



# **Red Hat Enterprise Linux 6**

## **Managing Confined Services**

Guide to configuring services under control of SELinux



# Red Hat Enterprise Linux 6 Managing Confined Services

---

Guide to configuring services under control of SELinux

Mirek Jahoda

Red Hat Customer Content Services

mjahoda@redhat.com

Robert Krátký

Red Hat Customer Content Services

Barbora Ančincová

Red Hat Customer Content Services

## Legal Notice

Copyright © 2016 Red Hat, Inc.

This document is licensed by Red Hat under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](#). If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## Abstract

This book provides assistance to advanced users and administrators when using and configuring Security-Enhanced Linux (SELinux). It focuses on Red Hat Enterprise Linux and describes the components of SELinux as they pertain to services an advanced user or administrator might need to configure. Also included are real-world examples of configuring those services and demonstrations of how SELinux complements their operation.

## Table of Contents

<b>CHAPTER 1. INTRODUCTION</b> .....	<b>4</b>
Targeted Policy .....	5
<b>CHAPTER 2. THE APACHE HTTP SERVER</b> .....	<b>6</b>
2.1. THE APACHE HTTP SERVER AND SELINUX .....	6
2.2. TYPES .....	8
2.3. BOOLEANS .....	11
2.4. CONFIGURATION EXAMPLES .....	13
2.4.1. Running a static site .....	14
2.4.2. Sharing NFS and CIFS volumes .....	15
2.4.3. Sharing files between services .....	15
2.4.4. Changing port numbers .....	19
<b>CHAPTER 3. SAMBA</b> .....	<b>21</b>
3.1. SAMBA AND SELINUX .....	21
3.2. TYPES .....	21
3.3. BOOLEANS .....	22
3.4. CONFIGURATION EXAMPLES .....	23
3.4.1. Sharing directories you create .....	23
3.4.2. Sharing a website .....	25
<b>CHAPTER 4. FILE TRANSFER PROTOCOL</b> .....	<b>28</b>
4.1. FTP AND SELINUX .....	28
4.2. TYPES .....	29
4.3. BOOLEANS .....	30
4.4. CONFIGURATION EXAMPLES .....	31
4.4.1. Uploading to an FTP site .....	31
<b>CHAPTER 5. NETWORK FILE SYSTEM</b> .....	<b>34</b>
5.1. NFS AND SELINUX .....	34
5.2. TYPES .....	34
5.3. BOOLEANS .....	34
<b>CHAPTER 6. BERKELEY INTERNET NAME DOMAIN</b> .....	<b>37</b>
6.1. BIND AND SELINUX .....	37
6.2. TYPES .....	37
6.3. BOOLEANS .....	38
6.4. CONFIGURATION EXAMPLES .....	39
6.4.1. Dynamic DNS .....	39
<b>CHAPTER 7. CONCURRENT VERSIONING SYSTEM</b> .....	<b>40</b>
7.1. CVS AND SELINUX .....	40
7.2. TYPES .....	40
7.3. BOOLEANS .....	40
7.4. CONFIGURATION EXAMPLES .....	41
7.4.1. Setting up CVS .....	41
<b>CHAPTER 8. SQUID CACHING PROXY</b> .....	<b>44</b>
8.1. SQUID CACHING PROXY AND SELINUX .....	44
8.2. TYPES .....	46
8.3. BOOLEANS .....	47
8.4. CONFIGURATION EXAMPLES .....	47
8.4.1. Squid Connecting to Non-Standard Ports .....	47

<b>CHAPTER 9. MYSQL</b> .....	<b>50</b>
9.1. MYSQL AND SELINUX	50
9.2. TYPES	50
9.3. BOOLEANS	51
9.4. CONFIGURATION EXAMPLES	52
9.4.1. MySQL Changing Database Location	52
<b>CHAPTER 10. POSTGRESQL</b> .....	<b>55</b>
10.1. POSTGRESQL AND SELINUX	55
10.2. TYPES	55
10.3. BOOLEANS	57
10.4. CONFIGURATION EXAMPLES	57
10.4.1. PostgreSQL Changing Database Location	57
<b>CHAPTER 11. RSYNC</b> .....	<b>60</b>
11.1. RSYNC AND SELINUX	60
11.2. TYPES	60
11.3. BOOLEANS	61
11.4. CONFIGURATION EXAMPLES	61
11.4.1. Rsync as a daemon	61
<b>CHAPTER 12. POSTFIX</b> .....	<b>66</b>
12.1. POSTFIX AND SELINUX	66
12.2. TYPES	66
12.3. BOOLEANS	67
12.4. CONFIGURATION EXAMPLES	67
12.4.1. SpamAssassin and Postfix	67
<b>CHAPTER 13. DHCP</b> .....	<b>70</b>
13.1. DHCP AND SELINUX	70
13.2. TYPES	70
<b>CHAPTER 14. OPENSIFT BY RED HAT</b> .....	<b>72</b>
14.1. OPENSIFT AND SELINUX	72
14.2. TYPES	72
14.3. BOOLEANS	73
14.4. CONFIGURATION EXAMPLES	73
14.4.1. Changing the Default OpenShift Directory	73
<b>CHAPTER 15. RED HAT GLUSTER STORAGE</b> .....	<b>75</b>
15.1. RED HAT GLUSTER STORAGE AND SELINUX	75
15.2. TYPES	75
15.3. BOOLEANS	76
15.4. CONFIGURATION EXAMPLES	77
15.4.1. Labeling Gluster Bricks	77
<b>CHAPTER 16. REFERENCES</b> .....	<b>79</b>
<b>APPENDIX A. REVISION HISTORY</b> .....	<b>81</b>



## CHAPTER 1. INTRODUCTION

Security-Enhanced Linux (SELinux) is an implementation of a *mandatory access control* mechanism in the Linux kernel, checking for allowed operations after standard *discretionary access controls* are checked. It was created by the National Security Agency and can enforce rules on files and processes in a Linux system, and on their actions, based on defined policy.

Security-Enhanced Linux (SELinux) refers to files, such as directories and devices, as objects. Processes, such as a user running a command or the Mozilla Firefox application, are referred to as subjects. Most operating systems use a Discretionary Access Control (DAC) system that controls how subjects interact with objects, and how subjects interact with each other. On operating systems using DAC, users control the permissions of files (objects) that they own. For example, on Linux operating systems, users could make their home directories world-readable, inadvertently giving other users and processes (subjects) access to potentially sensitive information.

DAC access decisions are only based on user identity and ownership, ignoring other security-relevant information such as the role of the user, the function and trustworthiness of the program, and the sensitivity and integrity of the data. Each user usually has complete discretion over their files, making it difficult to enforce a system-wide security policy. Furthermore, every program run by a user inherits all of the permissions granted to the user and is free to change access to the user's files, so minimal protection is provided against malicious software. Many system services and privileged programs must run with coarse-grained privileges that far exceed their requirements, so that a flaw in any one of these programs might be exploited to obtain further system access. [1]

The following is an example of permissions used on Linux operating systems that do not run Security-Enhanced Linux (SELinux). The permissions in these examples may differ from your system. Use the `ls -l` command to view file permissions:

```
$ ls -l file1
-rwxrw-r-- 1 user1 group1 0 2010-01-29 09:17 file1
```

The first three permission bits, `rwx`, control the access rights that the Linux `user1` user (in this case, the owner) has to `file1`. The next three permission bits, `rw-`, control the access rights that the Linux `group1` group has to `file1`. The last three permission bits, `r--`, control the access rights that everyone else has to `file1`, which includes all users and processes.

Security-Enhanced Linux (SELinux) adds Mandatory Access Control (MAC) to the Linux kernel, and is enabled by default in Red Hat Enterprise Linux. A general purpose MAC architecture needs the ability to enforce an administratively-set security policy over all processes and files in the system, basing decisions on labels containing a variety of security-relevant information. When properly implemented, it enables a system to adequately defend itself and offers critical support for application security by protecting against the tampering with, and bypassing of, secured applications. MAC provides strong separation of applications that permits the safe execution of untrustworthy applications. Its ability to limit the privileges associated with executing processes limits the scope of potential damage that can result from the exploitation of vulnerabilities in applications and system services. MAC enables information to be protected from legitimate users with limited authorization as well as from authorized users who have unwittingly executed malicious applications. [2]

The following is an example of the labels containing security-relevant information that are applied to processes, Linux users, and files, on Linux operating systems that run SELinux. This information is called the SELinux context, and is viewed using the `ls -Z` command:

```
$ ls -Z file1
-rwxrw-r-- user1 group1 unconfined_u:object_r:user_home_t:s0 file1
```



In this example, SELinux provides a user (`unconfined_u`), a role (`object_r`), a type (`user_home_t`), and a level (`s0`) for the `file1` file. This information is used to make access control decisions. This example also displays the DAC rules, which are shown in the SELinux context via the `ls -Z` command. SELinux policy rules are checked after DAC rules. SELinux policy rules are not applied if DAC rules deny access first.

### Targeted Policy

When SELinux is in enforcing mode, the default policy used in Red Hat Enterprise Linux, is the targeted policy. Processes that are targeted run in a confined domain, and processes that are not targeted run in an unconfined domain. Refer to the [Targeted Policy](#) chapter in the [Security-Enhanced Linux](#) guide for more information about targeted policy and confined and unconfined processes.

---

[1] "Integrating Flexible Support for Security Policies into the Linux Operating System", by Peter Loscocco and Stephen Smalley. This paper was originally prepared for the National Security Agency and is, consequently, in the public domain. Refer to the [original paper](#) for details.

[2] "Meeting Critical Security Objectives with Security-Enhanced Linux", by Peter Loscocco and Stephen Smalley. This paper was originally prepared for the National Security Agency and is in the public domain. Refer to the [original paper](#) for details.

## CHAPTER 2. THE APACHE HTTP SERVER

The Apache HTTP Server provides an open-source HTTP server with the current HTTP standards.<sup>[3]</sup>

In Red Hat Enterprise Linux, the `httpd` package provides the Apache HTTP Server. Run the `rpm -q httpd` command to see if the `httpd` package is installed. If it is not installed and you want to use the Apache HTTP Server, run the following command as the root user to install it:

```
~]# yum install httpd
```

### 2.1. THE APACHE HTTP SERVER AND SELINUX

When SELinux is enabled, the Apache HTTP Server (`httpd`) runs confined by default. Confined processes run in their own domains, and are separated from other confined processes. If a confined process is compromised by an attacker, depending on SELinux policy configuration, an attacker's access to resources and the possible damage they can do is limited. The following example demonstrates the `httpd` processes running in their own domain. This example assumes the `httpd`, `setroubleshoot`, `setroubleshoot-server` and `policycoreutils-python` packages are installed:

1. Run the `getenforce` command to confirm SELinux is running in enforcing mode:

```
~]$ getenforce
Enforcing
```

The `getenforce` command returns `Enforcing` when SELinux is running in enforcing mode.

2. Run the `service httpd start` command as the root user to start `httpd`:

```
~]# service httpd start
Starting httpd:                                     [ OK
]
```

3. Run the `ps -eZ | grep httpd` command to view the `httpd` processes:

```
~]$ ps -eZ | grep httpd
unconfined_u:system_r:httpd_t:s0 2850 ?        00:00:00 httpd
unconfined_u:system_r:httpd_t:s0 2852 ?        00:00:00 httpd
unconfined_u:system_r:httpd_t:s0 2853 ?        00:00:00 httpd
unconfined_u:system_r:httpd_t:s0 2854 ?        00:00:00 httpd
unconfined_u:system_r:httpd_t:s0 2855 ?        00:00:00 httpd
unconfined_u:system_r:httpd_t:s0 2856 ?        00:00:00 httpd
unconfined_u:system_r:httpd_t:s0 2857 ?        00:00:00 httpd
unconfined_u:system_r:httpd_t:s0 2858 ?        00:00:00 httpd
unconfined_u:system_r:httpd_t:s0 2859 ?        00:00:00 httpd
```

The SELinux context associated with the `httpd` processes is `unconfined_u:system_r:httpd_t:s0`. The second last part of the context, `httpd_t`, is the type. A type defines a domain for processes and a type for files. In this case, the `httpd` processes are running in the `httpd_t` domain.

SELinux policy defines how processes running in confined domains (such as `httpd_t`) interact with files, other processes, and the system in general. Files must be labeled correctly to allow `httpd` access

to them. For example, `httpd` can read files labeled with the `httpd_sys_content_t` type, but cannot write to them, even if Linux (DAC) permissions allow write access. Booleans must be enabled to allow certain behavior, such as allowing scripts network access, allowing `httpd` access to NFS and CIFS volumes, and `httpd` being allowed to execute Common Gateway Interface (CGI) scripts.

When `/etc/httpd/conf/httpd.conf` is configured so `httpd` listens on a port other than TCP ports 80, 443, 488, 8008, 8009, or 8443, the `semanage port` command must be used to add the new port number to SELinux policy configuration. The following example demonstrates configuring `httpd` to listen on a port that is not already defined in SELinux policy configuration for `httpd`, and, as a consequence, `httpd` failing to start. This example also demonstrates how to then configure the SELinux system to allow `httpd` to successfully listen on a non-standard port that is not already defined in the policy. This example assumes the `httpd` package is installed. Run each command in the example as the root user:

1. Run the `service httpd status` command to confirm `httpd` is not running:

```
~]# service httpd status
httpd is stopped
```

If the output differs, run the `service httpd stop` command to stop the process:

```
~]# service httpd stop
Stopping httpd:                               [ OK
]
```

2. Run the `semanage port -l | grep -w http_port_t` command to view the ports SELinux allows `httpd` to listen on:

```
~]# semanage port -l | grep -w http_port_t
http_port_t          tcp      80, 443, 488, 8008, 8009,
8443
```

3. Edit `/etc/httpd/conf/httpd.conf` as the root user. Configure the `Listen` option so it lists a port that is not configured in SELinux policy configuration for `httpd`. In this example, `httpd` is configured to listen on port 12345:

```
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses (0.0.0.0)
#
#Listen 12.34.56.78:80
Listen 127.0.0.1:12345
```

4. Run the `service httpd start` command to start `httpd`:

```
~]# service httpd start
Starting httpd: (13)Permission denied: make_sock: could not bind to
address 127.0.0.1:12345
no listening sockets available, shutting down
Unable to open logs                               [FAILED]
```

An SELinux denial similar to the following is logged:

```
setroubleshoot: SELinux is preventing the httpd (httpd_t) from
binding to port 12345. For complete SELinux messages. run sealert -l
f18bca99-db64-4c16-9719-1db89f0d8c77
```

5. For SELinux to allow `httpd` to listen on port 12345, as used in this example, the following command is required:

```
~]# semanage port -a -t http_port_t -p tcp 12345
```

6. Run `service httpd start` again to start `httpd` and have it listen on the new port:

```
~]# service httpd start
Starting httpd:          [ OK ]
```

7. Now that SELinux has been configured to allow `httpd` to listen on a non-standard port (TCP 12345 in this example), `httpd` starts successfully on this port.
8. To prove that `httpd` is listening and communicating on TCP port 12345, open a telnet connection to the specified port and issue a HTTP GET command, as follows:

```
~]# telnet localhost 12345
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Wed, 02 Dec 2009 14:36:34 GMT
Server: Apache/2.2.13 (Red Hat)
Accept-Ranges: bytes
Content-Length: 3985
Content-Type: text/html; charset=UTF-8
[...continues...]
```

## 2.2. TYPES

The main permission control method used in SELinux targeted policy to provide advanced process isolation is Type Enforcement. All files and processes are labeled with a type: types define a SELinux domain for processes and a SELinux type for files. SELinux policy rules define how types access each other, whether it be a domain accessing a type, or a domain accessing another domain. Access is only allowed if a specific SELinux policy rule exists that allows it.

The following example creates a new file in the `/var/www/html/` directory, and shows the file inheriting the `httpd_sys_content_t` type from its parent directory (`/var/www/html/`):

1. Run the `ls -dZ /var/www/html` command to view the SELinux context of `/var/www/html/`:

```
~]$ ls -dZ /var/www/html
drwxr-xr-x root root system_u:object_r:httpd_sys_content_t:s0
/var/www/html
```

This shows `/var/www/html/` is labeled with the `httpd_sys_content_t` type.

2. Run the `touch /var/www/html/file1` command as the root user to create a new file.
3. Run the `ls -Z /var/www/html/file1` command to view the SELinux context:

```
~]$ ls -Z /var/www/html/file1
-rw-r--r-- root root unconfined_u:object_r:httpd_sys_content_t:s0
/var/www/html/file1
```

The `ls -Z` command shows `file1` labeled with the `httpd_sys_content_t` type. SELinux allows `httpd` to read files labeled with this type, but not write to them, even if Linux permissions allow write access. SELinux policy defines what types a process running in the `httpd_t` domain (where `httpd` runs) can read and write to. This helps prevent processes from accessing files intended for use by another process.

For example, `httpd` can access files labeled with the `httpd_sys_content_t` type (intended for the Apache HTTP Server), but by default, cannot access files labeled with the `samba_share_t` type (intended for Samba). Also, files in user home directories are labeled with the `user_home_t` type: by default, this prevents `httpd` from reading or writing to files in user home directories.

