home/student/serverb-backup 目录。使用 **backup-home.sh** 脚本，以 serverb 上的 student 用户身份计划周期性作业。

- 重新启动系统，等待启动完成后再评分。

评估

在 workstation 上，运行 **lab rhcsa-compreview1 grade** 脚本来确认是否成功完成本练习。更正报告的所有错误并重新运行脚本，直到成功为止。

```
[student@workstation ~]$ lab rhcsa-compreview1 grade
```

完成

在 workstation 上，运行 **lab rhcsa-compreview1 finish** 来完成本练习。此脚本将删除在实验过程中创建的文件和资源，并确保环境清理干净。

```
[student@workstation ~]$ lab rhcsa-compreview1 finish
```

在进行下一项练习之前，将想要保留的任何文件或工作保存到其他系统中，然后重置 workstation、servera 和 serverb。

本总复习到此结束。

海量视频题库 myitpub.com QQ:556546 2
www.52myit.com

解决方案

修复启动问题和维护服务器

在本复习中，您将对启动问题进行故障排除和修复并更新系统默认目标。此外，您还将以普通用户的身份安排任务按重复计划运行。

成果

您应能够：

- 诊断问题并从紧急模式恢复系统。
- 将默认目标从 `graphical.target` 更改为 `multi-user.target`。
- 以普通用户的身份来计划运行周期性作业。

在你开始之前

在重置之前，将想要保留的任何文件或工作复制到其他系统中。现在重置 `workstation`、`servera` 和 `serverb` 系统。

以 `student` 用户身份并使用 `student` 作为密码登录 `workstation`。

在 `workstation` 上，运行 **`lab rhcsa-compreview1 start`** 以开始总复习。此脚本会创建必要的文件，以正确设置环境。

```
[student@workstation ~]$ lab rhcsa-compreview1 start
```

说明

在 `serverb` 上执行以下任务，以完成总复习：

- 在 `workstation` 上，运行 **`lab rhcsa-compreview1 break1`** 命令。此中断脚本将导致 `serverb` 上的启动过程失败。此外，它还将为 GRUB2 菜单设置更长的超时，以帮助中断启动过程并重新启动 `serverb`。

  对可能的原因进行故障排除并修复启动失败。修复工作必须确保 `serverb` 在无需干预的情况下重新启动。必要时，使用 `redhat` 作为该超级用户的密码。

- 在 `workstation` 上，运行 **`lab rhcsa-compreview1 break2`** 命令。此中断脚本将导致默认目标从 `multi-user` 目标切换到 `serverb` 上的 `graphical` 目标。此外，它还将为 GRUB2 菜单设置更长的超时，以帮助中断启动过程并重新启动 `serverb`。

  在 `serverb` 上，修复默认目标以使用 `multi-user` 目标。默认目标设置必须在重新启动后持久保留，且无需人工干预。

  使用 **`sudo`** 命令，以 `student` 用户身份并以 `student` 作为密码执行特权命令。

- 以 `student` 用户身份安排周期性作业，即在每天（周六、周日除外）下午 7 点到下午 9 点之间每小时执行一次 **`/home/student/backup-home.sh`** 脚本。

  从 http://materials.example.com/labs/backup-home.sh 中下载备份脚本。**`backup-home.sh`** 备份脚本会将 `serverb` 中的 **`/home/student`** 目录备份至 `servera` 中的 `/`

海量视频题库 myitpub.com QQ:556462
www.52myit.com

home/student/serverb-backup 目录。使用 **backup-home.sh** 脚本，以 serverb 上的 student 用户身份计划周期性作业。

· 重新启动系统，等待启动完成后再评分。

1. 在 workstation 上，运行 **lab rhcsa-compreview1 break1** 命令。

```
[student@workstation ~]$ lab rhcsa-compreview1 break1
```

2. 在 serverb 启动后，访问控制台并注意先前停止的启动过程。花一点时间来推测这种行为的可能原因。

   2.1. 根据您的课堂环境，找到 serverb 控制台的图标。打开控制台。

   2.2. 查看出现的错误，似乎至少部分系统仍在正常工作。

   2.3. 按 **Ctrl+Alt+Del** 重新启动 serverb。
   在显示启动加载器菜单后，按任意键（**Enter** 除外）中断倒计时。

   2.4. 编辑内存中默认的启动加载器条目，以登录紧急模式。
   按 **e** 编辑当前条目。

   2.5. 使用光标键导航到以 **linux** 开头的那一行。将 **systemd.unit=emergency.target** 附加到行末。

   2.6. 按 **Ctrl+x** 使用修改后的配置进行启动。

   2.7. 登录紧急模式。root 密码为 redhat。

```
Give root password for maintenance
(or press Control-D to continue): redhat
[root@serverb ~]#
```

3. 重新挂载 **/** 文件系统读/写。使用 **mount -a** 命令，尝试挂载其他所有文件系统。

   3.1. 重新挂载 **/** 文件系统读/写以编辑该文件系统。

```
[root@serverb ~]# mount -o remount,rw /
```

   3.2. 使用 **mount -a** 命令，尝试挂载其他所有文件系统。请注意，其中一个文件系统无法挂载。

```
[root@serverb ~]# mount -a
mount: /FakeMount: can't find UUID=fake.
```

