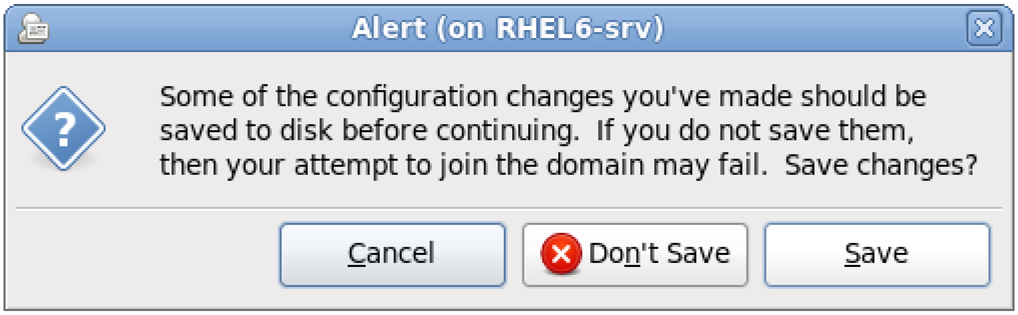
Authentication Configuration

Authentication Method: Winbind password

Revert | Cancel | Apply

Figure 6.5-2

then select “Join Domain”. An alert indicates the need to save the configuration changes to disk before continuing:



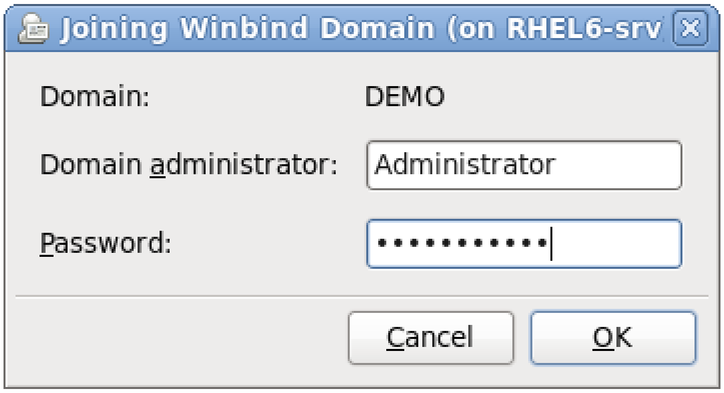
Some of the configuration changes you've made should be saved to disk before continuing. If you do not save them, then your attempt to join the domain may fail. Save changes?

Figure 6.5-3

Select “Save”. The terminal window shows the Winbind service was started:

```
# Starting Winbind services:           [  OK  ]
```

A new window prompts for the Domain administrator password:



Domain: DEMO

Domain administrator: Administrator

Password: •••••••••••

Figure 6.5-4

After entering it select “OK”. The terminal window displays the domain join status:

```
# Starting Winbind services:         [  OK  ]
[/usr/bin/net join -w DEMO -S WIN2008-
SRV.DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM -U Administrator]
Enter Administrator's password:<...>

Using short domain name -- DEMO
Joined 'RHEL6-SRV' to realm 'demo.cloud.lab.eng.bos.redhat.com'
#
```

Note: If the terminal displays either of the following errors:

```
Unable to find a suitable server for domain DEM

   ...or...

DNS update failed!
```

See **Section 6.8 Common Active Directory Integration Issues/Errors**

6.6 Verify/Test Active Directory

The join to the Active Directory domain should now be complete. Verify access by performing the following:

Test connection to Active Directory Domain Services:

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

List members in domain:

```
# wbinfo -u
RHEL6-SRV\demo
RHEL6-SRV\samba-user
DEMO\administrator
DEMO\guest
DEMO\krbtgt
DEMO\demo-user
#
```

List groups in domain:

```
# wbinfo -g
DEMO\domain computers
DEMO\domain controllers
DEMO\schema admins
DEMO\enterprise admins
DEMO\domain admins
DEMO\domain users
DEMO\domain guests
DEMO\group policy creator owners
DEMO\read-only domain controllers
DEMO\enterprise read-only domain controllers
DEMO\dnsupdateproxy
#
```

Note: If either of these fail to return all users or groups in the domain, increase the idmap UID, GID upper boundaries in the Samba configuration file then restart winbind and smb.

6.7 Modify Samba Configuration

The Samba configuration file can be modified to permit `winbind` to enumerate users and groups. For very large Active Directory environments enumeration may be less desirable as it can impact performance. Ranges for user and group ID's are increased from the default values. The default separator is changed to a '+' character to minimize the need to escape the shell when authenticating Active Directory accounts (e.g. - “DEMO+user” vs. “DEMO\\user”). Home directory and shell templates are also configured for future share mapping and shell access.

Make a safety copy of the Samba configuration file:

```
# cp -p /etc/samba/smb.conf /etc/samba/smb.conf.back
# ls -la smb.*
-rw-r--r--. 1 root root 2583 Apr  5 22:52 smb.conf
-rw-r--r--. 1 root root 2583 Apr  5 22:52 smb.conf.back
#
```

Edit and save the Samba configuration file as follows – changes are highlighted in bold:

```
[global]
   workgroup = DEMO
   password server = WIN2008-SRV.DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM *
   realm = DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
   security = ads
   idmap uid = 10000000-50000000 # increased for larger AD environments
   idmap gid = 10000000-50000000 # increased for larger AD environments
   winbind enum users=true       # set to false for large AD environments
   winbind enum groups=true      # set to false for large AD environments
   winbind separator=+
   winbind use default domain = false
   winbind offline logon = false
   template homedir = /home/%D/%u
   template shell = /bin/bash
```

Test the new configuration file:

```
# testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[samba-demo]"
Loaded services file OK.
'winbind separator = +' might cause problems with group membership.
Server role: ROLE_DOMAIN_MEMBER
Press enter to see a dump of your service definitions

[global]
        workgroup = DEMO
        realm = DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
        server string = Samba Server Version %v
        security = ADS
        password server = WIN2008-SRV.DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
        log file = /var/log/samba/log.%m
        max log size = 50
        idmap uid = 10000000-50000000
        idmap gid = 10000000-50000000
        template shell = /bin/bash
        winbind separator = +
        winbind enum users = Yes
        winbind enum groups = Yes
        cups options = raw

[homes]
        comment = Home Directories
        read only = No
        browseable = No

[printers]
        comment = All Printers
        path = /var/spool/samba
        printable = Yes
        browseable = No

[samba-demo]
        comment = RHEL6-Windows Demo Share
        path = /samba-demo
        valid users = samba-user
        read only = No
#
```

Re-start Samba and Winbind to activate the new configuration changes:

```
# service smb restart
Shutting down SMB services:                                [  OK  ]
Starting SMB services:                                     [  OK  ]
# service smb status
smbd (pid  2860) is running...
# ps -aef | grep smb
root      2860     1  0 12:28 ?        00:00:00 smbd -D
root      2863  2860  0 12:28 ?        00:00:00 smbd -D
root      2915  2709  0 12:29 pts/1    00:00:00 grep smb
# service winbind restart
Shutting down Winbind services:                            [  OK  ]
Starting Winbind services:                                 [  OK  ]
# service winbind status
winbindd (pid  2934) is running...
# ps -aef | grep winbind
root      2934     1  0 12:30 ?        00:00:00 winbindd
root      2936  2934  0 12:30 ?        00:00:00 winbindd
root      2948  2709  0 12:31 pts/1    00:00:00 grep winbind
#
```

Verify no Kerberos tickets are in use:

```
# kdestroy
kdestroy: No credentials cache found while destroying cache
# klist
klist: No credentials cache found (ticket cache FILE:/tmp/krb5cc_0)
#
```

Join the Active Directory Domain:

```
# net join -W DEMO -S WIN2008-SRV -U Administrator
Enter Administrator's password:
Using short domain name -- DEMO
Joined 'RHEL6-SRV' to realm 'demo.cloud.lab.eng.bos.redhat.com'
#
```

Test connection to Active Directory Domain Services:

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

List members in domain:

```
# wbinfo -u
RHEL6-SRV+samba-user
DEMO+administrator
DEMO+guest
DEMO+krbtgt
DEMO+demo-user
#
```

List groups in domain :

```
# wbinfo -g
DEMO+domain computers
DEMO+domain controllers
DEMO+schema admins
DEMO+enterprise admins
DEMO+cert publishers
DEMO+domain admins
DEMO+domain users
DEMO+domain guests
DEMO+group policy creator owners
DEMO+ras and ias servers
DEMO+allowed rodc password replication group
DEMO+denied rodc password replication group
DEMO+read-only domain controllers
DEMO+enterprise read-only domain controllers
```

```
DEMO+dnsadmins
DEMO+dnsupdateproxy
#
```

Note: users and groups are now enumerated with the '+' character.

This completes the integration of the Red Hat Enterprise Linux 6 server with Samba into the Windows Server 2008 R2 Active Directory domain. If any issues or errors were encountered during the integration process, see **Section 6.8 Common Active Directory Integration Issues/Errors**.

Once the integration has been completed, proceed to **Section 7 Common Use Cases** which details the two most common use cases – the management of Samba file shares and shell access for Active Directory users.