The following lists some of the types used with `httpd`. Different types allow you to configure flexible access:

#### `httpd_sys_content_t`

Use this type for static web content, such as `.html` files used by a static website. Files labeled with this type are accessible (read only) to `httpd` and scripts executed by `httpd`. By default, files and directories labeled with this type cannot be written to or modified by `httpd` or other processes. Note that by default, files created in or copied into `/var/www/html/` are labeled with the `httpd_sys_content_t` type.

#### `httpd_sys_script_exec_t`

Use this type for scripts you want `httpd` to execute. This type is commonly used for Common Gateway Interface (CGI) scripts in `/var/www/cgi-bin/`. By default, SELinux policy prevents `httpd` from executing CGI scripts. To allow this, label the scripts with the `httpd_sys_script_exec_t` type and enable the `httpd_enable_cgi` Boolean. Scripts labeled with `httpd_sys_script_exec_t` run in the `httpd_sys_script_t` domain when executed by `httpd`. The `httpd_sys_script_t` domain has access to other system domains, such as `postgresql_t` and `mysqld_t`.

#### `httpd_sys_rw_content_t`

Files labeled with this type can be written to by scripts labeled with the `httpd_sys_script_exec_t` type, but cannot be modified by scripts labeled with any other type. You must use the `httpd_sys_rw_content_t` type to label files that will be read from and written to by scripts labeled with the `httpd_sys_script_exec_t` type.

#### `httpd_sys_ra_content_t`

Files labeled with this type can be appended to by scripts labeled with the `httpd_sys_script_exec_t` type, but cannot be modified by scripts labeled with any other type. You must use the `httpd_sys_ra_content_t` type to label files that will be read from and appended to by scripts labeled with the `httpd_sys_script_exec_t` type.

## httpd\_unconfined\_script\_exec\_t

Scripts labeled with this type run without SELinux protection. Only use this type for complex scripts, after exhausting all other options. It is better to use this type instead of disabling SELinux protection for `httpd`, or for the entire system.



### NOTE

To see more of the available types for `httpd`, run the following command:

```
~]$ grep httpd
/etc/selinux/targeted/contexts/files/file_contexts
```

### Procedure 2.1. Changing the SELinux Context

The type for files and directories can be changed with the `chcon` command. Changes made with `chcon` do not survive a file system relabel or the `restorecon` command. SELinux policy controls whether users are able to modify the SELinux context for any given file. The following example demonstrates creating a new directory and an `index.html` file for use by `httpd`, and labeling that file and directory to allow `httpd` access to them:

1. Run the `mkdir -p /my/website` command as the root user to create a top-level directory structure to store files to be used by `httpd`.
2. Files and directories that do not match a pattern in file-context configuration may be labeled with the `default_t` type. This type is inaccessible to confined services:

```
~]$ ls -dZ /my
drwxr-xr-x root root unconfined_u:object_r:default_t:s0 /my
```

3. Run the `chcon -R -t httpd_sys_content_t /my/` command as the root user to change the type of the `/my/` directory and subdirectories, to a type accessible to `httpd`. Now, files created under `/my/website/` inherit the `httpd_sys_content_t` type, rather than the `default_t` type, and are therefore accessible to `httpd`:

```
~]# chcon -R -t httpd_sys_content_t /my/
~]# touch /my/website/index.html
~]# ls -Z /my/website/index.html
-rw-r--r-- root root unconfined_u:object_r:httpd_sys_content_t:s0
/my/website/index.html
```

Refer to the Temporary Changes: `chcon` section of the Red Hat Enterprise Linux 6 SELinux User Guide for further information about `chcon`.

Use the `semanage fcontext` command (`semanage` is provided by the `polycoreutils-python` package) to make label changes that survive a relabel and the `restorecon` command. This command adds changes to file-context configuration. Then, run `restorecon`, which reads file-context configuration, to apply the label change. The following example demonstrates creating a new directory and an `index.html` file for use by `httpd`, and persistently changing the label of that directory and file to allow `httpd` access to them:

1. Run the `mkdir -p /my/website` command as the root user to create a top-level directory structure to store files to be used by `httpd`.
2. Run the following command as the root user to add the label change to file-context configuration:

```
~]# semanage fcontext -a -t httpd_sys_content_t "/my(/.*)"?"
```

The `"/my(/.*)"?` expression means the label change applies to the `/my/` directory and all files and directories under it.

3. Run the `touch /my/website/index.html` command as the root user to create a new file.
4. Run the `restorecon -R -v /my/` command as the root user to apply the label changes (`restorecon` reads file-context configuration, which was modified by the `semanage` command in step 2):

```
~]# restorecon -R -v /my/
restorecon reset /my context unconfined_u:object_r:default_t:s0-
>system_u:object_r:httpd_sys_content_t:s0
restorecon reset /my/website context
unconfined_u:object_r:default_t:s0-
>system_u:object_r:httpd_sys_content_t:s0
restorecon reset /my/website/index.html context
unconfined_u:object_r:default_t:s0-
>system_u:object_r:httpd_sys_content_t:s0
```

Refer to the Persistent Changes: `semanage fcontext` section of the Red Hat Enterprise Linux SELinux User Guide for further information on `semanage`.

## 2.3. BOOLEANS

SELinux is based on the least level of access required for a service to run. Services can be run in a variety of ways; therefore, you need to specify how you run your services. This can be achieved via Booleans that allow parts of SELinux policy to be changed at runtime, without any knowledge of SELinux policy writing. This allows changes, such as allowing services access to NFS volumes, without reloading or recompiling SELinux policy.

To modify the state of a Boolean, use the `setsebool` command. For example, to enable the `allow_httpd_anon_write` Boolean, run the following command as the root user:

```
~]# setsebool -P allow_httpd_anon_write on
```

To disable a Boolean, using the same example, simply change `on` to `off` in the command, as shown below:

```
~]# setsebool -P allow_httpd_anon_write off
```



### NOTE

Do not use the `-P` option if you do not want `setsebool` changes to persist across reboots.

Below is a description of common Booleans available that cater for the way `httpd` is running:

#### `allow_httpd_anon_write`

When disabled, this Boolean allows `httpd` to only have read access to files labeled with the `public_content_rw_t` type. Enabling this Boolean will allow `httpd` to write to files labeled with the `public_content_rw_t` type, such as a public directory containing files for a public file transfer service.

#### `allow_httpd_mod_auth_ntlm_winbind`

Enabling this Boolean allows access to NTLM and Winbind authentication mechanisms via the `mod_auth_ntlm_winbind` module in `httpd`.

#### `allow_httpd_mod_auth_pam`

Enabling this Boolean allows access to PAM authentication mechanisms via the `mod_auth_pam` module in `httpd`.

#### `allow_httpd_sys_script_anon_write`

This Boolean defines whether or not HTTP scripts are allowed write access to files labeled with the `public_content_rw_t` type, as used in a public file transfer service.

#### `httpd_builtin_scripting`

This Boolean defines access to `httpd` scripting. Having this Boolean enabled is often required for PHP content.

#### `httpd_can_network_connect`

When disabled, this Boolean prevents HTTP scripts and modules from initiating a connection to a network or remote port. Enable this Boolean to allow this access.

#### `httpd_can_network_connect_db`

When disabled, this Boolean prevents HTTP scripts and modules from initiating a connection to database servers. Enable this Boolean to allow this access.

#### `httpd_can_network_relay`

Enable this Boolean when `httpd` is being used as a forward or reverse proxy.

#### `httpd_can_sendmail`

When disabled, this Boolean prevents HTTP modules from sending mail. This can prevent spam attacks should a vulnerability be found in `httpd`. Enable this Boolean to allow HTTP modules to send mail.

#### `httpd_dbus_avahi`

When off, this Boolean denies `httpd` access to the `avahi` service via `D-Bus`. Enable this Boolean to allow this access.

#### `httpd_enable_cgi`

When disabled, this Boolean prevents `httpd` from executing CGI scripts. Enable this Boolean to allow `httpd` to execute CGI scripts (CGI scripts must be labeled with the `httpd_sys_script_exec_t` type).



**httpd\_enable\_ftp\_server**

Enabling this Boolean will allow `httpd` to listen on the FTP port and act as an FTP server.

**httpd\_enable\_homedirs**

When disabled, this Boolean prevents `httpd` from accessing user home directories. Enable this Boolean to allow `httpd` access to user home directories; for example, content in `/home/*/*`.

**httpd\_execmem**

When enabled, this Boolean allows `httpd` to execute programs that require memory addresses that are both executable and writable. Enabling this Boolean is not recommended from a security standpoint as it reduces protection against buffer overflows, however certain modules and applications (such as Java and Mono applications) require this privilege.

**httpd\_ssi\_exec**

This Boolean defines whether or not server side include (SSI) elements in a web page can be executed.

**httpd\_tty\_comm**

This Boolean defines whether or not `httpd` is allowed access to the controlling terminal. Usually this access is not required, however in cases such as configuring an SSL certificate file, terminal access is required to display and process a password prompt.

**httpd\_unified**

When enabled, this Boolean allows `httpd_t` complete access to all of the `httpd` types (that is to execute, read, or write `sys_content_t`). When disabled, there is separation in place between web content that is read-only, writable or executable. Disabling this Boolean ensures an extra level of security but adds the administrative overhead of having to individually label scripts and other web content based on the file access that each should have.

**httpd\_use\_cifs**

Enable this Boolean to allow `httpd` access to files on CIFS volumes that are labeled with the `cifs_t` type, such as file systems mounted via Samba.

**httpd\_use\_nfs**

Enable this Boolean to allow `httpd` access to files on NFS volumes that are labeled with the `nfs_t` type, such as file systems mounted via NFS.

**NOTE**

Due to the continuous development of the SELinux policy, the list above might not contain all Booleans related to the service at all times. To list them, run the following command as root:

```
~]# semanage boolean -l | grep service_name
```

**2.4. CONFIGURATION EXAMPLES**

The following examples provide real-world demonstrations of how SELinux complements the Apache HTTP Server and how full function of the Apache HTTP Server can be maintained.

### 2.4.1. Running a static site

To create a static website, label the `.html` files for that website with the `httpd_sys_content_t` type. By default, the Apache HTTP Server cannot write to files that are labeled with the `httpd_sys_content_t` type. The following example creates a new directory to store files for a read-only website:

1. Run the `mkdir /mywebsite` command as the root user to create a top-level directory.
2. As the root user, create a `/mywebsite/index.html` file. Copy and paste the following content into `/mywebsite/index.html`:

```
<html>
<h2>index.html from /mywebsite/</h2>
</html>
```

3. To allow the Apache HTTP Server read only access to `/mywebsite/`, as well as files and subdirectories under it, label `/mywebsite/` with the `httpd_sys_content_t` type. Run the following command as the root user to add the label change to file-context configuration:

```
~]# semanage fcontext -a -t httpd_sys_content_t "/mywebsite(/.*)?"
```

4. Run the `restorecon -R -v /mywebsite` command as the root user to make the label changes:

```
~]# restorecon -R -v /mywebsite
restorecon reset /mywebsite context
unconfined_u:object_r:default_t:s0-
>system_u:object_r:httpd_sys_content_t:s0
restorecon reset /mywebsite/index.html context
unconfined_u:object_r:default_t:s0-
>system_u:object_r:httpd_sys_content_t:s0
```

5. For this example, edit `/etc/httpd/conf/httpd.conf` as the root user. Comment out the existing `DocumentRoot` option. Add a `DocumentRoot "/mywebsite"` option. After editing, these options should look as follows:

```
#DocumentRoot "/var/www/html"
DocumentRoot "/mywebsite"
```

6. Run the `service httpd status` command as the root user to see the status of the Apache HTTP Server. If the server is stopped, run the `service httpd start` command as the root user to start it. If the server is running, run the `service httpd restart` command as the root user to restart the service (this also applies any changes made to `httpd.conf`).
7. Use a web browser to navigate to `http://localhost/index.html`. The following is displayed:

```
index.html from /mywebsite/
```

## 2.4.2. Sharing NFS and CIFS volumes

By default, NFS mounts on the client side are labeled with a default context defined by policy for NFS volumes. In common policies, this default context uses the `nfs_t` type. Also, by default, Samba shares mounted on the client side are labeled with a default context defined by policy. In common policies, this default context uses the `cifs_t` type.

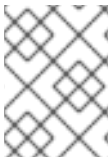
Depending on policy configuration, services may not be able to read files labeled with the `nfs_t` or `cifs_t` types. This may prevent file systems labeled with these types from being mounted and then read or exported by other services. Booleans can be enabled or disabled to control which services are allowed to access the `nfs_t` and `cifs_t` types.

Enable the `httpd_use_nfs` Boolean to allow `httpd` to access and share NFS volumes (labeled with the `nfs_t` type). Run the `setsebool` command as the root user to enable the Boolean:

```
~]# setsebool -P httpd_use_nfs on
```

Enable the `httpd_use_cifs` Boolean to allow `httpd` to access and share CIFS volumes (labeled with the `cifs_t` type). Run the `setsebool` command as the root user to enable the Boolean:

```
~]# setsebool -P httpd_use_cifs on
```



### NOTE

Do not use the `-P` option if you do not want `setsebool` changes to persist across reboots.

## 2.4.3. Sharing files between services

Type Enforcement helps prevent processes from accessing files intended for use by another process. For example, by default, Samba cannot read files labeled with the `httpd_sys_content_t` type, which are intended for use by the Apache HTTP Server. Files can be shared between the Apache HTTP Server, FTP, rsync, and Samba, if the desired files are labeled with the `public_content_t` or `public_content_rw_t` type.

The following example creates a directory and files, and allows that directory and files to be shared (read only) through the Apache HTTP Server, FTP, rsync, and Samba:

1. Run the `mkdir /shares` command as the root user to create a new top-level directory to share files between multiple services.
2. Files and directories that do not match a pattern in file-context configuration may be labeled with the `default_t` type. This type is inaccessible to confined services:

```
~]$ ls -dZ /shares
drwxr-xr-x root root unconfined_u:object_r:default_t:s0 /shares
```

3. As the root user, create a `/shares/index.html` file. Copy and paste the following content into `/shares/index.html`:

```
<html>
<body>
<p>Hello</p>
```

```
</body>
</html>
```

- Labeling `/shares/` with the `public_content_t` type allows read-only access by the Apache HTTP Server, FTP, rsync, and Samba. Run the following command as the root user to add the label change to file-context configuration:

```
~]# semanage fcontext -a -t public_content_t "/shares(/.*)?"
```

- Run the `restorecon -R -v /shares/` command as the root user to apply the label changes:

```
~]# restorecon -R -v /shares/
restorecon reset /shares context unconfined_u:object_r:default_t:s0-
>system_u:object_r:public_content_t:s0
restorecon reset /shares/index.html context
unconfined_u:object_r:default_t:s0-
>system_u:object_r:public_content_t:s0
```

To share `/shares/` through Samba:

- Run the `rpm -q samba samba-common samba-client` command to confirm the `samba`, `samba-common`, and `samba-client` packages are installed (version numbers may differ):

```
~]$ rpm -q samba samba-common samba-client
samba-3.4.0-0.41.el6.3.i686
samba-common-3.4.0-0.41.el6.3.i686
samba-client-3.4.0-0.41.el6.3.i686
```

If any of these packages are not installed, install them by running the `yum install package-name` command as the root user.

- Edit `/etc/samba/smb.conf` as the root user. Add the following entry to the bottom of this file to share the `/shares/` directory through Samba:

```
[shares]
comment = Documents for Apache HTTP Server, FTP, rsync, and Samba
path = /shares
public = yes
writable = no
```

- A Samba account is required to mount a Samba file system. Run the `smbpasswd -a username` command as the root user to create a Samba account, where `username` is an existing Linux user. For example, `smbpasswd -a testuser` creates a Samba account for the Linux `testuser` user:

```
~]# smbpasswd -a testuser
New SMB password: Enter a password
Retype new SMB password: Enter the same password again
Added user testuser.
```

Running `smbpasswd -a username`, where *username* is the user name of a Linux account that does not exist on the system, causes a **Cannot locate Unix account for '*username*'!** error.

4. Run the `service smb start` command as the root user to start the Samba service:

```
~]# service smb start
Starting SMB services:          [ OK
]
```

5. Run the `smbclient -U username -L localhost` command to list the available shares, where *username* is the Samba account added in step 3. When prompted for a password, enter the password assigned to the Samba account in step 3 (version numbers may differ):

```
~]$ smbclient -U username -L localhost
Enter username's password:
Domain=[HOSTNAME] OS=[Unix] Server=[Samba 3.4.0-0.41.e16]

Sharename      Type      Comment
-----      -
shares         Disk     Documents for Apache HTTP Server, FTP,
rsync, and Samba
IPC$           IPC      IPC Service (Samba Server Version 3.4.0-
0.41.e16)
username      Disk     Home Directories
Domain=[HOSTNAME] OS=[Unix] Server=[Samba 3.4.0-0.41.e16]

Server          Comment
-----
Workgroup       Master
-----
```

6. Run the `mkdir /test/` command as the root user to create a new directory. This directory will be used to mount the `shares` Samba share.
7. Run the following command as the root user to mount the `shares` Samba share to `/test/`, replacing *username* with the user name from step 3:

```
~]# mount //localhost/shares /test/ -o user=username
```

Enter the password for *username*, which was configured in step 3.