   3.3. 编辑 **/etc/fstab** 以修复问题。删除或注释掉不正确的行。

```
[root@serverb ~]# vim /etc/fstab
...output omitted...
#UUID=fake      /FakeMount  xfs   defaults    0 0
```

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

3.4. 更新系统的 systemd 以注册新的 **/etc/fstab** 配置。

```
[root@serverb ~]# systemctl daemon-reload
[ 206.828912] systemd[1]: Reloading.
```

3.5. 通过尝试挂载所有条目来验证 **/etc/fstab** 现在是否正确。

```
[root@serverb ~]# mount -a
```

3.6. 重新启动 serverb 并等待启动完成。现在，系统应当能正常启动。

```
[root@serverb ~]# systemctl reboot
```

4. 在 workstation 上，运行 **lab rhcsa-compreview1 break2** 命令。

```
[student@workstation ~]$ lab rhcsa-compreview1 break2
```

等待重启完成后再继续。

5. 在 serverb 上，切换到 multi-user 目标。将默认目标设为 multi-user。使用 **sudo** 命令运行所需的任何管理命令；收到提示时，使用 student 作为密码。

5.1. 从 workstation，以 student 用户身份打开连接 serverb 的 SSH 会话。

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$
```

5.2. 以 serverb 上的 student 用户身份，确定默认目标。

```
[student@serverb ~]$ systemctl get-default
graphical.target
```

5.3. 切换到 multi-user 目标。使用 **sudo** 命令；收到提示时，使用 student 作为密码。

```
[student@serverb ~]$ sudo systemctl isolate multi-user.target
[sudo] password for student: student
```

5.4. 将 serverb 设置为使用 multi-user 目标作为默认目标。

```
[student@serverb ~]$ sudo systemctl set-default multi-user.target
Removed /etc/systemd/system/default.target.
Created symlink /etc/systemd/system/default.target -> /usr/lib/systemd/system/
multi-user.target.
```

5.5. 重新启动 serverb，验证是否将 multi-user 目标设为默认目标。

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

```
[student@serverb ~]$ sudo systemctl reboot
Connection to serverb closed by remote host.
Connection to serverb closed.
[student@workstation ~]$
```

5.6. 重启后，以 student 用户身份打开连接 serverb 的 SSH 会话。验证是否将 multi-user 目标设为默认目标。

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
[student@serverb ~]$ systemctl get-default
multi-user.target
```

6. 以 student 用户身份安排周期性作业，即在每天（周六、周日除外）下午 7 点到下午 9 点之间每小时执行一次 **/home/student/backup-home.sh** 脚本。

使用 **backup-home.sh** 脚本来计划周期性作业。从 http://materials.example.com/labs/backup-home.sh 中下载备份脚本。

6.1. 在 serverb 上，从 http://materials.example.com/labs/backup-home.sh 中下载备份脚本。利用 **chmod** 使备份脚本成为可执行文件。

```
[student@serverb ~]$ wget http://materials.example.com/labs/backup-home.sh
...output omitted...
[student@serverb ~]$ chmod +x backup-home.sh
```

6.2. 使用 **crontab -e** 命令，以默认文本编辑器打开 crontab 文件。

```
[student@serverb ~]$ crontab -e
```

6.3. 编辑该文件以添加以下命令行：

```
0 19-21 * * Mon-Fri /home/student/backup-home.sh
```

保存更改，再退出编辑器。

6.4. 使用 **crontab -l** 命令列出计划的周期性作业。

```
[student@serverb ~]$ crontab -l
0 19-21 * * Mon-Fri /home/student/backup-home.sh
```

7. 重新启动 serverb，等待启动完成后再评分。

```
[student@serverb ~]$ sudo systemctl reboot
[sudo] password for student: student
Connection to serverb closed by remote host.
Connection to serverb closed.
[student@workstation ~]$
```

海量视频题库 myitpub.com QQ:556462
www.52myit.com

评估

在 workstation 上，运行 **lab rhcsa-compreview1 grade** 脚本来确认是否成功完成本练习。更正报告的所有错误并重新运行脚本，直到成功为止。

```
[student@workstation ~]$ lab rhcsa-compreview1 grade
```

完成

在 workstation 上，运行 **lab rhcsa-compreview1 finish** 来完成本练习。此脚本将删除在实验过程中创建的文件和资源，并确保环境清理干净。

```
[student@workstation ~]$ lab rhcsa-compreview1 finish
```

在进行下一项练习之前，将想要保留的任何文件或工作保存到其他系统中，然后重置 workstation、servera 和 serverb。

本总复习到此结束。

海量视频题库 myitpub.com QQ:556462
www.52myit.com

开放研究实验

配置和管理文件系统与存储

在本复习中，您将创建 LVM 逻辑卷，挂载网络文件系统，创建在启动时自动激活的交换分区，配置从系统中清理未使用的临时文件，以及使用 ACL 来保护目录。

成果

您应能够：

- 创建 LVM 逻辑卷。
- 挂载网络文件系统。
- 创建在启动时自动激活的交换分区。
- 配置从系统中清理未使用的临时文件。
- 使用 ACL 来保护目录。

在你开始之前

在重置之前，将想要保留的任何文件或工作复制到其他系统中。除非您在上一项练习结束时已进行重置，否则现在请重置 `workstation`、`servera` 和 `serverb` 系统。

