Configuration Risks Remediation report for ip-10-129-93-150

Scanned on 2016-06-09 20:04:28 using CIS Benchmark for Red Hat Enterprise Linux 6 v1 - MDM policies

Found Issues

Critical	Rule Violated	Status	Remediation Suggestion

	9.2.13 Check User Home Directory Ownership	Failed	**Failed: User *dbus* home directory / owned by *root (UID 0)***
			POLICY SETTINGS
			User: **dbus**
			Home directory: **/**
			Expected home directory owner: **dbus (UID 81)**
			Actual home directory owner: **root (UID 0)**
			
			REMEDIATION SUGGESTION
			Change the ownership any home directories that are not owned by the defined user to the correct user.
			
			This script checks to make sure users own the home directory they are assigned to in the /etc/passwd file.
			
			#!/bin/bash
			cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
			if [$uid -ge 500 -a -d "$dir" -a $user != "nfsnobody"]; then
			owner=$(stat -L -c "%U" "$dir")
			if ["$owner" != "$user"]; then
			echo "The home directory ($dir) of user $user is owned by $owner."
			fi
			fi
			done
			
			Failed: User *haldaemon* home directory / owned by *root (UID 0)*
			POLICY SETTINGS
			User: **haldaemon**
			Home directory: **/**
			Expected home directory owner: **haldaemon (UID 68)**
			Actual home directory owner: **root (UID 0)**
			
			REMEDIATION SUGGESTION
			Change the ownership any home directories that are not owned by the defined user to the correct user.
			
			This script checks to make sure users own the home directory they are assigned to in the /etc/passwd file.
			
			#!/bin/bash
			cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
			if [$uid -ge 500 -a -d "$dir" -a $user != "nfsnobody"]; then
			owner=$(stat -L -c "%U" "$dir")
			if ["$owner" != "$user"]; then
			echo "The home directory ($dir) of user $user is owned by $owner."
			fi
			fi
			done
			
			Failed: User *ntp* home directory */etc/ntp* owned by *root (UID 0)*
			POLICY SETTINGS
			User: **ntp**
			Home directory: **/etc/ntp**
			Expected home directory owner: **ntp (UID 38)**
			Actual home directory owner: **root (UID 0)**
			
			REMEDIATION SUGGESTION
			Change the ownership any home directories that are not owned by the defined user to the correct user.
			
			This script checks to make sure users own the home directory they are assigned to in the /etc/passwd file.
			
			#!/bin/bash
			cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
			if [$uid -ge 500 -a -d "$dir" -a $user != "nfsnobody"]; then
			owner=$(stat -L -c "%U" "$dir")
			if ["$owner" != "$user"]; then
			echo "The home directory ($dir) of user $user is owned by $owner."
			fi
			fi
			done

Critical	Rule Violated	Status	Failed: User *apache* home directory */var/www* owned by *root (UID 0)*	Remediation Suggestion

POLICY SETTINGS

User: **apache**
Home directory: **/var/www**
Expected home directory owner: **apache (UID 48)**
Actual home directory owner: **root (UID 0)**

REMEDIATION SUGGESTION

Change the ownership any home directories that are not owned by the defined user to the correct user.

This script checks to make sure users own the home directory they are assigned to in the /etc/passwd file.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a -d "$dir" -a $user != "nfsnobody" ]; then
owner=$(stat -L -c "%U" "$dir")
if [ "$owner" != "$user" ]; then
echo "The home directory ($dir) of user $user is owned by $owner."
fi
fi
done
```

Passed: User *root* home directory */root* owned by *root (UID 0)*

POLICY SETTINGS

User: **root**
Home directory: **/root**
Expected home directory owner: **root (UID 0)**
Actual home directory owner: **root (UID 0)**

REMEDIATION SUGGESTION

Change the ownership any home directories that are not owned by the defined user to the correct user.

This script checks to make sure users own the home directory they are assigned to in the /etc/passwd file.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a -d "$dir" -a $user != "nfsnobody" ]; then
owner=$(stat -L -c "%U" "$dir")
if [ "$owner" != "$user" ]; then
echo "The home directory ($dir) of user $user is owned by $owner."
fi
fi
done
```

Passed: User *ec2-user* home directory */home/ec2-user* owned by *ec2-user (UID 500)*

POLICY SETTINGS

User: **ec2-user**
Home directory: **/home/ec2-user**
Expected home directory owner: **ec2-user (UID 500)**
Actual home directory owner: **ec2-user (UID 500)**

REMEDIATION SUGGESTION

Change the ownership any home directories that are not owned by the defined user to the correct user.

This script checks to make sure users own the home directory they are assigned to in the /etc/passwd file.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a -d "$dir" -a $user != "nfsnobody" ]; then
owner=$(stat -L -c "%U" "$dir")
if [ "$owner" != "$user" ]; then
echo "The home directory ($dir) of user $user is owned by $owner."
fi
fi
done
```

Passed: User *scom* home directory */home/scom* owned by *scom (UID 501)*

POLICY SETTINGS

User: **scom**
Home directory: **/home/scom**
Expected home directory owner: **scom (UID 501)**
Actual home directory owner: **scom (UID 501)**

REMEDIATION SUGGESTION

Change the ownership any home directories that are not owned by the defined user to the correct user.

This script checks to make sure users own the home directory they are assigned to in the /etc/passwd file.

Critical	Rule Violated	Status	Remediation Suggestion

#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [$uid -ge 500 -a -d "$dir" -a $user != "nfsnobody"]; then
owner=$(stat -L -c "%U" "$dir")
if ["$owner" != "$user"]; then
echo "The home directory ($dir) of user $user is owned by $owner."
fi
fi
done

Passed: User *oracle* home directory */home/oracle* owned by *oracle (UID 54321)*

POLICY SETTINGS

User: **oracle**
Home directory: **/home/oracle**
Expected home directory owner: **oracle (UID 54321)**
Actual home directory owner: **oracle (UID 54321)**

REMEDIATION SUGGESTION

Change the ownership any home directories that are not owned by the defined user to the correct user.

This script checks to make sure users own the home directory they are assigned to in the /etc/passwd file.

#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [$uid -ge 500 -a -d "$dir" -a $user != "nfsnobody"]; then
owner=$(stat -L -c "%U" "$dir")
if ["$owner" != "$user"]; then
echo "The home directory ($dir) of user $user is owned by $owner."
fi
fi
done

Indeterminate: User *adm* home directory */var/adm* could not be found
The target user defined in your policy's home directory does not exist. Please check your server configuration.

POLICY SETTINGS

User: **adm**
Home directory: **/var/adm**
Expected home directory owner: **adm (UID 3)**
Actual home directory owner: Home directory does not exist

REMEDIATION SUGGESTION

Change the ownership any home directories that are not owned by the defined user to the correct user.

This script checks to make sure users own the home directory they are assigned to in the /etc/passwd file.

#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [$uid -ge 500 -a -d "$dir" -a $user != "nfsnobody"]; then
owner=$(stat -L -c "%U" "$dir")
if ["$owner" != "$user"]; then
echo "The home directory ($dir) of user $user is owned by $owner."
fi
fi
done

Indeterminate: User *uucp* home directory */var/spool/uucp* could not be found
The target user defined in your policy's home directory does not exist. Please check your server configuration.

POLICY SETTINGS

User: **uucp**
Home directory: **/var/spool/uucp**
Expected home directory owner: **uucp (UID 10)**
Actual home directory owner: Home directory does not exist

REMEDIATION SUGGESTION

Change the ownership any home directories that are not owned by the defined user to the correct user.

This script checks to make sure users own the home directory they are assigned to in the /etc/passwd file.

#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [$uid -ge 500 -a -d "$dir" -a $user != "nfsnobody"]; then
owner=$(stat -L -c "%U" "$dir")
if ["$owner" != "$user"]; then
echo "The home directory ($dir) of user $user is owned by $owner."
fi
fi

Critical Rule Violated	Status	Remediation Suggestion
	done	

Indeterminate: User *gopher* home directory */var/gopher* could not be found
The target user defined in your policy's home directory does not exist. Please check your server configuration.

POLICY SETTINGS

User: **gopher**
Home directory: **/var/gopher**
Expected home directory owner: **gopher (UID 13)**
Actual home directory owner: Home directory does not exist

REMEDIATION SUGGESTION

Change the ownership any home directories that are not owned by the defined user to the correct user.

This script checks to make sure users own the home directory they are assigned to in the /etc/passwd file.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a -d "$dir" -a $user != "nfsnobody" ]; then
owner=$(stat -L -c "%U" "$dir")
if [ "$owner" != "$user" ]; then
echo "The home directory ($dir) of user $user is owned by $owner."
fi
fi
done
```

Indeterminate: User *ftp* home directory */var/ftp* could not be found
The target user defined in your policy's home directory does not exist. Please check your server configuration.

POLICY SETTINGS

User: **ftp**
Home directory: **/var/ftp**
Expected home directory owner: **ftp (UID 14)**
Actual home directory owner: Home directory does not exist

REMEDIATION SUGGESTION

Change the ownership any home directories that are not owned by the defined user to the correct user.

This script checks to make sure users own the home directory they are assigned to in the /etc/passwd file.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a -d "$dir" -a $user != "nfsnobody" ]; then
owner=$(stat -L -c "%U" "$dir")
if [ "$owner" != "$user" ]; then
echo "The home directory ($dir) of user $user is owned by $owner."
fi
fi
done
```

Indeterminate: User *saslauth* home directory */var/empty/saslauth* could not be found
The target user defined in your policy's home directory does not exist. Please check your server configuration.

POLICY SETTINGS

User: **saslauth**
Home directory: **/var/empty/saslauth**
Expected home directory owner: **saslauth (UID 499)**
Actual home directory owner: Home directory does not exist

REMEDIATION SUGGESTION

Change the ownership any home directories that are not owned by the defined user to the correct user.

This script checks to make sure users own the home directory they are assigned to in the /etc/passwd file.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a -d "$dir" -a $user != "nfsnobody" ]; then
owner=$(stat -L -c "%U" "$dir")
if [ "$owner" != "$user" ]; then
echo "The home directory ($dir) of user $user is owned by $owner."
fi
fi
done
```

Indeterminate: User *oprofile* home directory */home/oprofile* could not be found
The target user defined in your policy's home directory does not exist. Please check your server configuration.

Critical	Rule Violated	Status	POLICY SETTINGS	Remediation Suggestion

			User: **oprofile**
			Home directory: **/home/oprofile**
			Expected home directory owner: **oprofile (UID 16)**
			Actual home directory owner: Home directory does not exist
			
			REMEDIATION SUGGESTION
			
			Change the ownership any home directories that are not owned by the defined user to the correct user.
			
			This script checks to make sure users own the home directory they are assigned to in the /etc/passwd file.
			
			#!/bin/bash
			cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
			if [$uid -ge 500 -a -d "$dir" -a $user != "nfsnobody"]; then
			owner=$(stat -L -c "%U" "$dir")
			if ["$owner" != "$user"]; then
			echo "The home directory ($dir) of user $user is owned by $owner."
			fi
			fi
			done	

	9.2.12 Check That Users Are Assigned Valid Home Directories	Failed	**Failed: User *abrt* home directory */etc/abrt* could not be found** **POLICY SETTINGS** User: **abrt** Home directory: **/etc/abrt** Expected presence: **true** Actual presence: **false** **REMEDIATION SUGGESTION** If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi assigned a home directory as appropriate. This script checks to make sure that home directories assigned in the /etc/passwd file exist. #!/bin/bash cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do if [$uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody"]; then echo "The home directory ($dir) of user $user does not exist." fi done **Failed: User *oprofile* home directory */home/oprofile* could not be found** **POLICY SETTINGS** User: **oprofile** Home directory: **/home/oprofile** Expected presence: **true** Actual presence: **false** **REMEDIATION SUGGESTION** If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi assigned a home directory as appropriate. This script checks to make sure that home directories assigned in the /etc/passwd file exist. #!/bin/bash cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do if [$uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody"]; then echo "The home directory ($dir) of user $user does not exist." fi done **Passed: User *root* home directory */root* exists** **POLICY SETTINGS** User: **root** Home directory: **/root** Expected presence: **true** Actual presence: **true** **REMEDIATION SUGGESTION** If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi assigned a home directory as appropriate. This script checks to make sure that home directories assigned in the /etc/passwd file exist. #!/bin/bash cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do	

Critical	Rule Violated	Status		Remediation Suggestion

if [$uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody"]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done

Passed: User *bin* home directory */bin* exists
POLICY SETTINGS

User: **bin**
Home directory: **/bin**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi
assigned a home directory as appropriate.

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [$uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody"]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done

Passed: User *daemon* home directory */sbin* exists
POLICY SETTINGS

User: **daemon**
Home directory: **/sbin**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi
assigned a home directory as appropriate.

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [$uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody"]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done

Passed: User *lp* home directory */var/spool/lpd* exists
POLICY SETTINGS

User: **lp**
Home directory: **/var/spool/lpd**

Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi
assigned a home directory as appropriate.

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [$uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody"]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done

Passed: User *mail* home directory */var/spool/mail* exists
POLICY SETTINGS

User: **mail**
Home directory: **/var/spool/mail**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi
assigned a home directory as appropriate.

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

Critical	Rule Violated	Status	Remediation Suggestion

#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [$uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody"]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done

Passed: User *operator* home directory */root* exists
POLICY SETTINGS

User: **operator**
Home directory: **/root**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi
assigned a home directory as appropriate.

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [$uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody"]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done

Passed: User *games* home directory */usr/games* exists
POLICY SETTINGS

User: **games**
Home directory: **/usr/games**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi
assigned a home directory as appropriate.

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [$uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody"]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done

Passed: User *nobody* home directory / exists
POLICY SETTINGS

User: **nobody**
Home directory: **/**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi
assigned a home directory as appropriate.

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [$uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody"]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done

Passed: User *dbus* home directory / exists
POLICY SETTINGS

User: **dbus**
Home directory: **/**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi
assigned a home directory as appropriate.

Critical	Rule Violated	Status	Remediation Suggestion

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody" ]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done
```

Passed: User *vcsa* home directory */dev* exists

POLICY SETTINGS

User: **vcsa**
Home directory: **/dev**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi
assigned a home directory as appropriate.

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody" ]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done
```

Passed: User *haldaemon* home directory */ exists

POLICY SETTINGS

User: **haldaemon**
Home directory: **/**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi
assigned a home directory as appropriate.

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody" ]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done
```

Passed: User *ntp* home directory */etc/ntp* exists

POLICY SETTINGS

User: **ntp**
Home directory: **/etc/ntp**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi
assigned a home directory as appropriate.

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody" ]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done
```

Passed: User *postfix* home directory */var/spool/postfix* exists

POLICY SETTINGS

User: **postfix**
Home directory: **/var/spool/postfix**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi

Critical	Rule Violated	Status	Remediation Suggestion

assigned a home directory as appropriate.

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody" ]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done
```

Passed: User *sshd* home directory */var/empty/sshd* exists

POLICY SETTINGS

User: **sshd**
Home directory: **/var/empty/sshd**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi
assigned a home directory as appropriate.

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody" ]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done
```

Passed: User *ec2-user* home directory */home/ec2-user* exists

POLICY SETTINGS

User: **ec2-user**
Home directory: **/home/ec2-user**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi
assigned a home directory as appropriate.

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody" ]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done
```

Passed: User *scom* home directory */home/scom* exists

POLICY SETTINGS

User: **scom**
Home directory: **/home/scom**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi
assigned a home directory as appropriate.

This script checks to make sure that home directories assigned in the /etc/passwd file exist.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody" ]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done
```

Passed: User *apache* home directory */var/www* exists

POLICY SETTINGS

User: **apache**
Home directory: **/var/www**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

Critical	Rule Violated	Status	Remediation Suggestion
			If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi assigned a home directory as appropriate. This script checks to make sure that home directories assigned in the /etc/passwd file exist. #!/bin/bash cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do if [$uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody"]; then echo "The home directory ($dir) of user $user does not exist." fi done **Passed: User *oracle* home directory */home/oracle* exists** **POLICY SETTINGS** User: **oracle** Home directory: **/home/oracle** Expected presence: **true** Actual presence: **true** **REMEDIATION SUGGESTION** If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users wi assigned a home directory as appropriate. This script checks to make sure that home directories assigned in the /etc/passwd file exist. #!/bin/bash cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do if [$uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody"]; then echo "The home directory ($dir) of user $user does not exist." fi done
	6.3.3 Set Lockout For Failed Password Attempts	Failed	**Failed: String presence state for */etc/pam.d/system-auth* violates policy** **POLICY SETTINGS** File: **/etc/pam.d/system-auth** Expected match: **Contains** ^auth.*pam_faillock\.so Actual match: **false** **REMEDIATION SUGGESTION** Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files and add the "auth" lines as highlighted below. Ensu indicated (additional items may also appear here): # cat /etc/pam.d/password-auth #%PAM-1.0 # This file is auto-generated. # User changes will be destroyed the next time authconfig is run. auth required pam_env.so _auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900_ _auth [success=1 default=bad] pam_unix.so_ _auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900_ _auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900_ auth required pam_deny.so # cat /etc/pam.d/system-auth #%PAM-1.0 # This file is auto-generated. # User changes will be destroyed the next time authconfig is run. auth required pam_env.so _auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900_ _auth [success=1 default=bad] pam_unix.so_ _auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900_ _auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900_ auth required pam_deny.so NOTE: If a user has been locked out because they have reached the maximum consecutive failure count defined by der issuing the command /usr/sbin/faillock -u --reset. This command sets the failed count to 0, effectively unlocking the use Perform the following to determine the current settings for userID lockout. # grep "pam_faillock" /etc/pam.d/password-auth auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900 auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900 auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900 # grep "pam_unix.so" /etc/pam.d/password-auth | grep success=1 auth [success=1 default=bad] pam_unix.so # grep "pam_faillock" /etc/pam.d/system-auth auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900 auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900 auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900 # grep "pam_unix.so" /etc/pam.d/system-auth | grep success=1 auth [success=1 default=bad] pam_unix.so

Critical	Rule Violated	Status	Remediation Suggestion
			Failed: String presence state for */etc/pam.d/password-auth* violates policy **POLICY SETTINGS** File: **/etc/pam.d/password-auth** Expected match: **Contains** ^auth.*pam_faillock\.so Actual match: **false** **REMEDIATION SUGGESTION** Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files and add the "auth" lines as highlighted below. Ensu indicated (additional items may also appear here): # cat /etc/pam.d/password-auth #%PAM-1.0 # This file is auto-generated. # User changes will be destroyed the next time authconfig is run. auth required pam_env.so _auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900_ _auth [success=1 default=bad] pam_unix.so_ _auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900_ _auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900_ auth required pam_deny.so # cat /etc/pam.d/system-auth #%PAM-1.0 # This file is auto-generated. # User changes will be destroyed the next time authconfig is run. auth required pam_env.so _auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900_ _auth [success=1 default=bad] pam_unix.so_ _auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900_ _auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900_ auth required pam_deny.so NOTE: If a user has been locked out because they have reached the maximum consecutive failure count defined by der issuing the command /usr/sbin/faillock -u --reset. This command sets the failed count to 0, effectively unlocking the use Perform the following to determine the current settings for userID lockout. # grep "pam_faillock" /etc/pam.d/password-auth auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900 auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900 auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900 # grep "pam_unix.so" /etc/pam.d/password-auth | grep success=1 auth [success=1 default=bad] pam_unix.so # grep "pam_faillock" /etc/pam.d/system-auth auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900 auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900 auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900 # grep "pam_unix.so" /etc/pam.d/system-auth | grep success=1 auth [success=1 default=bad] pam_unix.so
	6.3.2 Set Password Creation Requirement Parameters Using Pam Cracklib	Failed	**Failed: String presence state for */etc/pam.d/system-auth* violates policy** **POLICY SETTINGS** File: **/etc/pam.d/system-auth** Expected match: **Contains** ^password\s+required\s+pam_cracklib\.so\s+ Actual match: **false** **REMEDIATION SUGGESTION** Set the pam_cracklib.so parameters as follows in /etc/pam.d/system-auth: password required pam_cracklib.so try_first_pass retry=3 minlen=14 dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1 Perform the following to determine the current settings in the pam_cracklib.so file. # grep pam_cracklib.so /etc/pam.d/system-auth password required pam_cracklib.so try_first_pass retry=3 minlen=14 dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1
	6.2.12 Set Idle Timeout Interval For User Login	Failed	**Failed : Value for *ClientAliveInterval* setting in */etc/ssh/sshd_config* violates policy** **POLICY SETTINGS** Configuration file: **/etc/ssh/sshd_config** Configuration item: **ClientAliveInterval** Expected value: **300** Actual value: **900** **REMEDIATION SUGGESTION** Edit the /etc/ssh/sshd_config file to set the parameter as follows: ClientAliveInterval 300