8. Run the `cat /test/index.html` command to view the file, which is being shared through Samba:

```
~]$ cat /test/index.html
<html>
<body>
<p>Hello</p>
</body>
</html>
```

To share `/shares/` through the Apache HTTP Server:

1. Run the `rpm -q httpd` command to confirm the `httpd` package is installed (version number may differ):

```
~]$ rpm -q httpd
httpd-2.2.11-6.i386
```

If this package is not installed, run the `yum install httpd` command as the root user to install it.

2. Change into the `/var/www/html/` directory. Run the following command as the root user to create a link (named `shares`) to the `/shares/` directory:

```
~]# ln -s /shares/ shares
```

3. Run the `service httpd start` command as the root user to start the Apache HTTP Server:

```
~]# service httpd start
Starting httpd: [ OK
]
```

4. Use a web browser to navigate to `http://localhost/shares`. The `/shares/index.html` file is displayed.





By default, the Apache HTTP Server reads an `index.html` file if it exists. If `/shares/` did not have `index.html`, and instead had `file1`, `file2`, and `file3`, a directory listing would occur when accessing `http://localhost/shares`:

1. Run the `rm -i /shares/index.html` command as the root user to remove the `index.html` file.
2. Run the `touch /shares/file{1,2,3}` command as the root user to create three files in `/shares/`:

```
~]# touch /shares/file{1,2,3}
~]# ls -Z /shares/
-rw-r--r-- root root system_u:object_r:public_content_t:s0 file1
-rw-r--r-- root root unconfined_u:object_r:public_content_t:s0
file2
-rw-r--r-- root root unconfined_u:object_r:public_content_t:s0
file3
```

3. Run the `service httpd status` command as the root user to see the status of the Apache HTTP Server. If the server is stopped, run `service httpd start` as the root user to start it.
4. Use a web browser to navigate to `http://localhost/shares`. A directory listing is displayed:

# Index of /shares

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">file1</a>	25-Feb-2009 10:11	0	
 <a href="#">file2</a>	25-Feb-2009 10:11	0	
 <a href="#">file3</a>	25-Feb-2009 10:11	0	

## 2.4.4. Changing port numbers

Depending on policy configuration, services may only be allowed to run on certain port numbers. Attempting to change the port a service runs on without changing policy may result in the service failing to start. Run the `semanage port -l | grep -w "http_port_t"` command as the root user to list the ports SELinux allows `httpd` to listen on:

```
~]# semanage port -l | grep -w http_port_t
http_port_t          tcp          80, 443, 488, 8008, 8009, 8443
```

By default, SELinux allows `httpd` to listen on TCP ports 80, 443, 488, 8008, 8009, or 8443. If `/etc/httpd/conf/httpd.conf` is configured so that `httpd` listens on any port not listed for `http_port_t`, `httpd` fails to start.

To configure `httpd` to run on a port other than TCP ports 80, 443, 488, 8008, 8009, or 8443:

1. Edit `/etc/httpd/conf/httpd.conf` as the root user so the `Listen` option lists a port that is not configured in SELinux policy for `httpd`. The following example configures `httpd` to listen on the 10.0.0.1 IP address, and on TCP port 12345:

```
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses (0.0.0.0)
#
#Listen 12.34.56.78:80
Listen 10.0.0.1:12345
```

2. Run the `semanage port -a -t http_port_t -p tcp 12345` command as the root user to add the port to SELinux policy configuration.
3. Run the `semanage port -l | grep -w http_port_t` command as the root user to confirm the port is added:

```
~]# semanage port -l | grep -w http_port_t
http_port_t          tcp          12345, 80, 443, 488, 8008,
8009, 8443
```

If you no longer run `httpd` on port 12345, run the `semanage port -d -t http_port_t -p tcp 12345` command as the root user to remove the port from policy configuration.

---

[3] Refer to the [Apache HTTP Server Project](#) page for more information.



## CHAPTER 3. SAMBA

Samba is an open-source implementation of the Server Message Block (SMB) and Common Internet File System (CIFS) protocols that provides file and print services between clients across various operating systems.<sup>[4]</sup>

In Red Hat Enterprise Linux, the `samba` package provides the Samba server. Run the `rpm -q samba` command to see if the `samba` package is installed. If it is not installed and you want to use Samba, run the following command as the root user to install it:

```
~]# yum install samba
```

### 3.1. SAMBA AND SELINUX

When SELinux is enabled, the Samba server (`smbd`) runs confined by default. Confined services run in their own domains, and are separated from other confined services. The following example demonstrates the `smbd` process running in its own domain. This example assumes the `samba` package is installed:

1. Run the `getenforce` command to confirm SELinux is running in enforcing mode:

```
~]$ getenforce
Enforcing
```

The `getenforce` command returns `Enforcing` when SELinux is running in enforcing mode.

2. Run the `service smb start` command as the root user to start `smbd`:

```
~]# service smb start
Starting SMB services: [ OK
]
```

3. Run the `ps -eZ | grep smb` command to view the `smbd` processes:

```
~]$ ps -eZ | grep smb
unconfined_u:system_r:smbd_t:s0 16420 ?      00:00:00 smbd
unconfined_u:system_r:smbd_t:s0 16422 ?      00:00:00 smbd
```

The SELinux context associated with the `smbd` processes is `unconfined_u:system_r:smbd_t:s0`. The second last part of the context, `smbd_t`, is the type. A type defines a domain for processes and a type for files. In this case, the `smbd` processes are running in the `smbd_t` domain.

Files must be labeled correctly to allow `smbd` to access and share them. For example, `smbd` can read and write to files labeled with the `samba_share_t` type, but by default, cannot access files labeled with the `httpd_sys_content_t` type, which is intended for use by the Apache HTTP Server. Booleans must be enabled to allow certain behavior, such as allowing home directories and NFS volumes to be exported through Samba, as well as to allow Samba to act as a domain controller.

### 3.2. TYPES

The main permission control method used in SELinux targeted policy to provide advanced process

isolation is Type Enforcement. All files and processes are labeled with a type: types define a SELinux domain for processes and a SELinux type for files. SELinux policy rules define how types access each other, whether it be a domain accessing a type, or a domain accessing another domain. Access is only allowed if a specific SELinux policy rule exists that allows it.

Label files with the `samba_share_t` type to allow Samba to share them. Only label files you have created, and do not relabel system files with the `samba_share_t` type: Booleans can be enabled to share such files and directories. SELinux allows Samba to write to files labeled with the `samba_share_t` type, as long as `/etc/samba/smb.conf` and Linux permissions are set accordingly.

The `samba_etc_t` type is used on certain files in `/etc/samba/`, such as `smb.conf`. Do not manually label files with the `samba_etc_t` type. If files in `/etc/samba/` are not labeled correctly, run the `restorecon -R -v /etc/samba` command as the root user to restore such files to their default contexts. If `/etc/samba/smb.conf` is not labeled with the `samba_etc_t` type, the `service smb start` command may fail and an SELinux denial may be logged. The following is an example denial when `/etc/samba/smb.conf` was labeled with the `httpd_sys_content_t` type:

```
setroubleshoot: SELinux is preventing smbd (smbd_t) "read" to ./smb.conf
(httpd_sys_content_t). For complete SELinux messages. run sealert -l
deb33473-1069-482b-bb50-e4cd05ab18af
```

### 3.3. BOOLEANS

SELinux is based on the least level of access required for a service to run. Services can be run in a variety of ways; therefore, you need to specify how you run your services. Use the following Booleans to set up SELinux:

#### `allow_smbd_anon_write`

Having this Boolean enabled allows `smbd` to write to a public directory, such as an area reserved for common files that otherwise has no special access restrictions.

#### `samba_create_home_dirs`

Having this Boolean enabled allows Samba to create new home directories independently. This is often done by mechanisms such as PAM.

#### `samba_domain_controller`

When enabled, this Boolean allows Samba to act as a domain controller, as well as giving it permission to execute related commands such as `useradd`, `groupadd` and `passwd`.

#### `samba_enable_home_dirs`

Enabling this Boolean allows Samba to share users' home directories.

#### `samba_export_all_ro`

Export any file or directory, allowing read-only permissions. This allows files and directories that are not labeled with the `samba_share_t` type to be shared through Samba. When the `samba_export_all_ro` Boolean is on, but the `samba_export_all_rw` Boolean is off, write access to Samba shares is denied, even if write access is configured in `/etc/samba/smb.conf`, as well as Linux permissions allowing write access.

#### `samba_export_all_rw`

Export any file or directory, allowing read and write permissions. This allows files and directories that are not labeled with the `samba_share_t` type to be exported through Samba. Permissions in `/etc/samba/smb.conf` and Linux permissions must be configured to allow write access.

### `samba_run_unconfined`

Having this Boolean enabled allows Samba to run unconfined scripts in the `/var/lib/samba/scripts/` directory.

### `samba_share_fusefs`

This Boolean must be enabled for Samba to share fusefs file systems.

### `samba_share_nfs`

Disabling this Boolean prevents `smbd` from having full access to NFS shares via Samba. Enabling this Boolean will allow Samba to share NFS volumes.

### `use_samba_home_dirs`

Enable this Boolean to use a remote server for Samba home directories.

### `virt_use_samba`

Allow virtual machine access to CIFS files.



#### NOTE

Due to the continuous development of the SELinux policy, the list above might not contain all Booleans related to the service at all times. To list them, run the following command as root:

```
~]# semanage boolean -l | grep service_name
```

## 3.4. CONFIGURATION EXAMPLES

The following examples provide real-world demonstrations of how SELinux complements the Samba server and how full function of the Samba server can be maintained.

### 3.4.1. Sharing directories you create

The following example creates a new directory, and shares that directory through Samba:

1. Run the `rpm -q samba samba-common samba-client` command to confirm the `samba`, `samba-common`, and `samba-client` packages are installed. If any of these packages are not installed, install them by running the `yum install package-name` command as the root user.
2. Run the `mkdir /myshare` command as the root user to create a new top-level directory to share files through Samba.
3. Run the `touch /myshare/file1` command as the root user to create an empty file. This file is used later to verify the Samba share mounted correctly.

- SELinux allows Samba to read and write to files labeled with the `samba_share_t` type, as long as `/etc/samba/smb.conf` and Linux permissions are set accordingly. Run the following command as the root user to add the label change to file-context configuration:

```
~]# semanage fcontext -a -t samba_share_t "/myshare(/.*)?"
```

- Run the `restorecon -R -v /myshare` command as the root user to apply the label changes:

```
~]# restorecon -R -v /myshare
restorecon reset /myshare context
unconfined_u:object_r:default_t:s0-
>system_u:object_r:samba_share_t:s0
restorecon reset /myshare/file1 context
unconfined_u:object_r:default_t:s0-
>system_u:object_r:samba_share_t:s0
```

- Edit `/etc/samba/smb.conf` as the root user. Add the following to the bottom of this file to share the `/myshare/` directory through Samba:

```
[myshare]
comment = My share
path = /myshare
public = yes
writable = no
```

- A Samba account is required to mount a Samba file system. Run the `smbpasswd -a username` command as the root user to create a Samba account, where *username* is an existing Linux user. For example, `smbpasswd -a testuser` creates a Samba account for the Linux `testuser` user:

```
~]# smbpasswd -a testuser
New SMB password: Enter a password
Retype new SMB password: Enter the same password again
Added user testuser.
```

Running `smbpasswd -a username`, where *username* is the user name of a Linux account that does not exist on the system, causes a **Cannot locate Unix account for '*username*'!** error.

- Run the `service smb start` command as the root user to start the Samba service:

```
~]# service smb start
Starting SMB services: [ OK
]
```

- Run the `smbclient -U username -L localhost` command to list the available shares, where *username* is the Samba account added in step 7. When prompted for a password, enter the password assigned to the Samba account in step 7 (version numbers may differ):

```
~]$ smbclient -U username -L localhost
Enter username's password:
```

```

Domain=[HOSTNAME] OS=[Unix] Server=[Samba 3.4.0-0.41.el6]

Sharename      Type      Comment
-----      -
myshare        Disk      My share
IPC$           IPC       IPC Service (Samba Server Version 3.4.0-
0.41.el6)
username       Disk      Home Directories
Domain=[HOSTNAME] OS=[Unix] Server=[Samba 3.4.0-0.41.el6]

Server          Comment
-----
Workgroup       Master
-----

```

10. Run the `mkdir /test/` command as the root user to create a new directory. This directory will be used to mount the `myshare` Samba share.
11. Run the following command as the root user to mount the `myshare` Samba share to `/test/`, replacing `username` with the user name from step 7:

```
~]# mount //localhost/myshare /test/ -o user=username
```

Enter the password for `username`, which was configured in step 7.

12. Run the `ls /test/` command to view the `file1` file created in step 3:

```
~]$ ls /test/
file1
```

### 3.4.2. Sharing a website

It may not be possible to label files with the `samba_share_t` type, for example, when wanting to share a website in `/var/www/html/`. For these cases, use the `samba_export_all_ro` Boolean to share any file or directory (regardless of the current label), allowing read only permissions, or the `samba_export_all_rw` Boolean to share any file or directory (regardless of the current label), allowing read and write permissions.

The following example creates a file for a website in `/var/www/html/`, and then shares that file through Samba, allowing read and write permissions. This example assumes the `httpd`, `samba`, `samba-common`, `samba-client`, and `wget` packages are installed:

1. As the root user, create a `/var/www/html/file1.html` file. Copy and paste the following content into `/var/www/html/file1.html`:

```
<html>
<h2>File being shared through the Apache HTTP Server and Samba.</h2>
</html>
```

2. Run the `ls -Z /var/www/html/file1.html` command to view the SELinux context of `file1.html`:

```
~]$ ls -Z /var/www/html/file1.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0
/var/www/html/file1.html
```

`file1.index.html` is labeled with the `httpd_sys_content_t`. By default, the Apache HTTP Server can access this type, but Samba cannot.

3. Run the `service httpd start` command as the root user to start the Apache HTTP Server:

```
~]# service httpd start
Starting httpd:                                     [ OK
]
```

4. Change into a directory your user has write access to, and run the `wget http://localhost/file1.html` command. Unless there are changes to the default configuration, this command succeeds:

```
~]$ wget http://localhost/file1.html
Resolving localhost... 127.0.0.1
Connecting to localhost|127.0.0.1|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 84 [text/html]
Saving to: `file1.html.1'

100%[=====>] 84          --.-K/s   in 0s

`file1.html.1' saved [84/84]
```

5. Edit `/etc/samba/smb.conf` as the root user. Add the following to the bottom of this file to share the `/var/www/html/` directory through Samba:

```
[website]
comment = Sharing a website
path = /var/www/html/
public = no
writable = no
```

6. The `/var/www/html/` directory is labeled with the `httpd_sys_content_t` type. By default, Samba cannot access files and directories labeled with the `httpd_sys_content_t` type, even if Linux permissions allow it. To allow Samba access, run the following command as the root user to enable the `samba_export_all_ro` Boolean:

```
~]# setsebool -P samba_export_all_ro on
```

Do not use the `-P` option if you do not want the change to persist across reboots. Note that enabling the `samba_export_all_ro` Boolean allows Samba to access any type.

7. Run `service smb start` as the root user to start `smbd`:

```
~]# service smb start
Starting SMB services:                               [ OK
]
```

---

[4] Refer to the official [Samba](#) website for more information.

## CHAPTER 4. FILE TRANSFER PROTOCOL

File Transfer Protocol (FTP) is one of the oldest and most commonly used protocols found on the Internet today. Its purpose is to reliably transfer files between computer hosts on a network without requiring the user to log directly into the remote host or have knowledge of how to use the remote system. It allows users to access files on remote systems using a standard set of simple commands.

The Very Secure FTP Daemon (**vsftpd**) is designed from the ground up to be fast, stable, and, most importantly, secure. Its ability to handle large numbers of connections efficiently and securely is why **vsftpd** is the only stand-alone FTP distributed with Red Hat Enterprise Linux.

In Red Hat Enterprise Linux, the **vsftpd** package provides the Very Secure FTP daemon. Run the `rpm -q vsftpd` command to see if **vsftpd** is installed:

```
~]$ rpm -q vsftpd
```

If you want an FTP server and the **vsftpd** package is not installed, run the following command as the root user to install it:

```
~]# yum install vsftpd
```

### 4.1. FTP AND SELINUX

The **vsftpd** FTP daemon runs confined by default. SELinux policy defines how **vsftpd** interacts with files, processes, and with the system in general. For example, when an authenticated user logs in via FTP, they cannot read from or write to files in their home directories: SELinux prevents **vsftpd** from accessing user home directories by default. Also, by default, **vsftpd** does not have access to NFS or CIFS volumes, and anonymous users do not have write access, even if such write access is configured in `/etc/vsftpd/vsftpd.conf`. Booleans can be enabled to allow the previously mentioned access.