以 `student` 用户身份并使用 `student` 作为密码登录 `workstation`。

在 `workstation` 上，运行 **`lab rhcsa-compreview2 start`** 以开始总复习。此脚本会创建必要的文件，以正确设置环境。

```
[student@workstation ~]$ lab rhcsa-compreview2 start
```

说明

在 `serverb` 上执行以下任务，以完成总复习。

- 在新的 2 GiB 卷组 `extra_storage` 中配置新的 1 GiB 逻辑卷 `vol_home`。使用未分区的 `/dev/vdb` 磁盘来创建分区。
- 逻辑卷 `vol_home` 应使用 XFS 文件系统类型进行格式化，并持久挂载到 **`/home-directories`**。
- 确保名为 **`/share`** 的网络文件系统在重启持久挂载到 **`/local-share`**。NFS 服务器 `servera.lab.example.com` 会导出 **`/share`** 网络文件系统。NFS 导出路径为 `servera. lab.example.com:/share`。
- 在 `/dev/vdc` 磁盘上创建一个新的 512 MiB 分区，用作交换空间。在启动时，必须自动激活此交换空间。
- 创建一个名为 `production` 的新组。创建 `production1`、`production2`、`production3` 和 `production4` 用户。确保它们使用名为 `production` 的新组作为补充组。
- 对系统进行配置，使其使用名为 **`/run/volatile`** 的新目录来存储临时文件。如果有 30 秒以上未访问此目录中的文件，应对这些文件执行基于时间的清理。该目录的八进制权限必

海量视频题库 myitpub.com QQ:556462 www.52myit.com

须为 **0700**。确保使用 **/etc/tmpfiles.d/volatile.conf** 文件为 **/run/volatile** 中的文件配置基于时间的清理任务。

- 创建名为 **/webcontent** 的新目录。目录的所有者和组都应为 root。production 的组成员应该能读取和写入到此目录。production1 用户应该只能读取此目录。这些权限应当应用到 **/webcontent** 目录下创建的所有新文件和目录。

评估

在 workstation 上，运行 **lab rhcsa-compreview2 grade** 脚本来确认是否成功完成本练习。更正报告的所有错误并重新运行脚本，直到成功为止。

```
[student@workstation ~]$ lab rhcsa-compreview2 grade
```

完成

在 workstation 上，运行 **lab rhcsa-compreview2 finish** 来完成本练习。此脚本将删除在练习过程中创建的文件和资源，并确保环境清理干净。

```
[student@workstation ~]$ lab rhcsa-compreview2 finish
```

本总复习到此结束。

海量视频题库 myitpub.com QQ:556462
www.52myit.com

解决方案

配置和管理文件系统与存储

在本复习中，您将创建 LVM 逻辑卷，挂载网络文件系统，创建在启动时自动激活的交换分区，配置从系统中清理未使用的临时文件，以及使用 ACL 来保护目录。

成果

您应能够：

- 创建 LVM 逻辑卷。
- 挂载网络文件系统。
- 创建在启动时自动激活的交换分区。
- 配置从系统中清理未使用的临时文件。
- 使用 ACL 来保护目录。

在你开始之前

在重置之前，将想要保留的任何文件或工作复制到其他系统中。除非您在上一项练习结束时已进行重置，否则现在请重置 `workstation`、`servera` 和 `serverb` 系统。

以 `student` 用户身份并使用 `student` 作为密码登录 `workstation`。

在 `workstation` 上，运行 **`lab rhcsa-compreview2 start`** 以开始总复习。此脚本会创建必要的文件，以正确设置环境。

```
[student@workstation ~]$ lab rhcsa-compreview2 start
```

说明

在 `serverb` 上执行以下任务，以完成总复习。

- 在新的 2 GiB 卷组 `extra_storage` 中配置新的 1 GiB 逻辑卷 `vol_home`。使用未分区的 `/dev/vdb` 磁盘来创建分区。
- 逻辑卷 `vol_home` 应使用 XFS 文件系统类型进行格式化，并持久挂载到 **`/home-directories`**。
- 确保名为 **`/share`** 的网络文件系统在重启持久挂载到 **`/local-share`**。NFS 服务器 `servera.lab.example.com` 会导出 **`/share`** 网络文件系统。NFS 导出路径为 `servera. lab.example.com:/share`。
- 在 `/dev/vdc` 磁盘上创建一个新的 512 MiB 分区，用作交换空间。在启动时，必须自动激活此交换空间。
- 创建一个名为 `production` 的新组。创建 `production1`、`production2`、`production3` 和 `production4` 用户。确保它们使用名为 `production` 的新组作为补充组。
- 对系统进行配置，使其使用名为 **`/run/volatile`** 的新目录来存储临时文件。如果有 30 秒以上未访问此目录中的文件，应对这些文件执行基于时间的清理。该目录的八进制权限必