Critical	Rule Violated	Status	ClientAliveCountMax 0 Remediation Suggestion
			To verify the correct SSH setting, run the following command and verify that the output is as shown: # grep "^ClientAliveInterval" /etc/ssh/sshd_config ClientAliveInterval 300 # grep "^ClientAliveCountMax" /etc/ssh/sshd_config ClientAliveCountMax 0 **Passed : Value for *ClientAliveCountMax* setting in */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** Configuration file: **/etc/ssh/sshd_config** Configuration item: **ClientAliveCountMax** Expected value: **0** Actual value: **0** **REMEDIATION SUGGESTION** Edit the /etc/ssh/sshd_config file to set the parameter as follows: ClientAliveCountMax 0
	6.2.3 Set Permissions On /Etc/Ssh/Sshd Config	Failed	**Failed: ACL *644* for file */etc/ssh/sshd_config* violates policy** **POLICY SETTINGS** File: **/etc/ssh/sshd_config** Expected ACL: **600** Actual ACL: **644** **REMEDIATION SUGGESTION** # chmod 600 /etc/ssh/sshd_config **Passed: User owner *root* for file */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** File: **/etc/ssh/sshd_config** Expected owner: **root** Actual owner: **root** **REMEDIATION SUGGESTION** If the user and group ownership of the /etc/ssh/sshd_config file are incorrect, run the following command to correct then # chown root:root /etc/ssh/sshd_config If the permissions are incorrect, run the following command to correct them: # chmod 600 /etc/ssh/sshd_config Run the following command to determine the user and group ownership on the /etc/ssh/sshd_config file. # /bin/ls -l /etc/ssh/sshd_config -rw------- 1 root root 762 Sep 23 002 /etc/ssh/sshd_config **Passed: Group owner *root* for file */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** File: **/etc/ssh/sshd_config** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/ssh/sshd_config
	6.1.11 Restrict At/Cron To Authorized Users	Failed	**Failed: File presence state for */etc/cron.deny* violates policy** **POLICY SETTINGS** File: **/etc/cron.deny** Expected presence: **false** Actual presence: **true** **REMEDIATION SUGGESTION** If /etc/cron.allow or /etc/at.allow do not exist on your system create them. Run the following to ensure cron.deny and at.deny are removed and permissions are set correctly: # /bin/rm /etc/cron.deny # /bin/rm /etc/at.deny # chmod og-rwx /etc/cron.allow # chmod og-rwx /etc/at.allow

Critical	Rule Violated	Status	# chown root:root /etc/cron.allow # chown root:root /etc/at.allow	Remediation Suggestion

Perform the following to determine if the remediation in the section has been performed:

ls -l /etc/cron.deny
[no output returned]
ls -l /etc/at.deny
[no output returned]
ls -l /etc/cron.allow
-rw------- 1 root root /etc/cron.allow
ls -l /etc/at.allow
-rw------- 1 root root /etc/at.allow

Passed: File presence state for *_/etc/at.deny_* is compliant

POLICY SETTINGS

File: **/etc/at.deny**
Expected presence: **false**
Actual presence: **false**

REMEDIATION SUGGESTION

If /etc/cron.allow or /etc/at.allow do not exist on your system create them.

Run the following to ensure cron.deny and at.deny are removed and permissions are set correctly:

/bin/rm /etc/cron.deny
/bin/rm /etc/at.deny
chmod og-rwx /etc/cron.allow
chmod og-rwx /etc/at.allow
chown root:root /etc/cron.allow
chown root:root /etc/at.allow

Perform the following to determine if the remediation in the section has been performed:

ls -l /etc/cron.deny
[no output returned]
ls -l /etc/at.deny
[no output returned]
ls -l /etc/cron.allow
-rw------- 1 root root /etc/cron.allow
ls -l /etc/at.allow
-rw------- 1 root root /etc/at.allow

Passed: File presence state for *_/etc/cron.allow_* is compliant

POLICY SETTINGS

File: **/etc/cron.allow**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

touch /etc/cron.allow
touch /etc/at.allow

Passed: File presence state for *_/etc/at.allow_* is compliant

POLICY SETTINGS

File: **/etc/at.allow**
Expected presence: **true**
Actual presence: **true**

REMEDIATION SUGGESTION

touch /etc/cron.allow
touch /etc/at.allow

Passed: User owner *_root_* for file *_/etc/cron.allow_* is compliant

POLICY SETTINGS

File: **/etc/cron.allow**
Expected owner: **root**
Actual owner: **root**

REMEDIATION SUGGESTION

touch /etc/cron.allow
touch /etc/at.allow
chown root:root /etc/cron.allow
chown root:root /etc/at.allow

Passed: User owner *_root_* for file *_/etc/at.allow_* is compliant

POLICY SETTINGS

File: **/etc/at.allow**

Critical	Rule Violated	Status	Remediation Suggestion
			Expected owner: **root** Actual owner: **root** **REMEDIATION SUGGESTION** # touch /etc/cron.allow # touch /etc/at.allow # chown root:root /etc/cron.allow # chown root:root /etc/at.allow **Passed: Group owner *root* for file */etc/cron.allow* is compliant** **POLICY SETTINGS** File: **/etc/cron.allow** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** # touch /etc/cron.allow # touch /etc/at.allow # chown root:root /etc/cron.allow # chown root:root /etc/at.allow **Passed: Group owner *root* for file */etc/at.allow* is compliant** **POLICY SETTINGS** File: **/etc/at.allow** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** # touch /etc/cron.allow # touch /etc/at.allow # chown root:root /etc/cron.allow # chown root:root /etc/at.allow **Passed: ACL *600* for file */etc/cron.allow* is compliant** **POLICY SETTINGS** File: **/etc/cron.allow** Expected ACL: ***00** Actual ACL: **600** **REMEDIATION SUGGESTION** # chmod og-rwx /etc/cron.allow # chmod og-rwx /etc/at.allow **Passed: ACL *600* for file */etc/at.allow* is compliant** **POLICY SETTINGS** File: **/etc/at.allow** Expected ACL: ***00** Actual ACL: **600** **REMEDIATION SUGGESTION** # chmod og-rwx /etc/cron.allow # chmod og-rwx /etc/at.allow
	5.3 Configure Logrotate	Failed	**Failed: String presence state for */etc/logrotate.d/syslog* violates policy** **POLICY SETTINGS** File: **/etc/logrotate.d/syslog** Expected match: **Contains** \/var\/log\/boot\.log Actual match: **false** **REMEDIATION SUGGESTION** Edit the /etc/logrotate.d/syslog file to include appropriate system logs: /var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log /var/log/cron { **Passed: String presence state for */etc/logrotate.d/syslog* is compliant** **POLICY SETTINGS** File: **/etc/logrotate.d/syslog** Expected match: **Contains** \/var\/log\/messages Actual match: **true** **REMEDIATION SUGGESTION**

Critical	Rule Violated	Status	Remediation Suggestion
			Edit the /etc/logrotate.d/syslog file to include appropriate system logs: /var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log /var/log/cron { Perform the following to determine if the appropriate system logs are rotated. # grep '{' /etc/logrotate.d/syslog /var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log /var/log/cron { **Passed: String presence state for */etc/logrotate.d/syslog* is compliant** **POLICY SETTINGS** File: **/etc/logrotate.d/syslog** Expected match: **Contains** \/var\/log\/secure Actual match: **true** **REMEDIATION SUGGESTION** Edit the /etc/logrotate.d/syslog file to include appropriate system logs: /var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log /var/log/cron { **Passed: String presence state for */etc/logrotate.d/syslog* is compliant** **POLICY SETTINGS** File: **/etc/logrotate.d/syslog** Expected match: **Contains** \/var\/log\/maillog Actual match: **true** **REMEDIATION SUGGESTION** Edit the /etc/logrotate.d/syslog file to include appropriate system logs: /var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log /var/log/cron { **Passed: String presence state for */etc/logrotate.d/syslog* is compliant** **POLICY SETTINGS** File: **/etc/logrotate.d/syslog** Expected match: **Contains** \/var\/log\/spooler Actual match: **true** **REMEDIATION SUGGESTION** Edit the /etc/logrotate.d/syslog file to include appropriate system logs: /var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log /var/log/cron { **Passed: String presence state for */etc/logrotate.d/syslog* is compliant** **POLICY SETTINGS** File: **/etc/logrotate.d/syslog** Expected match: **Contains** \/var\/log\/cron Actual match: **true** **REMEDIATION SUGGESTION**

	5.2.1.2 Disable System On Audit Log Full	Failed	Edit the /etc/logrotate.d/syslog file to include appropriate system logs:
			/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log /var/log/cron {
			Failed : Value for *space_left_action* setting in */etc/audit/auditd.conf* violates policy
			POLICY SETTINGS
			Configuration file: **/etc/audit/auditd.conf**
			Configuration item: **space_left_action**
			Expected value: **email**
			Actual value: **SYSLOG**
			
			REMEDIATION SUGGESTION
			Add the following lines to the /etc/audit/auditd.conf file.
			
			space_left_action = email
			action_mail_acct = root
			admin_space_left_action = halt
			
			Perform the following to determine if auditd is configured to notify the administrator and halt the system when audit logs
			
			# grep space_left_action /etc/audit/auditd.conf
			space_left_action = email
			# grep action_mail_acct /etc/audit/auditd.conf
			action_mail_acct = root
			# grep admin_space_left_action /etc/audit/auditd.conf
			admin_space_left_action = halt
			Failed : Value for *admin_space_left_action* setting in */etc/audit/auditd.conf* violates policy
			POLICY SETTINGS
			Configuration file: **/etc/audit/auditd.conf**

Critical	Rule Violated	Status	Remediation Suggestion
			Configuration item: **admin_space_left_action** Expected value: **halt** Actual value: **SUSPEND** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/auditd.conf file: admin_space_left_action = halt **Passed : Value for *action_mail_acct* setting in */etc/audit/auditd.conf* is compliant** **POLICY SETTINGS** Configuration file: **/etc/audit/auditd.conf** Configuration item: **action_mail_acct** Expected value: **root** Actual value: **root** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/auditd.conf file: action_mail_acct = root
	5.1.6 Accept Remote Rsyslog Messages Only On Designated Log Hosts	Failed	**Failed: String presence state for */etc/rsyslog.conf* violates policy** **POLICY SETTINGS** File: **/etc/rsyslog.conf** Expected match: **Contains** ^\$InputTCPServerRun\s+514 Actual match: **false** **REMEDIATION SUGGESTION** On hosts that are designated as log hosts edit the /etc/rsyslog.conf file and un-comment the following lines: $ModLoad imtcp.so $InputTCPServerRun 514 NOTE: On hosts that are not designated log hosts these lines should be commented out instead. Execute the following command to restart rsyslogd: # pkill -HUP rsyslogd Run the following to determine if rsyslog is listening for remote messages: # grep '$ModLoad imtcp.so' /etc/rsyslog.conf $ModLoad imtcp.so # grep '$InputTCPServerRun' /etc/rsyslog.conf $InputTCPServerRun 514 **Failed: String presence state for */etc/rsyslog.conf* violates policy** **POLICY SETTINGS** File: **/etc/rsyslog.conf** Expected match: **Contains** ^\$ModLoad imtcp\.so Actual match: **false** **REMEDIATION SUGGESTION** For hosts that are designated as log hosts, edit the /etc/rsyslog.conf file and uncomment the following lines: $ModLoad imtcp.so Execute the following command to restart rsyslogd: # pkill -HUP rsyslogd
	4.5.4 Create /Etc/Hosts.Deny	Failed	**Failed : Value for *ALL* setting in */etc/hosts.deny* violates policy** **POLICY SETTINGS** Configuration file: **/etc/hosts.deny** Configuration item: **ALL** Expected value: **ALL** Actual value: ***Configuration item not found*** **REMEDIATION SUGGESTION** Create /etc/hosts.deny: # echo "ALL: ALL" >> /etc/hosts.deny Verify that /etc/hosts.deny exists and is configured to deny all hosts not explicitly listed in /etc/hosts.allow: # grep "ALL: ALL" /etc/hosts.deny ALL: ALL
	4.4.2 Disable I Pv6	Failed	**Failed : Value for *IPV6INIT* setting in */etc/sysconfig/network* violates policy** **POLICY SETTINGS**

Critical	Rule Violated	Status	Remediation Suggestion

			Configuration file: **/etc/sysconfig/network**
			Configuration item: **IPV6INIT**
			Expected value: **no**
			Actual value: ***Configuration item not found***
			
			REMEDIATION SUGGESTION
			
			Edit /etc/sysconfig/network, and add the following line:
			NETWORKING_IPV6=no
			IPV6INIT=no
			
			Create the file /etc/modprobe.d/ipv6.conf and add the following lines:
			options ipv6 disable=1
			
			Perform the following command to turn ip6tables off:
			# /sbin/chkconfig ip6tables off
			
			Passed : Value for *NETWORKING_IPV6* setting in */etc/sysconfig/network* is compliant
			POLICY SETTINGS
			
			Configuration file: **/etc/sysconfig/network**
			
			Configuration item: **NETWORKING_IPV6**
			Expected value: **no**
			Actual value: **no**
			
			REMEDIATION SUGGESTION
			
			Edit /etc/sysconfig/network, and add the following line:
			
			NETWORKING_IPV6=no
			IPV6INIT=no
			
			Create the file /etc/modprobe.d/ipv6.conf and add the following lines:
			
			options ipv6 disable=1
			
			Perform the following command to turn ip6tables off:
			
			# /sbin/chkconfig ip6tables off
			
			Perform the following to determine if IPv6 is enabled
			
			# grep NETWORKING_IPV6 /etc/sysconfig/network
			NETWORKING_IPV6=no
			# grep IPV6INIT /etc/sysconfig/network
			IPV6INIT=no
			# grep ipv6 /etc/modprobe.d/ipv6.conf
			options ipv6 disable=1
			
			Indeterminate: presence */etc/modprobe.d/ipv6.conf* could not be found
			POLICY SETTINGS
			
			File: **/etc/modprobe.d/ipv6.conf**
			Expected match: **Contains** ^options\s+ipv6\s+disable\s*=\s*1
			Actual match: **false**
			
			REMEDIATION SUGGESTION
			
			Edit /etc/sysconfig/network, and add the following line:
			NETWORKING_IPV6=no
			IPV6INIT=no
			
			Create the file /etc/modprobe.d/ipv6.conf and add the following lines:
			options ipv6 disable=1
			
			Perform the following command to turn ip6tables off:
			# /sbin/chkconfig ip6tables off

	4.4.1.2 Disable IPv6 Redirect Acceptance	Failed	**Failed : Value for setting in */proc/sys/net/ipv6/conf/all/accept_redirects* violates policy** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv6/conf/all/accept_redirects** Configuration item: Expected value: **0** Actual value: **1** **REMEDIATION SUGGESTION** Set the net.ipv6.conf.all.accept_redirects and net.ipv6.conf.default.accept_redirects parameters to 0 in /etc/sysctl.conf: net.ipv6.conf.all.accept_redirects=0 net.ipv6.conf.default.accept_redirects=0 Modify active kernel parameters to match:

Critical	Rule Violated	Status	Remediation Suggestion
			# /sbin/sysctl -w net.ipv6.conf.all.accept_redirects=0 # /sbin/sysctl -w net.ipv6.conf.default.accept_redirects=0 # /sbin/sysctl -w net.ipv6.route.flush=1 Perform the following to determine if IPv6 redirects are disabled. # /sbin/sysctl net.ipv6.conf.all.accept_redirects net.ipv6.conf.all.accept_redirect = 0 # /sbin/sysctl net.ipv6.conf.default.accept_redirects net.ipv6.conf.default.accept_redirect = 0 **Failed : Value for setting in *<u>/proc/sys/net/ipv6/conf/default/accept_redirects</u>* violates policy** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv6/conf/default/accept_redirects** Configuration item: Expected value: **0** Actual value: **1** **REMEDIATION SUGGESTION** Set the net.ipv6.conf.all.accept_redirects and net.ipv6.conf.default.accept_redirects parameters to 0 in /etc/sysctl.conf: net.ipv6.conf.all.accept_redirects=0 net.ipv6.conf.default.accept_redirects=0 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv6.conf.all.accept_redirects=0 # /sbin/sysctl -w net.ipv6.conf.default.accept_redirects=0 # /sbin/sysctl -w net.ipv6.route.flush=1
	4.4.1.1 Disable IPv6 Router Advertisements	Failed	**Failed : Value for setting in *<u>/proc/sys/net/ipv6/conf/all/accept_ra</u>* violates policy** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv6/conf/all/accept_ra** Configuration item: Expected value: **0** Actual value: **1** **REMEDIATION SUGGESTION** Set the net.ipv6.conf.all.accept_ra and net.ipv6.conf.default.accept_ra parameter to 0 in /etc/sysctl.conf: net.ipv6.conf.all.accept_ra=0 net.ipv6.conf.default.accept_ra=0 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv6.conf.all.accept_ra=0 # /sbin/sysctl -w net.ipv6.conf.default.accept_ra=0 # /sbin/sysctl -w net.ipv6.route.flush=1 Perform the following to determine if the system is disabled from accepting router advertisements: # /sbin/sysctl net.ipv6.conf.all.accept_ra net.ipv6.conf.all.accept_ra = 0 # /sbin/sysctl net.ipv6.conf.default.accept_ra net.ipv6.conf.default.accept_ra = 0 **Failed : Value for setting in *<u>/proc/sys/net/ipv6/conf/default/accept_ra</u>* violates policy** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv6/conf/default/accept_ra** Configuration item: Expected value: **0** Actual value: **1** **REMEDIATION SUGGESTION** Set the net.ipv6.conf.all.accept_ra and net.ipv6.conf.default.accept_ra parameter to 0 in /etc/sysctl.conf: net.ipv6.conf.all.accept_ra=0 net.ipv6.conf.default.accept_ra=0 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv6.conf.all.accept_ra=0 # /sbin/sysctl -w net.ipv6.conf.default.accept_ra=0 # /sbin/sysctl -w net.ipv6.route.flush=1
	3.11 Remove Http Server	Failed	**Failed : package presence state for package *<u>httpd</u>* violates policy** **POLICY SETTINGS** Package: **httpd** Expected presence: **false** Actual presence: **true**