The following example demonstrates an authenticated user logging in, and an SELinux denial when trying to view files in their home directory:

1. Run the `rpm -q ftp` command to see if the **ftp** package is installed. If it is not, run the `yum install ftp` command as the root user to install it.
2. Run the `rpm -q vsftpd` command to see if the **vsftpd** package is installed. If it is not, run the `yum install vsftpd` command as the root user to install it.
3. In Red Hat Enterprise Linux, **vsftpd** only allows anonymous users to log in by default. To allow authenticated users to log in, edit `/etc/vsftpd/vsftpd.conf` as the root user. Make sure the `local_enable=YES` option is uncommented:

```
# Uncomment this to allow local users to log in.  
local_enable=YES
```

4. Run the `service vsftpd start` command as the root user to start **vsftpd**. If the service was running before editing `vsftpd.conf`, run the `service vsftpd restart` command as the root user to apply the configuration changes:

```
~]# service vsftpd start  
Starting vsftpd for vsftpd: [ OK  
]
```



- 5. Run the `ftp localhost` command as the user you are currently logged in with. When prompted for your name, make sure your user name is displayed. If the correct user name is displayed, press **Enter**, otherwise, enter the correct user name:

```
~] ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPD 2.1.0)
Name (localhost:username):
331 Please specify the password.
Password: Enter your password
500 OOPS: cannot change directory:/home/username
Login failed.
ftp>
```

- 6. An SELinux denial similar to the following is logged:

```
setroubleshoot: SELinux is preventing the ftp daemon from reading
users home directories (username). For complete SELinux messages.
run sealert -l c366e889-2553-4c16-b73f-92f36a1730ce
```

- 7. Access to home directories has been denied by SELinux. This can be fixed by activating the `ftp_home_dir` Boolean. Enable this `ftp_home_dir` Boolean by running the following command as the root user:

```
~]# setsebool -P ftp_home_dir=1
```



#### NOTE

Do not use the `-P` option if you do not want changes to persist across reboots.

Try to log in again. Now that SELinux is allowing access to home directories via the `ftp_home_dir` Boolean, logging in will succeed.

## 4.2. TYPES

The main permission control method used in SELinux targeted policy to provide advanced process isolation is Type Enforcement. All files and processes are labeled with a type: types define a SELinux domain for processes and a SELinux type for files. SELinux policy rules define how types access each other, whether it be a domain accessing a type, or a domain accessing another domain. Access is only allowed if a specific SELinux policy rule exists that allows it.

By default, anonymous users have read access to files in `/var/ftp/` when they log in via FTP. This directory is labeled with the `public_content_t` type, allowing only read access, even if write access is configured in `/etc/vsftpd/vsftpd.conf`. The `public_content_t` type is accessible to other services, such as Apache HTTP Server, Samba, and NFS.

Use one of the following types to share files through FTP:

#### `public_content_t`

Label files and directories you have created with the `public_content_t` type to share them read-only through vsftpd. Other services, such as Apache HTTP Server, Samba, and NFS, also have

access to files labeled with this type. Files labeled with the `public_content_t` type cannot be written to, even if Linux permissions allow write access. If you require write access, use the `public_content_rw_t` type.

#### `public_content_rw_t`

Label files and directories you have created with the `public_content_rw_t` type to share them with read and write permissions through `vsftpd`. Other services, such as Apache HTTP Server, Samba, and NFS, also have access to files labeled with this type. Remember that Booleans for each service must be enabled before they can write to files labeled with this type.

### 4.3. BOOLEANS

SELinux is based on the least level of access required for a service to run. Services can be run in a variety of ways; therefore, you need to specify how you run your services. Use the following Booleans to set up SELinux:

#### `allow_ftp_anon_write`

When disabled, this Boolean prevents `vsftpd` from writing to files and directories labeled with the `public_content_rw_t` type. Enable this Boolean to allow users to upload files via FTP. The directory where files are uploaded to must be labeled with the `public_content_rw_t` type and Linux permissions set accordingly.

#### `allow_ftp_full_access`

When this Boolean is on, only Linux (DAC) permissions are used to control access, and authenticated users can read and write to files that are not labeled with the `public_content_t` or `public_content_rw_t` types.

#### `allow_ftp_use_cifs`

Having this Boolean enabled allows `vsftpd` to access files and directories labeled with the `cifs_t` type; therefore, having this Boolean enabled allows you to share file systems mounted via Samba through `vsftpd`.

#### `allow_ftp_use_nfs`

Having this Boolean enabled allows `vsftpd` to access files and directories labeled with the `nfs_t` type; therefore, having this Boolean enabled allows you to share file systems mounted via NFS through `vsftpd`.

#### `ftp_home_dir`

Having this Boolean enabled allows authenticated users to read and write to files in their home directories. When this Boolean is off, attempting to download a file from a home directory results in an error such as `550 Failed to open file`. An SELinux denial is logged.

#### `ftpd_connect_db`

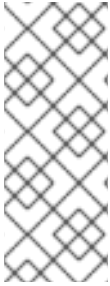
Allow FTP daemons to initiate a connection to a database.

#### `httpd_enable_ftp_server`

Allow `httpd` to listen on the FTP port and act as a FTP server.

## tftp\_anon\_write

Having this Boolean enabled allows TFTP access to a public directory, such as an area reserved for common files that otherwise has no special access restrictions.



### NOTE

Due to the continuous development of the SELinux policy, the list above might not contain all Booleans related to the service at all times. To list them, run the following command as root:

```
~]# semanage boolean -l | grep service_name
```

## 4.4. CONFIGURATION EXAMPLES

### 4.4.1. Uploading to an FTP site

The following example creates an FTP site that allows a dedicated user to upload files. It creates the directory structure and the required SELinux configuration changes:

1. Run the `setsebool tftp_home_dir=1` command as the root user to enable access to FTP home directories.
2. Run the `mkdir -p /myftp/pub` command as the root user to create a new top-level directory.
3. Set Linux permissions on the `/myftp/pub/` directory to allow a Linux user write access. This example changes the owner and group from root to owner `user1` and group root. Replace `user1` with the user you want to give write access to:

```
~]# chown user1:root /myftp/pub
~]# chmod 775 /myftp/pub
```

The `chown` command changes the owner and group permissions. The `chmod` command changes the mode, allowing the `user1` user read, write, and execute permissions, and members of the root group read, write, and execute permissions. Everyone else has read and execute permissions, which allows the Apache HTTP Server to read files from this directory.

4. When running SELinux, files and directories must be labeled correctly to allow access. Setting Linux permissions is not enough. Files labeled with the `public_content_t` type allow them to be read by FTP, Apache HTTP Server, Samba, and rsync. Files labeled with the `public_content_rw_t` type can be written to by FTP. Other services, such as Samba, require Booleans to be set before they can write to files labeled with the `public_content_rw_t` type. Label the top-level directory (`/myftp/`) with the `public_content_t` type, to prevent copied or newly-created files under `/myftp/` from being written to or modified by services. Run the following command as the root user to add the label change to file-context configuration:

```
~]# semanage fcontext -a -t public_content_t /myftp
```

5. Run the `restorecon -R -v /myftp/` command to apply the label change:

```
~]# restorecon -R -v /myftp/
restorecon reset /myftp context unconfined_u:object_r:default_t:s0-
>system_u:object_r:public_content_t:s0
```

6. Confirm `/myftp` is labeled with the `public_content_t` type, and `/myftp/pub/` is labeled with the `default_t` type:

```
~]$ ls -dZ /myftp/
drwxr-xr-x. root root system_u:object_r:public_content_t:s0 /myftp/
~]$ ls -dZ /myftp/pub/
drwxrwxr-x. user1 root unconfined_u:object_r:default_t:s0
/myftp/pub/
```

7. FTP must be allowed to write to a directory before users can upload files via FTP. SELinux allows FTP to write to directories labeled with the `public_content_rw_t` type. This example uses `/myftp/pub/` as the directory FTP can write to. Run the following command as the root user to add the label change to file-context configuration:

```
~]# semanage fcontext -a -t public_content_rw_t "/myftp/pub(/.*)?"
```

8. Run the `restorecon -R -v /myftp/pub` command as the root user to apply the label change:

```
~]# restorecon -R -v /myftp/pub
restorecon reset /myftp/pub context system_u:object_r:default_t:s0-
>system_u:object_r:public_content_rw_t:s0
```

9. The `allow_ftpd_anon_write` Boolean must be on to allow `vsftpd` to write to files that are labeled with the `public_content_rw_t` type. Run the following command as the root user to enable this Boolean:

```
~]# setsebool -P allow_ftpd_anon_write on
```

Do not use the `-P` option if you do not want changes to persist across reboots.

The following example demonstrates logging in via FTP and uploading a file. This example uses the `user1` user from the previous example, where `user1` is the dedicated owner of the `/myftp/pub/` directory:

1. Run the `cd ~/` command to change into your home directory. Then, run the `mkdir myftp` command to create a directory to store files to upload via FTP.
2. Run the `cd ~/myftp` command to change into the `~/myftp/` directory. In this directory, create an `ftpupload` file. Copy the following contents into this file:

```
File upload via FTP from a home directory.
```

3. Run the `getsebool allow_ftpd_anon_write` command to confirm the `allow_ftpd_anon_write` Boolean is on:

```
~]$ getsebool allow_ftpd_anon_write
allow_ftpd_anon_write --> on
```

-

If this Boolean is off, run the `setsebool -P allow_ftp_anon_write` on command as the root user to enable it. Do not use the `-P` option if you do not want the change to persist across reboots.

4. Run the `service vsftpd start` command as the root user to start `vsftpd`:

```
~]# service vsftpd start
Starting vsftpd for vsftpd: [ OK
]
```

5. Run the `ftp localhost` command. When prompted for a user name, enter the user name of the user who has write access, then, enter the correct password for that user:

```
~]$ ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.1.0)
Name (localhost:username):
331 Please specify the password.
Password: Enter the correct password
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd myftp
250 Directory successfully changed.
ftp> put ftpupload
local: ftpupload remote: ftpupload
227 Entering Passive Mode (127,0,0,1,241,41).
150 Ok to send data.
226 File receive OK.
ftp> 221 Goodbye.
```

The upload succeeds as the `allow_ftp_anon_write` Boolean is enabled.

## CHAPTER 5. NETWORK FILE SYSTEM

A Network File System (NFS) allows remote hosts to mount file systems over a network and interact with those file systems as though they are mounted locally. This enables system administrators to consolidate resources onto centralized servers on the network.<sup>[5]</sup>

In Red Hat Enterprise Linux, the `nfs-utils` package is required for full NFS support. Run the `rpm -q nfs-utils` command to see if the `nfs-utils` is installed. If it is not installed and you want to use NFS, run the following command as the root user to install it:

```
~]# yum install nfs-utils
```

### 5.1. NFS AND SELINUX

When running SELinux, the NFS daemons are confined by default. SELinux policy allows NFS to share files by default.

### 5.2. TYPES

The main permission control method used in SELinux targeted policy to provide advanced process isolation is Type Enforcement. All files and processes are labeled with a type: types define a SELinux domain for processes and a SELinux type for files. SELinux policy rules define how types access each other, whether it be a domain accessing a type, or a domain accessing another domain. Access is only allowed if a specific SELinux policy rule exists that allows it.

By default, mounted NFS volumes on the client side are labeled with a default context defined by policy for NFS. In common policies, this default context uses the `nfs_t` type. The following types are used with NFS. Different types allow you to configure flexible access:

#### `var_lib_nfs_t`

This type is used for existing and new files copied to or created in the `/var/lib/nfs/` directory. This type should not need to be changed in normal operation. To restore changes to the default settings, run the `restorecon -R -v /var/lib/nfs` command as the root user.

#### `nfdsd_exec_t`

The `/usr/sbin/rpc.nfsd` file is labeled with the `nfdsd_exec_t`, as are other system executables and libraries related to NFS. Users should not label any files with this type. `nfdsd_exec_t` will transition to `nfdsd_t`.

### 5.3. BOOLEANS

SELinux is based on the least level of access required for a service to run. Services can be run in a variety of ways; therefore, you need to specify how you run your services. Use the following Booleans to set up SELinux:

#### `allow_ftpd_use_nfs`

When enabled, this Boolean allows the `ftpd` daemon to access NFS volumes.

#### `cobbler_use_nfs`

When enabled, this Boolean allows the `cobblerd` daemon to access NFS volumes.

**git\_system\_use\_nfs**

When enabled, this Boolean allows the Git system daemon to read system shared repositories on NFS volumes.

**httpd\_use\_nfs**

When enabled, this Boolean allows the `httpd` daemon to access files stored on NFS volumes.

**qemu\_use\_nfs**

When enabled, this Boolean allows Qemu to use NFS volumes.

**rsync\_use\_nfs**

When enabled, this Boolean allows `rsync` servers to share NFS volumes.

**samba\_share\_nfs**

When enabled, this Boolean allows the `smbd` daemon to share NFS volumes. When disabled, this Boolean prevents `smbd` from having full access to NFS shares via Samba.

**sanlock\_use\_nfs**

When enabled, this Boolean allows the `sanlock` daemon to manage NFS volumes.

**sge\_use\_nfs**

When enabled, this Boolean allows the `sge` scheduler to access NFS volumes.

**use\_nfs\_home\_dirs**

When enabled, this Boolean adds support for NFS home directories.

**virt\_use\_nfs**

When enabled, this Boolean allows confident virtual guests to manage files on NFS volumes.

**xen\_use\_nfs**

When enabled, this Boolean allows Xen to manage files on NFS volumes.

**git\_cgi\_use\_nfs**

When enabled, this Boolean allows the Git Common Gateway Interface (CGI) to access NFS volumes.

**tftp\_use\_nfs**

When enabled, this Boolean allows The Trivial File Transfer Protocol (TFTP) to read from NFS volumes for public file transfer services.

**NOTE**

Due to the continuous development of the SELinux policy, the list above might not contain all Booleans related to the service at all times. To list them, run the following command as root:

```
~]# semanage boolean -l | grep service_name
```

---

[5] Refer to the [Storage Administration Guide](#) for more information.



## CHAPTER 6. BERKELEY INTERNET NAME DOMAIN

BIND performs name resolution services via the `named` daemon. BIND lets users locate computer resources and services by name instead of numerical addresses.

In Red Hat Enterprise Linux, the `bind` package provides a DNS server. Run the `rpm -q bind` command to see if the `bind` package is installed. If it is not installed, run the following command as the root user to install it:

```
~]# yum install bind
```

### 6.1. BIND AND SELINUX

The default permissions on the `/var/named/slaves/`, `/var/named/dynamic/` and `/var/named/data/` directories allow zone files to be updated via zone transfers and dynamic DNS updates. Files in `/var/named/` are labeled with the `named_zone_t` type, which is used for master zone files.

For a slave server, configure `/etc/named.conf` to place slave zones in `/var/named/slaves/`. The following is an example of a domain entry in `/etc/named.conf` for a slave DNS server that stores the zone file for `testdomain.com` in `/var/named/slaves/`:

```
zone "testdomain.com" {
    type slave;
    masters { IP-address; };
    file "/var/named/slaves/db.testdomain.com";
};
```

If a zone file is labeled `named_zone_t`, the `named_write_master_zones` Boolean must be enabled to allow zone transfers and dynamic DNS to update the zone file. Also, the mode of the parent directory has to be changed to allow the `named` user or group read, write and execute access.

If zone files in `/var/named/` are labeled with the `named_cache_t` type, a file system relabel or running `restorecon -R /var/` will change their type to `named_zone_t`.

### 6.2. TYPES

The main permission control method used in SELinux targeted policy to provide advanced process isolation is Type Enforcement. All files and processes are labeled with a type: types define a SELinux domain for processes and a SELinux type for files. SELinux policy rules define how types access each other, whether it be a domain accessing a type, or a domain accessing another domain. Access is only allowed if a specific SELinux policy rule exists that allows it.

The following types are used with BIND. Different types allow you to configure flexible access:

#### `named_zone_t`

Used for master zone files. Other services cannot modify files of this type. `named` can only modify files of this type if the `named_write_master_zones` Boolean is enabled.

#### `named_cache_t`

By default, `named` can write to files labeled with this type, without additional Booleans being set. Files copied or created in the `/var/named/slaves/`, `/var/named/dynamic/` and `/var/named/data/` directories are automatically labeled with the `named_cache_t` type.

#### `named_var_run_t`

Files copied or created in the `/var/run/bind/`, `/var/run/named/`, and `/var/run/unbound/` directories are automatically labeled with the `named_var_run_t` type.

#### `named_conf_t`

BIND-related configuration files, usually stored in the `/etc/` directory, are automatically labeled with the `named_conf_t` type.

#### `named_exec_t`

BIND-related executable files, usually stored in the `/usr/sbin/` directory, are automatically labeled with the `named_exec_t` type.

#### `named_log_t`

BIND-related log files, usually stored in the `/var/log/` directory, are automatically labeled with the `named_log_t` type.

#### `named_initrc_exec_t`

Executable BIND-related files in the `/etc/rc.d/init.d/` directory are automatically labeled with the `named_initrc_exec_t` type.

## 6.3. BOOLEANS

SELinux is based on the least level of access required for a service to run. Services can be run in a variety of ways; therefore, you need to specify how you run your services. Use the following Booleans to set up SELinux:

#### `named_write_master_zones`

When disabled, this Boolean prevents `named` from writing to zone files or directories labeled with the `named_zone_t` type. `named` does not usually need to write to zone files; but in the case that it needs to, or if a secondary server needs to write to zone files, enable this Boolean to allow this action.

#### `named_bind_http_port`

When enabled, this Boolean allows BIND to bind an Apache port.



#### NOTE

Due to the continuous development of the SELinux policy, the list above might not contain all Booleans related to the service at all times. To list them, run the following command as root:

```
~]# semanage boolean -l | grep service_name
```

## 6.4. CONFIGURATION EXAMPLES

### 6.4.1. Dynamic DNS

BIND allows hosts to update their records in DNS and zone files dynamically. This is used when a host computer's IP address changes frequently and the DNS record requires real-time modification.