海量视频题库 myitpub.com QQ:556462
www.52myit.com

须为 **0700**。确保使用 **/etc/tmpfiles.d/volatile.conf** 文件为 **/run/volatile** 中的文件配置基于时间的清理任务。

- 创建名为 **/webcontent** 的新目录。目录的所有者和组都应为 root。production 的组成员应该能读取和写入到此目录。production1 用户应该只能读取此目录。这些权限应当应用到 **/webcontent** 目录下创建的所有新文件和目录。

1. 从 workstation，以 student 用户身份打开连接 serverb 的 SSH 会话。

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
```

2. 切换到 root 用户。

```
[student@serverb ~]$ sudo -i
[sudo] password for student: student
[root@serverb ~]#
```

3. 在 /dev/vdb 上创建一个 2 GiB 分区。

```
[root@serverb ~]# parted /dev/vdb mklabel msdos
[root@serverb ~]# parted /dev/vdb mkpart primary 1GiB 3GiB
```

4. 利用在 /dev/vdb 上创建的 2 GiB 分区，创建一个名为 vol_home 的逻辑卷。命名卷组 extra_storage。

   4.1. 将 /dev/vdb1 块设备声明为物理卷。

```
[root@serverb ~]# pvcreate /dev/vdb1
...output omitted...
```

   4.2. 使用 /dev/vdb1 创建 extra_storage 卷组。

```
[root@serverb ~]# vgcreate extra_storage /dev/vdb1
...output omitted...
```

   4.3. 创建一个名为 vol_home 的 1 GiB 逻辑卷。

```
[root@serverb ~]# lvcreate -L 1GiB -n vol_home extra_storage
...output omitted...
```

5. 将 vol_home 格式化为 XFS 文件系统类型并挂载于 **/home-directories**。

   5.1. 创建名为 **/home-directories** 的目录。

```
[root@serverb ~]# mkdir /home-directories
```

   5.2. 将 /dev/extra_storage/vol_home 格式化为 XFS 文件系统类型。

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

```
[root@serverb ~]# mkfs -t xfs /dev/extra_storage/vol_home
...output omitted...
```

5.3. 将 /dev/extra_storage/vol_home 持久挂载到 **/home-directories**。在 **/etc/fstab** 中创建此条目时，请使用结构的 UUID。

```
[root@serverb ~]# lsblk -o UUID /dev/extra_storage/vol_home
UUID
988cf149-0667-4733-abca-f80c6ec50ab6
[root@serverb ~]# echo "UUID=988c...0ab6 /home-directories \
xfs defaults 0 0" >> /etc/fstab
[root@serverb ~]# mount -a
```

6. 确保名为 **/share** 的网络文件系统在重启持久挂载到 **/local-share**。NFS 服务器 servera.lab.example.com 会导出 **/share** 网络文件系统。NFS 导出路径为 servera.lab.example.com:/share。

6.1. 创建 **/local-share** 目录。

```
[root@serverb ~]# mkdir /local-share
```

6.2. 将相应的条目附加至 **/etc/fstab**，这样位于 servera.lab.example.com:/share 的网络文件系统就可以在重启后持久挂载到 **/local-share**。

```
[root@serverb ~]# echo "servera.lab.example.com:/share /local-share \
nfs rw,sync 0 0" >> /etc/fstab
```

6.3. 根据 **/etc/fstab** 中的条目，将网络文件系统挂载到 **/local-share**。

```
[root@serverb ~]# mount /local-share
```

7. 在 /dev/vdc 磁盘上创建一个新的 512 MiB 分区，用作交换空间。在启动时，必须自动激活此交换空间。

7.1. 在 /dev/vdc 上创建一个 512 MiB 分区。

```
[root@serverb ~]# parted /dev/vdc mklabel msdos
[root@serverb ~]# parted /dev/vdc mkpart primary 1MiB 513MiB
```

7.2. 在 /dev/vdc1 上生成交换空间。

```
[root@serverb ~]# mkswap /dev/vdc1
...output omitted...
```

7.3. 激活交换空间，使其在重启后持久挂载。在 **/etc/fstab** 中创建此条目时，请使用结构的 UUID。

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

```
[root@serverb ~]# lsblk -o UUID /dev/vdc1
UUID
cc18ccb6-bd29-48a5-8554-546bf3471b69
[root@serverb ~]# echo "UUID=cc18...1b69 swap \
swap defaults 0 0" >> /etc/fstab
[root@serverb ~]# swapon -a
```

8. 创建 production1、production2、production3 和 production4 用户。确保它们使用名为 production 的新组作为补充组。

```
[root@serverb ~]# groupadd production
[root@serverb ~]# for i in 1 2 3 4; do useradd -G production production$i; done
```

9. 配置系统，使其使用名为 **/run/volatile** 的新目录来存储临时文件。如果有 30 秒以上未访问此目录中的文件，应对这些文件执行基于时间的清理。此目录的八进制权限必须为 **0700**。确保使用 **/etc/tmpfiles.d/volatile.conf** 文件为 **/run/volatile** 中的文件配置基于时间的清理任务。

   9.1. 创建名为 **/etc/tmpfiles.d/volatile.conf** 并包含以下内容的文件。