Critical	Rule Violated	Status	REMEDIATION SUGGESTION	Remediation Suggestion
			# yum erase httpd Perform the following to determine if apache is disabled. # rpm -q httpd package httpd is not installed	
	1.7 Use The Latest Os Release	Failed	**Failed: String presence state for ** violates policy** **POLICY SETTINGS** File: **/etc/redhat-release** Expected match: **Contains** ^Red Hat Enterprise\s.*release\s+6\.7\s+(Santiago) Actual match: **false** **REMEDIATION SUGGESTION** Use the latest update when installing new systems and upgrade to or reinstall with the latest update as appropriate for Run the following command to determine the current OS level: # uname -r or # cat /etc/redhat-release	
	1.1.17 Set Sticky Bit On All World Writable Directories	Failed	**Failed: one or more directories are world writable without sticky bit.** **POLICY SETTINGS** Excluded Path(s): Expected world writable directories without sticky bit: **0** Actual world writable directories without sticky bit: **628**	

Path	
/mdminsdir	rc
/mdminsdir/installers	rc
/mdminsdir/installers/MDM10.1_HF1	U (1
/mdminsdir/installers/client	o
/mdminsdir/installers/client/install	o
/mdminsdir/installers/client/install/images	o
/mdminsdir/installers/client/install/resource	o
/mdminsdir/installers/client/response	o
/mdminsdir/installers/client/stage	o
/mdminsdir/installers/client/stage/Actions	o
/mdminsdir/installers/client/stage/Actions/OEMRegistry	o
/mdminsdir/installers/client/stage/Actions/OEMRegistry/1.5.6	o
/mdminsdir/installers/client/stage/Actions/OEMRegistry/1.5.6/1	o

Critical Rule Violated	Status		Remediation Suggestion
		/mdminsdir/installers/client/stage/Actions/ServiceProcessActions	o
		/mdminsdir/installers/client/stage/Actions/ServiceProcessActions/1.0	o
		/mdminsdir/installers/client/stage/Actions/ServiceProcessActions/1.0/1	o
		/mdminsdir/installers/client/stage/Actions/SpawnActions	o
		/mdminsdir/installers/client/stage/Actions/SpawnActions/10.1.0.3.4	o
		/mdminsdir/installers/client/stage/Actions/SpawnActions/10.1.0.3.4/1	o
		/mdminsdir/installers/client/stage/Actions/WindowsActionLib	o
		/mdminsdir/installers/client/stage/Actions/WindowsActionLib/12.0.0.0.0	o
		/mdminsdir/installers/client/stage/Actions/WindowsActionLib/12.0.0.0.0/1	o
		/mdminsdir/installers/client/stage/Actions/clusterActions	o
		/mdminsdir/installers/client/stage/Actions/clusterActions/10.1.0.2.0	o
		/mdminsdir/installers/client/stage/Actions/clusterActions/10.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Actions/customFileActions	o
		/mdminsdir/installers/client/stage/Actions/customFileActions/1.2.1	o
		/mdminsdir/installers/client/stage/Actions/customFileActions/1.2.1/1	o
		/mdminsdir/installers/client/stage/Actions/dbActions	o
		/mdminsdir/installers/client/stage/Actions/dbActions/10.1.0.2.0	o
		/mdminsdir/installers/client/stage/Actions/dbActions/10.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Actions/docActionLib	o
		/mdminsdir/installers/client/stage/Actions/docActionLib/2.2	o
		/mdminsdir/installers/client/stage/Actions/docActionLib/2.2/1	o
		/mdminsdir/installers/client/stage/Actions/fileActions	o

Critical	Rule Violated	Status	/mdminsdir/installers/client/stage/Actions/fileActions/11.2.0.2.0	Remediation Suggestion	o
			/mdminsdir/installers/client/stage/Actions/fileActions/11.2.0.2.0/1		o
			/mdminsdir/installers/client/stage/Actions/generalActions		o
			/mdminsdir/installers/client/stage/Actions/generalActions/10.2.0.9.0		o
			/mdminsdir/installers/client/stage/Actions/generalActions/10.2.0.9.0/1		o
			/mdminsdir/installers/client/stage/Actions/jarActions		o
			/mdminsdir/installers/client/stage/Actions/jarActions/10.2.0.0.0		o
			/mdminsdir/installers/client/stage/Actions/jarActions/10.2.0.0.0/1		o
			/mdminsdir/installers/client/stage/Actions/launchPadActions		o
			/mdminsdir/installers/client/stage/Actions/launchPadActions/10.1.0.2.0		o
			/mdminsdir/installers/client/stage/Actions/launchPadActions/10.1.0.2.0/1		o
			/mdminsdir/installers/client/stage/Actions/ntActionLib		o
			/mdminsdir/installers/client/stage/Actions/ntActionLib/11.1.0.0.0		o
			/mdminsdir/installers/client/stage/Actions/ntActionLib/11.1.0.0.0/1		o
			/mdminsdir/installers/client/stage/Actions/ntCrsActionLib		o
			/mdminsdir/installers/client/stage/Actions/ntCrsActionLib/10.2.0.1.0		o
			/mdminsdir/installers/client/stage/Actions/ntCrsActionLib/10.2.0.1.0/1		o
			/mdminsdir/installers/client/stage/Actions/ntGrpActionLib		o
			/mdminsdir/installers/client/stage/Actions/ntGrpActionLib/10.2.0.1.0		o
			/mdminsdir/installers/client/stage/Actions/ntGrpActionLib/10.2.0.1.0/1		o
			/mdminsdir/installers/client/stage/Actions/ntServicesActions		o
			/mdminsdir/installers/client/stage/Actions/ntServicesActions/10.2.0.6.0		o
			/mdminsdir/installers/client/stage/Actions/ntServicesActions/10.2.0.6.0/1		o

Critical	Rule Violated	Status		Remediation Suggestion
			/mdminsdir/installers/client/stage/Actions/ntw32FoldersActions	o
			/mdminsdir/installers/client/stage/Actions/ntw32FoldersActions/10.2.0.3.0	o
			/mdminsdir/installers/client/stage/Actions/ntw32FoldersActions/10.2.0.3.0/1	o
			/mdminsdir/installers/client/stage/Actions/oradim	o
			/mdminsdir/installers/client/stage/Actions/oradim/10.1.0.3.0	o
			/mdminsdir/installers/client/stage/Actions/oradim/10.1.0.3.0/1	o
			/mdminsdir/installers/client/stage/Actions/rgsActions	o
			/mdminsdir/installers/client/stage/Actions/rgsActions/10.1.0.3.0	o
			/mdminsdir/installers/client/stage/Actions/rgsActions/10.1.0.3.0/1	o
			/mdminsdir/installers/client/stage/Actions/textFileActions	o
			/mdminsdir/installers/client/stage/Actions/textFileActions/2.1.0.3.1	o
			/mdminsdir/installers/client/stage/Actions/textFileActions/2.1.0.3.1/1	o
			/mdminsdir/installers/client/stage/Actions/unixActions	o
			/mdminsdir/installers/client/stage/Actions/unixActions/10.2.0.3.0	o
			/mdminsdir/installers/client/stage/Actions/unixActions/10.2.0.3.0/1	o
			/mdminsdir/installers/client/stage/Actions/w32OcxRegActions	o
			/mdminsdir/installers/client/stage/Actions/w32OcxRegActions/10.2.0.1.0	o
			/mdminsdir/installers/client/stage/Actions/w32OcxRegActions/10.2.0.1.0/1	o
			/mdminsdir/installers/client/stage/Actions/w32RegActions	o
			/mdminsdir/installers/client/stage/Actions/w32RegActions/10.2.0.1.0	o
			/mdminsdir/installers/client/stage/Actions/w32RegActions/10.2.0.1.0/1	o
			/mdminsdir/installers/client/stage/Actions/wingeneralActions	o

Critical Rule Violated	Status			
		/mdminsdir/installers/client/stage/Actions/wingeneralActions/10.2.0.1.0	**Remediation Suggestion**	o
		/mdminsdir/installers/client/stage/Actions/wingeneralActions/10.2.0.1.0/1		o
		/mdminsdir/installers/client/stage/ComponentList		o
		/mdminsdir/installers/client/stage/Components		o
		/mdminsdir/installers/client/stage/Components/oracle.assistants.acf		o
		/mdminsdir/installers/client/stage/Components/oracle.assistants.acf/12.1.0.2.0		o
		/mdminsdir/installers/client/stage/Components/oracle.assistants.acf/12.1.0.2.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.assistants.acf/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.assistants.deconfig		o
		/mdminsdir/installers/client/stage/Components/oracle.assistants.deconfig/12.1.0.2.0		o
		/mdminsdir/installers/client/stage/Components/oracle.assistants.deconfig/12.1.0.2.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.assistants.deconfig/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.assistants.netca.client		o
		/mdminsdir/installers/client/stage/Components/oracle.assistants.netca.client/12.1.0.2.0		o
		/mdminsdir/installers/client/stage/Components/oracle.assistants.netca.client/12.1.0.2.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.assistants.netca.client/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.bali.dbui4		o
		/mdminsdir/installers/client/stage/Components/oracle.bali.dbui4/11.0.0.0.0		o
		/mdminsdir/installers/client/stage/Components/oracle.bali.dbui4/11.0.0.0.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.bali.dbui4/11.0.0.0.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.bali.ewt		o
		/mdminsdir/installers/client/stage/Components/oracle.bali.ewt/11.1.1.6.0		o
		/mdminsdir/installers/client/stage/Components/oracle.bali.ewt/11.1.1.6.0/1		o

Critical	Rule Violated	Status	Remediation Suggestion
		/mdminsdir/installers/client/stage/Components/oracle.bali.ewt/11.1.1.6.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.ice	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.ice/11.1.1.7.0	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.ice/11.1.1.7.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.ice/11.1.1.7.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.jewt	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.jewt/11.1.1.6.0	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.jewt/11.1.1.6.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.jewt/11.1.1.6.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.jle3	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.jle3/11.0.0.0.0	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.jle3/11.0.0.0.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.jle3/11.0.0.0.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.share	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.share/11.1.1.6.0	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.share/11.1.1.6.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.bali.share/11.1.1.6.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.buildtools.common	o
		/mdminsdir/installers/client/stage/Components/oracle.buildtools.common/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.buildtools.common/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.buildtools.common/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.buildtools.rsf	o

Critical Rule Violated	Status	Remediation Suggestion
	/mdminsdir/installers/client/stage/Components/oracle.buildtools.rsf/12.1.0.2.0	o
	/mdminsdir/installers/client/stage/Components/oracle.buildtools.rsf/12.1.0.2.0/1	o
	/mdminsdir/installers/client/stage/Components/oracle.buildtools.rsf/12.1.0.2.0/1/DataFiles	o
	/mdminsdir/installers/client/stage/Components/oracle.client	o
	/mdminsdir/installers/client/stage/Components/oracle.client/12.1.0.2.0	o
	/mdminsdir/installers/client/stage/Components/oracle.client/12.1.0.2.0/1	o
	/mdminsdir/installers/client/stage/Components/oracle.client/12.1.0.2.0/1/DataFiles	o
	/mdminsdir/installers/client/stage/Components/oracle.dbdev	o
	/mdminsdir/installers/client/stage/Components/oracle.dbdev/12.1.0.2.0	o
	/mdminsdir/installers/client/stage/Components/oracle.dbdev/12.1.0.2.0/1	o
	/mdminsdir/installers/client/stage/Components/oracle.dbdev/12.1.0.2.0/1/DataFiles	o
	/mdminsdir/installers/client/stage/Components/oracle.dbjava.ic	o
	/mdminsdir/installers/client/stage/Components/oracle.dbjava.ic/12.1.0.2.0	o
	/mdminsdir/installers/client/stage/Components/oracle.dbjava.ic/12.1.0.2.0/1	o
	/mdminsdir/installers/client/stage/Components/oracle.dbjava.ic/12.1.0.2.0/1/DataFiles	o
	/mdminsdir/installers/client/stage/Components/oracle.dbjava.jdbc	o
	/mdminsdir/installers/client/stage/Components/oracle.dbjava.jdbc/12.1.0.2.0	o
	/mdminsdir/installers/client/stage/Components/oracle.dbjava.jdbc/12.1.0.2.0/1	o
	/mdminsdir/installers/client/stage/Components/oracle.dbjava.jdbc/12.1.0.2.0/1/DataFiles	o
	/mdminsdir/installers/client/stage/Components/oracle.dbjava.jdbc/12.1.0.2.0/1/DataFiles/Expanded	o
	/mdminsdir/installers/client/stage/Components/oracle.dbjava.jdbc/12.1.0.2.0/1/DataFiles/Expanded/filegroup2	o
	/mdminsdir/installers/client/stage/Components/oracle.dbjava.jdbc/12.1.0.2.0/1/DataFiles/Expanded/filegroup3	o
	/mdminsdir/installers/client/stage/Components/oracle.dbjava.ucp	o

Critical	Rule Violated	Status		Remediation Suggestion
			/mdminsdir/installers/client/stage/Components/oracle.dbjava.ucp/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.dbjava.ucp/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.dbjava.ucp/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.dbjava.ucp/12.1.0.2.0/1/DataFiles/Expanded	o
			/mdminsdir/installers/client/stage/Components/oracle.dbjava.ucp/12.1.0.2.0/1/DataFiles/Expanded/filegroup2	o
			/mdminsdir/installers/client/stage/Components/oracle.dbjava.ucp/12.1.0.2.0/1/DataFiles/Expanded/filegroup3	o
			/mdminsdir/installers/client/stage/Components/oracle.duma	o
			/mdminsdir/installers/client/stage/Components/oracle.duma/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.duma/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.duma/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.has.common	o
			/mdminsdir/installers/client/stage/Components/oracle.has.common.cvu	o
			/mdminsdir/installers/client/stage/Components/oracle.has.common.cvu/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.has.common.cvu/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.has.common.cvu/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.has.common/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.has.common/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.has.common/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.has.deconfig	o
			/mdminsdir/installers/client/stage/Components/oracle.has.deconfig/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.has.deconfig/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.has.deconfig/12.1.0.2.0/1/DataFiles	o

Critical Rule Violated	Status		Remediation Suggestion
		/mdminsdir/installers/client/stage/Components/oracle.has.rsf	o
		/mdminsdir/installers/client/stage/Components/oracle.has.rsf/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.has.rsf/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.has.rsf/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.help.ohj	o
		/mdminsdir/installers/client/stage/Components/oracle.help.ohj/11.1.1.7.0	o
		/mdminsdir/installers/client/stage/Components/oracle.help.ohj/11.1.1.7.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.help.ohj/11.1.1.7.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.help.share	o
		/mdminsdir/installers/client/stage/Components/oracle.help.share/11.1.1.7.0	o
		/mdminsdir/installers/client/stage/Components/oracle.help.share/11.1.1.7.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.help.share/11.1.1.7.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.install.deinstalltool	o
		/mdminsdir/installers/client/stage/Components/oracle.install.deinstalltool/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.install.deinstalltool/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.install.deinstalltool/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.javavm.client	o
		/mdminsdir/installers/client/stage/Components/oracle.javavm.client/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.javavm.client/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.javavm.client/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.javavm.client/12.1.0.2.0/1/DataFiles/Expanded	o
		/mdminsdir/installers/client/stage/Components/oracle.javavm.client/12.1.0.2.0/1/DataFiles/Expanded/filegroup1	o

Critical Rule Violated	Status	/mdminsdir/installers/client/stage/Components/oracle.javavm.client/12.1.0.2.0/1/DataFiles/Expanded/filegroup2	Remediation Suggestion	o
		/mdminsdir/installers/client/stage/Components/oracle.jdk		o
		/mdminsdir/installers/client/stage/Components/oracle.jdk/1.6.0.75.0		o
		/mdminsdir/installers/client/stage/Components/oracle.jdk/1.6.0.75.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.jdk/1.6.0.75.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.admin		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.admin/12.1.0.2.0		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.admin/12.1.0.2.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.admin/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.client		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.client/12.1.0.2.0		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.client/12.1.0.2.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.client/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.owm		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.owm/12.1.0.2.0		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.owm/12.1.0.2.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.owm/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.rsf		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.rsf.ic		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.rsf.ic/12.1.0.2.0		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.rsf.ic/12.1.0.2.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.rsf.ic/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.ldap.rsf/12.1.0.2.0		o

Critical	Rule Violated	Status		Remediation Suggestion
			/mdminsdir/installers/client/stage/Components/oracle.ldap.rsf/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.ldap.rsf/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.ldap.security.osdt	o
			/mdminsdir/installers/client/stage/Components/oracle.ldap.security.osdt/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.ldap.security.osdt/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.ldap.security.osdt/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.ldap.ssl	o
			/mdminsdir/installers/client/stage/Components/oracle.ldap.ssl/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.ldap.ssl/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.ldap.ssl/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.network.aso	o
			/mdminsdir/installers/client/stage/Components/oracle.network.aso/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.network.aso/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.network.aso/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.network.client	o
			/mdminsdir/installers/client/stage/Components/oracle.network.client.jrf	o
			/mdminsdir/installers/client/stage/Components/oracle.network.client.jrf/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.network.client.jrf/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.network.client/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.network.client/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.network.client/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.network.cman	o

Critical Rule Violated	Status		Remediation Suggestion
		/mdminsdir/installers/client/stage/Components/oracle.network.cman/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.network.cman/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.network.cman/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.network.listener	o
		/mdminsdir/installers/client/stage/Components/oracle.network.listener/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.network.listener/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.network.listener/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.network.rsf	o
		/mdminsdir/installers/client/stage/Components/oracle.network.rsf/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.network.rsf/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.network.rsf/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf.core	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf.core/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf.core/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf.core/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf.ic	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf.ic/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf.ic/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf.ic/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf.lbuilder	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf.lbuilder/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf.lbuilder/12.1.0.2.0/1	o

Critical	Rule Violated	Status	Remediation Suggestion
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf.lbuilder/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.nlsrtl.rsf/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.odbc	o
		/mdminsdir/installers/client/stage/Components/oracle.odbc.ic	o
		/mdminsdir/installers/client/stage/Components/oracle.odbc.ic/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.odbc.ic/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.odbc.ic/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.odbc/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.odbc/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.odbc/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.ons	o
		/mdminsdir/installers/client/stage/Components/oracle.ons.ic	o
		/mdminsdir/installers/client/stage/Components/oracle.ons.ic/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.ons.ic/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.ons.ic/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.ons/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.ons/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.ons/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.oracore.rsf	o
		/mdminsdir/installers/client/stage/Components/oracle.oracore.rsf.core	o

Critical	Rule Violated	Status	Remediation Suggestion
		/mdminsdir/installers/client/stage/Components/oracle.oracore.rsf.core/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.oracore.rsf.core/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.oracore.rsf.core/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.oracore.rsf/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.oracore.rsf/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.oracore.rsf/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.oraolap.api	o
		/mdminsdir/installers/client/stage/Components/oracle.oraolap.api/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.oraolap.api/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.oraolap.api/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.oraolap.dbscripts	o
		/mdminsdir/installers/client/stage/Components/oracle.oraolap.dbscripts/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.oraolap.dbscripts/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.oraolap.dbscripts/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.oraolap.mgmt	o
		/mdminsdir/installers/client/stage/Components/oracle.oraolap.mgmt/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.oraolap.mgmt/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.oraolap.mgmt/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.ordim.client	o
		/mdminsdir/installers/client/stage/Components/oracle.ordim.client/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.ordim.client/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.ordim.client/12.1.0.2.0/1/DataFiles	o