Use the `/var/named/dynamic/` directory for zone files you want updated via dynamic DNS. Files created in or copied into `/var/named/dynamic/` inherit Linux permissions that allow `named` to write to them. As such files are labeled with the `named_cache_t` type, SELinux allows `named` to write to them.

If a zone file in `/var/named/dynamic/` is labeled with the `named_zone_t` type, dynamic DNS updates may not be successful for a certain period of time as the update needs to be written to a journal first before being merged. If the zone file is labeled with the `named_zone_t` type when the journal attempts to be merged, an error such as the following is logged:

```
named[PID]: dumping master file: rename: /var/named/dynamic/zone-name:
permission denied
```

Also, the following SELinux denial is logged:

```
setroubleshoot: SELinux is preventing named (named_t) "unlink" to zone-
name (named_zone_t)
```

To resolve this labeling issue, run the `restorecon -R -v /var/named/dynamic` command as the Linux root user.

## CHAPTER 7. CONCURRENT VERSIONING SYSTEM

The Concurrent Versioning System (CVS) is a free revision-control system. It is used to monitor and keep track of modifications to a central set of files which are usually accessed by several different users. It is commonly used by programmers to manage a source code repository and is widely used by open source programmers.

In Red Hat Enterprise Linux, the `cv`s package provides CVS. Run the `rpm -q cvs` command to see if the `cv`s package is installed. If it is not installed and you want to use CVS, run the following command as the root user to install it:

```
~]# yum install cvs
```

### 7.1. CVS AND SELINUX

The `cv`s daemon runs as `cv`s\_`t`. By default in Red Hat Enterprise Linux, CVS is only allowed to read and write certain directories. The label `cv`s\_`data_t` defines which areas the `cv`s daemon has read and write access to. When using CVS with SELinux, assigning the correct label is essential for clients to have full access to the area reserved for CVS data.

### 7.2. TYPES

The main permission control method used in SELinux targeted policy to provide advanced process isolation is Type Enforcement. All files and processes are labeled with a type: types define a SELinux domain for processes and a SELinux type for files. SELinux policy rules define how types access each other, whether it be a domain accessing a type, or a domain accessing another domain. Access is only allowed if a specific SELinux policy rule exists that allows it.

The following types are used with CVS. Different types allow you to configure flexible access:

#### `cv`s\_`data_t`

This type is used for data in a CVS repository. CVS can only gain full access to data if it has this type.

#### `cv`s\_`exec_t`

This type is used for the `/usr/bin/cvs` binary.

### 7.3. BOOLEANS

SELinux is based on the least level of access required for a service to run. Services can be run in a variety of ways; therefore, you need to specify how you run your services. Use the following Booleans to set up SELinux:

#### `allow_cv`s\_`read_shadow`

This Boolean allows the `cv`s daemon to access the `/etc/shadow` file for user authentication.

**NOTE**

Due to the continuous development of the SELinux policy, the list above might not contain all Booleans related to the service at all times. To list them, run the following command as root:

```
~]# semanage boolean -l | grep service_name
```

## 7.4. CONFIGURATION EXAMPLES

### 7.4.1. Setting up CVS

This example describes a simple CVS setup and an SELinux configuration which allows remote access. Two hosts are used in this example; a CVS server with a host name of `cvs-srv` with an IP address of `192.168.1.1` and a client with a host name of `cvs-client` and an IP address of `192.168.1.100`. Both hosts are on the same subnet (`192.168.1.0/24`). This is an example only and assumes that the `cvs` and `xinetd` packages are installed, that the SELinux targeted policy is used, and that SELinux is running in enforced mode.

This example will show that even with full DAC permissions, SELinux can still enforce policy rules based on file labels and only allow access to certain areas that have been specifically labeled for access by CVS.

**NOTE**

Steps 1-9 should be performed on the CVS server, `cvs-srv`.

1. This example requires the `cvs` and `xinetd` packages. Run the `rpm -q cvs` command to see if the `cvs` package is installed. If it is not installed, run the following command as the root user to install `cvs`:

```
~]# yum install cvs
```

Run the `rpm -q xinetd` command to see if the `xinetd` package is installed. If it is not installed, run the following command as the root user to install `xinetd`:

```
~]# yum install xinetd
```

2. Create a group named `CVS`. This can be done via the `groupadd CVS` command as the root user, or by using the `system-config-users` tool.
3. Create a user with a user name of `cvsuser` and make this user a member of the `CVS` group. This can be done using the `system-config-users` tool.
4. Edit the `/etc/services` file and make sure that the CVS server has uncommented entries looking similar to the following:

```
cvspserver 2401/tcp # CVS client/server operations
cvspserver 2401/udp # CVS client/server operations
```

5. Create the CVS repository in the root area of the file system. When using SELinux, it is best to

have the repository in the root file system so that recursive labels can be given to it without affecting any other subdirectories. For example, as the root user, create a `/cvs/` directory to house the repository:

```
[root@cvs-srv]# mkdir /cvs
```

6. Give full permissions to the `/cvs/` directory to all users:

```
[root@cvs-srv]# chmod -R 777 /cvs
```



### WARNING

This is an example only and these permissions should not be used in a production system.

7. Edit the `/etc/xinetd.d/cvs` file and make sure that the CVS section is uncommented and configured to use the `/cvs/` directory. The file should look similar to:

```
service cvspserver
{
  disable = no
  port    = 2401
  socket_type = stream
  protocol = tcp
  wait    = no
  user    = root
  passenv = PATH
  server  = /usr/bin/cvs
  env    = HOME=/cvs
  server_args = -f --allow-root=/cvs pserver
  # bind   = 127.0.0.1
```

8. Start the `xinetd` daemon by running the `service xinetd start` command as the root user.
9. Add a rule which allows inbound connections using TCP on port 2401 by using the `system-config-firewall` tool.
10. As the `cvsuser` user, run the following command:

```
[cvsuser@cvs-client]$ cvs -d /cvs init
```

11. At this point, CVS has been configured but SELinux will still deny logins and file access. To demonstrate this, set the `$CVSROOT` variable on `cvs-client` and try to log in remotely. The following step should be performed on `cvs-client`:

```
[cvsuser@cvs-client]$ export
CVSROOT=:pserver:cvsuser@192.168.1.1:/cvs
```

```
[cvsuser@cvs-client]$  
[cvsuser@cvs-client]$ cvs login  
Logging in to :pserver:cvsuser@192.168.1.1:2401/cvs  
CVS password: *****  
cvs [login aborted]: unrecognized auth response from 192.168.100.1:  
cvs pserver: cannot open /cvs/CVSR00T/config: Permission denied
```

SELinux has blocked access. In order to get SELinux to allow this access, the following step should be performed on **cvs-srv**:

12. Change the context of the **/cvs/** directory as the root user in order to recursively label any existing and new data in the **/cvs/** directory, giving it the **cvs\_data\_t** type:

```
[root@cvs-srv]# semanage fcontext -a -t cvs_data_t '/cvs(/.*)?'  
[root@cvs-srv]# restorecon -R -v /cvs
```

13. The client, **cvs-client** should now be able to log in and access all CVS resources in this repository:

```
[cvsuser@cvs-client]$ export  
CVSR00T=:pserver:cvsuser@192.168.1.1:/cvs  
[cvsuser@cvs-client]$  
[cvsuser@cvs-client]$ cvs login  
Logging in to :pserver:cvsuser@192.168.1.1:2401/cvs  
CVS password: *****  
[cvsuser@cvs-client]$
```

## CHAPTER 8. SQUID CACHING PROXY

Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects. It reduces bandwidth and improves response times by caching and reusing frequently-requested web pages.<sup>[6]</sup>

In Red Hat Enterprise Linux, the `squid` package provides the Squid Caching Proxy. Run the `rpm -q squid` command to see if the `squid` package is installed. If it is not installed and you want to use `squid`, run the following command as the root user to install it:

```
~]# yum install squid
```

### 8.1. SQUID CACHING PROXY AND SELINUX

When SELinux is enabled, `squid` runs confined by default. Confined processes run in their own domains, and are separated from other confined processes. If a confined process is compromised by an attacker, depending on SELinux policy configuration, an attacker's access to resources and the possible damage they can do is limited. The following example demonstrates the `squid` processes running in their own domain. This example assumes the `squid` package is installed:

1. Run the `getenforce` command to confirm SELinux is running in enforcing mode:

```
~]$ getenforce
Enforcing
```

The `getenforce` command returns `Enforcing` when SELinux is running in enforcing mode.

2. Run the `service squid start` command as the root user to start `squid`:

```
~]# service squid start
Starting squid: [ OK
]
```

3. Run the `ps -eZ | grep squid` command to view the `squid` processes:

```
~]$ ps -eZ | grep squid
unconfined_u:system_r:squid_t:s0 2522 ?        00:00:00 squid
unconfined_u:system_r:squid_t:s0 2524 ?        00:00:00 squid
unconfined_u:system_r:squid_t:s0 2526 ?        00:00:00 ncsa_auth
unconfined_u:system_r:squid_t:s0 2527 ?        00:00:00 ncsa_auth
unconfined_u:system_r:squid_t:s0 2528 ?        00:00:00 ncsa_auth
unconfined_u:system_r:squid_t:s0 2529 ?        00:00:00 ncsa_auth
unconfined_u:system_r:squid_t:s0 2530 ?        00:00:00 ncsa_auth
unconfined_u:system_r:squid_t:s0 2531 ?        00:00:00 unlinkd
```

The SELinux context associated with the `squid` processes is `unconfined_u:system_r:squid_t:s0`. The second last part of the context, `squid_t`, is the type. A type defines a domain for processes and a type for files. In this case, the `squid` processes are running in the `squid_t` domain.

SELinux policy defines how processes running in confined domains, such as `squid_t`, interact with files, other processes, and the system in general. Files must be labeled correctly to allow `squid` access to them.



When `/etc/squid/squid.conf` is configured so `squid` listens on a port other than the default TCP ports 3128, 3401 or 4827, the `semanage port` command must be used to add the required port number to the SELinux policy configuration. The following example demonstrates configuring `squid` to listen on a port that is not initially defined in SELinux policy configuration for `squid`, and, as a consequence, `squid` failing to start. This example also demonstrates how to then configure the SELinux system to allow `squid` to successfully listen on a non-standard port that is not already defined in the policy. This example assumes the `squid` package is installed. Run each command in the example as the root user:

1. Run the `service squid status` command to confirm `squid` is not running:

```
~]# service squid status
squid is stopped
```

If the output differs, run the `service squid stop` command to stop the process:

```
~]# service squid stop
Stopping squid: [ OK
]
```

2. Run the `semanage port -l | grep -w squid_port_t` command to view the ports SELinux allows `squid` to listen on:

```
~]# semanage port -l | grep -w -i squid_port_t
squid_port_t          tcp          3401, 4827
squid_port_t          udp          3401, 4827
```

3. Edit `/etc/squid/squid.conf` as the root user. Configure the `http_port` option so it lists a port that is not configured in SELinux policy configuration for `squid`. In this example, `squid` is configured to listen on port 10000:

```
# Squid normally listens to port 3128
http_port 10000
```

4. Run the `setsebool` command to make sure the `squid_connect_any` Boolean is set to off. This ensures `squid` is only permitted to operate on specific ports:

```
~]# setsebool -P squid_connect_any 0
```

5. Run the `service squid start` command to start `squid`:

```
~]# service squid start
Starting squid: ..... [FAILED]
```

An SELinux denial similar to the following is logged:

```
localhost settroubleshoot: SELinux is preventing the squid (squid_t)
from binding to port 10000. For complete SELinux messages. run
sealert -l 97136444-4497-4fff-a7a7-c4d8442db982
```

6. For SELinux to allow `squid` to listen on port 10000, as used in this example, the following

command is required:

```
~]# semanage port -a -t squid_port_t -p tcp 10000
```

7. Run `service squid start` again to start `squid` and have it listen on the new port:

```
~]# service squid start
Starting squid:          [ OK ]
```

8. Now that SELinux has been configured to allow `squid` to listen on a non-standard port (TCP 10000 in this example), `squid` starts successfully on this port.

## 8.2. TYPES

The main permission control method used in SELinux targeted policy to provide advanced process isolation is Type Enforcement. All files and processes are labeled with a type: types define a SELinux domain for processes and a SELinux type for files. SELinux policy rules define how types access each other, whether it be a domain accessing a type, or a domain accessing another domain. Access is only allowed if a specific SELinux policy rule exists that allows it.

The following types are used with `squid`. Different types allow you to configure flexible access:

### `httpd_squid_script_exec_t`

This type is used for utilities such as `cachemgr.cgi`, which provides a variety of statistics about `squid` and its configuration.

### `squid_cache_t`

Use this type for data that is cached by `squid`, as defined by the `cache_dir` directive in `/etc/squid/squid.conf`. By default, files created in or copied into `/var/cache/squid/` and `/var/spool/squid/` are labeled with the `squid_cache_t` type. Files for the [squidGuard](#) URL redirector plugin for `squid` created in or copied to `/var/squidGuard/` are also labeled with the `squid_cache_t` type. `Squid` is only able to use files and directories that are labeled with this type for its cached data.

### `squid_conf_t`

This type is used for the directories and files that `squid` uses for its configuration. Existing files, or those created in or copied to `/etc/squid/` and `/usr/share/squid/` are labeled with this type, including error messages and icons.

### `squid_exec_t`

This type is used for the `squid` binary, `/usr/sbin/squid`.

### `squid_log_t`

This type is used for logs. Existing files, or those created in or copied to `/var/log/squid/` or `/var/log/squidGuard/` must be labeled with this type.

### `squid_initrc_exec_t`

This type is used for the initialization file required to start `squid` which is located at `/etc/rc.d/init.d/squid`.

## squid\_var\_run\_t

This type is used by files in `/var/run/`, especially the process id (PID) named `/var/run/squid.pid` which is created by squid when it runs.

## 8.3. BOOLEANS

SELinux is based on the least level of access required for a service to run. Services can be run in a variety of ways; therefore, you need to specify how you run your services. Use the following Booleans to set up SELinux:

### squid\_connect\_any

When enabled, this Boolean permits squid to initiate a connection to a remote host on any port.



#### NOTE

Due to the continuous development of the SELinux policy, the list above might not contain all Booleans related to the service at all times. To list them, run the following command as root:

```
~]# semanage boolean -l | grep service_name
```

## 8.4. CONFIGURATION EXAMPLES

### 8.4.1. Squid Connecting to Non-Standard Ports

The following example provides a real-world demonstration of how SELinux complements Squid by enforcing the above Boolean and by default only allowing access to certain ports. This example will then demonstrate how to change the Boolean and show that access is then allowed.

Note that this is an example only and demonstrates how SELinux can affect a simple configuration of Squid. Comprehensive documentation of Squid is beyond the scope of this document. Refer to the official [Squid documentation](#) for further details. This example assumes that the Squid host has two network interfaces, Internet access, and that any firewall has been configured to allow access on the internal interface using the default TCP port on which Squid listens (TCP 3128).

1. As the root user, install the squid package. Run the `rpm -q squid` command to see if the squid package is installed. If it is not installed, run the `yum install squid` command as the root user to install it.
2. Edit the main configuration file, `/etc/squid/squid.conf` and confirm that the `cache_dir` directive is uncommented and looks similar to the following:

```
cache_dir ufs /var/spool/squid 100 16 256
```

This line specifies the default settings for the `cache_dir` directive to be used in this example; it consists of the Squid storage format (ufs), the directory on the system where the cache resides (`/var/spool/squid`), the amount of disk space in megabytes to be used for the cache (100), and finally the number of first-level and second-level cache directories to be created (16 and 256 respectively).

- In the same configuration file, make sure the `http_access allow localnet` directive is uncommented. This allows traffic from the `localnet` ACL which is automatically configured in a default installation of Squid on Red Hat Enterprise Linux. It will allow client machines on any existing RFC1918 network to have access through the proxy, which is sufficient for this simple example.
- In the same configuration file, make sure the `visible_hostname` directive is uncommented and is configured to the host name of the machine. The value should be the fully qualified domain name (FQDN) of the host:

```
visible_hostname squid.example.com
```

- As the root user, run the `service squid start` command to start `squid`. As this is the first time `squid` has started, this command will initialise the cache directories as specified above in the `cache_dir` directive and will then start the `squid` daemon. The output is as follows if `squid` starts successfully:

```
~]# /sbin/service squid start
init_cache_dir /var/spool/squid... Starting squid: .      [ OK ]
```

- Confirm that the `squid` process ID (PID) has started as a confined service, as seen here by the `squid_var_run_t` value:

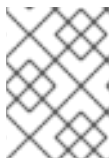
```
~]# ls -lZ /var/run/squid.pid
-rw-r--r--. root squid unconfined_u:object_r:squid_var_run_t:s0
/var/run/squid.pid
```

- At this point, a client machine connected to the `localnet` ACL configured earlier is successfully able to use the internal interface of this host as its proxy. This can be configured in the settings for all common web browsers, or system-wide. Squid is now listening on the default port of the target machine (TCP 3128), but the target machine will only allow outgoing connections to other services on the Internet via common ports. This is a policy defined by SELinux itself. SELinux will deny access to non-standard ports, as shown in the next step:
- When a client makes a request using a non-standard port through the Squid proxy such as a website listening on TCP port 10000, a denial similar to the following is logged:

```
SELinux is preventing the squid daemon from connecting to network
port 10000
```

- To allow this access, the `squid_connect_any` Boolean must be modified, as it is disabled by default. To enable the `squid_connect_any` Boolean, run the following command as the root user:

```
~]# setsebool -P squid_connect_any on
```



#### NOTE

Do not use the `-P` option if you do not want `setsebool` changes to persist across reboots.