```
d /run/volatile 0700 root root 30s
```

   9.2. 如果 **/run/volatile** 目录还不存在，请使用 **systemd-tmpfiles --create** 命令创建该目录。

```
[root@servera ~]# systemd-tmpfiles --create /etc/tmpfiles.d/volatile.conf
```

10. 创建新目录 **/webcontent**。目录的所有者和组所有者都应为 root。production 的组成员应该能读取和写入到此目录。production1 用户应该只能读取此目录。这些权限应当应用到 **/webcontent** 目录下创建的所有新文件和目录。

   10.1.创建 **/webcontent** 目录。

```
[root@serverb ~]# mkdir /webcontent
```

   10.2.使用 **setfacl** 在 **/webcontent** 上配置权限，使 production 的组成员具有读写权限，但 production1 用户除外，该用户应只被授予读取权限。

```
[root@serverb ~]# setfacl -m u:production1:rx /webcontent
[root@serverb ~]# setfacl -m g:production:rwx /webcontent
```

   10.3.使用 **setfacl** 在 **/webcontent** 上设置默认权限，以便将上一步中应用的权限也同样应用于在 **/webcontent** 目录下创建的所有新文件和目录。

```
[root@serverb ~]# setfacl -m d:u:production1:rx /webcontent
[root@serverb ~]# setfacl -m d:g:production:rwx /webcontent
```

   10.4.退出 root 用户的 shell。

海量视频题库 myitpub.com QQ:556546 2
www.52myit.com

```
[root@serverb ~]# exit
logout
```

10.5.从 serverb 注销。

```
[student@serverb ~]$ exit
logout
Connection to serverb closed.
```

评估

在 workstation 上，运行 **lab rhcsa-compreview2 grade** 脚本来确认是否成功完成本练习。更正报告的所有错误并重新运行脚本，直到成功为止。

```
[student@workstation ~]$ lab rhcsa-compreview2 grade
```

完成

在 workstation 上，运行 **lab rhcsa-compreview2 finish** 来完成本练习。此脚本将删除在练习过程中创建的文件和资源，并确保环境清理干净。

```
[student@workstation ~]$ lab rhcsa-compreview2 finish
```

本总复习到此结束。

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

开放研究实验

配置和管理服务器安全性

在本复习中，您将配置基于 SSH 密钥的身份验证，更改防火墙设置，调整 SELinux 模式和 SELinux 布尔值，并对 SELinux 问题进行故障排除。

成果

您应能够：

- 为基于密钥的身份验证配置 SSH 密钥。
- 配置防火墙设置。
- 调整 SELinux 模式和 SELinux 布尔值。
- 对 SELinux 问题进行故障排除。

在你开始之前

以 `student` 用户身份并使用 `student` 作为密码登录 `workstation`。

在 `workstation` 上，运行 **`lab rhcsa-compreview3 start`** 以开始总复习。此脚本会创建必要的文件，以正确设置环境。

```
[student@workstation ~]$ lab rhcsa-compreview3 start
```

说明

执行以下任务以完成总复习：

- 为 `serverb` 上的 `student` 用户生成 SSH 密钥。不要用密语对该私钥进行保护。
- 在 `servera` 上配置 `student` 用户，使之接受利用为 `serverb` 上的 `student` 创建的 SSH 密钥对所进行的登录身份验证。`serverb` 上的 `student` 用户应该能在不输入密码的情况下，使用 SSH 来登录 `servera`。如需要，请使用 `student` 作为 `student` 用户的密码。
- 在 `servera` 上，将默认 SELinux 模式更改为 **`permissive`**。
- 配置 `serverb`，使其在 `production5` 用户登录时使用网络文件系统 **`/home-directories/production5`** 自动挂载该用户的主目录。此网络文件系统是从 `servera.lab.example.com` 中导出的。调整相应的 SELinux 布尔值，使 `production5` 在完成基于 SSH 密钥的身份验证后可以使用 `serverb` 上的 NFS 挂载主目录。`production5` 用户的密码为 `redhat`。
- 在 `serverb` 上，调整防火墙设置以拒绝来自 `servera` 的 SSH 连接。
- 在 `serverb` 上，调查并修复 Apache HTTPD 守护进程的问题，该守护进程被配置为侦听端口 `30080/TCP`，但未能启动。对防火墙设置进行相应调整，使端口 `30080/TCP` 对于传入连接保持打开状态。

海量视频题库 myitpub.com QQ:556462
www.52myit.com

评估

在 workstation 上，运行 **lab rhcsa-compreview3 grade** 脚本来确认是否成功完成本练习。更正报告的所有错误并重新运行脚本，直到成功为止。

```
[student@workstation ~]$ lab rhcsa-compreview3 grade
```

完成

在 workstation 上，运行 **lab rhcsa-compreview3 finish** 来完成本练习。此脚本将删除在实验过程中创建的文件和资源，并确保环境清理干净。