Critical Rule Violated	Status	/mdminsdir/installers/client/stage/Components/oracle.perlint	Remediation Suggestion	o
		/mdminsdir/installers/client/stage/Components/oracle.perlint.expat		o
		/mdminsdir/installers/client/stage/Components/oracle.perlint.expat/2.0.1.0.2		o
		/mdminsdir/installers/client/stage/Components/oracle.perlint.expat/2.0.1.0.2/1		o
		/mdminsdir/installers/client/stage/Components/oracle.perlint.expat/2.0.1.0.2/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.perlint.modules		o
		/mdminsdir/installers/client/stage/Components/oracle.perlint.modules/5.14.1.0.0		o
		/mdminsdir/installers/client/stage/Components/oracle.perlint.modules/5.14.1.0.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.perlint.modules/5.14.1.0.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.perlint/5.14.1.0.0		o
		/mdminsdir/installers/client/stage/Components/oracle.perlint/5.14.1.0.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.perlint/5.14.1.0.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.precomp		o
		/mdminsdir/installers/client/stage/Components/oracle.precomp.common		o
		/mdminsdir/installers/client/stage/Components/oracle.precomp.common.core		o
		/mdminsdir/installers/client/stage/Components/oracle.precomp.common.core/12.1.0.2.0		o
		/mdminsdir/installers/client/stage/Components/oracle.precomp.common.core/12.1.0.2.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.precomp.common.core/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.precomp.common/12.1.0.2.0		o
		/mdminsdir/installers/client/stage/Components/oracle.precomp.common/12.1.0.2.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.precomp.common/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.precomp.lang		o
		/mdminsdir/installers/client/stage/Components/oracle.precomp.lang/12.1.0.2.0		o

Critical	Rule Violated	Status		Remediation Suggestion
			/mdminsdir/installers/client/stage/Components/oracle.precomp.lang/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.precomp.lang/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.precomp.rsf	o
			/mdminsdir/installers/client/stage/Components/oracle.precomp.rsf/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.precomp.rsf/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.precomp.rsf/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.precomp/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.precomp/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.rdbms.crs	o
			/mdminsdir/installers/client/stage/Components/oracle.rdbms.crs/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.rdbms.crs/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.rdbms.crs/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.rdbms.dbscripts	o
			/mdminsdir/installers/client/stage/Components/oracle.rdbms.dbscripts/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.rdbms.dbscripts/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.rdbms.dbscripts/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.rdbms.deconfig	o
			/mdminsdir/installers/client/stage/Components/oracle.rdbms.deconfig/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.rdbms.deconfig/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.rdbms.deconfig/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.rdbms.ic	o
			/mdminsdir/installers/client/stage/Components/oracle.rdbms.ic/12.1.0.2.0	o

Critical Rule Violated	Status	/mdminsdir/installers/client/stage/Components/oracle.rdbms.ic/12.1.0.2.0	Remediation Suggestion	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.ic/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.install.common		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.install.common/12.1.0.2.0		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.install.common/12.1.0.2.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.install.common/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.install.plugins		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.install.plugins/12.1.0.2.0		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.install.plugins/12.1.0.2.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.install.plugins/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.oci		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.oci/12.1.0.2.0		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.oci/12.1.0.2.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.oci/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.plsql		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.plsql/12.1.0.2.0		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.plsql/12.1.0.2.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.plsql/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rman		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rman/12.1.0.2.0		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rman/12.1.0.2.0/1		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rman/12.1.0.2.0/1/DataFiles		o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rsf		o

Critical	Rule Violated	Status	Remediation Suggestion
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rsf.ic	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rsf.ic/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rsf.ic/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rsf.ic/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rsf.runtime	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rsf.runtime/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rsf.runtime/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rsf/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rsf/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.rsf/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.scheduler	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.scheduler/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.scheduler/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.scheduler/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.util	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.util/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.util/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.rdbms.util/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.rsf	o
		/mdminsdir/installers/client/stage/Components/oracle.rsf/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.rsf/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.rsf/12.1.0.2.0/1/DataFiles	o

Critical	Rule Violated	Status		Remediation Suggestion
			/mdminsdir/installers/client/stage/Components/oracle.slax.rsf	o
			/mdminsdir/installers/client/stage/Components/oracle.slax.rsf/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.slax.rsf/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.slax.rsf/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlj	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlj.sqljruntime	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlj.sqljruntime/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlj.sqljruntime/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlj.sqljruntime/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlj/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlj/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlj/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlplus	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlplus.ic	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlplus.ic/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlplus.ic/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlplus.ic/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlplus.rsf	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlplus.rsf/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlplus.rsf/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlplus.rsf/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlplus/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.sqlplus/12.1.0.2.0/1	o

Critical	Rule Violated	Status		Remediation Suggestion
			/mdminsdir/installers/client/stage/Components/oracle.sqlplus/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.opatch	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.opatch/12.1.0.1.2	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.opatch/12.1.0.1.2/1	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.opatch/12.1.0.1.2/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui.core	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui.core.min	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui.core.min/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui.core.min/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui.core.min/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui.core/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui.core/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui.core/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui/12.1.0.2.0/1/DataFiles	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui/12.1.0.2.0/1/DataFiles/Expanded	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui/12.1.0.2.0/1/DataFiles/Expanded/oui	o
			/mdminsdir/installers/client/stage/Components/oracle.swd.oui/12.1.0.2.0/1/DataFiles/Expanded/oui/instImages	o
			/mdminsdir/installers/client/stage/Components/oracle.sysman.ccr.deconfig	o
			/mdminsdir/installers/client/stage/Components/oracle.sysman.ccr.deconfig/10.3.1.0.0	o

Critical	Rule Violated	Status	Remediation Suggestion
		/mdminsdir/installers/client/stage/Components/oracle.sysman.ccr.deconfig/10.3.1.0.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.sysman.ccr.deconfig/10.3.1.0.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.usm.deconfig	o
		/mdminsdir/installers/client/stage/Components/oracle.usm.deconfig/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.usm.deconfig/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.usm.deconfig/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.wwg.plsql	o
		/mdminsdir/installers/client/stage/Components/oracle.wwg.plsql/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.wwg.plsql/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.wwg.plsql/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.xdk	o
		/mdminsdir/installers/client/stage/Components/oracle.xdk.core	o
		/mdminsdir/installers/client/stage/Components/oracle.xdk.core/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.xdk.core/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.xdk.parser.java	o
		/mdminsdir/installers/client/stage/Components/oracle.xdk.parser.java/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.xdk.parser.java/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.xdk.parser.java/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.xdk.rsf	o
		/mdminsdir/installers/client/stage/Components/oracle.xdk.rsf/12.1.0.2.0	o
		/mdminsdir/installers/client/stage/Components/oracle.xdk.rsf/12.1.0.2.0/1	o
		/mdminsdir/installers/client/stage/Components/oracle.xdk.rsf/12.1.0.2.0/1/DataFiles	o
		/mdminsdir/installers/client/stage/Components/oracle.xdk.xquery	o

Critical	Rule Violated	Status	/mdminsdir/installers/client/stage/Components/oracle.xdk.xquery	Remediation Suggestion	o
			/mdminsdir/installers/client/stage/Components/oracle.xdk.xquery/12.1.0.2.0		o
			/mdminsdir/installers/client/stage/Components/oracle.xdk.xquery/12.1.0.2.0/1		o
			/mdminsdir/installers/client/stage/Components/oracle.xdk.xquery/12.1.0.2.0/1/DataFiles		o
			/mdminsdir/installers/client/stage/Components/oracle.xdk/12.1.0.2.0		o
			/mdminsdir/installers/client/stage/Components/oracle.xdk/12.1.0.2.0/1		o
			/mdminsdir/installers/client/stage/Components/oracle.xdk/12.1.0.2.0/1/DataFiles		o
			/mdminsdir/installers/client/stage/Dialogs		o
			/mdminsdir/installers/client/stage/Dialogs/OiDynamicXYSpreadTable		o
			/mdminsdir/installers/client/stage/Dialogs/OiDynamicXYSpreadTable/2.5.0.2.5		o
			/mdminsdir/installers/client/stage/Dialogs/OiDynamicXYSpreadTable/2.5.0.2.5/1		o
			/mdminsdir/installers/client/stage/Dialogs/TwoRadioStaticDynamicDialogs		o
			/mdminsdir/installers/client/stage/Dialogs/TwoRadioStaticDynamicDialogs/2.5.0.0.27		o
			/mdminsdir/installers/client/stage/Dialogs/TwoRadioStaticDynamicDialogs/2.5.0.0.27/1		o
			/mdminsdir/installers/client/stage/Dialogs/customDialogs		o
			/mdminsdir/installers/client/stage/Dialogs/customDialogs/10.2.0.1.0		o
			/mdminsdir/installers/client/stage/Dialogs/customDialogs/10.2.0.1.0/1		o
			/mdminsdir/installers/client/stage/Dialogs/standardDialogs		o
			/mdminsdir/installers/client/stage/Dialogs/standardDialogs/10.2.0.1.0		o
			/mdminsdir/installers/client/stage/Dialogs/standardDialogs/10.2.0.1.0/1		o
			/mdminsdir/installers/client/stage/Queries		o
			/mdminsdir/installers/client/stage/Queries/ASMQueries		o
			/mdminsdir/installers/client/stage/Queries/ASMQueries/12.1.0.2.0		o

Critical	Rule Violated	Status		Remediation Suggestion
			/mdminsdir/installers/client/stage/Queries/ASMQueries/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Queries/ClusterPreinstQueries	o
			/mdminsdir/installers/client/stage/Queries/ClusterPreinstQueries/1.2.1	o
			/mdminsdir/installers/client/stage/Queries/ClusterPreinstQueries/1.2.1/1	o
			/mdminsdir/installers/client/stage/Queries/ClusterQueries	o
			/mdminsdir/installers/client/stage/Queries/ClusterQueries/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Queries/ClusterQueries/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Queries/DLLQueries	o
			/mdminsdir/installers/client/stage/Queries/DLLQueries/1.1	o
			/mdminsdir/installers/client/stage/Queries/DLLQueries/1.1/1	o
			/mdminsdir/installers/client/stage/Queries/EmQueries	o
			/mdminsdir/installers/client/stage/Queries/EmQueries/4.2.2	o
			/mdminsdir/installers/client/stage/Queries/EmQueries/4.2.2/1	o
			/mdminsdir/installers/client/stage/Queries/HealthCheckQueries	o
			/mdminsdir/installers/client/stage/Queries/HealthCheckQueries/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Queries/HealthCheckQueries/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Queries/IP_DBQueries	o
			/mdminsdir/installers/client/stage/Queries/IP_DBQueries/1.0	o
			/mdminsdir/installers/client/stage/Queries/IP_DBQueries/1.0/1	o
			/mdminsdir/installers/client/stage/Queries/JDevOUIQueries	o
			/mdminsdir/installers/client/stage/Queries/JDevOUIQueries/0.01.00.12	o
			/mdminsdir/installers/client/stage/Queries/JDevOUIQueries/0.01.00.12/1	o

Critical	Rule Violated	Status			
			/mdminsdir/installers/client/stage/Queries/LDAPGlobalQueries	**Remediation Suggestion**	o
			/mdminsdir/installers/client/stage/Queries/LDAPGlobalQueries/1.2.1		o
			/mdminsdir/installers/client/stage/Queries/LDAPGlobalQueries/1.2.1/1		o
			/mdminsdir/installers/client/stage/Queries/LDAPQueries		o
			/mdminsdir/installers/client/stage/Queries/LDAPQueries/1.1.2		o
			/mdminsdir/installers/client/stage/Queries/LDAPQueries/1.1.2/1		o
			/mdminsdir/installers/client/stage/Queries/LangQueries		o
			/mdminsdir/installers/client/stage/Queries/LangQueries/1.3.6.4		o
			/mdminsdir/installers/client/stage/Queries/LangQueries/1.3.6.4/1		o
			/mdminsdir/installers/client/stage/Queries/MemorySizeQuery		o
			/mdminsdir/installers/client/stage/Queries/MemorySizeQuery/1.2.8.0.6		o
			/mdminsdir/installers/client/stage/Queries/MemorySizeQuery/1.2.8.0.6/1		o
			/mdminsdir/installers/client/stage/Queries/NLSQueries		o
			/mdminsdir/installers/client/stage/Queries/NLSQueries/12.1.0.2.0		o
			/mdminsdir/installers/client/stage/Queries/NLSQueries/12.1.0.2.0/1		o
			/mdminsdir/installers/client/stage/Queries/NtServicesQueries		o
			/mdminsdir/installers/client/stage/Queries/NtServicesQueries/10.2.0.3.0		o
			/mdminsdir/installers/client/stage/Queries/NtServicesQueries/10.2.0.3.0/1		o
			/mdminsdir/installers/client/stage/Queries/OCAQueries		o
			/mdminsdir/installers/client/stage/Queries/OCAQueries/1.0.1		o
			/mdminsdir/installers/client/stage/Queries/OCAQueries/1.0.1/1		o
			/mdminsdir/installers/client/stage/Queries/OraBase_Queries		o
			/mdminsdir/installers/client/stage/Queries/OraBase_Queries/1.2.1		o

Critical	Rule Violated	Status		Remediation Suggestion
			/mdminsdir/installers/client/stage/Queries/OraBase_Queries/1.2.1/1	o
			/mdminsdir/installers/client/stage/Queries/PasswordQueries	o
			/mdminsdir/installers/client/stage/Queries/PasswordQueries/0.0.3	o
			/mdminsdir/installers/client/stage/Queries/PasswordQueries/0.0.3/1	o
			/mdminsdir/installers/client/stage/Queries/PrerequisiteQueries	o
			/mdminsdir/installers/client/stage/Queries/PrerequisiteQueries/1.1.12	o
			/mdminsdir/installers/client/stage/Queries/PrerequisiteQueries/1.1.12/1	o
			/mdminsdir/installers/client/stage/Queries/Protocol_Queries	o
			/mdminsdir/installers/client/stage/Queries/Protocol_Queries/1.1.4	o
			/mdminsdir/installers/client/stage/Queries/Protocol_Queries/1.1.4/1	o
			/mdminsdir/installers/client/stage/Queries/RepositoryQueries	o
			/mdminsdir/installers/client/stage/Queries/RepositoryQueries/3.0.0.2.17	o
			/mdminsdir/installers/client/stage/Queries/RepositoryQueries/3.0.0.2.17/1	o
			/mdminsdir/installers/client/stage/Queries/RunningProcessQuery	o
			/mdminsdir/installers/client/stage/Queries/RunningProcessQuery/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Queries/RunningProcessQuery/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Queries/SIDQueries	o
			/mdminsdir/installers/client/stage/Queries/SIDQueries/1.2.7	o
			/mdminsdir/installers/client/stage/Queries/SIDQueries/1.2.7/1	o
			/mdminsdir/installers/client/stage/Queries/SpawnQueries	o
			/mdminsdir/installers/client/stage/Queries/SpawnQueries/1.1.4	o
			/mdminsdir/installers/client/stage/Queries/SpawnQueries/1.1.4/1	o

Critical Rule Violated	Status	Remediation Suggestion
	/mdminsdir/installers/client/stage/Queries/UtilQueries	o
	/mdminsdir/installers/client/stage/Queries/UtilQueries/12.1.0.2.0	o
	/mdminsdir/installers/client/stage/Queries/UtilQueries/12.1.0.2.0/1	o
	/mdminsdir/installers/client/stage/Queries/WinSetAclQuery	o
	/mdminsdir/installers/client/stage/Queries/WinSetAclQuery/1.0.7	o
	/mdminsdir/installers/client/stage/Queries/WinSetAclQuery/1.0.7/1	o
	/mdminsdir/installers/client/stage/Queries/WindowsGeneralQueries	o
	/mdminsdir/installers/client/stage/Queries/WindowsGeneralQueries/10.2.0.1.0	o
	/mdminsdir/installers/client/stage/Queries/WindowsGeneralQueries/10.2.0.1.0/1	o
	/mdminsdir/installers/client/stage/Queries/XMLFileQueries	o
	/mdminsdir/installers/client/stage/Queries/XMLFileQueries/2.1.0.4.2	o
	/mdminsdir/installers/client/stage/Queries/XMLFileQueries/2.1.0.4.2/1	o
	/mdminsdir/installers/client/stage/Queries/areasQueries	o
	/mdminsdir/installers/client/stage/Queries/areasQueries/10.2.0.1.0	o
	/mdminsdir/installers/client/stage/Queries/areasQueries/10.2.0.1.0/1	o
	/mdminsdir/installers/client/stage/Queries/ccrQueries	o
	/mdminsdir/installers/client/stage/Queries/ccrQueries/10.3.0.1.0	o
	/mdminsdir/installers/client/stage/Queries/ccrQueries/10.3.0.1.0/1	o
	/mdminsdir/installers/client/stage/Queries/cfsprereqQueries	o
	/mdminsdir/installers/client/stage/Queries/cfsprereqQueries/10.2.0.2.0	o
	/mdminsdir/installers/client/stage/Queries/cfsprereqQueries/10.2.0.2.0/1	o
	/mdminsdir/installers/client/stage/Queries/clusterQueriesEx	o
	/mdminsdir/installers/client/stage/Queries/clusterQueriesEx/10.2.0.1.0	o

Critical	Rule Violated	Status		Remediation Suggestion
			/mdminsdir/installers/client/stage/Queries/clusterQueriesEx/10.2.0.1.0/1	o
			/mdminsdir/installers/client/stage/Queries/dbQueries	o
			/mdminsdir/installers/client/stage/Queries/dbQueries/10.1.0.2.0	o
			/mdminsdir/installers/client/stage/Queries/dbQueries/10.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Queries/encryptionQueries	o
			/mdminsdir/installers/client/stage/Queries/encryptionQueries/1.1	o
			/mdminsdir/installers/client/stage/Queries/encryptionQueries/1.1/1	o
			/mdminsdir/installers/client/stage/Queries/fileQueries	o
			/mdminsdir/installers/client/stage/Queries/fileQueries/10.1.0.3.0	o
			/mdminsdir/installers/client/stage/Queries/fileQueries/10.1.0.3.0/1	o
			/mdminsdir/installers/client/stage/Queries/generalPortQueries	o
			/mdminsdir/installers/client/stage/Queries/generalPortQueries/2.1.0.19.8	o
			/mdminsdir/installers/client/stage/Queries/generalPortQueries/2.1.0.19.8/1	o
			/mdminsdir/installers/client/stage/Queries/generalQueries	o
			/mdminsdir/installers/client/stage/Queries/generalQueries/10.2.0.2.1	o
			/mdminsdir/installers/client/stage/Queries/generalQueries/10.2.0.2.1/1	o
			/mdminsdir/installers/client/stage/Queries/globalVarQueries	o
			/mdminsdir/installers/client/stage/Queries/globalVarQueries/12.1.0.2.0	o
			/mdminsdir/installers/client/stage/Queries/globalVarQueries/12.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Queries/netQueries	o
			/mdminsdir/installers/client/stage/Queries/netQueries/10.2.0.2.0	o
			/mdminsdir/installers/client/stage/Queries/netQueries/10.2.0.2.0/1	o

Critical	Rule Violated	Status		Remediation Suggestion
			/mdminsdir/installers/client/stage/Queries/portQueries	o
			/mdminsdir/installers/client/stage/Queries/portQueries/2.1.0.16.4	o
			/mdminsdir/installers/client/stage/Queries/portQueries/2.1.0.16.4/1	o
			/mdminsdir/installers/client/stage/Queries/rgsQueries	o
			/mdminsdir/installers/client/stage/Queries/rgsQueries/10.1.0.3.0	o
			/mdminsdir/installers/client/stage/Queries/rgsQueries/10.1.0.3.0/1	o
			/mdminsdir/installers/client/stage/Queries/textFileQueries	o
			/mdminsdir/installers/client/stage/Queries/textFileQueries/2.1.0.4 .0	o
			/mdminsdir/installers/client/stage/Queries/textFileQueries/2.1.0.4 .0/1	o
			/mdminsdir/installers/client/stage/Queries/unixQueries	o
			/mdminsdir/installers/client/stage/Queries/unixQueries/10.1.0.2.0	o
			/mdminsdir/installers/client/stage/Queries/unixQueries/10.1.0.2.0/1	o
			/mdminsdir/installers/client/stage/Queries/w32RegQueries	o
			/mdminsdir/installers/client/stage/Queries/w32RegQueries/10.2.0.1.0	o
			/mdminsdir/installers/client/stage/Queries/w32RegQueries/10.2.0.1.0/1	o
			/mdminsdir/installers/client/stage/UserActions	o
			/mdminsdir/installers/client/stage/UserActions/oracle.client	o
			/mdminsdir/installers/client/stage/UserActions/oracle.client/UnixActions	o
			/mdminsdir/installers/client/stage/cvu	o
			/mdminsdir/installers/client/stage/cvu/cv	o
			/mdminsdir/installers/client/stage/cvu/cv/admin	o
			/mdminsdir/installers/client/stage/cvu/cv/cvdata	o