- The client will now be able to access non-standard ports on the Internet as Squid is now

permitted to initiate connections to any port, on behalf of its clients.

---

[6] Refer to the [Squid Caching Proxy](#) project page for more information.

## CHAPTER 9. MYSQL

The MySQL database is a multi-user, multi-threaded SQL database server that consists of the MySQL server daemon (`mysqld`) and many client programs and libraries. [7]

In Red Hat Enterprise Linux, the `mysql-server` package provides MySQL. Run the `rpm -q mysql-server` command to see if the `mysql-server` package is installed. If it is not installed, run the following command as the root user to install it:

```
~]# yum install mysql-server
```

### 9.1. MYSQL AND SELINUX

When MySQL is enabled, it runs confined by default. Confined processes run in their own domains, and are separated from other confined processes. If a confined process is compromised by an attacker, depending on SELinux policy configuration, an attacker's access to resources and the possible damage they can do is limited. The following example demonstrates the MySQL processes running in their own domain. This example assumes the `mysql` package is installed:

1. Run the `getenforce` command to confirm SELinux is running in enforcing mode:

```
~]$ getenforce
Enforcing
```

The `getenforce` command returns **Enforcing** when SELinux is running in enforcing mode.

2. Run the `service mysqld start` command as the root user to start `mysqld`:

```
~]# service mysqld start
Initializing MySQL database: Installing MySQL system tables... [
OK ]
Starting MySQL: [ OK
]
```

3. Run the `ps -eZ | grep mysqld` command to view the `mysqld` processes:

```
~]$ ps -eZ | grep mysqld
unconfined_u:system_r:mysqld_safe_t:s0 6035 pts/1 00:00:00
mysqld_safe
unconfined_u:system_r:mysqld_t:s0 6123 pts/1 00:00:00 mysqld
```

The SELinux context associated with the `mysqld` processes is `unconfined_u:system_r:mysqld_t:s0`. The second last part of the context, `mysqld_t`, is the type. A type defines a domain for processes and a type for files. In this case, the `mysqld` processes are running in the `mysqld_t` domain.

### 9.2. TYPES

The main permission control method used in SELinux targeted policy to provide advanced process isolation is Type Enforcement. All files and processes are labeled with a type: types define a SELinux domain for processes and a SELinux type for files. SELinux policy rules define how types access each

other, whether it be a domain accessing a type, or a domain accessing another domain. Access is only allowed if a specific SELinux policy rule exists that allows it.

The following types are used with `mysql`. Different types allow you to configure flexible access:

#### `mysqld_db_t`

This type is used for the location of the MySQL database. In Red Hat Enterprise Linux, the default location for the database is `/var/lib/mysql/`, however this can be changed. If the location for the MySQL database is changed, the new location must be labeled with this type. Refer to the following example for instructions on how to change the default database location and how to label the new section appropriately.

#### `mysqld_etc_t`

This type is used for the MySQL main configuration file `/etc/my.cnf` and any other configuration files in the `/etc/mysql/` directory.

#### `mysqld_exec_t`

This type is used for the `mysqld` binary located at `/usr/libexec/mysqld`, which is the default location for the MySQL binary on Red Hat Enterprise Linux. Other systems may locate this binary at `/usr/sbin/mysqld` which should also be labeled with this type.

#### `mysqld_initrc_exec_t`

This type is used for the initialization file for MySQL, located at `/etc/rc.d/init.d/mysqld` by default in Red Hat Enterprise Linux.

#### `mysqld_log_t`

Logs for MySQL need to be labeled with this type for proper operation. All log files in `/var/log/` matching the `mysql.*` wildcard must be labeled with this type.

#### `mysqld_var_run_t`

This type is used by files in `/var/run/mysqld/`, specifically the process id (PID) named `/var/run/mysqld/mysqld.pid` which is created by the `mysqld` daemon when it runs. This type is also used for related socket files such as `/var/lib/mysql/mysql.sock`. Files such as these must be labeled correctly for proper operation as a confined service.

## 9.3. BOOLEANS

SELinux is based on the least level of access required for a service to run. Services can be run in a variety of ways; therefore, you need to specify how you run your services. Use the following Booleans to set up SELinux:

#### `allow_user_mysql_connect`

When enabled, this Boolean allows users to connect to MySQL.

#### `exim_can_connect_db`

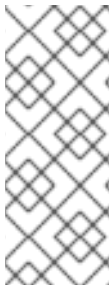
When enabled, this Boolean allows the `exim` mailer to initiate connections to a database server.

#### `ftpd_connect_db`

When enabled, this Boolean allows `ftp` daemons to initiate connections to a database server.

### `httpd_can_network_connect_db`

Enabling this Boolean is required for a web server to communicate with a database server.



#### NOTE

Due to the continuous development of the SELinux policy, the list above might not contain all Booleans related to the service at all times. To list them, run the following command as root:

```
~]# semanage boolean -l | grep service_name
```

## 9.4. CONFIGURATION EXAMPLES

### 9.4.1. MySQL Changing Database Location

When using Red Hat Enterprise Linux 6, the default location for MySQL to store its database is `/var/lib/mysql/`. This is where SELinux expects it to be by default, and hence this area is already labeled appropriately for you, using the `mysqld_db_t` type.

The location where the database is stored can be changed depending on individual environment requirements or preferences, however it is important that SELinux is aware of this new location; that it is labeled accordingly. This example explains how to change the location of a MySQL database and then how to label the new location so that SELinux can still provide its protection mechanisms to the new area based on its contents.

Note that this is an example only and demonstrates how SELinux can affect MySQL. Comprehensive documentation of MySQL is beyond the scope of this document. Refer to the official [MySQL documentation](#) for further details. This example assumes that the `mysql-server` and `setroubleshoot-server` packages are installed, that the `auditd` service is running, and that there is a valid database in the default location of `/var/lib/mysql/`.

1. Run the `ls -lZ /var/lib/mysql` command to view the SELinux context of the default database location for `mysql`:

```
~]# ls -lZ /var/lib/mysql
drwx----- . mysql mysql unconfined_u:object_r:mysqld_db_t:s0 mysql
```

This shows `mysqld_db_t` which is the default context element for the location of database files. This context will have to be manually applied to the new database location that will be used in this example in order for it to function properly.

2. Enter `mysqlshow -u root -p` and enter the `mysqld` root password to show the available databases:

```
~]# mysqlshow -u root -p
Enter password: *****
+-----+
|   Databases   |
+-----+
```



```
| information_schema |
| mysql              |
| test               |
| wikidb             |
+-----+

```

3. Shut down the `mysqld` daemon with the `service mysqld stop` command as the root user:

```
~]# service mysqld stop
Stopping MySQL: [ OK
]
```

4. Create a new directory for the new location of the database(s). In this example, `/mysql/` is used:

```
~]# mkdir -p /mysql
```

5. Copy the database files from the old location to the new location:

```
~]# cp -R /var/lib/mysql/* /mysql/
```

6. Change the ownership of this location to allow access by the `mysql` user and group. This sets the traditional Unix permissions which SELinux will still observe.

```
~]# chown -R mysql:mysql /mysql
```

7. Run the `ls -lZ /opt` command to see the initial context of the new directory:

```
~]# ls -lZ /opt
drwxr-xr-x. mysql mysql unconfined_u:object_r:usr_t:s0 mysql
```

The context `usr_t` of this newly created directory is not currently suitable to SELinux as a location for MySQL database files. Once the context has been changed, MySQL will be able to function properly in this area.

8. Open the main MySQL configuration file `/etc/my.cnf` with a text editor and modify the `datadir` option so that it refers to the new location. In this example the value that should be entered is `/mysql`.

```
[mysqld]
datadir=/mysql
```

Save this file and exit.

9. Run the `service mysqld start` command as the root user to start `mysqld`. The service should fail to start, and a denial will be logged to the `/var/log/messages` file. However, if the `audit` daemon is running alongside the `setroubleshoot` service, the denial will be logged to the `/var/log/audit/audit.log` file instead:

```
SELinux is preventing /usr/libexec/mysqld "write" access on /mysql.
For complete SELinux messages. run sealert -l b3f01aff-7fa6-4ebe-
ad46-abaef6f8ad71
```

The reason for this denial is that `/mysql/` is not labeled correctly for MySQL data files. SELinux is stopping MySQL from having access to the content labeled as `usr_t`. Perform the following steps to resolve this problem:

10. Run the following `semanage` command to add a context mapping for `/mysql`. Note that `semanage` is not installed by default. If it is missing on your system, install the `policycoreutils-python` package.

```
~]# semanage fcontext -a -t mysqld_db_t "/mysql(/.*)?"
```

11. This mapping is written to the `/etc/selinux/targeted/contexts/files/file_contexts.local` file:

```
~]# grep -i mysql
/etc/selinux/targeted/contexts/files/file_contexts.local
/mysql(/.*)?    system_u:object_r:mysqld_db_t:s0
```

12. Now use the `restorecon` command to apply this context mapping to the running system:

```
~]# restorecon -R -v /mysql
```

13. Now that the `/mysql/` location has been labeled with the correct context for MySQL, the `mysqld` daemon starts:

```
~]# service mysqld start
Starting MySQL:                                     [ OK
]
```

14. Confirm the context has changed for `/mysql/`:

```
~]$ ls -lZ /opt
drwxr-xr-x. mysql mysql system_u:object_r:mysqld_db_t:s0 mysql
```

15. The location has been changed and labeled, and the `mysqld` daemon has started successfully. At this point all running services should be tested to confirm normal operation.

---

[7] Refer to the [MySQL](#) project page for more information.

## CHAPTER 10. POSTGRESQL

PostgreSQL is an Object-Relational database management system (DBMS).<sup>[8]</sup>

In Red Hat Enterprise Linux 6, the `postgresql-server` package provides PostgreSQL. Run the `rpm -q postgresql-server` command to see if the `postgresql-server` package is installed. If it is not installed, run the following command as the root user to install it:

```
~]# yum install postgresql-server
```

### 10.1. POSTGRESQL AND SELINUX

When PostgreSQL is enabled, it runs confined by default. Confined processes run in their own domains, and are separated from other confined processes. If a confined process is compromised by an attacker, depending on SELinux policy configuration, an attacker's access to resources and the possible damage they can do is limited. The following example demonstrates the PostgreSQL processes running in their own domain. This example assumes the `postgresql-server` package is installed:

1. Run the `getenforce` command to confirm SELinux is running in enforcing mode:

```
~]$ getenforce
Enforcing
```

The `getenforce` command returns `Enforcing` when SELinux is running in enforcing mode.

2. Run the `service postgresql start` command as the root user to start `postgresql`:

```
~]# service postgresql start
Starting postgresql service: [ OK
]
```

3. Run the `ps -eZ | grep postgres` command to view the `postgresql` processes:

```
~]$ ps -eZ | grep postgres
unconfined_u:system_r:postgresql_t:s0 395 ?    00:00:00 postmaster
unconfined_u:system_r:postgresql_t:s0 397 ?    00:00:00 postmaster
unconfined_u:system_r:postgresql_t:s0 399 ?    00:00:00 postmaster
unconfined_u:system_r:postgresql_t:s0 400 ?    00:00:00 postmaster
unconfined_u:system_r:postgresql_t:s0 401 ?    00:00:00 postmaster
unconfined_u:system_r:postgresql_t:s0 402 ?    00:00:00 postmaster
```

The SELinux context associated with the `postgresql` processes is `unconfined_u:system_r:postgresql_t:s0`. The second last part of the context, `postgresql_t`, is the type. A type defines a domain for processes and a type for files. In this case, the `postgresql` processes are running in the `postgresql_t` domain.

### 10.2. TYPES

The main permission control method used in SELinux targeted policy to provide advanced process isolation is Type Enforcement. All files and processes are labeled with a type: types define a SELinux domain for processes and a SELinux type for files. SELinux policy rules define how types access each

other, whether it be a domain accessing a type, or a domain accessing another domain. Access is only allowed if a specific SELinux policy rule exists that allows it.

The following types are used with `postgresql`. Different types allow you to configure flexible access:

#### `postgresql_db_t`

This type is used for several locations. The locations labeled with this type are used for data files for PostgreSQL:

- `/usr/lib/pgsql/test/regres`
- `/usr/share/jonas/pgsql`
- `/var/lib/pgsql/data`
- `/var/lib/postgres(ql)?`

#### `postgresql_etc_t`

This type is used for configuration files in `/etc/postgresql/`.

#### `postgresql_exec_t`

This type is used for several locations. The locations labeled with this type are used for binaries for PostgreSQL:

- `/usr/bin/initdb(.sepgsql)?`
- `/usr/bin/(se)?postgres`
- `/usr/lib(64)?/postgresql/bin/*.*`
- `/usr/lib/phsql/test/regress/pg_regress`

#### `postgresql_initrc_exec_t`

This type is used for the PostgreSQL initialization file located at `/etc/rc.d/init.d/postgresql`.

#### `postgresql_log_t`

This type is used for several locations. The locations labeled with this type are used for log files:

- `/var/lib/pgsql/logfile`
- `/var/lib/pgsql/pgstartup.log`
- `/var/lib/sepgsql/pgstartup.log`
- `/var/log/postgresql`
- `/var/log/postgres.log.*`
- `/var/log/rhdb/rhdb`
- `/var/log/sepostgresql.log.*`

## postgresql\_var\_run\_t

This type is used for run-time files for PostgreSQL, such as the process id (PID) in `/var/run/postgresql/`.

## 10.3. BOOLEANS

SELinux is based on the least level of access required for a service to run. Services can be run in a variety of ways; therefore, you need to specify how you run your services. Use the following Booleans to set up SELinux:

### allow\_user\_postgresql\_connect

Having this Boolean enabled allows any user domain (as defined by PostgreSQL) to make connections to the database server.

### postgresql\_can\_rsync

When enabled, this Boolean allows PostgreSQL to use the SSH protocol and the `rsync` utility.



#### NOTE

Due to the continuous development of the SELinux policy, the list above might not contain all Booleans related to the service at all times. To list them, run the following command as root:

```
~]# semanage boolean -l | grep service_name
```

## 10.4. CONFIGURATION EXAMPLES

### 10.4.1. PostgreSQL Changing Database Location

When using Red Hat Enterprise Linux 6, the default location for PostgreSQL to store its database is `/var/lib/pgsql/data`. This is where SELinux expects it to be by default, and hence this area is already labeled appropriately for you, using the `postgresql_db_t` type.

The area where the database is located can be changed depending on individual environment requirements or preferences, however it is important that SELinux is aware of this new location; that it is labeled accordingly. This example explains how to change the location of a PostgreSQL database and then how to label the new location so that SELinux can still provide its protection mechanisms to the new area based on its contents.

Note that this is an example only and demonstrates how SELinux can affect PostgreSQL. Comprehensive documentation of PostgreSQL is beyond the scope of this document. Refer to the official [PostgreSQL documentation](#) for further details. This example assumes that the `postgresql-server` package is installed.

1. Run the `ls -lZ /var/lib/pgsql` command to view the SELinux context of the default database location for `postgresql`:

```
~]# ls -lZ /var/lib/pgsql
drwx----- . postgres postgres system_u:object_r:postgresql_db_t:s0
data
```

- This shows `postgresql_db_t` which is the default context element for the location of database files. This context will have to be manually applied to the new database location that will be used in this example in order for it to function properly.
- 2. Create a new directory for the new location of the database(s). In this example, `/opt/postgresql/data/` is used. If you use a different location, replace the text in the following steps with your location:

```
~]# mkdir -p /opt/postgresql/data
```

- 3. Perform a directory listing of the new location. Note that the initial context of the new directory is `usr_t`. This context is not sufficient for SELinux to offer its protection mechanisms to PostgreSQL. Once the context has been changed, it will be able to function properly in the new area.

```
~]# ls -lZ /opt/postgresql/  
drwxr-xr-x. root root unconfined_u:object_r:usr_t:s0 data
```

- 4. Change the ownership of the new location to allow access by the postgres user and group. This sets the traditional Unix permissions which SELinux will still observe.

```
~]# chown -R postgres:postgres /opt/postgresql
```

- 5. Open the PostgreSQL init file `/etc/rc.d/init.d/postgresql` with a text editor and modify the `PGDATA` and `PGLOG` variables to point to the new location:

```
~]# vi /etc/rc.d/init.d/postgresql  
PGDATA=/opt/postgresql/data  
PGLOG=/opt/postgresql/data/pgstartup.log
```

Save this file and exit the text editor.