```
[student@workstation ~]$ lab rhcsa-compreview3 finish
```

将想要保留的任何文件或工作保存到其他系统中，然后重置 workstation、servera 和 serverb。

本总复习到此结束。

海量视频题库 myitpub.com QQ:556462
www.52myit.com

解决方案

配置和管理服务器安全性

在本复习中，您将配置基于 SSH 密钥的身份验证，更改防火墙设置，调整 SELinux 模式和 SELinux 布尔值，并对 SELinux 问题进行故障排除。

成果

您应能够：

- 为基于密钥的身份验证配置 SSH 密钥。
- 配置防火墙设置。
- 调整 SELinux 模式和 SELinux 布尔值。
- 对 SELinux 问题进行故障排除。

在你开始之前

以 `student` 用户身份并使用 `student` 作为密码登录 `workstation`。

在 `workstation` 上，运行 **`lab rhcsa-compreview3 start`** 以开始总复习。此脚本会创建必要的文件，以正确设置环境。

```
[student@workstation ~]$ lab rhcsa-compreview3 start
```

说明

执行以下任务以完成总复习：

- 为 `serverb` 上的 `student` 用户生成 SSH 密钥。不要用密语对该私钥进行保护。
- 在 `servera` 上配置 `student` 用户，使之接受利用为 `serverb` 上的 `student` 创建的 SSH 密钥对所进行的登录身份验证。`serverb` 上的 `student` 用户应该能在不输入密码的情况下，使用 SSH 来登录 `servera`。如需要，请使用 `student` 作为 `student` 用户的密码。
- 在 `servera` 上，将默认 SELinux 模式更改为 **`permissive`**。
- 配置 `serverb`，使其在 `production5` 用户登录时使用网络文件系统 **`/home-directories/production5`** 自动挂载该用户的主目录。此网络文件系统是从 `servera.lab.example.com` 中导出的。调整相应的 SELinux 布尔值，使 `production5` 在完成基于 SSH 密钥的身份验证后可以使用 `serverb` 上的 NFS 挂载主目录。`production5` 用户的密码为 `redhat`。
- 在 `serverb` 上，调整防火墙设置以拒绝来自 `servera` 的 SSH 连接。
- 在 `serverb` 上，调查并修复 Apache HTTPD 守护进程的问题，该守护进程被配置为侦听端口 `30080/TCP`，但未能启动。对防火墙设置进行相应调整，使端口 `30080/TCP` 对于传入连接保持打开状态。

1. 从 `workstation`，以 `student` 用户身份打开连接 `serverb` 的 SSH 会话。

海量视频题库 myitpub.com QQ:556462
www.52myit.com

```
[student@workstation ~]$ ssh student@serverb
...output omitted...
```

2. 使用 **ssh-keygen** 命令，为 serverb 上的 student 用户生成 SSH 密钥。不要用密语对该私钥进行保护。

```
[student@serverb ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa): Enter
Created directory '/home/student/.ssh'.
Enter passphrase (empty for no passphrase): Enter
Enter same passphrase again: Enter
Your identification has been saved in /home/student/.ssh/id_rsa.
Your public key has been saved in /home/student/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:1TPZ4TXYwiGWfExUGtRTHgfKQbF9hVuLa+VmH4vgkFY student@serverb.lab.example.com
The key's randomart image is:
+---[RSA 2048]----+
|          .+@BO**|
|          .=.#+B*|
|          . X.*o=|
|         . E +.+ |
|        S o   +  |
|         + . o = |
|        . o o + +|
|           . . ..|
|                 |
+----[SHA256]-----+
```

3. 在 servera 上配置 student 用户，使之接受利用为 serverb 上的 student 创建的 SSH 密钥对所进行的登录身份验证。serverb 上的 student 用户应该能在不输入密码的情况下，使用 SSH 来登录 servera。必要时，请使用 student 作为 student 用户的密码。

   3.1. 使用 **ssh-copy-id** 命令，将 serverb 上 student 的 SSH 密钥对的公钥传给 servera 上的 student。如有提示，请使用 student 作为 student 用户的密码。

```
[student@serverb ~]$ ssh-copy-id student@servera
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/student/.ssh/
id_rsa.pub"
The authenticity of host 'servera (172.25.250.10)' can't be established.
ECDSA key fingerprint is SHA256:g/fIMtVzDWTbTi1l0OwC30sL6cHmro9Tf563NxmeyyE.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
 out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted
 now it is to install the new keys
student@servera's password: student

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'student@servera'"
and check to make sure that only the key(s) you wanted were added.
```

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

3.2. 使用 **ssh** 命令，验证 student 用户能否在不输入密码的情况下从 serverb 登录 servera。

```
[student@serverb ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

4. 在 servera 上，将默认 SELinux 模式更改为 **permissive**。

4.1. 编辑 **/etc/sysconfig/selinux**，将参数 **SELINUX** 的值设为 **permissive**。您可以使用 **sudo vi /etc/sysconfig/selinux** 命令，以超级用户身份编辑配置文件。收到提示时，使用密码 student。

```
...output omitted...
#SELINUX=enforcing
SELINUX=permissive
...output omitted...
```

4.2. 使用 **sudo systemctl reboot** 命令，以超级用户身份重新启动系统。

```
[student@servera ~]$ sudo systemctl reboot
Connection to servera closed by remote host.
Connection to servera closed.
[student@serverb ~]$
```