6.8 Common Active Directory Integration Issues/Errors

Some of the most common integration issues/error conditions encountered are discussed in this section. For each issue the symptom and most likely explanation demonstrated.

Kerberos Init Fails

Symptom

```
# kinit administrator@DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
Password for administrator@DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM:
kinit: Preauthentication failed while getting initial credentials
#
```

Explanation

The specified username or password was invalid. Run `kinit` again and then verify the ticket was granted:

```
# kinit administrator@DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
Password for administrator@DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM:

# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM

Valid starting     Expires            Service principal
03/21/11 17:50:40  03/22/11 03:50:46
krbtgt/DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM@DEMO.CLOUD.LAB.ENG.BOS.REDHAT.C
OM
                                       renew until 03/28/11 17:50:40
#
```

If username and password are known to be valid then the failure is most likely due to time server clock skew. See **Section 6.1 Synchronize Time Servers** to verify NTP has been configured correctly.

Domain Join Succeeds – DNS Update Fails

Symptom

```
# net join -w DEMO -S WIN2008-SRV -U Administrator
Enter Administrator's password:<...>

Using short domain name -- DEMO
Joined 'RHEL6-SRV' to realm 'demo.cloud.lab.eng.bos.redhat.com'
DNS update failed!
#
```

Explanation

The hostname on the Red Hat Enterprise Linux 6 server needs to be set to the fully qualified domain name (FQDN) in */etc/hosts*:

```
127.0.0.1      localhost
10.16.143.162 RHEL6-srv.demo.cloud.lab.eng.bos.redhat.com    \
              RHEL6-srv.cloud.lab.eng.bos.redhat.com         \
              RHEL6-srv
10.16.143.163 Win2008-srv.demo.cloud.lab.eng.bos.redhat.com  \
              Win2008-srv.cloud.lab.eng.bos.redhat.com       \
              Win2008-srv
```

Note: FQDN entries are specified for hosts both with and without the AD domain.

Domain Join Failure – No Suitable Server

Symptom

```
# net join -w DEMO -S WIN2008-SRV -U Administrator

Unable to find a suitable server for domain DEMO
#
```

Explanation

Verify the fully qualified domain name (FQDN) is specified in */etc/sysconfig/network*:

```
NETWORKING=yes
HOSTNAME=RHEL6-srv.cloud.lab.eng.bos.redhat.com
```

Restart the network service or reboot the Red Hat Enterprise Linux 6 server to activate the change.

Also verify that DNS lookups are pointing to the Windows Active Directory domain server in the file */etc/resolv.conf*:

```
domain cloud.lab.eng.bos.redhat.com
search cloud.lab.eng.bos.redhat.com
nameserver 10.16.143.163
nameserver 10.16.255.2
```

After correcting these files run the `system-config-authentication` tool and select “Join Domain”

Error Looking Up Domain Users/Groups – Active Directory Join is OK

Symptom

```
# wbinfo -u
Error looking up domain users

# wbinfo -g
Error looking up domain groups

 # net ads testjoin
Join is OK
#
```

Explanation

The *winbind* daemon is not running or requires a restart:

```
# service winbind status
winbindd is stopped

# service winbind start
Starting Winbind services:                                 [  OK  ]

# wbinfo -u
RHEL6-SRV\samba-user
DEMO\administrator
DEMO\guest
DEMO\krbtgt
DEMO\demo-user

# wbinfo -g
DEMO\domain computers
DEMO\domain controllers
DEMO\schema admins
DEMO\enterprise admins
DEMO\cert publishers
DEMO\domain admins
DEMO\domain users
DEMO\domain guests
DEMO\group policy creator owners
DEMO\ras and ias servers
DEMO\allowed rodc password replication group
DEMO\denied rodc password replication group
DEMO\read-only domain controllers
DEMO\enterprise read-only domain controllers
DEMO\dnsadmins
DEMO\dnsupdateproxy
#
```

7 Common Use Cases

This section outlines the two most common use cases for integrating a Red Hat Enterprise Linux 6 server with Samba and Windows Server 2008 R2 with Active Directory Domain Services:

- Managing Samba file shares
- Managing shell access

7.1 Managing Samba File Shares for Active Directory Users

The process for managing Samba file shares for Active Directory users is similar to that for local Samba users. This sections details the creation and removal of file shares on a Red Hat Enterprise Linux 6 server with Active Directory authentication.

7.1.1 Create a New File Share

Make a safety copy of the Samba configuration file:

```
# cp -p /etc/samba/smb.conf /etc/samba/smb.conf.back
```

Edit the Samba configuration file and add the following new file share definition:

```
#
# Demo share for RHEL6-Windows Server 2008 R2 Interoperability – AD
Verification
#
[ad-demo]
        comment = RHEL6-Windows Active Directory Demo Share
        path=/ad-demo
        create mask = 0660
        directory mask = 770
        writeable = yes
        browseable = yes
        valid users = +"DEMO+domain users"
        guest ok = no
```

This entry defines a file share called '*ad-demo*' located on the */ad-demo* file system. Access is restricted to Active Directory domain users in the '*DEMO*' domain.

Save the file then test the configuration:

```
# testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[samba-demo]"
Processing section "[ad-demo]"
Loaded services file OK.
'winbind separator = +' might cause problems with group membership.
Server role: ROLE_DOMAIN_MEMBER
Press enter to see a dump of your service definitions

[global]
        workgroup = DEMO
        realm = DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
        server string = Samba Server Version %v
        security = ADS
        password server = WIN2008-SRV.DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
        log file = /var/log/samba/log.%m
        max log size = 50
        idmap uid = 10000000-50000000
        idmap gid = 10000000-50000000
        template shell = /bin/bash
        winbind separator = +
        winbind enum users = Yes
        winbind enum groups = Yes
        cups options = raw

[homes]
        comment = Home Directories
        read only = No
        browseable = No

[printers]
        comment = All Printers
        path = /var/spool/samba
        printable = Yes
        browseable = No

[samba-demo]
        comment = RHEL6-Windows Demo Share
        path = /samba-demo
        valid users = samba-user
        read only = No

[ad-demo]
        comment = RHEL6-Windows Active Directory Demo Share
        path = /ad-demo
        valid users = "+DEMO+domain users"
        read only = No
        create mask = 0660
        directory mask = 0770
#
```

Create a top level directory where Active Directory user accounts will reside under:

```
# mkdir /ad-demo
# chmod 2770 -R /ad-demo
# chgrp -R "DEMO+domain users" /ad-demo
# ls -la /ad-demo
total 8
drwxrws---.  2 root DEMO+domain users 4096 Apr  7 15:36 .
dr-xr-xr-x. 29 root root              4096 Apr  7 15:36 ..
#
```

Populate the new file share with a test file:

```
# echo “This file was placed in the /ad-demo file share on the RHEL6
server” > /ad-demo/This_is_the_RHEL6_server_ad_demo_share
# ls -la /ad-demo
total 12
drwxrws---.  2 root DEMO+domain users 4096 Apr  8 15:53 .
dr-xr-xr-x. 29 root root              4096 Apr  7 15:36 ..
-rw-r--r--.  1 root DEMO+domain users   68 Apr  8 15:54
This_is_the_RHEL6_server_ad_demo_share
#
```

Configure SELinux security parameters for the new file share:

```
# semanage fcontext -a -t samba_share_t "/ad-demo(/.*)?"
# restorecon -R -v /ad-demo
restorecon reset /ad-demo context unconfined_u:object_r:default_t:s0-
>system_u:object_r:samba_share_t:s0
# ls -laZ /ad-demo
drwxrws---. root DEMO+domain users system_u:object_r:samba_share_t:s0 .
dr-xr-xr-x. root root              system_u:object_r:root_t:s0       ..
-rw-r--r--. root DEMO+domain users
unconfined_u:object_r:samba_share_t:s0
This_is_the_RHEL6_server_ad_demo_share
#
```

Restart Samba and Winbind to activate the new configuration:

```
# service smb restart
Shutting down SMB services:                                [  OK  ]
Starting SMB services:                                     [  OK  ]
```

```
# service smb status
smbd (pid  2860) is running...

# service winbind restart
Shutting down Winbind services:                            [  OK  ]
Starting Winbind services:                                 [  OK  ]
# service winbind status
winbindd (pid  2934) is running...

#
```

Now that the new file share has been created it can be mapped from the Windows client as described in **Section 5.5 Verify Samba**.

Note: When using the command prompt method to map the new file share, the domain name must be specified:

```
C:\Users\win7-user> net use T: \\RHEL6-srv\ad-demo /user:DEMO\demo-user
Enter the password for 'DEMO\demo-user' to connect to 'RHEL6-srv':
The command completed successfully.


C:\Users\win7-user> T:

T:\> dir
 Volume in drive T is ad-demo
 Volume Serial Number is 5756-130D

 Directory of T:\

04/09/2011  07:55 PM    <DIR>          .
04/09/2011  06:00 PM    <DIR>          ..
04/08/2011  03:54 PM                68
This_is_the_RHEL6_server_ad_demo_share
               1 File(s)             68 bytes
               2 Dir(s)  46,749,351,936 bytes free

T:\>
```

7.1.2 Remove a File Share

Removing an existing file share requires modifying the Samba configuration file, restarting the Samba daemon and (optionally) the share directories and files.