- 6. Initialize the database in the new location.

```
~]$ su - postgres -c "initdb -D /opt/postgresql/data"
```

- 7. Having changed the database location, starting the service will fail at this point:

```
~]# service postgresql start  
Starting postgresql service: [FAILED]
```

SELinux has caused the service to not start. This is because the new location is not properly labelled. The following steps explain how to label the new location (`/opt/postgresql/`) and start the postgresql service properly:

- 8. Run the `semanage` command to add a context mapping for `/opt/postgresql/` and any other directories/files within it:

```
~]# semanage fcontext -a -t postgresql_db_t "/opt/postgresql(/.*)?"
```

9. This mapping is written to the `/etc/selinux/targeted/contexts/files/file_contexts.local` file:

```
~]# grep -i postgresql
/etc/selinux/targeted/contexts/files/file_contexts.local
/opt/postgresql(/.*)?    system_u:object_r:postgresql_db_t:s0
```

10. Now use the `restorecon` command to apply this context mapping to the running system:

```
~]# restorecon -R -v /opt/postgresql
```

11. Now that the `/opt/postgresql/` location has been labeled with the correct context for PostgreSQL, the `postgresql` service will start successfully:

```
~]# service postgresql start
Starting postgresQL service:
[ OK ]
```

12. Confirm the context is correct for `/opt/postgresql/`:

```
~]$ ls -lZ /opt
drwxr-xr-x. root root system_u:object_r:postgresql_db_t:s0
postgresql
```

13. Check with the `ps` command that the `postgresql` process displays the new location:

```
~]# ps aux | grep -i postmaster

postgres 21564  0.3  0.3  42308  4032 ?        S    10:13   0:00
/usr/bin/postmaster -p 5432 -D /opt/postgresql/data/
```

14. The location has been changed and labeled, and the `postgresql` daemon has started successfully. At this point all running services should be tested to confirm normal operation.

---

[8] Refer to the [PostgreSQL](#) project page for more information.

## CHAPTER 11. RSYNC

The `rsync` utility performs fast file transfer and it is used for synchronizing data between systems. [9]

When using Red Hat Enterprise Linux, the `rsync` package provides `rsync`. Run the `rpm -q rsync` command to see if the `rsync` package is installed. If it is not installed, run the following command as the root user to install it:

```
~]# yum install rsync
```

### 11.1. RSYNC AND SELINUX

SELinux requires files to have an extended attribute to define the file type. Policy governs the access daemons have to these files. If you want to share files using the `rsync` daemon, you must label the files and directories with the `public_content_t` type. Like most services, correct labeling is required for SELinux to perform its protection mechanisms over `rsync`.<sup>[10]</sup>

### 11.2. TYPES

The main permission control method used in SELinux targeted policy to provide advanced process isolation is Type Enforcement. All files and processes are labeled with a type: types define a SELinux domain for processes and a SELinux type for files. SELinux policy rules define how types access each other, whether it be a domain accessing a type, or a domain accessing another domain. Access is only allowed if a specific SELinux policy rule exists that allows it.

The following types are used with `rsync`. Different types allow you to configure flexible access:

#### `public_content_t`

This is a generic type used for the location of files (and the actual files) to be shared via `rsync`. If a special directory is created to house files to be shared with `rsync`, the directory and its contents need to have this label applied to them.

#### `rsync_exec_t`

This type is used for the `/usr/bin/rsync` system binary.

#### `rsync_log_t`

This type is used for the `rsync` log file, located at `/var/log/rsync.log` by default. To change the location of the file `rsync` logs to, use the `--log-file=FILE` option to the `rsync` command at run-time.

#### `rsync_var_run_t`

This type is used for the `rsyncd` lock file, located at `/var/run/rsyncd.lock`. This lock file is used by the `rsync` server to manage connection limits.

#### `rsync_data_t`

This type is used for files and directories which you want to use as `rsync` domains and isolate them from the access scope of other services. Also, the `public_content_t` is a general SELinux context type, which can be used when a file or a directory interacts with multiple services (for example, FTP and NFS directory as an `rsync` domain).



## rsync\_etc\_t

This type is used for `rsync`-related files in the `/etc/` directory.

## 11.3. BOOLEANS

SELinux is based on the least level of access required for a service to run. Services can be run in a variety of ways; therefore, you need to specify how you run your services. Use the following Booleans to set up SELinux:

### allow\_rsync\_anon\_write

Having this Boolean enabled allows `rsync` in the `rsync_t` domain to manage files, links and directories that have a type of `public_content_rw_t`. Often these are public files used for public file transfer services. Files and directories must be labeled `public_content_rw_t`.

### rsync\_client

Having this Boolean enabled allows `rsync` to initiate connections to ports defined as `rsync_port_t`, as well as allowing `rsync` to manage files, links and directories that have a type of `rsync_data_t`. Note that the `rsync` daemon must be in the `rsync_t` domain in order for SELinux to enact its control over `rsync`. The configuration example in this chapter demonstrates `rsync` running in the `rsync_t` domain.

### rsync\_export\_all\_ro

Having this Boolean enabled allows `rsync` in the `rsync_t` domain to export NFS and CIFS volumes with read-only access to clients.



#### NOTE

Due to the continuous development of the SELinux policy, the list above might not contain all Booleans related to the service at all times. To list them, run the following command as root:

```
~]# semanage boolean -l | grep service_name
```

## 11.4. CONFIGURATION EXAMPLES

### 11.4.1. Rsync as a daemon

When using Red Hat Enterprise Linux, `rsync` can be used as a daemon, so that multiple clients can directly communicate with it as a central server in order to house centralized files and keep them synchronized. The following example demonstrates running `rsync` as a daemon over a network socket in the correct domain, and how SELinux expects this daemon to be running on a pre-defined (in SELinux policy) TCP port. This example then shows how to modify SELinux policy to allow the `rsync` daemon to run normally on a non-standard port.

This example is performed on a single system to demonstrate SELinux policy and its control over local daemons and processes. Note that this is an example only and demonstrates how SELinux can affect `rsync`. Comprehensive documentation of `rsync` is beyond the scope of this document. See the official

[rsync documentation](#) for further details. This example assumes that the `rsync`, `setroublesheet-server` and `audit` packages are installed, that the SELinux targeted policy is used, and that SELinux is running in enforcing mode.

### Procedure 11.1. Getting `rsync` to launch as `rsync_t`

1. Run the `getenforce` command to confirm SELinux is running in enforcing mode:

```
~]$ getenforce
Enforcing
```

The `getenforce` command returns `Enforcing` when SELinux is running in enforcing mode.

2. Run the `which` command to confirm that the `rsync` binary is in the system path:

```
~]$ which rsync
/usr/bin/rsync
```

3. When running `rsync` as a daemon, a configuration file should be used and saved as `/etc/rsyncd.conf`. Note that the following configuration file used in this example is very simple and is not indicative of all the possible options that are available, rather it is just enough to demonstrate the `rsync` daemon:

```
log file = /var/log/rsync.log
pid file = /var/run/rsyncd.pid
lock file = /var/run/rsync.lock
[files]
    path = /srv/files
    comment = file area
    read only = false
    timeout = 300
```

4. Now that a simple configuration file exists for `rsync` to operate in daemon mode, this step demonstrates that simply running the `rsync --daemon` command is not sufficient for SELinux to offer its protection over `rsync`. See the following output:

```
~]# rsync --daemon

~]# ps x | grep rsync
 8231 ?        Ss        0:00 rsync --daemon
 8233 pts/3    S+        0:00 grep rsync

~]# ps -eZ | grep rsync
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 8231 ?
00:00:00 rsync
```

Note that in the output from the final `ps` command, the context shows the `rsync` daemon running in the `unconfined_t` domain. This indicates that `rsync` has not transitioned to the `rsync_t` domain as it was launched by the `rsync --daemon` command. At this point, SELinux cannot enforce its rules and policy over this daemon. See the following steps to see how to fix this problem.

In the following steps, `rsync` transitions to the `rsync_t` domain because it launched it from a properly-labeled init script. Only then can SELinux and its protection mechanisms have an effect over `rsync`. This `rsync` process should be killed before proceeding to the next step.

5. A custom init script for `rsync` is needed for this step. Save the following to `/etc/rc.d/init.d/rsyncd`.

```
#!/bin/bash

# Source function library.
. /etc/rc.d/init.d/functions

[ -f /usr/bin/rsync ] || exit 0

case "$1" in
start)
action "Starting rsyncd: " /usr/bin/rsync --daemon
;;
stop)
action "Stopping rsyncd: " killall rsync
;;
*)
echo "Usage: rsyncd {start|stop}"
exit 1
esac
exit 0
```

The following steps show how to label this script as `initrc_exec_t`:

6. Run the `semanage` command to add a context mapping for `/etc/rc.d/init.d/rsyncd`:

```
~]# semanage fcontext -a -t initrc_exec_t "/etc/rc.d/init.d/rsyncd"
```

7. This mapping is written to the `/etc/selinux/targeted/contexts/files/file_contexts.local` file:

```
~]# grep rsync
/etc/selinux/targeted/contexts/files/file_contexts.local

/etc/rc.d/init.d/rsyncd    system_u:object_r:initrc_exec_t:s0
```

8. Now use the `restorecon` command to apply this context mapping to the running system:

```
~]# restorecon -R -v /etc/rc.d/init.d/rsyncd
```

9. Run the `ls -lZ` command to confirm the script has been labeled appropriately. Note that in the following output, the script has been labeled as `initrc_exec_t`:

```
~]$ ls -lZ /etc/rc.d/init.d/rsyncd
-rwxr-xr-x. root root system_u:object_r:initrc_exec_t:s0
/etc/rc.d/init.d/rsyncd
```

10. Turn on the `rsync_server` SELinux boolean:

```
~]# setsebool rsync_server on
```

Note that this setting is not permanent and as such, it will revert to its original state after a reboot. To make the setting permanent, use the **-P** option with the `setsebool` command.

11. Launch `rsyncd` via the new script. Now that `rsync` has started from an init script that had been appropriately labeled, the process has started as `rsync_t`:

```
~]# service rsyncd start
Starting rsyncd:                                     [ OK
]

$ ps -eZ | grep rsync
unconfined_u:system_r:rsync_t:s0 9794 ?           00:00:00 rsync
```

SELinux can now enforce its protection mechanisms over the `rsync` daemon as it is now running in the `rsync_t` domain.

This example demonstrated how to get `rsyncd` running in the `rsync_t` domain. The next example shows how to get this daemon successfully running on a non-default port. TCP port 10000 is used in the next example.

#### Procedure 11.2. Running the rsync daemon on a non-default port

1. Modify the `/etc/rsyncd.conf` file and add the `port = 10000` line at the top of the file in the global configuration area (that is, before any file areas are defined). The new configuration file will look like:

```
log file = /var/log/rsyncd.log
pid file = /var/run/rsyncd.pid
lock file = /var/run/rsync.lock
port = 10000
[files]
    path = /srv/files
    comment = file area
    read only = false
    timeout = 300
```

2. After launching `rsync` from the init script with this new setting, a denial similar to the following is logged by SELinux:

```
Jul 22 10:46:59 localhost setroubleshoot: SELinux is preventing the
rsync (rsync_t) from binding to port 10000. For complete SELinux
messages, run sealert -l c371ab34-639e-45ae-9e42-18855b5c2de8
```

3. Run `semanage` to add TCP port 10000 to SELinux policy in `rsync_port_t`:

```
~]# semanage port -a -t rsync_port_t -p tcp 10000
```

4. Now that TCP port 10000 has been added to SELinux policy for `rsync_port_t`, `rsyncd` will start and operate normally on this port:

```
~]# service rsyncd start
```

```
Starting rsyncd: [ OK
]

~]# netstat -ltnp | grep 10000
tcp        0      0 0.0.0.0:10000  0.0.0.0:*        LISTEN
9910/rsync
```

SELinux has had its policy modified and is now permitting `rsyncd` to operate on TCP port 10000.

---

[9] Refer to the [Rsync](#) project page for more information.

[10] Refer to the `rsync_selinux(8)` manual page for more information about `rsync` and SELinux.

## CHAPTER 12. POSTFIX

Postfix is an open-source Mail Transport Agent (MTA), which supports protocols like LDAP, SMTP AUTH (SASL), and TLS.<sup>[11]</sup>

In Red Hat Enterprise Linux, the `postfix` package provides postfix. Run the `rpm -q postfix` command to see if the postfix package is installed. If it is not installed, run the following command as the root user to install it:

```
~]# yum install postfix
```

### 12.1. POSTFIX AND SELINUX

When Postfix is enabled, it runs confined by default. Confined processes run in their own domains, and are separated from other confined processes. If a confined process is compromised by an attacker, depending on SELinux policy configuration, an attacker's access to resources and the possible damage they can do is limited. The following example demonstrates the Postfix and related processes running in their own domain. This example assumes the postfix package is installed and that the Postfix service has been started:

1. Run the `getenforce` command to confirm SELinux is running in enforcing mode:

```
~]$ getenforce
Enforcing
```

The `getenforce` command returns `Enforcing` when SELinux is running in enforcing mode.

2. Run the `service postfix start` command as the root user to start `postfix`:

```
~]# service postfix start
Starting postfix: [ OK ]
```

3. Run the `ps -eZ | grep postfix` command to view the `postfix` processes:

```
~]$ ps -eZ | grep postfix
system_u:system_r:postfix_master_t:s0 1651 ? 00:00:00 master
system_u:system_r:postfix_pickup_t:s0 1662 ? 00:00:00 pickup
system_u:system_r:postfix_qmgr_t:s0 1663 ? 00:00:00 qmgr
```

In the output above, the SELinux context associated with the Postfix `master` process is `system_u:system_r:postfix_master_t:s0`. The second last part of the context, `postfix_master_t`, is the type for this process. A type defines a domain for processes and a type for files. In this case, the `master` process is running in the `postfix_master_t` domain.

### 12.2. TYPES

The main permission control method used in SELinux targeted policy to provide advanced process isolation is Type Enforcement. All files and processes are labeled with a type: types define a SELinux domain for processes and a SELinux type for files. SELinux policy rules define how types access each other, whether it be a domain accessing a type, or a domain accessing another domain. Access is only allowed if a specific SELinux policy rule exists that allows it.

The following types are used with Postfix. Different types allow you to configure flexible access:

#### **postfix\_etc\_t**

This type is used for configuration files for Postfix in the `/etc/postfix/` directory.

#### **postfix\_data\_t**

This type is used for Postfix data files in the `/var/lib/postfix/` directory.

#### **postfix\_var\_run\_t**

This type is used for Postfix files stored in the `/run/` directory.

#### **postfix\_initrc\_exec\_t**

This type is used for transition of Postfix executable files to the `postfix_initrc_t` domain.

#### **postfix\_spool\_t**

This type is used for Postfix files stored in the `/var/spool/` directory.



#### **NOTE**

To see the full list of files and their types for Postfix, run the following command:

```
~]$ grep postfix
/etc/selinux/targeted/contexts/files/file_contexts
```

## **12.3. BOOLEANS**

SELinux is based on the least level of access required for a service to run. Services can be run in a variety of ways; therefore, you need to specify how you run your services. Use the following Booleans to set up SELinux:

#### **allow\_postfix\_local\_write\_mail\_spool**

Having this Boolean enables Postfix to write to the local mail spool on the system. Postfix requires this Boolean to be enabled for normal operation when local spools are used.



#### **NOTE**

Due to the continuous development of the SELinux policy, the list above might not contain all Booleans related to the service at all times. To list them, run the following command as root:

```
~]# semanage boolean -l | grep service_name
```

## **12.4. CONFIGURATION EXAMPLES**

### **12.4.1. SpamAssassin and Postfix**

SpamAssassin is an open-source mail filter that provides a way to filter unsolicited email (spam messages) from incoming email.<sup>[12]</sup>

When using Red Hat Enterprise Linux, the `spamassassin` package provides SpamAssassin. Run the `rpm -q spamassassin` command to see if the `spamassassin` package is installed. If it is not installed, run the following command as the root user to install it:

```
~]# yum install spamassassin
```

SpamAssassin operates in tandem with a mailer such as Postfix to provide spam-filtering capabilities. In order for SpamAssassin to effectively intercept, analyze and filter mail, it must listen on a network interface. The default port for SpamAssassin is TCP/783, however this can be changed. The following example provides a real-world demonstration of how SELinux complements SpamAssassin by only allowing it access to a certain port by default. This example will then demonstrate how to change the port and have SpamAssassin operate on a non-default port.

Note that this is an example only and demonstrates how SELinux can affect a simple configuration of SpamAssassin. Comprehensive documentation of SpamAssassin is beyond the scope of this document. Refer to the official [SpamAssassin documentation](#) for further details. This example assumes the `spamassassin` is installed, that any firewall has been configured to allow access on the ports in use, that the SELinux targeted policy is used, and that SELinux is running in enforcing mode:

### Procedure 12.1. Running SpamAssassin on a non-default port

1. Run the `semanage` command to show the port that SELinux allows `spamd` to listen on by default:

```
~]# semanage port -l | grep spamd
spamd_port_t    tcp 783
```

This output shows that TCP/783 is defined in `spamd_port_t` as the port for SpamAssassin to operate on.

2. Edit the `/etc/sysconfig/spamassassin` configuration file and modify it so that it will start SpamAssassin on the example port TCP/10000:

```
# Options to spamd
SPAMDOPTIONS="-d -p 10000 -c m5 -H"
```

This line now specifies that SpamAssassin will operate on port 10000. The rest of this example will show how to modify SELinux policy to allow this socket to be opened.

3. Start SpamAssassin and an error message similar to the following will appear:

```
~]# service spamassassin start
Starting spamd: [2203] warn: server socket setup failed, retry 1:
spamd: could not create INET socket on 127.0.0.1:10000: Permission
denied
[2203] warn: server socket setup failed, retry 2: spamd: could not
create INET socket on 127.0.0.1:10000: Permission denied
[2203] error: spamd: could not create INET socket on
127.0.0.1:10000: Permission denied
spamd: could not create INET socket on 127.0.0.1:10000: Permission
```



```
denied
[FAILED]
```

This output means that SELinux has blocked access to this port.