Critical	Rule Violated	Status			
			/mdminsdir/installers/client/stage/cvu/cv/remenv	**Remediation Suggestion**	o
			/mdminsdir/installers/client/stage/cvu/cv/remenv/jlib		o
			/mdminsdir/installers/client/stage/cvu/cv/remenv/pluggable		o
			/mdminsdir/installers/client/stage/cvu/jlib		o
			/mdminsdir/installers/client/stage/ext		o
			/mdminsdir/installers/client/stage/ext/jlib		o
			/mdminsdir/installers/client/stage/fastcopy		o
			/mdminsdir/installers/client/stage/globalvariables		o
			/mdminsdir/installers/client/stage/properties		o
			/mdminsdir/installers/client/stage/sizes		o

REMEDIATION SUGGESTION

df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type d \(-perm -0002 -a ! -perm -1000 \) 2>/dev/nu

df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type d \(-perm -0002 -a ! -perm -1000 \) 2>/dev/nu

9.2.19 Check For Presence Of User .Forward Files	Indeterminate	**Passed: User *root* home directory */root* does not contain specified files**	

POLICY SETTINGS

User: **root**
Home directory: **/root**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and un
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *bin* home directory */bin* does not contain specified files

POLICY SETTINGS

User: **bin**
Home directory: **/bin**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

Critical	Rule Violated	Status	Remediation Suggestion

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *daemon* home directory */sbin* does not contain specified files

POLICY SETTINGS

User: **daemon**
Home directory: **/sbin**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *lp* home directory */var/spool/lpd* does not contain specified files

POLICY SETTINGS

User: **lp**
Home directory: **/var/spool/lpd**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *mail* home directory */var/spool/mail* does not contain specified files

POLICY SETTINGS

User: **mail**
Home directory: **/var/spool/mail**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

Critical	Rule Violated	Status	Remediation Suggestion

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *operator* home directory */root* does not contain specified files

POLICY SETTINGS

User: **operator**
Home directory: **/root**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and un
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *games* home directory */usr/games* does not contain specified files

POLICY SETTINGS

User: **games**
Home directory: **/usr/games**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and un
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *nobody* home directory */ does not contain specified files

POLICY SETTINGS

User: **nobody**
Home directory: **/**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and un
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
```

Critical	Rule Violated	Status	Remediation Suggestion

if [! -h "$dir/.forward" -a -f "$dir/.forward"]; then
echo ".forward file $dir/.forward exists"
fi
done

Passed: User *dbus* home directory / does not contain specified files

POLICY SETTINGS

User: **dbus**
Home directory: **/**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *vcsa* home directory */dev* does not contain specified files

POLICY SETTINGS

User: **vcsa**
Home directory: **/dev**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *haldaemon* home directory / does not contain specified files

POLICY SETTINGS

User: **haldaemon**
Home directory: **/**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *ntp* home directory */etc/ntp* does not contain specified files

Critical	Rule Violated	Status	POLICY SETTINGS	Remediation Suggestion

User: **ntp**
Home directory: **/etc/ntp**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *postfix* home directory */var/spool/postfix* does not contain specified files

POLICY SETTINGS

User: **postfix**
Home directory: **/var/spool/postfix**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *sshd* home directory */var/empty/sshd* does not contain specified files

POLICY SETTINGS

User: **sshd**
Home directory: **/var/empty/sshd**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *ec2-user* home directory */home/ec2-user* does not contain specified files

POLICY SETTINGS

User: **ec2-user**
Home directory: **/home/ec2-user**
Expected file(s): **.forward**
Expected presence: **false**

Critical	Rule Violated	Status		Remediation Suggestion

Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *scom* home directory */home/scom* does not contain specified files

POLICY SETTINGS

User: **scom**
Home directory: **/home/scom**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *apache* home directory */var/www* does not contain specified files

POLICY SETTINGS

User: **apache**
Home directory: **/var/www**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

This script checks for the presence of .forward files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
echo ".forward file $dir/.forward exists"
fi
done
```

Passed: User *oracle* home directory */home/oracle* does not contain specified files

POLICY SETTINGS

User: **oracle**
Home directory: **/home/oracle**
Expected file(s): **.forward**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

Critical	Rule Violated	Status	Remediation Suggestion
			REMEDIATION SUGGESTION Making global modifications to users' files without alerting the user community can result in unexpected outages and uni policy be established to report user .forward files and determine the action to be taken in accordance with site policy. This script checks for the presence of .forward files that may be in violation of the site security policy. #!/bin/bash for dir in `/bin/cat /etc/passwd |\ /bin/awk -F: '{ print $6 }'`; do if [! -h "$dir/.forward" -a -f "$dir/.forward"]; then echo ".forward file $dir/.forward exists" fi done **Indeterminate: User *abrt* home directory */etc/abrt* could not be found** **POLICY SETTINGS** User: **abrt** Home directory: **/etc/abrt** Expected file(s): **.forward** Expected presence: **false** Actual presence: Files found: **0** **REMEDIATION SUGGESTION** Making global modifications to users' files without alerting the user community can result in unexpected outages and uni policy be established to report user .forward files and determine the action to be taken in accordance with site policy. This script checks for the presence of .forward files that may be in violation of the site security policy. #!/bin/bash for dir in `/bin/cat /etc/passwd |\ /bin/awk -F: '{ print $6 }'`; do if [! -h "$dir/.forward" -a -f "$dir/.forward"]; then echo ".forward file $dir/.forward exists" fi done **Indeterminate: User *oprofile* home directory */home/oprofile* could not be found** **POLICY SETTINGS** User: **oprofile** Home directory: **/home/oprofile** Expected file(s): **.forward** Expected presence: **false** Actual presence: Files found: **0** **REMEDIATION SUGGESTION** Making global modifications to users' files without alerting the user community can result in unexpected outages and uni policy be established to report user .forward files and determine the action to be taken in accordance with site policy. This script checks for the presence of .forward files that may be in violation of the site security policy. #!/bin/bash for dir in `/bin/cat /etc/passwd |\ /bin/awk -F: '{ print $6 }'`; do if [! -h "$dir/.forward" -a -f "$dir/.forward"]; then echo ".forward file $dir/.forward exists" fi done
	9.2.18 Check For Presence Of User .Netrc Files	Indeterminate	**Passed: User *root* home directory */root* does not contain specified files** **POLICY SETTINGS** User: **root** Home directory: **/root** Expected file(s): **.netrc** Expected presence: **false** Actual presence: **false** Files found: **0** **REMEDIATION SUGGESTION** Making global modifications to users' files without alerting the user community can result in unexpected outages and uni policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

Critical	Rule Violated	Status	Remediation Suggestion

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *bin* home directory */bin* does not contain specified files

POLICY SETTINGS

User: **bin**
Home directory: **/bin**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *daemon* home directory */sbin* does not contain specified files

POLICY SETTINGS

User: **daemon**
Home directory: **/sbin**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *lp* home directory */var/spool/lpd* does not contain specified files

POLICY SETTINGS

User: **lp**
Home directory: **/var/spool/lpd**
Expected file(s): **.netrc**

Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *mail* home directory */var/spool/mail* does not contain specified files

POLICY SETTINGS

Critical	Rule Violated	Status		Remediation Suggestion

User: **mail**
Home directory: **/var/spool/mail**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *operator* home directory */root* does not contain specified files
POLICY SETTINGS

User: **operator**
Home directory: **/root**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *games* home directory */usr/games* does not contain specified files
POLICY SETTINGS

User: **games**
Home directory: **/usr/games**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *nobody* home directory / does not contain specified files
POLICY SETTINGS

User: **nobody**
Home directory: **/**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Critical	Rule Violated	Status	Remediation Suggestion

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *dbus* home directory / does not contain specified files

POLICY SETTINGS

User: **dbus**
Home directory: **/**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *vcsa* home directory */dev* does not contain specified files

POLICY SETTINGS

User: **vcsa**
Home directory: **/dev**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *haldaemon* home directory / does not contain specified files

POLICY SETTINGS

User: **haldaemon**
Home directory: **/**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Critical	Rule Violated	Status	Remediation Suggestion

Passed: User *ntp* home directory */etc/ntp* does not contain specified files

POLICY SETTINGS

User: **ntp**
Home directory: **/etc/ntp**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *postfix* home directory */var/spool/postfix* does not contain specified files

POLICY SETTINGS

User: **postfix**
Home directory: **/var/spool/postfix**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *sshd* home directory */var/empty/sshd* does not contain specified files

POLICY SETTINGS

User: **sshd**
Home directory: **/var/empty/sshd**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *ec2-user* home directory */home/ec2-user* does not contain specified files

POLICY SETTINGS

User: **ec2-user**
Home directory: **/home/ec2-user**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

Critical	Rule Violated	Status	Remediation Suggestion

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *scom* home directory */home/scom* does not contain specified files

POLICY SETTINGS

User: **scom**
Home directory: **/home/scom**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *apache* home directory */var/www* does not contain specified files

POLICY SETTINGS

User: **apache**
Home directory: **/var/www**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
fi
done
```

Passed: User *oracle* home directory */home/oracle* does not contain specified files

POLICY SETTINGS

User: **oracle**
Home directory: **/home/oracle**
Expected file(s): **.netrc**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

Making global modifications to users' files without alerting the user community can result in unexpected outages and uni
policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
/bin/awk -F: '{ print $6 }'`; do
if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
echo ".netrc file $dir/.netrc exists"
```

Critical	Rule Violated	Status	Remediation Suggestion
			fi done **Indeterminate: User *abrt* home directory */etc/abrt* could not be found** **POLICY SETTINGS** User: **abrt** Home directory: **/etc/abrt** Expected file(s): **.netrc** Expected presence: **false** Actual presence: Files found: **0** **REMEDIATION SUGGESTION** Making global modifications to users' files without alerting the user community can result in unexpected outages and uni policy be established to report user .netrc files and determine the action to be taken in accordance with site policy. #!/bin/bash for dir in `/bin/cat /etc/passwd |\ /bin/awk -F: '{ print $6 }'`; do if [! -h "$dir/.netrc" -a -f "$dir/.netrc"]; then echo ".netrc file $dir/.netrc exists" fi done **Indeterminate: User *oprofile* home directory */home/oprofile* could not be found** **POLICY SETTINGS** User: **oprofile** Home directory: **/home/oprofile** Expected file(s): **.netrc** Expected presence: **false** Actual presence: Files found: **0** **REMEDIATION SUGGESTION** Making global modifications to users' files without alerting the user community can result in unexpected outages and uni policy be established to report user .netrc files and determine the action to be taken in accordance with site policy. #!/bin/bash for dir in `/bin/cat /etc/passwd |\ /bin/awk -F: '{ print $6 }'`; do if [! -h "$dir/.netrc" -a -f "$dir/.netrc"]; then echo ".netrc file $dir/.netrc exists" fi done
	9.2.10 Check For Presence Of User .Rhosts Files	Indeterminate	**Passed: User *root* home directory */root* does not contain specified files** **POLICY SETTINGS** User: **root** Home directory: **/root** Expected file(s): **.rhosts** Expected presence: **false** Actual presence: **false** Files found: **0** **REMEDIATION SUGGESTION** If any users have .rhosts files determine why they have them. #!/bin/bash for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\ /bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do for file in $dir/.rhosts; do if [! -h "$file" -a -f "$file"]; then echo ".rhosts file in $dir" fi done done **Passed: User *bin* home directory */bin* does not contain specified files** **POLICY SETTINGS** User: **bin** Home directory: **/bin** Expected file(s): **.rhosts** Expected presence: **false** Actual presence: **false**

Critical	Rule Violated	Status	Actual presence: **false** Files found: **0**	Remediation Suggestion

REMEDIATION SUGGESTION

If any users have .rhosts files determine why they have them.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
for file in $dir/.rhosts; do
if [ ! -h "$file" -a -f "$file" ]; then
echo ".rhosts file in $dir"
fi done
done
```

Passed: User *daemon* home directory */sbin* does not contain specified files

POLICY SETTINGS

User: **daemon**
Home directory: **/sbin**
Expected file(s): **.rhosts**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

If any users have .rhosts files determine why they have them.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
for file in $dir/.rhosts; do
if [ ! -h "$file" -a -f "$file" ]; then
echo ".rhosts file in $dir"
fi done
done
```

Passed: User *lp* home directory */var/spool/lpd* does not contain specified files

POLICY SETTINGS

User: **lp**
Home directory: **/var/spool/lpd**
Expected file(s): **.rhosts**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

If any users have .rhosts files determine why they have them.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
for file in $dir/.rhosts; do
if [ ! -h "$file" -a -f "$file" ]; then
echo ".rhosts file in $dir"
fi done
done
```

Passed: User *mail* home directory */var/spool/mail* does not contain specified files

POLICY SETTINGS

User: **mail**
Home directory: **/var/spool/mail**
Expected file(s): **.rhosts**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

If any users have .rhosts files determine why they have them.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
```

Critical	Rule Violated	Status	Remediation Suggestion

/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
for file in $dir/.rhosts; do
if [! -h "$file" -a -f "$file"]; then
echo ".rhosts file in $dir"
fi done
done

Passed: User *operator* home directory */root* does not contain specified files

POLICY SETTINGS

User: **operator**
Home directory: **/root**
Expected file(s): **.rhosts**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

If any users have .rhosts files determine why they have them.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
for file in $dir/.rhosts; do
if [ ! -h "$file" -a -f "$file" ]; then
echo ".rhosts file in $dir"
fi done
done
```

Passed: User *games* home directory */usr/games* does not contain specified files

POLICY SETTINGS

User: **games**
Home directory: **/usr/games**
Expected file(s): **.rhosts**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

If any users have .rhosts files determine why they have them.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
for file in $dir/.rhosts; do
if [ ! -h "$file" -a -f "$file" ]; then
echo ".rhosts file in $dir"
fi done
done
```

Passed: User *nobody* home directory / does not contain specified files

POLICY SETTINGS

User: **nobody**
Home directory: **/**
Expected file(s): **.rhosts**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

If any users have .rhosts files determine why they have them.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
for file in $dir/.rhosts; do
if [ ! -h "$file" -a -f "$file" ]; then
echo ".rhosts file in $dir"
fi done
done
```

Passed: User *dbus* home directory / does not contain specified files

POLICY SETTINGS

User: **dbus**
Home directory: **/**

Critical	Rule Violated	Status		Remediation Suggestion
			Expected file(s): **.rhosts** Expected presence: **false** Actual presence: **false** Files found: **0** **REMEDIATION SUGGESTION** If any users have .rhosts files determine why they have them. #!/bin/bash for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\ /bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do for file in $dir/.rhosts; do if [! -h "$file" -a -f "$file"]; then echo ".rhosts file in $dir" fi done done	
			Passed: User *vcsa* home directory */dev* does not contain specified files **POLICY SETTINGS** User: **vcsa** Home directory: **/dev** Expected file(s): **.rhosts** Expected presence: **false** Actual presence: **false** Files found: **0** **REMEDIATION SUGGESTION** If any users have .rhosts files determine why they have them. #!/bin/bash for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\ /bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do for file in $dir/.rhosts; do if [! -h "$file" -a -f "$file"]; then echo ".rhosts file in $dir" fi done done	
			Passed: User *haldaemon* home directory */* does not contain specified files **POLICY SETTINGS** User: **haldaemon** Home directory: **/** Expected file(s): **.rhosts** Expected presence: **false** Actual presence: **false** Files found: **0** **REMEDIATION SUGGESTION** If any users have .rhosts files determine why they have them. #!/bin/bash for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\ /bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do for file in $dir/.rhosts; do if [! -h "$file" -a -f "$file"]; then echo ".rhosts file in $dir" fi done done	
			Passed: User *ntp* home directory */etc/ntp* does not contain specified files **POLICY SETTINGS** User: **ntp** Home directory: **/etc/ntp** Expected file(s): **.rhosts** Expected presence: **false** Actual presence: **false** Files found: **0** **REMEDIATION SUGGESTION** If any users have .rhosts files determine why they have them.	

Critical	Rule Violated	Status	Remediation Suggestion

#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
for file in $dir/.rhosts; do
if [! -h "$file" -a -f "$file"]; then
echo ".rhosts file in $dir"
fi done
done

Passed: User *postfix* home directory */var/spool/postfix* does not contain specified files

POLICY SETTINGS

User: **postfix**
Home directory: **/var/spool/postfix**
Expected file(s): **.rhosts**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

If any users have .rhosts files determine why they have them.

#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
for file in $dir/.rhosts; do
if [! -h "$file" -a -f "$file"]; then
echo ".rhosts file in $dir"
fi done
done

Passed: User *sshd* home directory */var/empty/sshd* does not contain specified files

POLICY SETTINGS

User: **sshd**
Home directory: **/var/empty/sshd**
Expected file(s): **.rhosts**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

If any users have .rhosts files determine why they have them.

#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
for file in $dir/.rhosts; do
if [! -h "$file" -a -f "$file"]; then
echo ".rhosts file in $dir"
fi done
done

Passed: User *ec2-user* home directory */home/ec2-user* does not contain specified files

POLICY SETTINGS

User: **ec2-user**
Home directory: **/home/ec2-user**
Expected file(s): **.rhosts**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

If any users have .rhosts files determine why they have them.

#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
for file in $dir/.rhosts; do
if [! -h "$file" -a -f "$file"]; then
echo ".rhosts file in $dir"
fi done
done

Passed: User *scom* home directory */home/scom* does not contain specified files

POLICY SETTINGS

Critical	Rule Violated	Status	Remediation Suggestion

User: **scom**
Home directory: **/home/scom**
Expected file(s): **.rhosts**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

If any users have .rhosts files determine why they have them.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
for file in $dir/.rhosts; do
if [ ! -h "$file" -a -f "$file" ]; then
echo ".rhosts file in $dir"
fi done
done
```

Passed: User *apache* home directory */var/www* does not contain specified files
POLICY SETTINGS

User: **apache**
Home directory: **/var/www**
Expected file(s): **.rhosts**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

If any users have .rhosts files determine why they have them.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
for file in $dir/.rhosts; do
if [ ! -h "$file" -a -f "$file" ]; then
echo ".rhosts file in $dir"
fi done
done
```

Passed: User *oracle* home directory */home/oracle* does not contain specified files
POLICY SETTINGS

User: **oracle**
Home directory: **/home/oracle**
Expected file(s): **.rhosts**
Expected presence: **false**
Actual presence: **false**
Files found: **0**

REMEDIATION SUGGESTION

If any users have .rhosts files determine why they have them.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
for file in $dir/.rhosts; do
if [ ! -h "$file" -a -f "$file" ]; then
echo ".rhosts file in $dir"
fi done
done
```

Indeterminate: User *abrt* home directory */etc/abrt* could not be found
POLICY SETTINGS

User: **abrt**
Home directory: **/etc/abrt**
Expected file(s): **.rhosts**
Expected presence: **false**
Actual presence:
Files found: **0**

REMEDIATION SUGGESTION

Critical	Rule Violated	Status	Remediation Suggestion
			If any users have .rhosts files determine why they have them. #!/bin/bash for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\ /bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do for file in $dir/.rhosts; do if [! -h "$file" -a -f "$file"]; then echo ".rhosts file in $dir" fi done done **Indeterminate: User *oprofile* home directory */home/oprofile* could not be found** **POLICY SETTINGS** User: **oprofile** Home directory: **/home/oprofile** Expected file(s): **.rhosts** Expected presence: **false** Actual presence: Files found: **0** **REMEDIATION SUGGESTION** If any users have .rhosts files determine why they have them. #!/bin/bash for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\ /bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do for file in $dir/.rhosts; do if [! -h "$file" -a -f "$file"]; then echo ".rhosts file in $dir" fi done done

	9.2.6 Ensure Root Path Integrity	Indeterminate	**Passed: User *root* home directory */root* contains no matching files with unsafe path statements**
			POLICY SETTINGS
			
			User: **root**
			Home: **/root**
			Files:
			
			/root/.bash_profile
			Path statements:
			PATH=$PATH:$HOME/bin
			export PATH
			
			REMEDIATION SUGGESTION
			
			Correct or justify any items discovered in the Audit step.
			