Make safety copy of original configuration file:

```
# cp -p /etc/samba/smb.conf /etc/samba/smb.conf.back
```

Edit the Samba configuration file and remove the existing file share definition to be deleted:

```
#
# Demo share for RHEL6-Windows Server 2008 R2 Interoperability – AD
Verification
#
[ad-demo]
        comment = RHEL6-Windows Active Directory Demo Share
        path=/ad-demo
        create mask = 0660
        directory mask = 770
        writeable = yes
        browseable = yes
        valid users = +"DEMO+domain users"
        guest ok = no
```

Save the file then test the configuration:

```
# testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[samba-demo]"
Loaded services file OK.
'winbind separator = +' might cause problems with group membership.
Server role: ROLE_DOMAIN_MEMBER
Press enter to see a dump of your service definitions

[global]
        workgroup = DEMO
        realm = DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
        server string = Samba Server Version %v
        security = ADS
        password server = WIN2008-SRV.DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
        log file = /var/log/samba/log.%m
        max log size = 50
        idmap uid = 10000000-50000000
        idmap gid = 10000000-50000000
        template shell = /bin/bash
        winbind separator = +
        winbind enum users = Yes
        winbind enum groups = Yes
        cups options = raw

[homes]
        comment = Home Directories
        read only = No
        browseable = No

[printers]
        comment = All Printers
        path = /var/spool/samba
        printable = Yes
        browseable = No

[samba-demo]
        comment = RHEL6-Windows Demo Share
        path = /samba-demo
        valid users = samba-user
        read only = No
#
```

Delete and verify removal of the Active Directory users home directory (optional):

```
# rm -r /ad-demo
# ls -l /ad-demo
ls: cannot access /ad-demo: No such file or directory
#
```

Re-start Samba to activate the new configuration:

```
# service smb restart
Shutting down SMB services:                                 [  OK  ]
Starting SMB services:                                      [  OK  ]
# service smb status
smbd (pid  2860) is running...
#
```

This completes the process of removing a Samba file share with Active Directory authentication from a Red Hat Enterprise Linux 6 server.

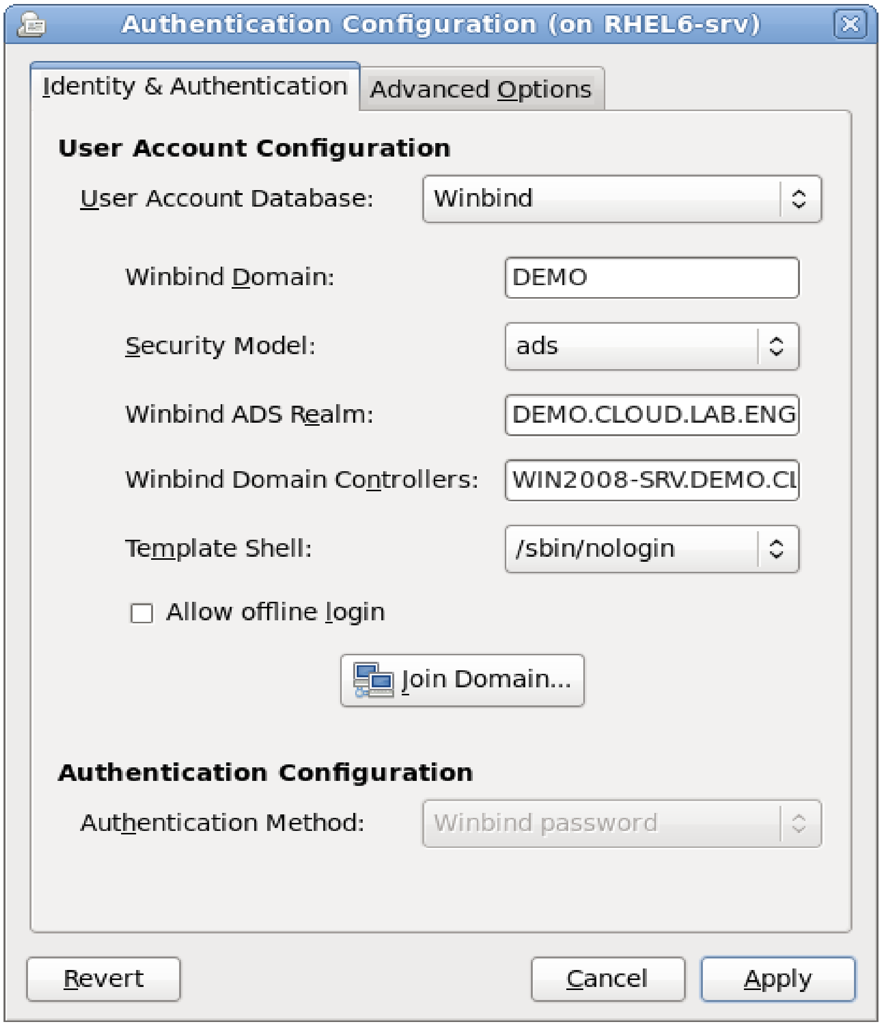
7.2 Managing Shell Access for Active Directory Users

The second common use case is managing secure shell (`ssh`) access. The next two sections detail how to configure a Red Hat Enterprise Linux 6 server with Samba to grant or revoke remote login access to users authenticated through Active Directory.

7.2.1 Granting Shell Access

The `system-config-authentication` tool can be used to grant login access to users authenticated through Active Directory. Invoke the tool as follows:

```
# system-config-authentication &
```



Authentication Configuration (on RHEL6-srv)

User Account Configuration

User Account Database: Winbind

Winbind Domain: DEMO

Security Model: ads

Winbind ADS Realm: DEMO.CLOUD.LAB.ENG

Winbind Domain Controllers: WIN2008-SRV.DEMO.CL

Template Shell: /sbin/nologin

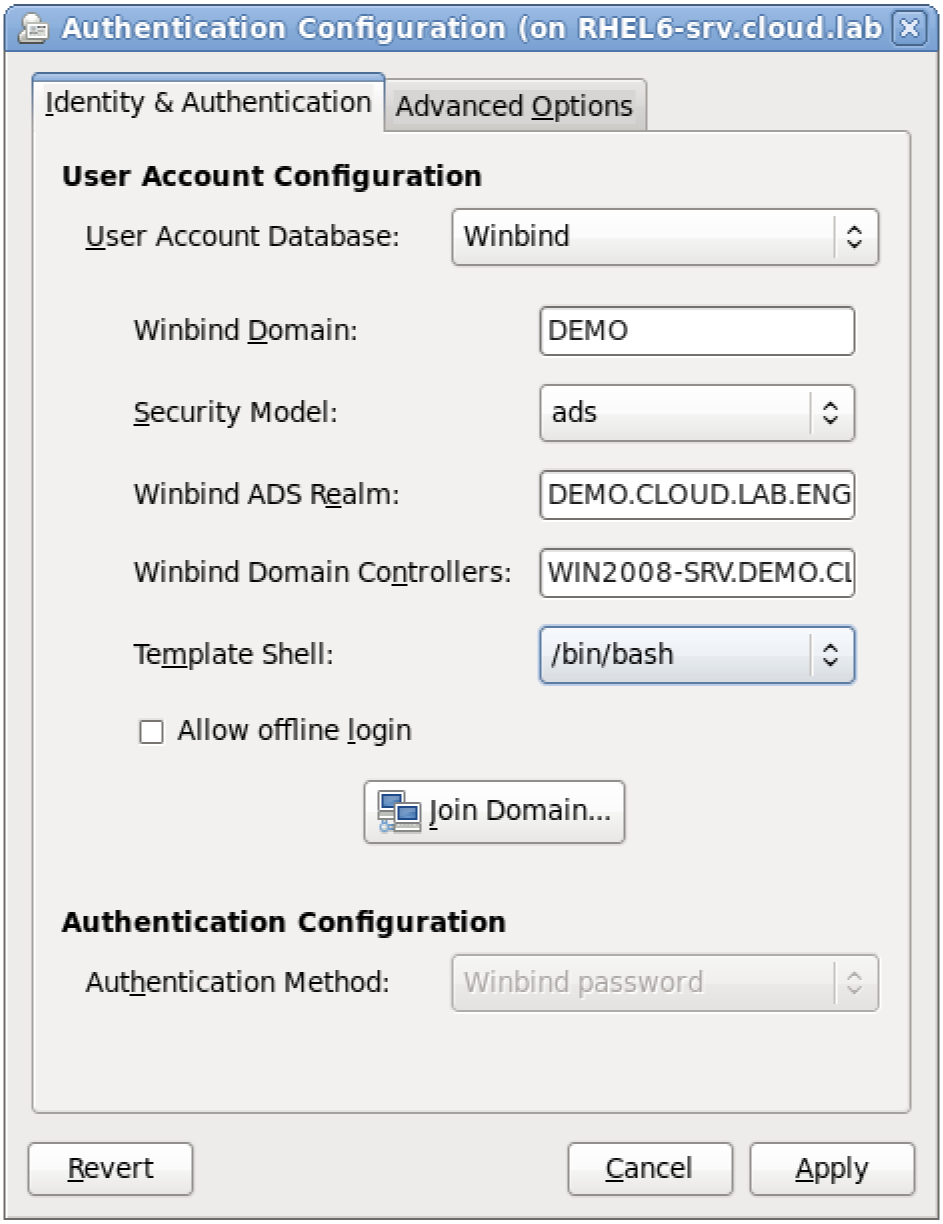
□ Allow offline login

Authentication Configuration

Authentication Method: Winbind password

Figure 7.2-1

Under the “Identity & Authentication” tab, change the Template Shell to */bin/bash*:


Authentication Configuration (on RHEL6-srv.cloud.lab
Identity & Authentication
Advanced Options
Join Domain...
Revert
Cancel
Apply

User Account Configuration

User Account Database: Winbind

Winbind Domain: DEMO

Security Model: ads

Winbind ADS Realm: DEMO.CLOUD.LAB.ENG

Winbind Domain Controllers: WIN2008-SRV.DEMO.Cl

Template Shell: /bin/bash

□ Allow offline login

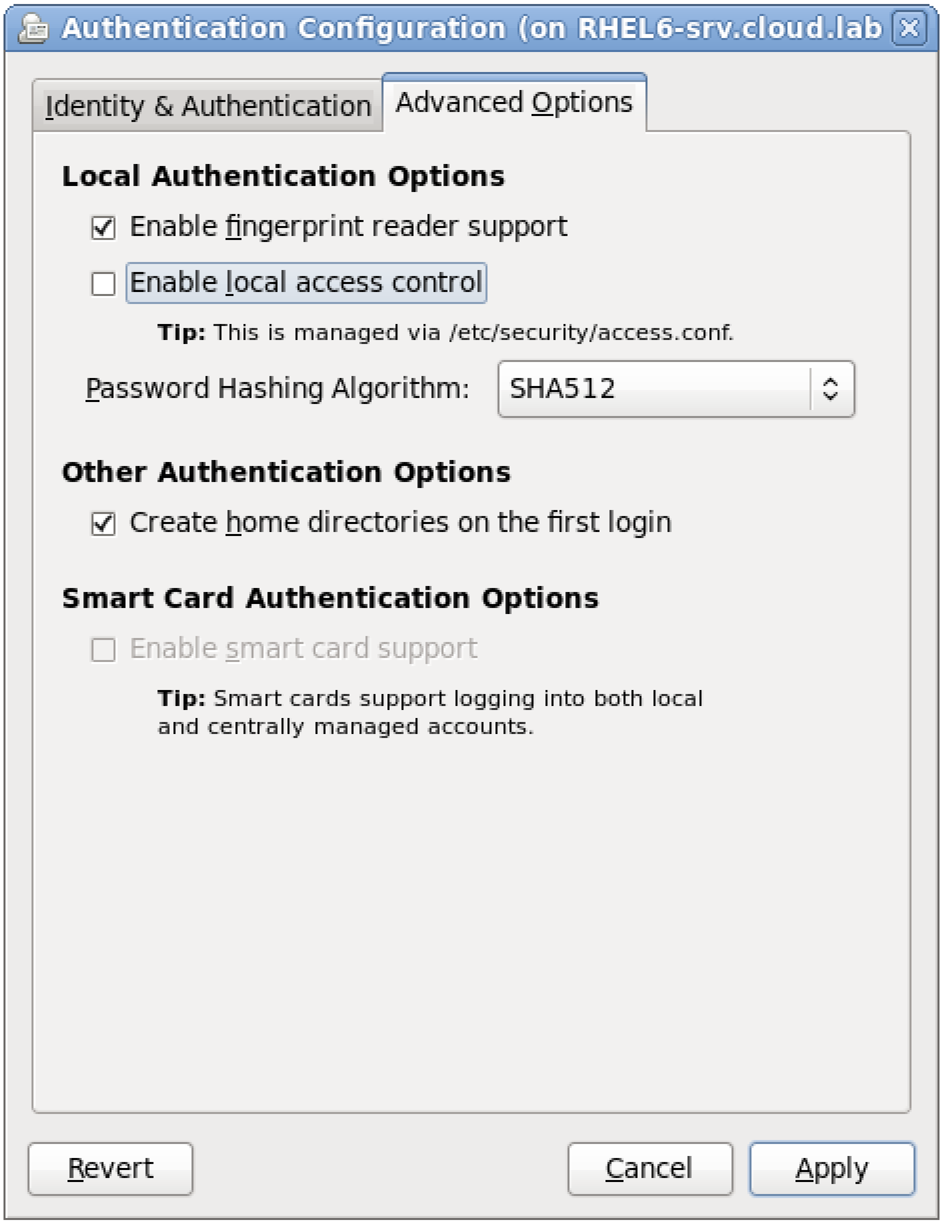
Authentication Configuration

Authentication Method: Winbind password

Figure 7.2-2

All shell logins authenticated through Active Directory now use */bin/bash*.

Under the “Advanced Options” tab, click on “Create home directories on the first login” then click “Apply”:


Authentication Configuration (on RHEL6-srv.cloud.lab
Identity & Authentication
Advanced Options
Revert
Cancel
Apply

Local Authentication Options

☑ Enable fingerprint reader support

□ Enable local access control

Tip: This is managed via /etc/security/access.conf.

Password Hashing Algorithm: SHA512

Other Authentication Options

☑ Create home directories on the first login

Smart Card Authentication Options

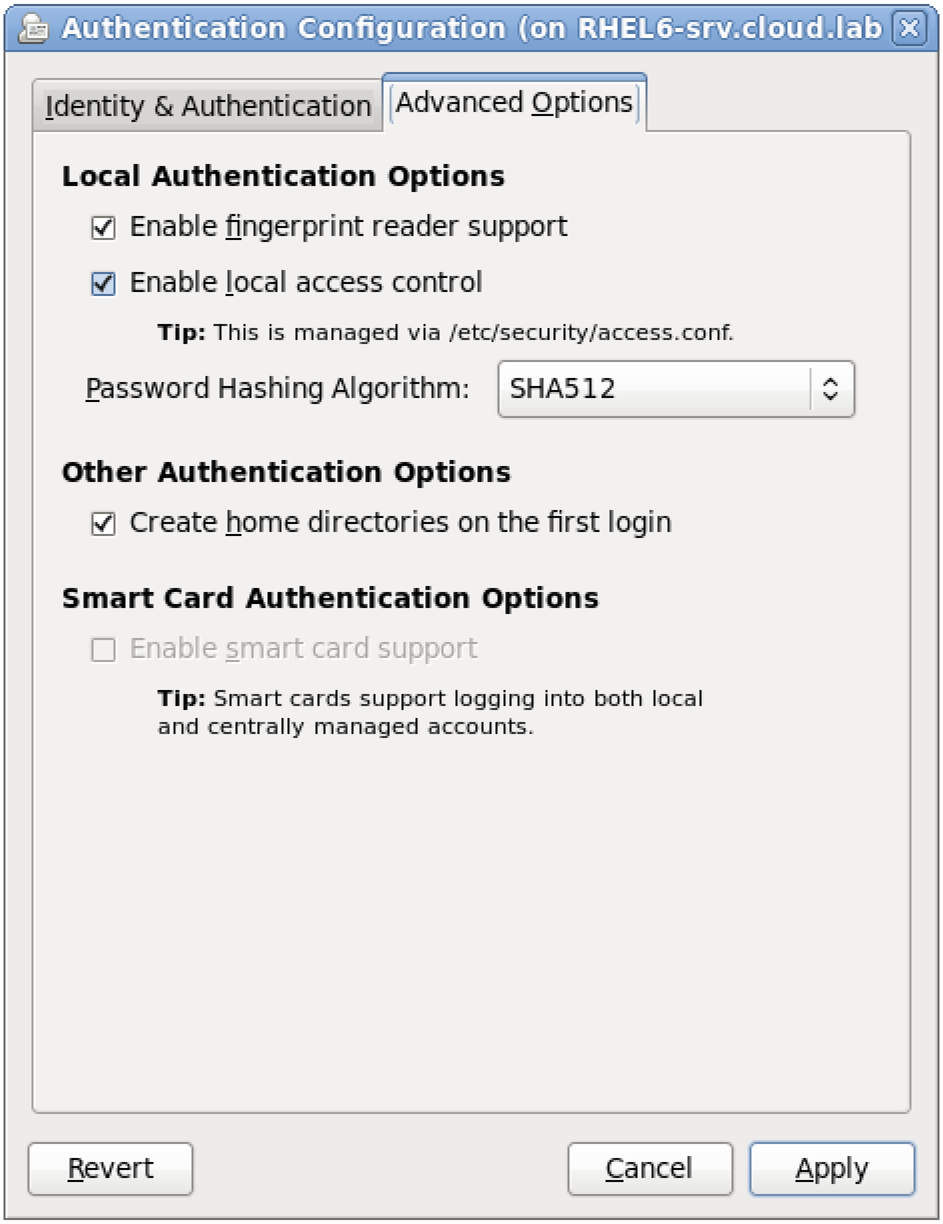
□ Enable smart card support

Tip: Smart cards support logging into both local and centrally managed accounts.