4. A denial similar to the following will be logged by SELinux:

```
SELinux is preventing the spamd (spamd_t) from binding to port
10000.
```

5. As the root user, run **semanage** to modify SELinux policy in order to allow SpamAssassin to operate on the example port (TCP/10000):

```
~]# semanage port -a -t spamd_port_t -p tcp 10000
```

6. Confirm that SpamAssassin will now start and is operating on TCP port 10000:

```
~]# service spamassassin start
Starting spamd:      [ OK ]

~]# netstat -lntp | grep 10000
tcp 0 0 127.0.0.1:10000 0.0.0.0:* LISTEN 2224/spamd.pid
```

7. At this point, **spamd** is properly operating on TCP port 10000 as it has been allowed access to that port by SELinux policy.

---

[11] Refer to the [Postfix](#) project page for more information.

[12] Refer to the [SpamAssassin](#) project page for more information.

## CHAPTER 13. DHCP

DHCPD is the daemon used in Red Hat Enterprise Linux to dynamically deliver and configure Layer 3 TCP/IP details for clients.

The `dhcp` package provides the DHCP server, `dhcpd`. Run the `rpm -q dhcp` command to see if the `dhcp` package is installed. If it is not installed, run the following command as the root user to install it:

```
~]# yum install dhcp
```

### 13.1. DHCP AND SELINUX

When DHCPD is enabled, it runs confined by default. Confined processes run in their own domains, and are separated from other confined processes. If a confined process is compromised by an attacker, depending on SELinux policy configuration, an attacker's access to resources and the possible damage they can do is limited. The following example demonstrates the DHCPD and related processes running in their own domain. This example assumes the `dhcp` package is installed and that the DHCPD service has been started:

1. Run the `getenforce` command to confirm SELinux is running in enforcing mode:

```
~]$ getenforce
Enforcing
```

The `getenforce` command returns `Enforcing` when SELinux is running in enforcing mode.

2. Run the `service dhcpd start` command as the root user to start **DHCPD**:

```
~]# service dhcpd start
Starting dhcpd: [ OK ]
```

3. Run the `ps -eZ | grep dhcpd` command to view the `dhcpd` processes:

```
~]$ ps -eZ | grep dhcpd
unconfined_u:system_r:dhcpd_t:s0 5483 ?          00:00:00 dhcpd
```

The SELinux context associated with the `dhcpd` process is `unconfined_u:system_r:dhcpd_t:s0`.

### 13.2. TYPES

The main permission control method used in SELinux targeted policy to provide advanced process isolation is Type Enforcement. All files and processes are labeled with a type: types define a SELinux domain for processes and a SELinux type for files. SELinux policy rules define how types access each other, whether it be a domain accessing a type, or a domain accessing another domain. Access is only allowed if a specific SELinux policy rule exists that allows it.

The following types are used with `dhcpd`:

#### `dhcp_etc_t`

This type is mainly used for files in `/etc`, including configuration files.

**dhcpd\_var\_run\_t**

This type is used for the PID file for dhcpd, in `/var/run`.

**dhcpd\_exec\_t**

This type is used for transition of DHCP executable files to the `dhcpd_t` domain.

**dhcpd\_initrc\_exec\_t**

This type is used for transition of DHCP executable files to the `dhcpd_initrc_t` domain.

**NOTE**

To see the full list of files and their types for dhcp, run the following command:

```
~]$ grep dhcp  
/etc/selinux/targeted/contexts/files/file_contexts
```

## CHAPTER 14. OPENSIFT BY RED HAT

OpenShift by Red Hat is a Platform as a Service (PaaS) that enables developers to build and deploy web applications. OpenShift provides a wide selection of programming languages and frameworks including Java, Ruby, and PHP. It also provides integrated developer tools to support the application life cycle, including Eclipse integration, JBoss Developer Studio, and Jenkins. OpenShift uses an open source ecosystem to provide a platform for mobile applications, database services, and more. <sup>[13]</sup>

### 14.1. OPENSIFT AND SELINUX

SELinux provides better security control over applications that use OpenShift because all processes are labeled according to the SELinux policy. Therefore, SELinux protects OpenShift from possible malicious attacks within different gears running on the same node.

See the [Dan Walsh's presentation](#) for more information about SELinux and OpenShift.

### 14.2. TYPES

The main permission control method used in SELinux targeted policy to provide advanced process isolation is Type Enforcement. All files and processes are labeled with a type: types define a SELinux domain for processes and a SELinux type for files. SELinux policy rules define how types access each other, whether it be a domain accessing a type, or a domain accessing another domain. Access is only allowed if a specific SELinux policy rule exists that allows it.

The following types are used with OpenShift. Different types allow you to configure flexible access:

#### Process types

##### `openshift_t`

The OpenShift process is associated with the `openshift_t` SELinux type.

#### Types on executables

##### `openshift_cgroup_read_exec_t`

SELinux allows files with this type to transition an executable to the `openshift_cgroup_read_t` domain.

##### `openshift_cron_exec_t`

SELinux allows files with this type to transition an executable to the `openshift_cron_t` domain.

##### `openshift_initrc_exec_t`

SELinux allows files with this type to transition an executable to the `openshift_initrc_t` domain.

#### Writable types

##### `openshift_cgroup_read_tmp_t`

This type allows OpenShift control groups (cgroup) read and access temporary files in the `/tmp/` directory.

**openshift\_cron\_tmp\_t**

This type allows storing temporary files of the OpenShift cron jobs in `/tmp/`.

**openshift\_initrc\_tmp\_t**

This type allows storing the OpenShift `initrc` temporary files in `/tmp/`.

**openshift\_log\_t**

Files with this type are treated as OpenShift log data, usually stored under the `/var/log/` directory.

**openshift\_rw\_file\_t**

OpenShift have permission to read and to write to files labeled with this type.

**openshift\_tmp\_t**

This type is used for storing the OpenShift temporary files in `/tmp/`.

**openshift\_tmpfs\_t**

This type allows storing the OpenShift data on a tmpfs file system.

**openshift\_var\_lib\_t**

This type allows storing the OpenShift files in the `/var/lib/` directory.

**openshift\_var\_run\_t**

This type allows storing the OpenShift files in the `/run/` or `/var/run/` directory.

## 14.3. BOOLEANS

SELinux is based on the least level of access required for a service to run. Services can be run in a variety of ways; therefore, you need to specify how you run your services. Use the following Booleans to set up SELinux:

**openshift\_use\_nfs**

Having this Boolean enabled allows installing OpenShift on an NFS share.

**NOTE**

Due to the continuous development of the SELinux policy, the list above might not contain all Booleans related to the service at all times. To list them, run the following command as root:

```
~]# semanage boolean -l | grep service_name
```

## 14.4. CONFIGURATION EXAMPLES

### 14.4.1. Changing the Default OpenShift Directory

By default, OpenShift stores its data in the `/var/lib/openshift/` directory, which is labeled with the `openshift_var_lib_t` SELinux type. To allow OpenShift to store data in a different directory, label the new directory with the proper SELinux context.

The following procedure shows how to change the default OpenShift directory for storing data to `/srv/openshift/`:

#### Procedure 14.1. Changing the Default OpenShift Directory for Storing Data

1. As root, create a new `/openshift/` directory within the `/srv/` directory. The new directory is labeled with the `var_t` type:

```
~]# mkdir /srv/openshift
```

```
~]$ ls -Zd /srv/openshift
drwxr-xr-x. root root unconfined_u:object_r:var_t:s0  openshift/
```

2. As root, use the `semanage` utility to map `/srv/openshift/` to the proper SELinux context:

```
~]# semanage fcontext -a -e /var/lib/openshift /srv/openshift
```

3. Then, use the `restorecon` utility as root to apply the changes:

```
~]# restorecon -R -v /srv/openshift
```

4. The `/srv/openshift/` directory is now labeled with the correct `openshift_var_lib_t` type:

```
~]$ ls -Zd /srv/openshift
drwxr-xr-x. root root unconfined_u:object_r:openshift_var_lib_t:s0
openshift/
```

---

[13] To learn more about OpenShift, see [OpenShift Enterprise documentation](#) and [OpenShift Online documentation](#).

## CHAPTER 15. RED HAT GLUSTER STORAGE

*Red Hat Gluster Storage* provides flexible and affordable unstructured data storage for the enterprise. *GlusterFS*, a key building block of Gluster, is based on a stackable user-space design and aggregates various storage servers over a network and interconnects them into one large parallel network file system. The POSIX-compatible GlusterFS servers, which use the XFS file system format to store data on disks, can be accessed using industry standard access protocols including NFS and CIFS.

See the [Red Hat Gluster Storage](#) collection of guides for more information.

The `glusterfs` package provides Red Hat Gluster Storage. For detailed information about its installation process, see the [Installation Guide](#) for Red Hat Gluster Storage.

### 15.1. RED HAT GLUSTER STORAGE AND SELINUX

When enabled, SELinux serves as an additional security layer by providing flexible mandatory access control for the `glusterd` (GlusterFS Management Service) and `glusterfsd` (NFS server) processes as a part of Red Hat Gluster Storage. These processes have advanced process isolation unbounded with the `glusterd_t` SELinux type.

### 15.2. TYPES

The main permission control method used in SELinux targeted policy to provide advanced process isolation is Type Enforcement. All files and processes are labeled with a type: types define a SELinux domain for processes and a SELinux type for files. SELinux policy rules define how types access each other, whether it be a domain accessing a type, or a domain accessing another domain. Access is only allowed if a specific SELinux policy rule exists that allows it.

The following types are used with Red Hat Gluster Storage. Different types allow you to configure flexible access:

#### Process types

##### `glusterd_t`

The Gluster processes are associated with the `glusterd_t` SELinux type.

#### Types on executables

##### `glusterd_initrc_exec_t`

The SELinux-specific script type context for the Gluster init script files.

##### `glusterd_exec_t`

The SELinux-specific executable type context for the Gluster executable files.

#### Port Types

##### `gluster_port_t`

This type is defined for `glusterd`. By default, `glusterd` uses 204007-24027, and 38465-38469 TCP ports.

## File Contexts

### **glusterd\_brick\_t**

This type is used for files treated as **glusterd** brick data.

### **glusterd\_conf\_t**

This type is associated with the **glusterd** configuration data, usually stored in the **/etc/** directory.

### **glusterd\_log\_t**

Files with this type are treated as **glusterd** log data, usually stored under the **/var/log/** directory.

### **glusterd\_tmp\_t**

This type is used for storing the **glusterd** temporary files in the **/tmp/** directory.

### **glusterd\_var\_lib\_t**

This type allows storing the **glusterd** files in the **/var/lib/** directory.

### **glusterd\_var\_run\_t**

This type allows storing the **glusterd** files in the **/run/** or **/var/run/** directory.

## 15.3. BOOLEANS

SELinux is based on the least level of access required for a service to run. Services can be run in a variety of ways; therefore, you need to specify how you run your services. Use the following Booleans to set up SELinux:

### **gluster\_export\_all\_ro**

Having this Boolean enabled allows **glusterfsd** to share files and directory as read-only. This Boolean is disabled by default.

### **gluster\_export\_all\_rw**

Having this Boolean enabled allows **glusterfsd** to share files and directories with read and write access. This Boolean is enabled by default.

### **gluster\_anon\_write**

Having this Boolean enabled allows **glusterfsd** to modify public files labeled with the **public\_content\_rw\_t** SELinux type.



**NOTE**

Due to the continuous development of the SELinux policy, the list above might not contain all Booleans related to the service at all times. To list them, run the following command as root:

```
~]# semanage boolean -l | grep service_name
```

## 15.4. CONFIGURATION EXAMPLES

### 15.4.1. Labeling Gluster Bricks

A Gluster brick is an export directory on a server in the trusted storage pool. In case that the brick is not labeled with the correct SELinux context, `glusterd_brick_t`, SELinux denies certain file access operations and generates various AVC messages.

The following procedure shows how to label Gluster bricks with the correct SELinux context. The procedure assumes that you previously created and formatted a logical volume, for example `/dev/rhgs/gluster`, to be used as the Gluster brick.

For detailed information about Gluster bricks, see the [Red Hat Gluster Storage Volumes](#) chapter in the [Administration Guide](#) for Red Hat Gluster Storage.

#### Procedure 15.1. How to Label a Gluster Brick

1. Create a directory to mount the previously formatted logical volume. For example:

```
~]# mkdir /mnt/brick1
```

2. Mount the logical volume, in this case `/dev/vg-group/gluster`, to the `/mnt/brick1/` directory created in the previous step.

```
~]# mount /dev/vg-group/gluster /mnt/brick1/
```

Note that the `mount` command mounts devices only temporarily. To mount the device permanently, add an entry similar as the following one to the `/etc/fstab` file:

```
/dev/vg-group/gluster    /mnt/brick1  xfs rw,inode64,noatime,nouuid
1 2
```

For more information, see the `fstab(5)` manual page.

3. Check the SELinux context of `/mnt/brick1/`:

```
~]$ ls -lzd /mnt/brick1/
drwxr-xr-x. root root system_u:object_r:unlabeled_t:s0 /mnt/brick1/
```

The directory is labeled with the `unlabeled_t` SELinux type.

4. Change the SELinux type of `/mnt/brick1/` to the `glusterd_brick_t` SELinux type:

```
~]# semanage fcontext -a -t glusterd_brick_t "/mnt/brick1(/.*)?"
```

- 
5. Use the `restorecon` utility to apply the changes:

```
~]# restorecon -Rv /mnt/brick1
```

6. Finally, verify that the context has been successfully changed:

```
~]$ ls -lZd /mnt/brick1
drwxr-xr-x. root root system_u:object_r:glusterd_brick_t:s0
/mnt/brick1/
```

## CHAPTER 16. REFERENCES

The following references are pointers to additional information that is relevant to SELinux but beyond the scope of this guide. Note that due to the rapid development of SELinux, some of this material may only apply to specific releases of Red Hat Enterprise Linux.

### Books

#### SELinux by Example

Mayer, MacMillan, and Caplan

Prentice Hall, 2007

#### SELinux: NSA's Open Source Security Enhanced Linux

Bill McCarty

O'Reilly Media Inc., 2004

### Tutorials and Help

#### Tutorials and talks from Russell Coker

<http://www.coker.com.au/selinux/talks/ibmtu-2004/>

#### Dan Walsh's Journal

<http://danwalsh.livejournal.com/>

#### Red Hat Knowledgebase

<https://access.redhat.com/site/>

### General Information

#### NSA SELinux main website

<http://www.nsa.gov/research/selinux/index.shtml>

#### NSA SELinux FAQ

<http://www.nsa.gov/research/selinux/faqs.shtml>

### Mailing Lists

#### NSA SELinux mailing list

<http://www.nsa.gov/research/selinux/list.shtml>

#### Fedora SELinux mailing list

<http://www.redhat.com/mailman/listinfo/fedora-selinux-list>

### Community

**SELinux Project Wiki**

[http://selinuxproject.org/page/Main\\_Page](http://selinuxproject.org/page/Main_Page)

**SELinux community page**

<http://selinux.sourceforge.net/>

**IRC**

irc.freenode.net, #selinux

## APPENDIX A. REVISION HISTORY

<b>Revision 9-1</b> Version for 6.9 GA publication.	<b>Wed Mar 15 2017</b>	<b>Mirek Jahoda</b>
<b>Revision 9-0</b> Version for 6.9 Beta publication.	<b>Wed Dec 21 2016</b>	<b>Mirek Jahoda</b>
<b>Revision 8-0</b> Red Hat Enterprise Linux 6.8 GA release of the Managing Confined Services guide.	<b>Wed May 3 2016</b>	<b>Robert Krátký</b>
<b>Revision 7-1</b> Red Hat Enterprise Linux 6.7 GA release of the Managing Confined Services guide.	<b>Thu Jul 9 2015</b>	<b>Barbora Ančincová</b>
<b>Revision 6-0</b> Red Hat Enterprise Linux 6.4 GA release of the Managing Confined Services guide.	<b>Fri Oct 10 2014</b>	<b>Barbora Ančincová</b>
<b>Revision 5-0</b> Red Hat Enterprise Linux 6.5 GA release of the Managing Confined Services guide.	<b>Tue Nov 19 2013</b>	<b>Tomáš Čapek</b>
<b>Revision 4-0</b> Red Hat Enterprise Linux 6.4 GA release of the Managing Confined Services guide.	<b>Fri Feb 22 2013</b>	<b>Tomáš Čapek</b>
<b>Revision 3-0</b> Red Hat Enterprise Linux 6.3 GA release of the Managing Confined Services guide.	<b>Wed Jun 20 2012</b>	<b>Martin Prpič</b>
<b>Revision 2-0</b> Red Hat Enterprise Linux 6.2 GA release of the Managing Confined Services guide.	<b>Tue Dec 6 2011</b>	<b>Martin Prpič</b>
<b>Revision 1-0</b> Red Hat Enterprise Linux 6.1 GA release of the Managing Confined Services guide.	<b>Thu May 19 2011</b>	<b>Martin Prpič</b>
<b>Revision 0-0</b> 6.0 GA release	<b>Tue Nov 9 2010</b>	<b>Scott Radvan</b>