			#!/bin/bash
			if ["`echo $PATH | /bin/grep :: `" != ""]; then
			echo "Empty Directory in PATH (::)"
			fi
			if ["`echo $PATH \| bin/grep :$`" != ""]; then
			echo "Trailing : in PATH"
			fi
			p=`echo $PATH \| /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
			set -- $p
			while ["$1" != ""]; do
			if ["$1" = "."]; then
			echo "PATH contains ."
			shift
			continue
			fi
			if [-d $1]; then
			dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
			if [`echo $dirperm | /bin/cut -c6 ` != "-"]; then
			echo "Group Write permission set on directory $1"
			fi
			if [`echo $dirperm | /bin/cut -c9 ` != "-"]; then
			echo "Other Write permission set on directory $1"
			fi
			dirown=`ls -ldH $1 | awk '{print $3}'`
			if ["$dirown" != "root"] ; then
			echo $1 is not owned by root
			fi
			else
			echo $1 is not a directory
			fi
			shift
			done

Critical Rule Violated	Status	Passed: User *bin* home directory */bin* contains no matching files with unsafe path statements	Remediation Suggestion

POLICY SETTINGS

User: **bin**
Home: **/bin**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *daemon* home directory */sbin* contains no matching files with unsafe path statements

POLICY SETTINGS

User: **daemon**
Home: **/sbin**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Critical	Rule Violated	Status	Remediation Suggestion

done

Passed: User *lp* home directory */var/spool/lpd* contains no matching files with unsafe path statements

POLICY SETTINGS

User: **lp**
Home: **/var/spool/lpd**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *sync* home directory */sbin* contains no matching files with unsafe path statements

POLICY SETTINGS

User: **sync**
Home: **/sbin**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
```

Critical	Rule Violated	Status	Remediation Suggestion

done

Passed: User *shutdown* home directory */sbin* contains no matching files with unsafe path statements

POLICY SETTINGS

User: **shutdown**
Home: **/sbin**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *halt* home directory */sbin* contains no matching files with unsafe path statements

POLICY SETTINGS

User: **halt**
Home: **/sbin**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
```

Critical	Rule Violated	Status	done	Remediation Suggestion

Passed: User *mail* home directory */var/spool/mail* contains no matching files with unsafe path stateme

POLICY SETTINGS

User: **mail**
Home: **/var/spool/mail**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *operator* home directory */root* contains no matching files with unsafe path statements

POLICY SETTINGS

User: **operator**
Home: **/root**
Files:

/root/.bash_profile
Path statements:
PATH=$PATH:$HOME/bin
export PATH

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash

if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
```

Critical	Rule Violated	Status		Remediation Suggestion

```
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *games* home directory */usr/games* contains no matching files with unsafe path statemen

POLICY SETTINGS

User: **games**
Home: **/usr/games**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *nobody* home directory / contains no matching files with unsafe path statements

POLICY SETTINGS

User: **nobody**
Home: **/**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
```

```
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *dbus* home directory / contains no matching files with unsafe path statements

POLICY SETTINGS

User: **dbus**
Home: **/**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *vcsa* home directory */dev* contains no matching files with unsafe path statements

POLICY SETTINGS

User: **vcsa**
Home: **/dev**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
```

Critical	Rule Violated	Status	Remediation Suggestion

```
''
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *haldaemon* home directory / contains no matching files with unsafe path statements

POLICY SETTINGS

User: **haldaemon**
Home: **/**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *ntp* home directory */etc/ntp* contains no matching files with unsafe path statements

POLICY SETTINGS

User: **ntp**
Home: **/etc/ntp**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
```

Critical	Rule Violated	Status	Remediation Suggestion

```
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *postfix* home directory */var/spool/postfix* contains no matching files with unsafe path sta

POLICY SETTINGS

User: **postfix**
Home: **/var/spool/postfix**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *sshd* home directory */var/empty/sshd* contains no matching files with unsafe path statem

POLICY SETTINGS

User: **sshd**
Home: **/var/empty/sshd**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
```

Critical	Rule Violated	Status	Remediation Suggestion

```
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *ec2-user* home directory */home/ec2-user* contains no matching files with unsafe path stat

POLICY SETTINGS

User: **ec2-user**
Home: **/home/ec2-user**
Files:

/home/ec2-user/.bash_profile
Path statements:
PATH=$JAVA_HOME/bin:$ORACLE_HOME/bin:$PATH:$HOME/bin
export PATH

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *scom* home directory */home/scom* contains no matching files with unsafe path statemen

POLICY SETTINGS

User: **scom**
Home: **/home/scom**
Files:

/home/scom/.bash_profile
Path statements:
PATH=$PATH:$HOME/bin
export PATH

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g`
```

Critical	Rule Violated	Status	Remediation Suggestion

```
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *apache* home directory */var/www* contains no matching files with unsafe path statement

POLICY SETTINGS

User: **apache**
Home: **/var/www**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Passed: User *oracle* home directory */home/oracle* contains no matching files with unsafe path stateme

POLICY SETTINGS

User: **oracle**
Home: **/home/oracle**
Files:

/home/oracle/.bash_profile
Path statements:
PATH=$PATH:$HOME/bin
export PATH

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

Critical	Rule Violated	Status	Remediation Suggestion

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Indeterminate: User *adm* home directory */var/adm* could not be found
The target user defined in your policy's home directory does not exist. Please check your server configuration.

POLICY SETTINGS

User: **adm**
Home: **/var/adm**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Indeterminate: User *uucp* home directory */var/spool/uucp* could not be found
The target user defined in your policy's home directory does not exist. Please check your server configuration.

POLICY SETTINGS

User: **uucp**
Home: **/var/spool/uucp**
Files:

Files:

Critical	Rule Violated	Status	Remediation Suggestion

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Indeterminate: User *gopher* home directory */var/gopher* could not be found
The target user defined in your policy's home directory does not exist. Please check your server configuration.

POLICY SETTINGS

User: **gopher**
Home: **/var/gopher**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Indeterminate: User *ftp* home directory */var/ftp* could not be found
The target user defined in your policy's home directory does not exist. Please check your server configuration.

Critical	Rule Violated	Status	Remediation Suggestion

POLICY SETTINGS

User: **ftp**
Home: **/var/ftp**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Indeterminate: User *abrt* home directory */etc/abrt* could not be found
The target user defined in your policy's home directory does not exist. Please check your server configuration.

POLICY SETTINGS

User: **abrt**
Home: **/etc/abrt**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
```

Critical	Rule Violated	Status	Remediation Suggestion

```
fi
shift
done
```

Indeterminate: User *saslauth* home directory */var/empty/saslauth* could not be found
The target user defined in your policy's home directory does not exist. Please check your server configuration.

POLICY SETTINGS

User: **saslauth**
Home: **/var/empty/saslauth**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Indeterminate: User *oprofile* home directory */home/oprofile* could not be found
The target user defined in your policy's home directory does not exist. Please check your server configuration.

POLICY SETTINGS

User: **oprofile**
Home: **/home/oprofile**
Files:

REMEDIATION SUGGESTION

Correct or justify any items discovered in the Audit step.

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
```

Critical	Rule Violated	Status	Remediation Suggestion

			fi
			dirown=`ls -ldH $1 | awk '{print $3}'`
			if ["$dirown" != "root"] ; then
			echo $1 is not owned by root
			fi
			else
			echo $1 is not a directory
			fi
			shift
			done

	7.4 Set Default Umask For Users	Indeterminate	**Passed : Value for *umask* setting in */etc/bashrc* is compliant** **POLICY SETTINGS** Configuration file: **/etc/bashrc** Configuration item: **umask** Expected value: **077** Actual value: **077** **REMEDIATION SUGGESTION** Edit the /etc/bashrc and /etc/profile.d/cis.sh files (and the appropriate files for any other shell supported on your system umask 77 # grep "^umask 077" /etc/bashrc umask 077 # grep "^umask 077" /etc/profile.d/* umask 077 **Indeterminate: configuration file */etc/profile.d/cis.sh* could not be found** The target configuration file defined in your policy could not be located. Please check this policy rule or your server conf **POLICY SETTINGS** Configuration file: **/etc/profile.d/cis.sh** Configuration item: **umask** Expected value: **077** Actual value: ***Configuration item not found*** **REMEDIATION SUGGESTION** Edit the /etc/bashrc and /etc/profile files (and the appropriate files for any other shell supported on your system) and ad umask 077
	4.6.4 Disable Tipc	Indeterminate	**Indeterminate: presence */etc/modprobe.d/CIS.conf* could not be found** **POLICY SETTINGS** File: **/etc/modprobe.d/CIS.conf** Expected match: **Contains** ^install\s+tipc\s+\/bin\/true Actual match: **false** **REMEDIATION SUGGESTION** # echo "install tipc /bin/true" >> /etc/modprobe.d/CIS.conf Perform the following to determine if TIPC is disabled. # grep "install tipc /bin/true" /etc/modprobe.d/CIS.conf install tipc /bin/true
	4.6.3 Disable Rds	Indeterminate	**Indeterminate: presence */etc/modprobe.d/CIS.conf* could not be found** **POLICY SETTINGS** File: **/etc/modprobe.d/CIS.conf** Expected match: **Contains** ^install\s+rds\s+\/bin\/true Actual match: **false** **REMEDIATION SUGGESTION** # echo "install rds /bin/true" >> /etc/modprobe.d/CIS.conf Perform the following to determine if RDS is disabled. # grep "install rds /bin/true" /etc/modprobe.d/CIS.conf install rds /bin/true
	4.6.2 Disable Sctp	Indeterminate	**Indeterminate: presence */etc/modprobe.d/CIS.conf* could not be found** **POLICY SETTINGS** File: **/etc/modprobe.d/CIS.conf** Expected match: **Contains** ^install\s+sctp\s+\/bin\/true Actual match: **false**

Critical	Rule Violated	Status	REMEDIATION SUGGESTION / Remediation Suggestion
			# echo "install sctp /bin/true" >> /etc/modprobe.d/CIS.conf Perform the following to determine if SCTP is disabled. # grep "install sctp /bin/true" /etc/modprobe.d/CIS.conf install sctp /bin/true
	4.6.1 Disable Dccp	Indeterminate	**Indeterminate: presence */etc/modprobe.d/CIS.conf* could not be found** **POLICY SETTINGS** File: **/etc/modprobe.d/CIS.conf** Expected match: **Contains** ^install\s+dccp\s+\/bin\/true Actual match: **false** **REMEDIATION SUGGESTION** # echo "install dccp /bin/true" >> /etc/modprobe.d/CIS.conf Perform the following to determine if DCCP is disabled. # grep "install dccp /bin/true" /etc/modprobe.d/CIS.conf install dccp /bin/true
	1.1.24 Disable Mounting Of Udf Filesystems	Indeterminate	**Indeterminate: presence */etc/modprobe.d/CIS.conf* could not be found** **POLICY SETTINGS** File: **/etc/modprobe.d/CIS.conf** Expected match: **Contains** ^install\s+udf\s+\/bin\/true Actual match: **false** **REMEDIATION SUGGESTION** Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install udf /bin/true # /sbin/modprobe -n -v udf install /bin/true # /sbin/lsmod | grep udf
	1.1.23 Disable Mounting Of Squashfs Filesystems	Indeterminate	**Indeterminate: presence */etc/modprobe.d/CIS.conf* could not be found** **POLICY SETTINGS** File: **/etc/modprobe.d/CIS.conf** Expected match: **Contains** ^install\s+squashfs\s+\/bin\/true Actual match: **false** **REMEDIATION SUGGESTION** Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install squashfs /bin/true # /sbin/modprobe -n -v squashfs install /bin/true # /sbin/lsmod | grep squashfs
	1.1.22 Disable Mounting Of Hfsplus Filesystems	Indeterminate	**Indeterminate: presence */etc/modprobe.d/CIS.conf* could not be found** **POLICY SETTINGS** File: **/etc/modprobe.d/CIS.conf** Expected match: **Contains** ^install\s+hfsplus\s+\/bin\/true Actual match: **false** **REMEDIATION SUGGESTION** Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install hfsplus /bin/true # /sbin/modprobe -n -v hfsplus install /bin/true # /sbin/lsmod | grep hfsplus
	1.1.21 Disable Mounting Of Hfs Filesystems	Indeterminate	**Indeterminate: presence */etc/modprobe.d/CIS.conf* could not be found** **POLICY SETTINGS** File: **/etc/modprobe.d/CIS.conf** Expected match: **Contains** ^install\s+hfs\s+\/bin\/true Actual match: **false** **REMEDIATION SUGGESTION**

Critical	Rule Violated	Status	Remediation Suggestion
			REMEDIATION SUGGESTION Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install hfs /bin/true # /sbin/modprobe -n -v hfs install /bin/true # /sbin/lsmod | grep hfs
	1.1.20 Disable Mounting Of Jffs2 Filesystems	Indeterminate	**Indeterminate: presence */etc/modprobe.d/CIS.conf* could not be found** **POLICY SETTINGS** File: **/etc/modprobe.d/CIS.conf** Expected match: **Contains** ^install\s+jffs2\s+\/bin\/true Actual match: **false** **REMEDIATION SUGGESTION** Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install jffs2 /bin/true # /sbin/modprobe -n -v jffs2 install /bin/true # /sbin/lsmod | grep jffs2
	1.1.19 Disable Mounting Of Freevxfs Filesystems	Indeterminate	**Indeterminate: presence */etc/modprobe.d/CIS.conf* could not be found** **POLICY SETTINGS** File: **/etc/modprobe.d/CIS.conf** Expected match: **Contains** ^install\s+freevxfs\s+\/bin\/true Actual match: **false** **REMEDIATION SUGGESTION** Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install freevxfs /bin/true # /sbin/modprobe -n -v freevxfs install /bin/true # /sbin/lsmod | grep freevxfs
	1.1.18 Disable Mounting Of Cramfs Filesystems	Indeterminate	**Indeterminate: presence */etc/modprobe.d/CIS.conf* could not be found** **POLICY SETTINGS** File: **/etc/modprobe.d/CIS.conf** Expected match: **Contains** ^install\s+cramfs\s+\/bin\/true Actual match: **false** **REMEDIATION SUGGESTION** Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install cramfs /bin/true # /sbin/modprobe -n -v cramfs install /bin/true # /sbin/lsmod | grep cramfs
	9.2.4 Verify No Legacy "+" Entries Exist In /Etc/Group File	Passed	**Passed: String presence state for */etc/group* is compliant** **POLICY SETTINGS** File: **/etc/group** Expected match: **Does not contain** ^\+: Actual match: **false** **REMEDIATION SUGGESTION** Delete these entries if they exist. Run the following command and verify that no output is returned: # /bin/grep '^+:' /etc/group
	9.2.3 Verify No Legacy "+" Entries Exist In /Etc/Shadow File	Passed	**Passed: String presence state for */etc/shadow* is compliant** **POLICY SETTINGS** File: **/etc/shadow** Expected match: **Does not contain** ^\+: Actual match: **false**

Critical	Rule Violated	Status	REMEDIATION SUGGESTION	Remediation Suggestion
			Delete these entries if they exist. Run the following command and verify that no output is returned: # /bin/grep '^+:' /etc/shadow	
	9.2.2 Verify No Legacy "+" Entries Exist In /Etc/Passwd File	Passed	**Passed: String presence state for */etc/passwd* is compliant** **POLICY SETTINGS** File: **/etc/passwd** Expected match: **Does not contain** ^\+: Actual match: **false** **REMEDIATION SUGGESTION** Delete these entries if they exist. Run the following command and verify that no output is returned: # /bin/grep '^+:' /etc/passwd	
	9.2.1 Ensure Password Fields Are Not Empty	Passed	**Passed: No password check for user *halt* is compliant** **POLICY SETTINGS** User: **halt** Password present: **true** **REMEDIATION SUGGESTION** If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca # /usr/bin/passwd -l Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force Run the following command and verify that no output is returned: # /bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}' **Passed: No password check for user *oracle* is compliant** **POLICY SETTINGS** User: **oracle** Password present: **true** **REMEDIATION SUGGESTION** If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca # /usr/bin/passwd -l Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force Run the following command and verify that no output is returned: # /bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}' **Passed: No password check for user *apache* is compliant** **POLICY SETTINGS** User: **apache** Password present: **true** **REMEDIATION SUGGESTION** If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca # /usr/bin/passwd -l Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force Run the following command and verify that no output is returned: # /bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}' **Passed: No password check for user *ftp* is compliant** **POLICY SETTINGS** User: **ftp** Password present: **true**	

Critical	Rule Violated	Status	REMEDIATION SUGGESTION	Remediation Suggestion

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *ntp* is compliant
POLICY SETTINGS

User: **ntp**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *oprofile* is compliant
POLICY SETTINGS

User: **oprofile**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *lp* is compliant
POLICY SETTINGS

User: **lp**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *dbus* is compliant
POLICY SETTINGS

User: **dbus**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *postfix* is compliant
POLICY SETTINGS

Critical	Rule Violated	Status	Remediation Suggestion

User: **postfix**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *sshd* is compliant
POLICY SETTINGS

User: **sshd**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *ec2-user* is compliant
POLICY SETTINGS

User: **ec2-user**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *bin* is compliant
POLICY SETTINGS

User: **bin**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *haldaemon* is compliant
POLICY SETTINGS

User: **haldaemon**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Critical	Rule Violated	Status	Run the following command and verify that no output is returned:	Remediation Suggestion

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *saslauth* is compliant
POLICY SETTINGS

User: **saslauth**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *abrt* is compliant
POLICY SETTINGS

User: **abrt**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *scom* is compliant
POLICY SETTINGS

User: **scom**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *root* is compliant
POLICY SETTINGS

User: **root**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *uucp* is compliant
POLICY SETTINGS

User: **uucp**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

Critical	Rule Violated	Status	Remediation Suggestion

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *vcsa* is compliant

POLICY SETTINGS

User: **vcsa**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *operator* is compliant

POLICY SETTINGS

User: **operator**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *games* is compliant

POLICY SETTINGS

User: **games**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *nobody* is compliant

POLICY SETTINGS

User: **nobody**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *sync* is compliant

POLICY SETTINGS

User: **sync**
Password present: **true**

Critical	Rule Violated	Status	Password present: **true**	Remediation Suggestion

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *shutdown* is compliant
POLICY SETTINGS

User: **shutdown**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *mail* is compliant
POLICY SETTINGS

User: **mail**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *gopher* is compliant
POLICY SETTINGS

User: **gopher**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Passed: No password check for user *adm* is compliant
POLICY SETTINGS

User: **adm**
Password present: **true**

REMEDIATION SUGGESTION

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca

/usr/bin/passwd -l

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force

Run the following command and verify that no output is returned:

/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Critical	Rule Violated	Status	Remediation Suggestion
			Passed: No password check for user *daemon* is compliant **POLICY SETTINGS** User: **daemon** Password present: **true** **REMEDIATION SUGGESTION** If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it ca # /usr/bin/passwd -l Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be force
	9.1.9 Verify User/Group Ownership On /Etc/Group	Passed	**Passed: User owner *root* for file */etc/group* is compliant** **POLICY SETTINGS** File: **/etc/group** Expected owner: **root** Actual owner: **root** **REMEDIATION SUGGESTION** If the ownership of the /etc/group file are incorrect, run the following command to correct them: # /bin/chown root:root /etc/group Run the following command to determine the permissions on the /etc/group file. # /bin/ls -l /etc/group -rw-r--r-- 1 root root 762 Sep 23 002 /etc/group **Passed: Group owner *root* for file */etc/group* is compliant** **POLICY SETTINGS** File: **/etc/group** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** If the group ownership of the /etc/group file are incorrect, run the following command to correct them: /bin/chown root:root /etc/group
	9.1.8 Verify User/Group Ownership On /Etc/Gshadow	Passed	**Passed: User owner *root* for file */etc/gshadow* is compliant** **POLICY SETTINGS** File: **/etc/gshadow** Expected owner: **root** Actual owner: **root** **REMEDIATION SUGGESTION** If the ownership of the /etc/gshadow file are incorrect, run the following command to correct them: # /bin/chown root:root /etc/gshadow Run the following command to determine the permissions on the /etc/gshadow file. # /bin/ls -l /etc/gshadow ---------- 1 root root 633 Sep 23 2002 /etc/gshadow **Passed: Group owner *root* for file */etc/gshadow* is compliant** **POLICY SETTINGS** File: **/etc/gshadow** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** If the group ownership of the /etc/gshadow file are incorrect, run the following command to correct them: /bin/chown root:root /etc/gshadow
	9.1.7 Verify User/Group Ownership On /Etc/Shadow	Passed	**Passed: User owner *root* for file */etc/shadow* is compliant** **POLICY SETTINGS** File: **/etc/shadow** Expected owner: **root** Actual owner: **root** **REMEDIATION SUGGESTION** If the ownership of the /etc/shadow file are incorrect, run the following command to correct them:

Run the following command and verify that no output is returned:
/bin/cat /etc/shadow | /bin/awk -F: '($2 == "") { print $1 " does not have a password "}'

Critical	Rule Violated	Status	Remediation Suggestion
			# /bin/chown root:root /etc/shadow Run the following command to determine the permissions on the /etc/shadow file. # /bin/ls -l /etc/shadow ---------- 1 root root 762 Sep 23 2002 /etc/shadow **Passed: Group owner *root* for file */etc/shadow* is compliant** **POLICY SETTINGS** File: **/etc/shadow** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** If the group ownership of the /etc/shadow file are incorrect, run the following command to correct them: /bin/chown root:root /etc/shadow
	9.1.6 Verify User/Group Ownership On /Etc/Passwd	Passed	**Passed: User owner *root* for file */etc/passwd* is compliant** **POLICY SETTINGS** File: **/etc/passwd** Expected owner: **root** Actual owner: **root** **REMEDIATION SUGGESTION** If the user and group ownership of the /etc/passwd file are incorrect, run the following command to correct them: # /bin/chown root:root /etc/passwd Run the following command to determine the user and group ownership on the /etc/passwd file. # /bin/ls -l /etc/passwd -rw-r--r-- 1 root root 762 Sep 23 002 /etc/passwd **Passed: Group owner *root* for file */etc/passwd* is compliant** **POLICY SETTINGS** File: **/etc/passwd** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** If the group ownership of the /etc/passwd file are incorrect, run the following command to correct them: /bin/chown root:root /etc/passwd
	9.1.5 Verify Permissions On /Etc/Group	Passed	**Passed: ACL *644* for file */etc/group* is compliant** **POLICY SETTINGS** File: **/etc/group** Expected ACL: **644** Actual ACL: **644** **REMEDIATION SUGGESTION** If the permissions of the /etc/group file are incorrect, run the following command to correct them: # /bin/chmod 644 /etc/group Run the following command to determine the permissions on the /etc/group file. # /bin/ls -l /etc/group -rw-r--r-- 1 root root 762 Sep 23 002 /etc/group
	9.1.4 Verify Permissions On /Etc/Gshadow	Passed	**Passed: ACL *000* for file */etc/gshadow* is compliant** **POLICY SETTINGS** File: **/etc/gshadow** Expected ACL: **000** Actual ACL: **000** **REMEDIATION SUGGESTION** If the permissions of the /etc/gshadow file are incorrect, run the following command to correct them: # /bin/chmod 000 /etc/gshadow Run the following command to determine the permissions on the /etc/gshadow file. # /bin/ls -l /etc/gshadow

Critical	Rule Violated	Status	---------- 1 root root 633 Sep 23 2002 /etc/gshadow **Remediation Suggestion**
	9.1.3 Verify Permissions On /Etc/Shadow	Passed	**Passed: ACL *000* for file */etc/shadow* is compliant** **POLICY SETTINGS** File: **/etc/shadow** Expected ACL: **000** Actual ACL: **000** **REMEDIATION SUGGESTION** If the permissions of the /etc/shadow file are incorrect, run the following command to correct them: # /bin/chmod 000 /etc/shadow Run the following command to determine the permissions on the /etc/shadow file. # /bin/ls -l /etc/shadow ---------- 1 root root 633 Sep 23 2002 /etc/shadow
	9.1.2 Verify Permissions On /Etc/Passwd	Passed	**Passed: ACL *644* for file */etc/passwd* is compliant** **POLICY SETTINGS** File: **/etc/passwd** Expected ACL: **644** Actual ACL: **644** **REMEDIATION SUGGESTION** If the permissions of the /etc/passwd file are incorrect, run the following command to correct them: # /bin/chmod 644 /etc/passwd Run the following command to determine the permissions on the /etc/passwd file. # /bin/ls -l /etc/passwd -rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/passwd
	8.2 Remove Os Information From Login Warning Banners	Passed	**Passed: String presence state for */etc/motd* is compliant** **POLICY SETTINGS** File: **/etc/motd** Expected match: **Does not contain** \\[msrv] Actual match: **false** **REMEDIATION SUGGESTION** Edit the /etc/motd, /etc/issue and /etc/issue.net files and remove any lines containing \m, \r, \s or \v. Perform the following commands to check if OS information is set to be displayed in the system login banners: # egrep '(\\v|\\r|\\m|\\s)' /etc/issue # egrep '(\\v|\\r|\\m|\\s)' /etc/motd # egrep'(\\v|\\r|\\m|\\s)' /etc/issue.net **Passed: String presence state for */etc/issue* is compliant** **POLICY SETTINGS** File: **/etc/issue** Expected match: **Does not contain** \\[msrv] Actual match: **false** **REMEDIATION SUGGESTION** Edit the /etc/motd, /etc/issue and /etc/issue.net files and remove any lines containing \m, \r, \s or \v. Perform the following commands to check if OS information is set to be displayed in the system login banners: # egrep '(\\v|\\r|\\m|\\s)' /etc/issue # egrep '(\\v|\\r|\\m|\\s)' /etc/motd # egrep'(\\v|\\r|\\m|\\s)' /etc/issue.net **Passed: String presence state for */etc/issue.net* is compliant** **POLICY SETTINGS** File: **/etc/issue.net** Expected match: **Does not contain** \\[msrv] Actual match: **false** **REMEDIATION SUGGESTION** Edit the /etc/motd, /etc/issue and /etc/issue.net files and remove any lines containing \m, \r, \s or \v.

Critical	Rule Violated	Status	Remediation Suggestion
			Perform the following commands to check if OS information is set to be displayed in the system login banners: # egrep '(\\v|\\r|\\m|\\s)' /etc/issue # egrep '(\\v|\\r|\\m|\\s)' /etc/motd # egrep'(\\v|\\r|\\m|\\s)' /etc/issue.net
	8.1 Set Warning Banner For Standard Login Services	Passed	**Passed: File presence state for *[/etc/motd](#)* is compliant** **POLICY SETTINGS** File: **/etc/motd** Expected presence: **true** Actual presence: **true** **REMEDIATION SUGGESTION** # touch /etc/motd # echo "Authorized uses only. All activity may be \ monitored and reported." > /etc/issue # echo "Authorized uses only. All activity may be \ monitored and reported." > /etc/issue.net # chown root:root /etc/motd # chmod 644 /etc/motd # chown root:root /etc/issue # chmod 644 /etc/issue # chown root:root /etc/issue.net # chmod 644 /etc/issue.net Run the following commands and ensure that the files exist and have the correct permissions. # /bin/ls -l /etc/motd -rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/motd # ls /etc/issue -rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/issue # ls /etc/issue.net -rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/issue.net The commands above simply validate the presence of the /etc/motd, /etc/issue and /etc/issue.net files. Review the conte appropriate for your organization. **Passed: File presence state for *[/etc/issue](#)* is compliant** **POLICY SETTINGS** File: **/etc/issue** Expected presence: **true** Actual presence: **true** **REMEDIATION SUGGESTION** # touch /etc/motd # echo "Authorized uses only. All activity may be \ monitored and reported." > /etc/issue # echo "Authorized uses only. All activity may be \ monitored and reported." > /etc/issue.net # chown root:root /etc/motd # chmod 644 /etc/motd # chown root:root /etc/issue # chmod 644 /etc/issue # chown root:root /etc/issue.net # chmod 644 /etc/issue.net Run the following commands and ensure that the files exist and have the correct permissions. # /bin/ls -l /etc/motd -rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/motd # ls /etc/issue -rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/issue # ls /etc/issue.net -rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/issue.net The commands above simply validate the presence of the /etc/motd, /etc/issue and /etc/issue.net files. Review the conte appropriate for your organization. **Passed: File presence state for *[/etc/issue.net](#)* is compliant** **POLICY SETTINGS** File: **/etc/issue.net** Expected presence: **true** Actual presence: **true** **REMEDIATION SUGGESTION** # touch /etc/motd # echo "Authorized uses only. All activity may be \ monitored and reported." > /etc/issue # echo "Authorized uses only. All activity may be \ monitored and reported." > /etc/issue.net

Critical	Rule Violated	Status	Remediation Suggestion

chown root:root /etc/motd
chmod 644 /etc/motd
chown root:root /etc/issue
chmod 644 /etc/issue
chown root:root /etc/issue.net
chmod 644 /etc/issue.net

Run the following commands and ensure that the files exist and have the correct permissions.

/bin/ls -l /etc/motd
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/motd
ls /etc/issue
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/issue
ls /etc/issue.net
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/issue.net

The commands above simply validate the presence of the /etc/motd, /etc/issue and /etc/issue.net files. Review the conte
appropriate for your organization.

Passed: User owner *root* for file */etc/motd* is compliant

POLICY SETTINGS

File: **/etc/motd**
Expected owner: **root**
Actual owner: **root**

REMEDIATION SUGGESTION

chown root:root /etc/motd
chown root:root /etc/issue
chown root:root /etc/issue.net

Passed: User owner *root* for file */etc/issue* is compliant

POLICY SETTINGS

File: **/etc/issue**
Expected owner: **root**
Actual owner: **root**

REMEDIATION SUGGESTION

chown root:root /etc/motd
chown root:root /etc/issue

chown root:root /etc/issue.net

Passed: User owner *root* for file */etc/issue.net* is compliant

POLICY SETTINGS

File: **/etc/issue.net**
Expected owner: **root**
Actual owner: **root**

REMEDIATION SUGGESTION

chown root:root /etc/motd
chown root:root /etc/issue
chown root:root /etc/issue.net

Passed: Group owner *root* for file */etc/motd* is compliant

POLICY SETTINGS

File: **/etc/motd**
Expected group owner: **root**
Actual group owner: **root**

REMEDIATION SUGGESTION

chown root:root /etc/motd
chown root:root /etc/issue
chown root:root /etc/issue.net

Passed: Group owner *root* for file */etc/issue* is compliant

POLICY SETTINGS

File: **/etc/issue**
Expected group owner: **root**
Actual group owner: **root**

REMEDIATION SUGGESTION

chown root:root /etc/motd
chown root:root /etc/issue
chown root:root /etc/issue.net

Passed: Group owner *root* for file */etc/issue.net* is compliant

POLICY SETTINGS

Critical	Rule Violated	Status	Remediation Suggestion
			File: **/etc/issue.net** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/motd # chown root:root /etc/issue # chown root:root /etc/issue.net **Passed: ACL *644* for file */etc/motd* is compliant** **POLICY SETTINGS** File: **/etc/motd** Expected ACL: **644** Actual ACL: **644** **REMEDIATION SUGGESTION** # chmod 644 /etc/motd # chmod 644 /etc/issue # chmod 644 /etc/issue.net **Passed: ACL *644* for file */etc/issue* is compliant** **POLICY SETTINGS** File: **/etc/issue** Expected ACL: **644** Actual ACL: **644** **REMEDIATION SUGGESTION** # chmod 644 /etc/motd # chmod 644 /etc/issue # chmod 644 /etc/issue.net **Passed: ACL *644* for file */etc/issue.net* is compliant** **POLICY SETTINGS** File: **/etc/issue.net** Expected ACL: **644** Actual ACL: **644** **REMEDIATION SUGGESTION** # chmod 644 /etc/motd # chmod 644 /etc/issue # chmod 644 /etc/issue.net
	7.5 Lock Inactive User Accounts	Passed	**Passed : Value for *INACTIVE* setting in */etc/default/useradd* is compliant** **POLICY SETTINGS** Configuration file: **/etc/default/useradd** Configuration item: **INACTIVE** Expected value: **35** Actual value: **35** **REMEDIATION SUGGESTION** # useradd -D -f 35 # useradd -D | grep INACTIVE
	7.3 Set Default Group For Root Account	Passed	**Passed: String presence state for */etc/passwd* is compliant** **POLICY SETTINGS** File: **/etc/passwd** Expected match: **Contains** ^root:x:0:0 Actual match: **true** **REMEDIATION SUGGESTION** # usermod -g 0 root # grep "^root:" /etc/passwd | cut -f4 -d: 0
	7.1.3 Set Password Expiring Warning Days	Passed	**Passed : Value for *PASS_WARN_AGE* setting in */etc/login.defs* is compliant** **POLICY SETTINGS** Configuration file: **/etc/login.defs** Configuration item: **PASS_WARN_AGE**

Critical	Rule Violated	Status	Remediation Suggestion
			Configuration item: **PASS_WARN_AGE** Expected value: **7** Actual value: **7** **REMEDIATION SUGGESTION** Set the PASS_WARN_AGE parameter to 7 in /etc/login.defs: PASS_WARN_AGE 7 Modify active user parameters to match: # chage --warndays 7 # grep PASS_WARN_AGE /etc/login.defs PASS_WARN_AGE 7 # chage --list Number of days of warning before password expires: 7
	7.1.2 Set Password Change Minimum Number Of Days	Passed	**Passed : Value for *PASS_MIN_DAYS* setting in */etc/login.defs* is compliant** **POLICY SETTINGS** Configuration file: **/etc/login.defs** Configuration item: **PASS_MIN_DAYS** Expected value: **7** Actual value: **7** **REMEDIATION SUGGESTION** Set the PASS_MIN_DAYS parameter to 7 in /etc/login.defs: PASS_MIN_DAYS 7 Modify active user parameters to match: # chage --mindays 7 # grep PASS_MIN_DAYS /etc/login.defs PASS_MAX_DAYS 7 # chage --list Minimum number of days between password change: 7
	7.1.1 Set Password Expiration Days	Passed	**Passed : Value for *PASS_MAX_DAYS* setting in */etc/login.defs* is compliant** **POLICY SETTINGS** Configuration file: **/etc/login.defs** Configuration item: **PASS_MAX_DAYS** Expected value: **90** Actual value: **90** **REMEDIATION SUGGESTION** Set the PASS_MAX_DAYS parameter to 90 in /etc/login.defs: PASS_MAX_DAYS 90 Modify active user parameters to match: # chage --maxdays 90 # grep PASS_MAX_DAYS /etc/login.defs PASS_MAX_DAYS 90 # chage --list Maximum number of days between password change: 90
	6.5 Restrict Access To The Su Command	Passed	**Passed: String presence state for */etc/pam.d/su* is compliant** **POLICY SETTINGS** File: **/etc/pam.d/su** Expected match: **Contains** ^auth\s+required\s+pam_wheel\.so\s+use_uid Actual match: **true** **REMEDIATION SUGGESTION** Set the pam_wheel.so parameters as follows in /etc/pam.d/su: auth required pam_wheel.so use_uid Set the proper list of users to be included in the wheel group in /etc/groups. # grep pam_wheel.so /etc/pam.d/su auth required pam_wheel.so use_uid # grep wheel /etc/group wheel:x:10:root,

Critical	Rule Violated	Status	Remediation Suggestion
	6.3.4 Limit Password Reuse	Passed	**Passed: String presence state for *etc/pam.d/system-auth* is compliant** **POLICY SETTINGS** File: **/etc/pam.d/system-auth** Expected match: **Contains** ^password\s+sufficient\s+pam_unix.*remember\s*=\s*5 Actual match: **true** **REMEDIATION SUGGESTION** Set the pam_unix.so remember parameter to 5 in /etc/pam.d/system-auth: password sufficient pam_unix.so remember=5 Perform the following to determine the current setting for reuse of older passwords: # grep "remember" /etc/pam.d/system-auth password sufficient pam_unix.so remember=5 **Passed: File presence state for */etc/security/opasswd* is compliant** **POLICY SETTINGS** File: **/etc/security/opasswd** Expected presence: **true** Actual presence: **true** **REMEDIATION SUGGESTION** Make sure /etc/security/opasswd file exists
	6.3.1 Upgrade Password Hashing Algorithm To Sha 512	Passed	**Passed : Value for *ENCRYPT_METHOD* setting in */etc/login.defs* is compliant** **POLICY SETTINGS** Configuration file: **/etc/login.defs** Configuration item: **ENCRYPT_METHOD** Expected value: **SHA512** Actual value: **SHA512** **REMEDIATION SUGGESTION** Perform the following to configure the system as recommended: # authconfig --passalgo=sha512 --update NOTE: If it is determined that the password algorithm being used is not SHA-512, once it is changed, it is recommended their passwords on next login. To accomplish that, the following commands can be used. Any system accounts that nee system administrator to prevent any potential problems. # cat /etc/passwd | awk -F: '($3 >=500 && $1 != "nfsnobody") { print $1 }' | xargs -n 1 chage -d 0 Perform the following to determine if the password-hashing algorithm is set to SHA-512: # authconfig --test | grep hashing | grep sha512 If the above command emits no output then the system is not configured as recommended
	6.2.14 Set Ssh Banner	Passed	**Passed : Value for *Banner* setting in */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** Configuration file: **/etc/ssh/sshd_config** Configuration item: **Banner** Expected value: **/etc/issue.net** Actual value: **/etc/issue.net** **REMEDIATION SUGGESTION** Edit the /etc/ssh/sshd_config file to set the parameter as follows: Banner /etc/issue.net To verify the correct SSH setting, run the following command and verify that is either /etc/issue or /etc/issue.net: # grep "^Banner" /etc/ssh/sshd_config Banner
	6.2.13 Limit Access Via Ssh	Passed	**Passed: String presence state for */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** File: **/etc/ssh/sshd_config** Expected match: **Contains** ^[AD][le][ln][oy][wUG][UGsr][sreo][eoru][rusp][sp]* Actual match: **true** **REMEDIATION SUGGESTION**