Figure 7.2-3

Optional Access Control:

Local shell access can be restricted through the use of the */etc/security/access.conf*. To use it, click on the “Advanced Options” tab and enable the option “Enable local access control”:



Authentication Configuration (on RHEL6-srv.cloud.lab
Identity & Authentication
Advanced Options

Local Authentication Options

☑ Enable fingerprint reader support

☑ Enable local access control

Tip: This is managed via /etc/security/access.conf.

Password Hashing Algorithm: SHA512

Other Authentication Options

☑ Create home directories on the first login

Smart Card Authentication Options

☐ Enable smart card support

Tip: Smart cards support logging into both local and centrally managed accounts.

Figure 7.2-4

Use of */etc/security/access.conf* provides finer levels of control to user shell access. For example, to allow a specific Active Directory domain user to have shell access edit the file an add the line:

```
+ : DEMO+demo-user : ALL
```

This entry allows the user named '*demo-user*' in the Active Directory domain called '*DEMO*' to log into the Red Hat Enterprise Linux 6 server.

Verify the change by using `ssh` to login to the account:

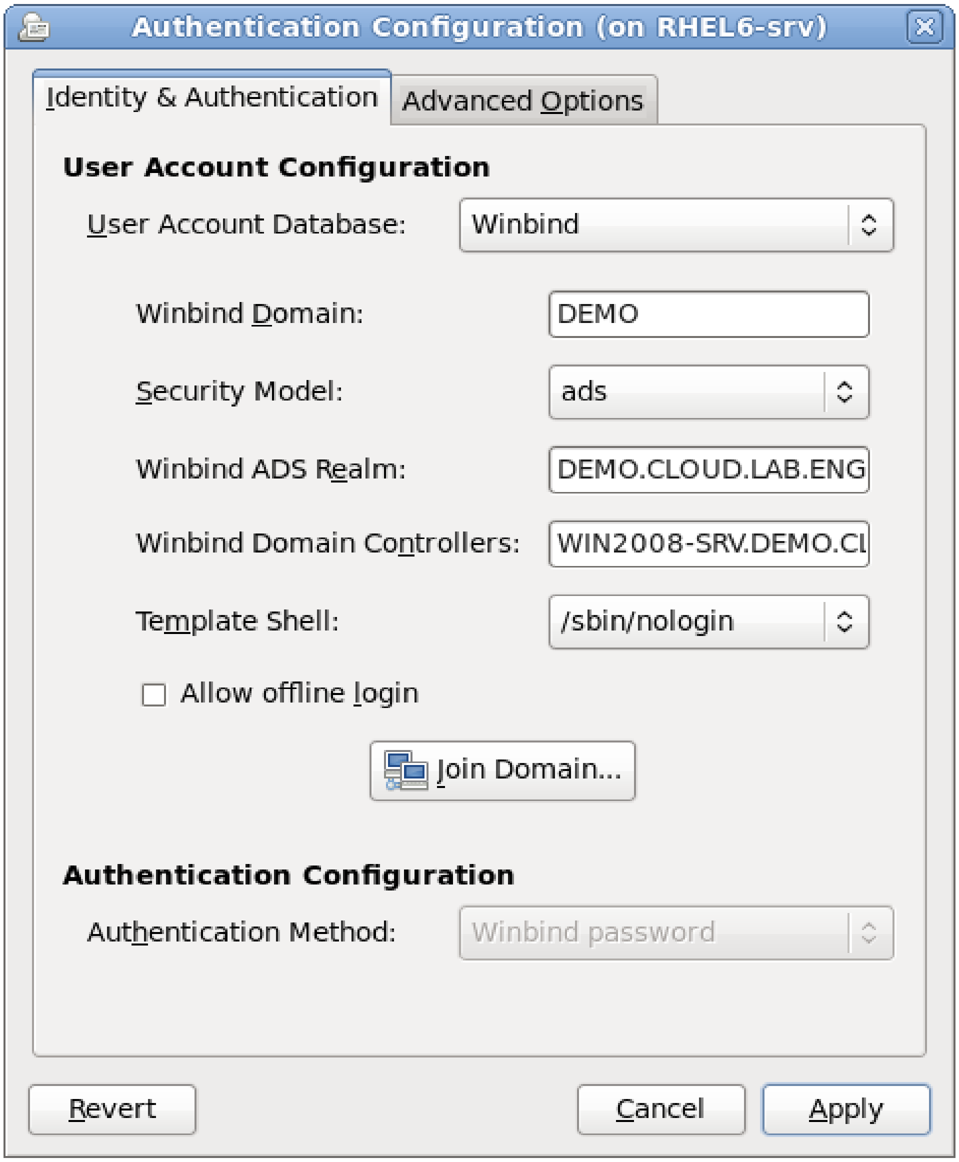
```
$ ssh DEMO+demo-user@RHEL6-srv
DEMO+demo-user@rhel6-srv's password:
Last login: Sat Apr  9 17:01:08 2011 from vpn-8-95.rdu.redhat.com
$ id
uid=16777216(DEMO+demo-user) gid=16777221(DEMO+domain users)
groups=16777221(DEMO+domain users)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
$ pwd
/home/DEMO/demo-user
$ ls -ld
total 32
drwxr-sr-x. 4 DEMO+demo-user DEMO+domain users 4096 Apr  9 17:08 .
#
```

For most situations global access through the `system-config-authentication` tool is sufficient but for environments requiring stricter control the above method can be used.

7.2.2 Revoking Shell Access

The `system-config-authentication` tool can be used to revoke login access from users authenticated through Active Directory. Invoke the tool as follows:

```
# system-config-authentication &
```



Authentication Configuration (on RHEL6-srv)

User Account Configuration

User Account Database: Winbind

Winbind Domain: DEMO

Security Model: ads

Winbind ADS Realm: DEMO.CLOUD.LAB.ENG

Winbind Domain Controllers: WIN2008-SRV.DEMO.CL

Template Shell: /sbin/nologin

□ Allow offline login

Authentication Configuration

Authentication Method: Winbind password

Figure 7.2-5

Under the “Identity & Authentication” tab, change the Template Shell to */sbin/nologin*. This disables shell access for all Active Directory domain users. Click “Apply”.

Optional Access Control:

Shell access for individual Active Directory domain users can be removed by modifying entries in the */etc/security/access.conf* file. For example, to deny a specific Active Directory domain user from having shell access, edit the file and add the line:

```
- : DEMO+demo-user : ALL
```

This entry prohibits the user named '*demo-user*' in the Active Directory domain called '*DEMO*' from logging into the Red Hat Enterprise Linux 6 server.

Verify the change by using ssh to login to the account:

```
$ ssh DEMO+demo-user@RHEL6-srv
DEMO+demo-user@rhel6-srv's password:
Connection closed by 10.16.143.162
$
```

7.3 Common Use Case Issues/Errors

Below are some of the most common use case issues/error conditions that may be encountered.

Shell Logs In Successfully - Immediately Logs Out

Symptom

```
$ ssh DEMO+demo-user@RHEL6-srv
DEMO+demo-user@rhel6-srv's password:
Creating home directory for DEMO+demo-user.
Last login: Sat Apr  9 15:43:53 2011 from vpn-8-95.rdu.redhat.com
Connection to RHEL6-srv closed.

$
```

Explanation

No template shell is enabled. Run `system-config-authentication` and then select a shell (e.g. - */bin/bash*) in the Template Shell drop-down menu.

Shell Logs In Successfully – Can not change to home directory

Symptom

```
$ ssh DEMO+demo-user@RHEL6-srv
DEMO+demo-user@rhel6-srv's password:
Creating home directory for DEMO+demo-user.
Last login: Sat Apr  9 15:43:53 2011 from vpn-8-95.rdu.redhat.com
Could not chdir to home directory /home/DEMO/demo-user: No such file or
directory
$
```

Explanation

No parent directory exists - create it:

```
# mkdir -p /home/DEMO
# chmod 2770 -R /home/DEMO
# chgrp -R "DEMO+domain users" /home/DEMO
# ls -la /home/DEMO
total 8
drwxrws---. 2 root DEMO+domain users 4096 Apr  9 16:51 .
drwxr-xr-x. 5 root root              4096 Apr  9 16:51 ..
#
```

Verify from the Red Hat Enterprise Linux 6 server:

```
# su - 'DEMO+demo-user'
Creating home directory for DEMO+demo-user.
$ id
uid=16777216(DEMO+demo-user) gid=16777221(DEMO+domain users)
groups=16777221(DEMO+domain users)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
$ pwd
/home/DEMO/demo-user
$ ls -la
total 28
drwxr-sr-x. 4 DEMO+demo-user DEMO+domain users 4096 Apr  9 16:54 .
drwxrws---. 3 root           DEMO+domain users 4096 Apr  9 16:54 ..
-rw-r--r--. 1 DEMO+demo-user DEMO+domain users   18 Apr  9 16:54
.bash_logout
-rw-r--r--. 1 DEMO+demo-user DEMO+domain users  176 Apr  9 16:54
.bash_profile
-rw-r--r--. 1 DEMO+demo-user DEMO+domain users  124 Apr  9 16:54 .bashrc
drwxr-sr-x. 2 DEMO+demo-user DEMO+domain users 4096 Apr  9 16:54 .gnome2
drwxr-sr-x. 4 DEMO+demo-user DEMO+domain users 4096 Apr  9 16:54
.mozilla
$
```