5. 配置 serverb，使其在 production5 用户登录时使用网络文件系统 **/home-directories/production5** 自动挂载该用户的主目录。此网络文件系统是从 servera.lab.example.com 中导出的。调整相应的 SELinux 布尔值，使 production5 在完成基于 SSH 密钥的身份验证后可以使用 serverb 上的 NFS 挂载主目录。production5 用户的密码为 redhat。

5.1. 在 serverb 上，使用 **sudo -i** 命令切换为 root 用户帐户。

```
[student@serverb ~]$ sudo -i
[sudo] password for student: student
[root@serverb ~]#
```

5.2. 安装 autofs 软件包。

```
[root@serverb ~]# yum install autofs
...output omitted...
Is this ok [y/N]: y
...output omitted...
Installed:
  autofs-1:5.1.4-29.el8.x86_64

Complete!
```

5.3. 创建名为 **/etc/auto.master.d/production5.autofs** 并包含以下内容的 autofs 主映射文件。

海量视频题库 myitpub.com QQ:556546 2
www.52myit.com

```
/- /etc/auto.production5
```

5.4. 创建包含以下内容的 **/etc/auto.production5** 文件。

```
/localhome/production5 -rw servera.lab.example.com:/home-directories/production5
```

5.5. 重新启动 autofs 服务。

```
[root@serverb ~]# systemctl restart autofs
```

6. 在 servera 上，验证 production5 用户无法使用 SSH 公钥身份验证方式登录 serverb。这是由 SELinux 布尔值引起的，您将在以下步骤中修复此问题。

6.1. 从 workstation，以 student 用户身份打开连接 servera 的 SSH 会话。

```
[student@workstation ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

6.2. 将 redhat 用作密码，切换到 production5 用户。

```
[student@servera ~]$ su - production5
Password: redhat
[production5@servera ~]$
```

6.3. 以 production5 用户身份，使用 **ssh-keygen** 命令来生成 SSH 密钥。

```
[production5@servera ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/production5/.ssh/id_rsa): Enter
Created directory '/home/production5/.ssh'.
Enter passphrase (empty for no passphrase): Enter
Enter same passphrase again: Enter
Your identification has been saved in /home/production5/.ssh/id_rsa.
Your public key has been saved in /home/production5/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:zmin1nmCt4H8LA+4FPimtdg81nl7ATbInUFW3HSPxk4
 production5@servera.lab.example.com
The key's randomart image is:
+---[RSA 2048]----+
|        .oo.o. .  |
|        .. . .o o |
|      . o o    E .|
|   .  o *    +    |
|  . .  .So    .   |
|   . + =  .       |
|    *.*+=. .      |
|   Oo+***.o       |
|  o.=o.=**        |
+----[SHA256]-----+
```

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

6.4. 使用 **ssh-copy-id** 命令，将 servera 上 production5 的 SSH 密钥对的公钥发送给 serverb 上的 production5。如有提示，请使用 redhat 作为 production5 用户的密码。

```
[production5@servera ~]$ ssh-copy-id production5@serverb
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/
production5/.ssh/id_rsa.pub"
The authenticity of host 'serverb (172.25.250.11)' can't be established.
ECDSA key fingerprint is SHA256:ciCkaRWF4g6eR9nSdPxQ7KL8czpViXal6BousK544TY.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
 out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted
 now it is to install the new keys
production5@serverb's password: redhat

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'production5@serverb'"
and check to make sure that only the key(s) you wanted were added.
```

6.5. 以 production5 用户身份，使用基于 SSH 公钥的身份验证（而非基于密码的身份验证）登录 serverb。此命令应失败。

```
[production5@servera ~]$ ssh -o pubkeyauthentication=yes \
-o passwordauthentication=no production5@serverb
production5@serverb: Permission denied (publickey,gssapi-keyex,gssapi-with-
mic,password).
```

7. 在 serverb 上设置相应的 SELinux 布尔值，以便 production5 可以使用基于 SSH 公钥的验证方式登录 serverb 并使用主目录。

7.1. 在 serverb 上，以 root 用户身份将 use_nfs_home_dirs SELinux 布尔值设为 **true**。

```
[root@serverb ~]# setsebool -P use_nfs_home_dirs true
```

7.2. 以 production5 用户身份，使用基于 SSH 公钥的身份验证（而非基于密码的身份验证）登录 serverb。此命令应该会成功。

```
[production5@servera ~]$ ssh -o pubkeyauthentication=yes \
-o passwordauthentication=no production5@serverb
...output omitted...
[production5@serverb ~]$
```

8. 在 serverb 上，调整防火墙设置以拒绝来自 servera 的 SSH 连接。servera 系统使用 IPv4 地址 172. 25.250.10。

8.1. 使用 **firewall-cmd** 命令将 servera 的 IPv4 地址添加到名为 block 的 firewalld 区域中。

海量视频题库 mvitpub.com QQ:5565462
www.52mvit.com

```
[root@serverb ~]# firewall-cmd --add-source=172.25.250.10/32 \
--zone=block --permanent
success
```

8.2. 使用 **firewall-cmd --reload** 命令重新加载防火墙设置的更改。