Verify from the Windows client:

```
# ssh DEMO+demo-user@RHEL6-srv
DEMO+demo-user@rhel6-srv's password:
Creating home directory for DEMO+demo-user.
Last login: Sat Apr  9 16:12:19 2011 from vpn-8-95.rdu.redhat.com
$ id
uid=16777216(DEMO+demo-user) gid=16777221(DEMO+domain users)
groups=16777221(DEMO+domain users)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
$ pwd
/home/DEMO/demo-user
$ ls -la
total 28
drwxr-sr-x. 4 DEMO+demo-user DEMO+domain users 4096 Apr  9 17:01 .
drwxrws---. 4 root           DEMO+domain users 4096 Apr  9 17:01 ..
-rw-r--r--. 1 DEMO+demo-user DEMO+domain users   18 Apr  9 17:01
.bash_logout
-rw-r--r--. 1 DEMO+demo-user DEMO+domain users  176 Apr  9 17:01
.bash_profile
-rw-r--r--. 1 DEMO+demo-user DEMO+domain users  124 Apr  9 17:01 .bashrc
drwxr-sr-x. 2 DEMO+demo-user DEMO+domain users 4096 Apr  9 17:01 .gnome2
drwxr-sr-x. 4 DEMO+demo-user DEMO+domain users 4096 Apr  9 17:01
.mozilla
$
```

8 Conclusion

This paper detailed the steps necessary to deploy and integrate Red Hat Enterprise Linux 6 with Samba services into Microsoft Windows Server 2008 R2 Active Directory domains. Microsoft Windows system administrators are guided through the full deployment, integration and verification process. Basic concepts as well as detailed step-by-step installation, configuration and integration tasks have been provided. Solutions to the most commonly encountered issues and errors are also described. The configurations and common use cases demonstrated within provide a framework that can be customized to meet the requirements of specific computing environments.

Appendices

Appendix A: Example Samba Configuration File (smb.conf)

```
# File: /etc/samba/smb.conf
# Date: 2011-04-05
# Auth: M. Heslin
# Desc: Main Samba configuration file. See the smb.conf(5) manual page
#          and default for more details. This version reflects the configuration
#          developed for the Red Hat Enterprise Linux 6/Samba - Windows Server 2008 R2/Active Directory
#          Interoperability Reference Architecture project.
# Note(s):
#       1. Entries within the lines beginning with '#--authconfig--'
#          reflect changes made by the 'authconfig' utilites
#          (system-config-authentication, authconfig,  authconfig-tui).
#          Edits made directly to the file here may be overwritten
#          by these utilities the next time they are run.
#       2. Always run the samba 'testparm' utility after making manual changes
#
#======================== Global Settings =====================================

[global]
#--authconfig--start-line--

# Generated by authconfig on 2011/04/09 16:09:15
# DO NOT EDIT THIS SECTION (delimited by --start-line--/--end-line--)
# Any modification may be deleted or altered by authconfig in future

   workgroup = DEMO
   password server = WIN2008-SRV.DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
   realm = DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
   security = ads
   idmap uid = 10000000-50000000              # increase or adjust as needed  for larger AD environments
   idmap gid = 10000000-50000000              # increase or adjust as needed  for larger AD environments
   winbind enum users = true                  # set to false for larger AD environments
   winbind enum groups = true                 # set to false for larger AD environments
   winbind separator = +
   winbind use default domain = false
   winbind offline logon = false
   template homedir = /home/%D/%u
   template shell = /bin/bash

#--authconfig--end-line--

# ---------------------- Network Related Options ------------------------

server string = Samba Server Version %v

# -------------------------- Logging Options ----------------------------

# logs split per machine
```

```
log file = /var/log/samba/log.%m
 # max 50KB per log file, then rotate
max log size = 50

# ---------------------- Standalone Server Options -----------------------

passdb backend = tdbsam

# -------------------------- Printing Options ----------------------------

load printers = yes
cups options = raw

#============================ Share Definitions ==============================

[homes]
        comment = Home Directories
        browseable = no
        writable = yes
;       valid users = %S
;       valid users = MYDOMAIN\%S

[printers]
        comment = All Printers
        path = /var/spool/samba
        browseable = no
        guest ok = no
        writable = no
        printable = yes

#
# Demo share for RHEL6-Windows Server 2008 R2 Interoperability – Samba Verification
#
[samba-demo]
        comment = RHEL6-Windows Demo Share
        path=/samba-demo
        writeable = yes
        browseable = yes
        valid users = samba-user

#
# Demo share for RHEL6-Windows Server 2008 R2 Interoperability – AD Verification
#
[ad-demo]
        comment = RHEL6-Windows Active Directory Demo Share
        path=/ad-demo
        create mask = 0660
        directory mask = 770
        writeable = yes
        browseable = yes
        valid users = "+DEMO+domain users"
        guest ok = no
```

Appendix B: Example Kerberos Configuration File (krb5.conf)

```
[logging]
  default = FILE:/var/log/krb5libs.log
  kdc = FILE:/var/log/krb5kdc.log
  admin_server = FILE:/var/log/kadmind.log

[libdefaults]
  default_realm = DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
  dns_lookup_realm = true
  dns_lookup_kdc = true
  ticket_lifetime = 24h
  renew_lifetime = 7d
  forwardable = false

[realms]
  DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM = {
    kdc = WIN2008-SRV.DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
    admin_server = WIN2008-SRV.DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
 }

[domain_realm]
  .demo = DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
   demo = DEMO.CLOUD.LAB.ENG.BOS.REDHAT.COM
```

Appendix C: Windows Server 2008 R2 – Installation Summary

This summary configuration guide is provide as a convenience to administrators and is intended to serve as a summary to the installation and configuration of Microsoft Windows Server 2008 R2. Refer to the following Microsoft TechNet article for the most current and comprehensive details on installing and deploying Windows Server 2008 R2:

http://technet.microsoft.com/en-us/library/dd283085.aspx

Step 1. Insert media and boot

Step 2. Select installation language and regional options

Step 3. Select the operating system

e.g. - Windows Server 2008 R2 Enterprise (Full Installation)

Step 4. Select type of installation - i.e. Upgrade vs. Custom (advanced)

Step 5. Select where (target drive) to install Windows

- If installing to a disk connected to a SCSI controller, select Load Driver and insert the media provided by the controller's manufacturer
- If installing to a Virtual Machine, install the Virtual SCSI Controller Driver
- Partition, format drive as required (*optional*)

...setup copies files from media to installation disk...

Step 6. System reboots

...setup updates registry settings...
...setup starts services...

Step 7. Installation completes

...system reboots...
...setup prepares computer for first use...

Step 8. Login as Administrator and change the default password

...desktop is prepared...

Step 9. Configure network

Step 10. Run Microsoft Update

...system reboots to apply updates...

Step 11. Login as Administrator

Step 12. Activate Windows

Step 13. Configure Date, Time

Step 14. Change computer name

...system reboots to activate...

Step 15. Enable Remote Desktop

- Open Server Manager from the Quick Launch toolbar
- Open Server Summary
- Open Computer Information
- Select "Configure Remote Desktop"
- In the System Properties window, select the "Remote" tab
- Under Remote Desktop select either:

  - "Allow connections from computers running any version of Remote Desktop (less secure)"

  ...or...

  - "Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)"

- Select "OK" to continue.

Appendix D: Active Directory Domain Services – Configuration Summary

This summary configuration guide is provide as a convenience to administrators and is intended to serve as a summary to the installation and configuration of Active Directory Domain Services on Windows Server 2008 R2. Refer to the following Microsoft TechNet article for the most current and comprehensive details:

http://technet.microsoft.com/en-us/library/cc770946.aspx

Prerequisites

The following are required before Active Directory can be configured on a Windows Server 2008 R2 server:

- Administrator account access
- Properly configured NIC (Static IP)
- NTFS partition with 250mb free space for Active Directory
- Functional DNS server (can be installed on the AD server itself or point to an existing DNS server)
- Domain name to use

Installation Summary

An Active Directory installation involves the following series of steps on a Windows Server 2008 R2 server:

1. Install Active Directory Domain Services Role
2. Configure Active Directory Domain Services
3. Configure Windows Time Service
4. Create DNS Forward Lookup Zone
5. Restart DNS Service
6. Verify Active Directory Domain Services
7. Create User Accounts
8. Verify Client Access to Active Directory Domain
9. Add Red Hat Enterprise Linux 6 Server DNS A Record (*optional*)

Details on each of these steps are provided below.

Step 1. Install Active Directory Domain Services Role

- Open Server Manager from the Quick Launch toolbar
- Select Roles -> Add Roles

- The **Add Roles Wizard** opens. Select “Next” to continue.
- Under Roles select "Active Directory Domain Services"

  Note: If .NET Framework 3.5.1 is not installed you are prompted whether or not to install it. Select "Add Required Features" to continue.

- Select “Next”
- Select “Next” (after reading **Introduction to Active Directory Domain Services**)
- Select “Install” (**Confirm Installation Selections**)
- Select “Close” after confirming the Active Directory Domain Services (and if applicable .Net Framework 3.5.1) **Installation Results**.

Step 2. Configure Active Directory Domain Services

- Under **Roles Summary**, select the "Active Directory Domain Services" link
- At the top of the **Summary** section select the "Run the Active Directory Domain Services Installation Wizard (dcpromo.exe) link
- Select “Next” (**Welcome to the Active Directory Domain Services Installation Wizard)**
- Select “Next” (**Operating System Compatibility**)
- In the **Choose a Deployment Configuration** window select "Create a new domain in a new forest", then select "Next"
- Enter the Fully Qualified Domain Name (FQDN) of the new forest domain

  Note: Do not use single label domain names – e.g. mycorp, eng, finance, etc. but use a fully qualified domain name (FQDN) – e.g. mycorp.com, eng.net, finance.mycorp.com, etc.

  Example: ***demo.cloud.lab.eng.bos.redhat.com***

- Select “Next” to continue after the wizard has verified the domain name is not already in use on the local network
- Select the appropriate Forest functional level. In this case "Windows Server 2008 R2".

  Note: If this is a forest in an existing domain then select the appropriate minimum server level appropriate to your environment.

- Select “Next” to continue
- In the **Additional Domain Controller Options** window, make sure "DNS server" is selected then select “Next”
- If a static IP address was not previously configured, then the **Static IP Assignment** window warns "This computer had dynamically assigned IP address(es)" if one or more network interfaces is set to a dynamic IP.

  Depending on your configuration select either of the following options below:

"Yes, the computer will use an IP address automatically assigned
by a DHCP server (not recommended)"
...or...
"No, I will assign static IP addresses to all physical network adapters"

Note: For production servers it is ***highly recommended*** that static IP addresses be used.

- The **Active Directory Domain Services Installation Wizard** warns that no DNS has been configured yet. Select "Yes" to continue.
- Select the locations for the Active Directory domain controller database, log files and SYSVOL folders. The default locations are:

  Database folder: C:\Windows\NTDS
  Log files folder: C:\Windows\NTDS
  SYSVOL folder: C:\Windows\SYSVOL

  Note: For large installations each of these should be placed on separate volumes to maximize performance and recoverability

- Select “Next” to continue
- Enter the password for the **Directory Restore Mode Administrator Password**

  Note: Unlike regular domain user passwords this password remains constant and must remain secure and confidential. This password should be complex and at least 7 characters long. It is highly recommended not to use the administrator's password and that you securely store it.

  Example: ***restore1234!!***

- Select “Next”
- After reviewing the **Summary** window select “Next “
- After the wizard creates the Active Directory Domain select "Finish"
- Select "Restart Now" to activate the changes

Step 3. Configure Windows Time Service

- From a Command Window (Start -> Run: cmd.exe) run:

```
C:\Users\Administrator.WIN2008-SRV> w32tm /config
/manualpeerlist:"ns1.bos.redhat.com" /syncfromflags:manual /update
```

Note: Use the time server most appropriate to your environment

- To verify, enter:

```
C:\Users\Administrator.WIN2008-SRV> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 3 (secondary reference - syncd by (S)NTP)
Precision: -6 (15.625ms per tick)
Root Delay: 0.1021423s
Root Dispersion: 0.0621398s
ReferenceId: 0x0A10FF02 (source IP:  10.16.255.2)
Last Successful Sync Time: 3/20/2011 3:57:43 PM
Source: ns1.bos.redhat.com
Poll Interval: 10 (1024s)
```

Step 4. Create DNS Forward Lookup Zone

- Open Server Manager from the Quick Launch toolbar
- Select on Roles -> DNS Server
- Expand DNS Server
- Expand DNS
- Expand computer name (Win2008-srv)
- Right click "Forward Lookup Zones" and select "New Zone" from the drop-down
- The **New Zone Wizard** opens – select "Next"
- Select "Secondary zone"
- Select "Next"
- Enter Zone name: cloud.lab.eng.bos.redhat.com
- Select "Next"
- Enter the IP Address of the Master Server: 10.16.255.2
- Select "Next"
- Select "Finish"

Step 5. Restart DNS Service

- Server Manager
- Select Configuration -> Services

In the list of Services select "DNS Server"

- Select "Restart the service"

- Verify DNS is forwarding lookups. Open a Command Window and run:

```
C:\Users\Administrator.WIN2008-SRV> nslookup www.redhat.com
Server:  localhost
Address:  127.0.0.1
```

```
Non-authoritative answer:
Name:    origin-www.redhat.com
Address:  10.4.127.15
Aliases:  www.redhat.com

C:\Users\Administrator.WIN2008-SRV> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Win2008-srv
   Primary Dns Suffix  . . . . . . . : demo.cloud.lab.eng.bos.redhat.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : demo.cloud.lab.eng.bos.redhat.com

Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Broadcom BCM5708C NetXtreme II
GigE (NDIS
 VBD Client) #2
   Physical Address. . . . . . . . . : 00-1E-0B-CE-42-78
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.16.143.163(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Default Gateway . . . . . . . . . : 10.16.143.254
   DNS Servers . . . . . . . . . . . : 127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Step 6. Verify Active Directory Domain Services

- Run the **Microsoft AD DS Best Practices Analyzer**:
- Select Roles -> Active Directory Domain Services
- Scroll down to the Best Practices Analyzer
- Select "Scan This Role"

Review the results and correct any errors or warnings.

Note: The most common error is not having an NTP server set to synchronize time services. If this has not yet been done, follow the steps outlined in **Step 3. Configure Windows Time Service** before continuing.

If this has already been done, then synchronize/update by running the following:

```
C:\Users\Administrator.WIN2008-SRV> w32tm /config /computer:
{hostname}.{domain} /syncfromflags:domhier /update
```

Example:

```
C:\Users\Administrator.WIN2008-SRV> w32tm /config
/computer:Win2008-srv.demo.cloud.lab.eng.bos.redhat.com
/syncfromflags:domhier /update
```

- Open a Command Window (Start -> Run: cmd.exe) and run the dcdiag tool:

```
C:\Users\Administrator.WIN2008-SRV> dcdiag
```

- If any errors are found, run the 'dcdiag tool' in verbose mode for additional details:

```
C:\Users\Administrator.WIN2008-SRV> dcdiag /v
```

Step 7. Create User Accounts

- Open Server Manager from the Quick Launch toolbar
- Select Roles -> Active Directory Domain Services
- Select Active Directory Users and Computers
- Open **demo.cloud.lab.eng.bos.redhat.com** (Domain)
- Right click on “Users”, select "New User" and enter:

First name: **Demo** Initials: DU
Last Name: **User**
Full name: **Demo DU. User**
User logon name: **demo-user@demo.cloud.lab.eng.bos.redhat.com**

- Select "Next"
- Enter Password: ********** (e.g. - dem01234!!)
  Confirm password: ********** (e.g. - dem01234!!)
- Optionally uncheck the option “User must change password at next logon”
- Select "Password never expires"
- Select "Next"
- Select "Finish”

For more detail on Windows password policy requirements, see the following Microsoft TechNet article:

http://technet.microsoft.com/en-us/library/cc736605.aspx

Step 8. Verify Client Access to Active Directory Domain

Join Win7 Client to the domain

- Computer -> Properties
- Under "Computer name, domain and workgroup settings" right click on "Change settings"
- Under the Computer Name tab, select "Change"
- Under "Member of" click "Domain" and enter the name of the domain

*Example: **DEMO***

- In the "Windows Security" window, enter the username and password created on the Windows 2008 Server in the previous step:

User name: **demo-user**
Password: ************** (e.g. - dem01234!!)

- Select "OK"
- Select "OK" to activate the changes
- Select "Restart Now" to apply the changes

Note: After the restart, be sure to login as the new domain user:
e.g. - DEMO\demo-user

Create "Win-Data" file share (on Windows 2008 Server)

- Computer -> Open (or Start -> Computer)
- Right click on drive to share
- Select "Open"
- Select "New Folder", enter a name (e.g. - "Win-Data")
- Right click on the new folder:
  - Select "Share with"
  - Select "Specific People"
  - Enter the name of the domain user to grant file sharing access to *(eg. demo-user)*
  - Select "Add"
  - Adjust the Permission Level accordingly (e.g. - Read, Read/Write)
  - Select "Share"
  - Select "Done"

Populate "Win-Data" file share with a test file (on Windows 2008 Server)

- Computer -> Open (or Start -> Computer)
- Right click on drive containing the new share
- Select "Open"

- Right click on share folder (e.g. - “Win-Data”)
- Select “Open”
- Right click in empty folder
- Select “New”, “Text Document”
- Enter name (e.g. - “This_is_the_Win2008_server”)
- Press “Enter”
- Right click on the new file
- Select “Open”
- Enter text into the test file with Notepad