```
[root@serverb ~]# firewall-cmd --reload
success
```

9. 在 serverb 上，调查并修复 Apache HTTPD 守护进程的问题，该守护进程被配置为侦听端口 30080/TCP，但未能启动。对防火墙设置进行相应调整，使端口 30080/TCP 对于传入连接保持打开状态。

9.1. 使用 **systemctl** 命令来重启 **httpd** 服务。此命令在重启该服务时失败。

```
[root@serverb ~]# systemctl restart httpd.service
Job for httpd.service failed because the control process exited with error code.
See "systemctl status httpd.service" and "journalctl -xe" for details.
```

9.2. 使用 **systemctl status** 命令调查 **httpd** 服务失败的原因。

```
[root@serverb ~]# systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset:
 disabled)
   Active: failed (Result: exit-code) since Mon 2019-04-15 06:42:41 EDT; 5min ago
     Docs: man:httpd.service(8)
  Process: 27313 ExecStart=/usr/sbin/httpd $OPTIONS -DFOREGROUND (code=exited,
 status=1/FAILURE)
 Main PID: 27313 (code=exited, status=1/FAILURE)
   Status: "Reading configuration..."

Apr 15 06:42:41 serverb.lab.example.com systemd[1]: Starting The Apache HTTP
 Server...
Apr 15 06:42:41 serverb.lab.example.com httpd[27313]: (13)Permission denied:
 AH00072: make_sock: could not bind to address [::]:30080
Apr 15 06:42:41 serverb.lab.example.com httpd[27313]: (13)Permission denied:
 AH00072: make_sock: could not bind to address 0.0.0.0:30080
Apr 15 06:42:41 serverb.lab.example.com httpd[27313]: no listening sockets
 available, shutting down
Apr 15 06:42:41 serverb.lab.example.com httpd[27313]: AH00015: Unable to open logs
Apr 15 06:42:41 serverb.lab.example.com systemd[1]: httpd.service: Main process
 exited, code=exited, status=1/FAILURE
Apr 15 06:42:41 serverb.lab.example.com systemd[1]: httpd.service: Failed with
 result 'exit-code'.
Apr 15 06:42:41 serverb.lab.example.com systemd[1]: Failed to start The Apache
 HTTP Server.
```

注意上述输出中的权限错误，这表明 **httpd** 守护进程未能绑定到端口 30080/TCP。SELinux 策略可能会限制某个应用绑定到端口。按 **q** 退出上述 **systemctl** 命令。

9.3. 使用 **sealert** 命令，确定 SELinux 策略是否阻止了 **httpd** 绑定到端口 30080/TCP。

海量视频题库 mylpub.com QQ:556462 www.52mylt.com

```
[root@serverb ~]# sealert -a /var/log/audit/audit.log
100% done
found 1 alerts in /var/log/audit/audit.log
--------------------------------------------------------------------------------

SELinux is preventing /usr/sbin/httpd from name_bind access on the tcp_socket port
 30080.

*****  Plugin bind_ports (92.2 confidence) suggests   ************************

If you want to allow /usr/sbin/httpd to bind to network port 30080
Then you need to modify the port type.
Do
# semanage port -a -t PORT_TYPE -p tcp 30080
    where PORT_TYPE is one of the following: http_cache_port_t, http_port_t,
 jboss_management_port_t, jboss_messaging_port_t, ntop_port_t, puppet_port_t.
...output omitted...
```

上述日志消息显示，端口 30080/TCP 没有相应的 SELinux 上下文 **http_port_t**，从而导致 SELinux 禁止 **httpd** 绑定到此端口。该日志消息还生成了 **semanage port** 命令的语法，以方便您解决此问题。

9.4. 使用 **semanage port** 命令在端口 30080/TCP 上为 **httpd** 设置适当的 SELinux 上下文，以便能绑定到此端口。

```
[root@serverb ~]# semanage port -a -t http_port_t -p tcp 30080
```

9.5. 使用 **systemctl** 命令来重启 **httpd**。此命令应该能成功重启该服务。

```
[root@serverb ~]# systemctl restart httpd
```

9.6. 向名为 **public** 的默认 **firewalld** 区域中添加端口 30080/TCP。

```
[root@serverb ~]# firewall-cmd --add-port=30080/tcp --permanent
success
[root@serverb ~]# firewall-cmd --reload
success
```

9.7. 退出 **root** 用户的 shell。

```
[root@serverb ~]# exit
logout
```

9.8. 从 **serverb** 注销。

```
[student@serverb ~]$ exit
logout
Connection to serverb closed.
```

海量视频题库 myitpub.com QQ:5565462
www.52myit.com

评估

在 workstation 上，运行 **lab rhcsa-compreview3 grade** 脚本来确认是否成功完成本练习。更正报告的所有错误并重新运行脚本，直到成功为止。

```
[student@workstation ~]$ lab rhcsa-compreview3 grade
```

完成

在 workstation 上，运行 **lab rhcsa-compreview3 finish** 来完成本练习。此脚本将删除在实验过程中创建的文件和资源，并确保环境清理干净。

```
[student@workstation ~]$ lab rhcsa-compreview3 finish
```

将想要保留的任何文件或工作保存到其他系统中，然后重置 workstation、servera 和 serverb。

本总复习到此结束。

海量视频题库 myitpub.com QQ:556462
www.52myit.com