```
This file was placed in the Win-Data file share area on the  Win2008  server
```

- Select “File”, “Save”
- Select “File”, “Exit”

Verify "Win-Data" File Share Mapping (from Windows 7 Client)

- Computer -> "Map Network Drive"
- Select Drive: W:
- Enter Folder: \\Win2008-srv.demo.cloud.lab.bos.redhat.com\Win-Data

...or...

\\Win2008-srv\Win-Data (NetBIOS name)

- User name: **demo-user**
- Password: ********** (e.g. - dem01234!!)
- Select “Finish”

The new test file should be seen in the drive window. Verify write access on the Win-Data share from the Win7 client by creating a new file.

Step 9. Add Red Hat Enterprise Linux 6 Server DNS A Record (Optional)

In some configurations it may be necessary to add a DNS A (Address) record.

- Open Server Manager from the Quick Launch toolbar
- Select Roles -> DNS Server
- Expand DNS Server
- Expand DNS
- Expand computer name (Win2008-srv)
- Expand Forward Lookup Zones
- Right click on the Active Directory domain (“demo.cloud.lab.eng.bos.redhat.com”)
- Select “New Host (A or AAAA)...
- Enter Name: RHEL6-srv
- Enter IP address: 10.16.143.162
- Select “Add Host”

Appendix E: Red Hat Enterprise Linux 6 – Installation Summary

Step 1. Insert media and boot

- Red Hat Enterprise Linux can be booted from local media (DVD, Hard drive), network (NFS directory, PXE boot) or URL.

Step 2. Select “Install or upgrade an existing system”

Step 3. Media check (*optional*)

- Select “OK” to perform a media check or “Skip” to continue without checking the media.

- To verify the distribution media select “Test”. The media is then verified before the installation continues. If any errors are found a warning is issued and installation stops.

- This step takes time as each disc is fully scanned. Red Hat recommends
  this step the first time a disc is used or if a disc is suspect.
  Press “OK” after the media check has successfully completed.
  To verify additional media, insert the next disc and select “Test” for each disc.
  After each media check discs are dismounted and must be mounted in order to proceed with the installation.

Step 4. Graphical installer starts

Step 5. Choose installation Language

- Select an appropriate language then select “Next” to continue.

Step 6. Choose keyboard type

Step 7. Select storage devices

- Select “Basic Storage Devices” to install to a local disk.

Step 8. Enter hostname

- Select “Configure Network” to continue.

Step 9. Configure network

- Select the appropriate network interface. Select “Edit” to continue.

  After confirming the device MAC address is for the correct interface, check the option “Connect automatically” and select “Apply”. If the option “Connect automatically” is not selected then the network may not be available for applying updates after FirstBoot.

Step 10. Select time zone

Step 11. Enter password for root user

Step 12. Select installation type

- Select “Use All Space” and check the box “Review and modify the partitoning layout”.

Step 13. Select device

- The default device partitioning layout for boot disks creates a volume group (VG) and logical volumes (LV) for:

      - root   (lv_root)
      - home (lv_home)
      - swap (lv_swap)

  These can be customized (re-sized, re-named, etc.) as appropriate for each server installation.

Step 14. Write storage configuration to disk

- The boot disk partitions are formatted.

Step 15. Install boot loader

- Check “Install boot loader” on default device if not already enabled.

Step 16. Select software to install and optional components

- Select “Basic Server”, “Red Hat Enterprise Linux” and “Customize Now”.

- Under “Base System” accept the defaults. (Do not click on “Next”)

- Select “Servers” and select:

  - CIFS files server
  - Directory Server
  - Network Infrastructure Server
  - Print Server

- Server Platform
- System administration tools

*Do **not** click on “Next”*

- Select “Desktops” and select:

  - Desktop (GNOME)
  - Fonts
  - General Purpose Desktop (GNOME)
  - Graphical Administration Tools
  - KDE Desktop
  - Legacy X Window System compatibility
  - Remote Desktop Clients
  - X Window System

Package dependencies are checked, the installation image transferred to the hard drive and the installation begins. After the installation has successfully completed select “Reboot” to continue.

Step 17. Welcome screen (FirstBoot)

- After the system boots the welcome screen displays.

Step 18. License Information

- Select “Yes, I agree to the License Agreement”.

Step 19. Configure software updates

- Select “Yes, I'd like to register now.
- Select “I'd like to receive updates from Red Hat Network.“
- Enter the Red Hat Network user login and password.
- If the system is unable to contact Red Hat Network then the network option “Connect automatically” was probably not set in **Step 9. Configure network**. Continue on to **Step 20. Create user**. After the system boots, login as the new user and enable the network before **Step 24. Apply updates**.
- Create a profile by entering in the system name.
- Review the subscription summary.
- Software updates setup is now complete.

Step 20. Create user

- Create a user login account by entering the username, full name and password.

Step 21. Set date and time

- If NTP is in use check the box “Synchronize date and time over the network”.
- Select “Add” to enter NTP server names.

Step 22. Set Kdump options

- The defaults are fine for most installations but can be adjusted accordingly.
- Select “Yes” to acknowledge a reboot is required.
- Select “Finish” to reboot. This completes the Red Hat Enterprise Linux 6 installation.

Step 23. Login as new user

- Select the RHEL 6 user account to login.
- Enter the password and select “Log In” to continue.
- After login the desktop displays. Continue on to the next step to apply the most current updates to the system.

Step 24. Apply updates

- Run the update tool by selecting System -> Administration -> Software Update
- The first set of updates are for the update tools. Select “Install Updates”.
- Updates require super user (root) privileges. Enter the password for root (previously set in **Step 11. Enter password for root user**) and select “Authenticate” to continue.
- Select “Yes” to accept the GPG key.
- After the updates have completed select “OK”.
- After any updates are applied to the update tools themselves, the number of updates available can be seen by hovering the mouse over the update tool.
- Select the update tool to view the latest updates and descriptions. To apply them select “Install Updates”.
- The system prompts for any updates that require a reboot. At this point the installation of your Red Hat Enterprise Linux 6 server is complete.

Appendix F: References

1. Red Hat Enterprise Linux 6 Installation Guide
   Edition 1.0
   http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/pdf/
   Installation_Guide/Red_Hat_Enterprise_Linux-6-Installation_Guide-en-US.pdf

2. Red Hat Enterprise Linux 6 Deployment Guide
   Edition 1.0
   http://docs.redhat.com/docs/en-
   US/Red_Hat_Enterprise_Linux/6/pdf/Deployment_Guide/Red_Hat_Enterprise_Linux-6-
   Deployment_Guide-en-US.pdf
   Chapter 8 - Authentication Configuration

3. The Official Samba 3.5 HOWTO and Reference Guide
   http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/

4. Install and Deploy Windows Server
   August 6, 2009
   http://technet.microsoft.com/en-us/library/dd283085(WS.10).aspx

5. Active Directory Domain Services
   April 18, 2008
   http://technet.microsoft.com/en-us/library/cc770946(WS.10).aspx

6. Active Directory Lightweight Directory Services
   August 18, 2008
   http://technet.microsoft.com/en-us/library/cc731868(WS.10).aspx

7. "How do I configure kerberos for Active Directory (AD) integration on Linux?"
   Red Hat Knowledge Base Article - KB4735
   http://access.redhat.com/kb/docs/DOC-4735

8. "What changes do I need to make to nsswitch.conf for winbind to work?"
   Red Hat Knowledge Base Article - KB4762
   http://access.redhat.com/kb/docs/DOC-4762

9. "What steps do I need to follow to join a Red Hat Enterprise Linux Samba server to an Active Directory domain in security = ADS mode?"
   Red Hat Knowledge Base Article - KB3051
   http://access.redhat.com/kb/docs/DOC-3051

Appendix G: Deployment and Integration Checklist

Task	Task Description	Location	Details
Deployment Tasks			
1	Windows Server 2008 R2 Installation	Windows Server 2008 R2 Server	Appendix C
2	Active Directory Configuration	Windows Server 2008 R2 Server	Appendix D
3	Red Hat Enterprise Linux 6 Installation	Red Hat Enterprise Linux 6 Server	Appendix E
4	Install Samba	Red Hat Enterprise Linux 6 Server	Section 5.1
5	Configure Samba	Red Hat Enterprise Linux 6 Server	Section 5.2
6	Configure SELinux Security Parameters	Red Hat Enterprise Linux 6 Server	Section 5.3
7	Configure Red Hat Enterprise Linux 6 Firewall	Red Hat Enterprise Linux 6 Server	Section 5.4
8	Verify Samba	Red Hat Enterprise Linux 6 Server	Section 5.5
Integration Tasks			
9	Synchronize Time Servers	Red Hat Enterprise Linux 6 Server	Section 6.1
10	Configure DNS	Red Hat Enterprise Linux 6 Server	Section 6.2
11	Install Kerberos	Red Hat Enterprise Linux 6 Server	Section 6.3
12	Configure/Test Kerberos	Red Hat Enterprise Linux 6 Server	Section 6.4
13	Configure Authentication	Red Hat Enterprise Linux 6 Server	Section 6.5
14	Verify/Test Active Directory	Red Hat Enterprise Linux 6 Server	Section 6.6
15	Modify Samba Configuration	Red Hat Enterprise Linux 6 Server	Section 6.7