Critical	Rule Violated	Status	Remediation Suggestion
			Edit the /etc/ssh/sshd_config file to set one or more of the parameter as follows: AllowUsers AllowGroups DenyUsers DenyGroups To verify the correct SSH setting, run the following command and verify that the output is as shown: # grep "^AllowUsers" /etc/ssh/sshd_config AllowUsers # grep "^AllowGroups" /etc/ssh/sshd_config AllowGroups # grep "^DenyUsers" /etc/ssh/sshd_config DenyUsers # grep "^DenyGroups" /etc/ssh/sshd_config DenyGroups
	6.2.11 Use Only Approved Cipher In Counter Mode	Passed	**Passed : Value for *Ciphers* setting in */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** Configuration file: **/etc/ssh/sshd_config** Configuration item: **Ciphers** Expected value: **aes128-ctr,aes192-ctr,aes256-ctr** Actual value: **aes128-ctr,aes192-ctr,aes256-ctr** **REMEDIATION SUGGESTION** Edit the /etc/ssh/sshd_config file to set the parameter as follows: Ciphers aes128-ctr,aes192-ctr,aes256-ctr To verify the correct SSH setting, run the following command and verify that the output is as shown: # grep "Ciphers" /etc/ssh/sshd_config Ciphers aes128-ctr,aes192-ctr,aes256-ctr
	6.2.10 Do Not Allow Users To Set Environment Options	Passed	**Passed : Value for *PermitUserEnvironment* setting in */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** Configuration file: **/etc/ssh/sshd_config** Configuration item: **PermitUserEnvironment** Expected value: **no** Actual value: **no** **REMEDIATION SUGGESTION** Edit the /etc/ssh/sshd_config file to set the parameter as follows: PermitUserEnvironment no To verify the correct SSH setting, run the following command and verify that the output is as shown: # grep PermitUserEnvironment /etc/ssh/sshd_config PermitUserEnvironment no
	6.2.9 Set Ssh Permit Empty Passwords To No	Passed	**Passed : Value for *PermitEmptyPasswords* setting in */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** Configuration file: **/etc/ssh/sshd_config** Configuration item: **PermitEmptyPasswords** Expected value: **no** Actual value: **no** **REMEDIATION SUGGESTION** Edit the /etc/ssh/sshd_config file to set the parameter as follows: PermitEmptyPasswords no To verify the correct SSH setting, run the following command and verify that the output is as shown: # grep "^PermitEmptyPasswords" /etc/ssh/sshd_config PermitEmptyPasswords no
	6.2.8 Disable Ssh Root Login	Passed	**Passed : Value for *PermitRootLogin* setting in */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** Configuration file: **/etc/ssh/sshd_config** Configuration item: **PermitRootLogin** Expected value: **no** Actual value: **no**

Critical	Rule Violated	Status	REMEDIATION SUGGESTION — Remediation Suggestion
			Edit the /etc/ssh/sshd_config file to set the parameter as follows: PermitRootLogin no To verify the correct SSH setting, run the following command and verify that the output is as shown: # grep "^PermitRootLogin" /etc/ssh/sshd_config PermitRootLogin no
	6.2.7 Set Ssh Hostbased Authentication To No	Passed	**Passed : Value for *HostbasedAuthentication* setting in */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** Configuration file: **/etc/ssh/sshd_config** Configuration item: **HostbasedAuthentication** Expected value: **no** Actual value: **no** **REMEDIATION SUGGESTION** Edit the /etc/ssh/sshd_config file to set the parameter as follows: HostbasedAuthentication no To verify the correct SSH setting, run the following command and verify that the output is as shown: # grep "^HostbasedAuthentication" /etc/ssh/sshd_config HostbasedAuthentication no
	6.2.6 Set Ssh Ignore Rhosts To Yes	Passed	**Passed : Value for *IgnoreRhosts* setting in */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** Configuration file: **/etc/ssh/sshd_config** Configuration item: **IgnoreRhosts** Expected value: **yes** Actual value: **yes** **REMEDIATION SUGGESTION** Edit the /etc/ssh/sshd_config file to set the parameter as follows: IgnoreRhosts yes To verify the correct SSH setting, run the following command and verify that the output is as shown: # grep "^IgnoreRhosts" /etc/ssh/sshd_config IgnoreRhosts yes
	6.2.5 Set Ssh Max Auth Tries To 4 Or Less	Passed	**Passed : Value for *MaxAuthTries* setting in */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** Configuration file: **/etc/ssh/sshd_config** Configuration item: **MaxAuthTries** Expected value: **4** Actual value: **4** **REMEDIATION SUGGESTION** Edit the /etc/ssh/sshd_config file to set the parameter as follows: MaxAuthTries 4 To verify the correct SSH setting, run the following command and verify that the output is as shown: # grep "^MaxAuthTries" /etc/ssh/sshd_config MaxAuthTries 4
	6.2.4 Disable Ssh X11 Forwarding	Passed	**Passed : Value for *X11Forwarding* setting in */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** Configuration file: **/etc/ssh/sshd_config** Configuration item: **X11Forwarding** Expected value: **no** Actual value: **no** **REMEDIATION SUGGESTION** Edit the /etc/ssh/sshd_config file to set the parameter as follows: X11Forwarding no To verify the correct SSH setting, run the following command and verify that the output is as shown:

Critical	Rule Violated	Status	Remediation Suggestion
			# grep "^X11Forwarding" /etc/ssh/sshd_config X11Forwarding no
	6.2.2 Set Log Level To Info	Passed	**Passed : Value for *LogLevel* setting in */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** Configuration file: **/etc/ssh/sshd_config** Configuration item: **LogLevel** Expected value: **INFO** Actual value: **INFO** **REMEDIATION SUGGESTION** Edit the /etc/ssh/sshd_config file to set the parameter as follows: LogLevel INFO To verify the correct SSH setting, run the following command and verify that the output is as shown: # grep "^LogLevel" /etc/ssh/sshd_config LogLevel INFO
	6.2.1 Set Ssh Protocol To 2	Passed	**Passed : Value for *Protocol* setting in */etc/ssh/sshd_config* is compliant** **POLICY SETTINGS** Configuration file: **/etc/ssh/sshd_config** Configuration item: **Protocol** Expected value: **2** Actual value: **2** **REMEDIATION SUGGESTION** Edit the /etc/ssh/sshd_config file to set the parameter as follows: Protocol 2 To verify the correct SSH setting, run the following command and verify that the output is as shown: # grep "^Protocol" /etc/ssh/sshd_config Protocol 2
	6.1.10 Restrict At Daemon	Passed	**Passed: File presence state for */etc/at.deny* is compliant** **POLICY SETTINGS** File: **/etc/at.deny** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # rm /etc/at.deny # touch /etc/at.allow # chown root:root /etc/at.allow # chmod og-rwx /etc/at.allow Perform the following to determine if at jobs are restricted. # stat -L /etc/at.deny > /dev/null # stat -L -c "%a %u %g" /etc/at.allow | egrep ".00 0 0" If the above command emits no output then the system is not configured as recommended. **Passed: File presence state for */etc/at.allow* is compliant** **POLICY SETTINGS** File: **/etc/at.allow** Expected presence: **true** Actual presence: **true** **REMEDIATION SUGGESTION** # touch /etc/at.allow **Passed: User owner *root* for file */etc/at.allow* is compliant** **POLICY SETTINGS** File: **/etc/at.allow** Expected owner: **root** Actual owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/at.allow

Critical	Rule Violated	Status	Remediation Suggestion
			# chown root:root /etc/at.allow **Passed: Group owner *root* for file */etc/at.allow* is compliant** **POLICY SETTINGS** File: **/etc/at.allow** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/at.allow **Passed: ACL *600* for file */etc/at.allow* is compliant** **POLICY SETTINGS** File: **/etc/at.allow** Expected ACL: ***00** Actual ACL: **600** **REMEDIATION SUGGESTION** # chmod og-rwx /etc/at.allow
	6.1.9 Set User/Group Owner And Permission On /Etc/Cron.D	Passed	**Passed: ACL *700* for directory */etc/cron.d* is compliant** **POLICY SETTINGS** Directory: **/etc/cron.d** Expected ACL: ***00** Actual ACL: **700** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.d # chmod og-rwx /etc/cron.d Perform the following to determine if the /etc/cron.d directory has the correct permissions. # stat -L -c "%a %u %g" /etc/cron.d | egrep ".00 0 0" If the above command emits no output then the system is not configured as recommended. **Passed: User owner *root* for directory */etc/cron.d* is compliant** **POLICY SETTINGS** Directory: **/etc/cron.d** Expected owner: **root** Actual owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.d **Passed: Group owner *root* for directory */etc/cron.d* is compliant** **POLICY SETTINGS** Directory: **/etc/cron.d** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.d
	6.1.8 Set User/Group Owner And Permission On /Etc/Cron.Monthly	Passed	**Passed: ACL *700* for directory */etc/cron.monthly* is compliant** **POLICY SETTINGS** Directory: **/etc/cron.monthly** Expected ACL: ***00** Actual ACL: **700** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.monthly # chmod og-rwx /etc/cron.monthly Perform the following to determine if the /etc/cron.monthly directory has the correct permissions. # stat -L -c "%a %u %g" /etc/cron.monthly | egrep ".00 0 0" If the above command emits no output then the system is not configured as recommended. **Passed: User owner *root* for directory */etc/cron.monthly* is compliant** **POLICY SETTINGS**

Critical	Rule Violated	Status	Remediation Suggestion
			Directory: **/etc/cron.monthly** Expected owner: **root** Actual owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.monthly **Passed: Group owner *root* for directory */etc/cron.monthly* is compliant** **POLICY SETTINGS** Directory: **/etc/cron.monthly** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.monthly
	6.1.7 Set User/Group Owner And Permission On /Etc/Cron.Weekly	Passed	**Passed: ACL *700* for directory */etc/cron.weekly* is compliant** **POLICY SETTINGS** Directory: **/etc/cron.weekly** Expected ACL: ***00** Actual ACL: **700** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.weekly # chmod og-rwx /etc/cron.weekly Perform the following to determine if the /etc/cron.weekly directory has the correct permissions. # stat -L -c "%a %u %g" /etc/cron.weekly | egrep ".00 0 0" If the above command emits no output then the system is not configured as recommended. **Passed: User owner *root* for directory */etc/cron.weekly* is compliant** **POLICY SETTINGS** Directory: **/etc/cron.weekly** Expected owner: **root** Actual owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.weekly **Passed: Group owner *root* for directory */etc/cron.weekly* is compliant** **POLICY SETTINGS** Directory: **/etc/cron.weekly** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.weekly
	6.1.6 Set User/Group Owner And Permission On /Etc/Cron.Daily	Passed	**Passed: ACL *700* for directory */etc/cron.daily* is compliant** **POLICY SETTINGS** Directory: **/etc/cron.daily** Expected ACL: ***00** Actual ACL: **700** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.daily # chmod og-rwx /etc/cron.daily Perform the following to determine if the /etc/cron.daily directory has the correct permissions. # stat -L -c "%a %u %g" /etc/cron.daily | egrep ".00 0 0" If the above command emits no output then the system is not configured as recommended. **Passed: User owner *root* for directory */etc/cron.daily* is compliant** **POLICY SETTINGS** Directory: **/etc/cron.daily** Expected owner: **root**

Critical	Rule Violated	Status	Remediation Suggestion
			Actual owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.daily **Passed: Group owner *root* for directory */etc/cron.daily* is compliant** **POLICY SETTINGS** Directory: **/etc/cron.daily** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.daily
	6.1.5 Set User/Group Owner And Permission On /Etc/Cron.Hourly	Passed	**Passed: ACL *700* for directory */etc/cron.hourly* is compliant** **POLICY SETTINGS** Directory: **/etc/cron.hourly** Expected ACL: ***00** Actual ACL: **700** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.hourly # chmod og-rwx /etc/cron.hourly Perform the following to determine if the /etc/cron.hourly file has the correct permissions. # stat -L -c "%a %u %g" /etc/cron.hourly | egrep ".00 0 0" If the above command emits no output then the system is not configured as recommended. **Passed: User owner *root* for directory */etc/cron.hourly* is compliant** **POLICY SETTINGS** Directory: **/etc/cron.hourly** Expected owner: **root** Actual owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.hourly **Passed: Group owner *root* for directory */etc/cron.hourly* is compliant** **POLICY SETTINGS** Directory: **/etc/cron.hourly** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/cron.hourly
	6.1.4 Set User/Group Owner And Permission On /Etc/Crontab	Passed	**Passed: User owner *root* for file */etc/crontab* is compliant** **POLICY SETTINGS** File: **/etc/crontab** Expected owner: **root** Actual owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/crontab # chmod og-rwx /etc/crontab Perform the following to determine if the /etc/crontab file has the correct permissions. # stat -L -c "%a %u %g" /etc/crontab | egrep ".00 0 0" If the above command emits no output then the system is not configured as recommended. **Passed: Group owner *root* for file */etc/crontab* is compliant** **POLICY SETTINGS** File: **/etc/crontab** Expected group owner: **root** Actual group owner: **root**

Critical	Rule Violated	Status	Remediation Suggestion
			REMEDIATION SUGGESTION # chown root:root /etc/crontab **Passed: ACL *600* for file */etc/crontab* is compliant** **POLICY SETTINGS** File: **/etc/crontab** Expected ACL: ***00** Actual ACL: **600** **REMEDIATION SUGGESTION** # chmod og-rwx /etc/crontab
	6.1.3 Set User/Group Owner And Permission On /Etc/Anacrontab	Passed	**Passed: User owner *root* for file */etc/anacrontab* is compliant** **POLICY SETTINGS** File: **/etc/anacrontab** Expected owner: **root** Actual owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/anacrontab # chmod og-rwx /etc/anacrontab Perform the following to determine if the /etc/anacrontab file has the correct permissions. # stat -L -c "%a %u %g" /etc/anacrontab | egrep ".00 0 0" If the above command emits no output then the system is not configured as recommended. **Passed: Group owner *root* for file */etc/anacrontab* is compliant** **POLICY SETTINGS** File: **/etc/anacrontab** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/anacrontab **Passed: ACL *600* for file */etc/anacrontab* is compliant** **POLICY SETTINGS** File: **/etc/anacrontab** Expected ACL: ***00** Actual ACL: **600** **REMEDIATION SUGGESTION** # chmod og-rwx /etc/anacrontab
	6.1.2 Enable Crond Daemon	Passed	**Passed: process presence state for *crond* is compliant** **POLICY SETTINGS** Process: **crond** Expected presence: **true** Actual presence: **true** **REMEDIATION SUGGESTION** # chkconfig crond on Perform the following to determine if cron is enabled. # chkconfig --list crond crond: 0:off 1:off 2:on 3:on 4:on 5:on 6:off
	6.1.1 Enable Anacron Daemon	Passed	**Passed : package presence state for package *cronie-anacron* is compliant** **POLICY SETTINGS** Package: **cronie-anacron** Expected presence: **true** Actual presence: **true** **REMEDIATION SUGGESTION** # yum install cronie-anacron

Critical	Rule Violated	Status	Remediation Suggestion
			NOTE: NSA Guidance recommends disabling anacron for systems that are intended to be up 24X7, with the rationale th However, even systems that are designed to be up at all times can experience downtime that could prevent important sy for your site to determine your appropriate risk level. Perform the following to determine if anacron is enabled. # rpm -q cronie-anacron cronie-anacron..
	5.2.18 Make The Audit Configuration Immutable	Passed	**Passed: String presence state for */etc/audit/audit.rules* is compliant** **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-e\s+2\s*$ Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file. -e 2 NOTE: This must be the last entry in the /etc/audit/audit.rules file Perform the following to determine if the audit configuration is immutable. # grep "^-e 2" /etc/audit/audit.rules -e 2
	5.2.16 Collect System Administrator Actions (Sudolog)	Passed	**Passed: String presence state for */etc/audit/audit.rules* is compliant** **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-w\s+\/var\/log\/sudo\.log\s+\-p\s+wa\s+\-k\s+actions Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file. -w /var/log/sudo.log -p wa -k actions # Execute the following command to restart auditd # pkill -HUP -P 1 auditd NOTE: The system must be configured with su disabled (See Item 7.6 Restrict Access to the su Command) to force all the console, as administrators can log in as root. Perform the following to determine if administrator activity is recorded. # grep actions /etc/audit/audit.rules -w /var/log/sudo.log -p wa -k actions
	5.2.15 Collect Changes To System Administration Scope (Sudoers)	Passed	**Passed: String presence state for */etc/audit/audit.rules* is compliant** **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-w\s+\/etc\/sudoers\s+\-p\s+wa\s+\-k\s+scope Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file. -w /etc/sudoers -p wa -k scope # Execute the following command to restart auditd # pkill -HUP -P 1 auditd Perform the following to determine if changes to /etc/sudoers are recorded. # grep scope /etc/audit/audit.rules -w /etc/sudoers -p wa -k scope
	5.2.9 Collect Session Initiation Information	Passed	**Passed: String presence state for */etc/audit/audit.rules* is compliant** **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-w\s+\/var\/run\/utmp\s+\-p\s+wa\s+\-k\s+session Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file. -w /var/run/utmp -p wa -k session

Critical	Rule Violated	Status	Remediation Suggestion
			-w /var/log/wtmp -p wa -k session -w /var/log/btmp -p wa -k session # Execute the following command to restart auditd # pkill -HUP -P 1 auditd NOTE: Use the last command to read /var/log/wtmp (last with no parameters) and /var/run/utmp (last -f /var/run/utmp) Perform the following to determine if session initiation information is collected. # grep session /etc/audit/audit.rules -w /var/run/utmp -p wa -k session -w /var/log/wtmp -p wa -k session -w /var/log/btmp -p wa -k session **Passed: String presence state for *<u>/etc/audit/audit.rules</u>* is compliant** **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-w\s+\/var\/log\/wtmp\s+\-p\s+wa\s+\-k\s+session Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file. -w /var/log/wtmp -p wa -k session # Execute the following command to restart auditd # pkill -HUP -P 1 auditd NOTE: Use the last command to read /var/log/wtmp (last with no parameters) and /var/run/utmp (last -f /var/run/utmp) **Passed: String presence state for *<u>/etc/audit/audit.rules</u>* is compliant** **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-w\s+\/var\/log\/btmp\s+\-p\s+wa\s+\-k\s+session Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file. -w /var/log/btmp -p wa -k session # Execute the following command to restart auditd # pkill -HUP -P 1 auditd NOTE: Use the last command to read /var/log/wtmp (last with no parameters) and /var/run/utmp (last -f /var/run/utmp)
	5.2.8 Collect Login And Logout Events	Passed	**Passed: String presence state for *<u>/etc/audit/audit.rules</u>* is compliant** **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-w\s+\/var\/log\/faillog\s+\-p\s+wa\s+\-k\s+logins Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file. -w /var/log/faillog -p wa -k logins -w /var/log/lastlog -p wa -k logins -w /var/log/tallylog -p wa -k logins # Execute the following command to restart auditd # pkill -HUP -P 1 auditd Perform the following to determine if login and logout events are recorded. # grep logins /etc/audit/audit.rules -w /var/log/faillog -p wa -k logins -w /var/log/lastlog -p wa -k logins -w /var/log/tallylog -p wa -k logins **Passed: String presence state for *<u>/etc/audit/audit.rules</u>* is compliant** **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-w\s+\/var\/log\/lastlog\s+\-p\s+wa\s+\-k\s+logins Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file.

Critical	Rule Violated	Status	-w /var/log/lastlog -p wa -k logins Remediation Suggestion
			# Execute the following command to restart auditd # pkill -HUP -P 1 auditd
			Passed: String presence state for */etc/audit/audit.rules* is compliant **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-w\s+\/var\/log\/tallylog\s+\-p\s+wa\s+\-k\s+logins Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file. -w /var/log/tallylog -p wa -k logins # Execute the following command to restart auditd # pkill -HUP -P 1 auditd
	5.2.7 Record Events That Modify The System's Mandatory Access Controls	Passed	**Passed: String presence state for */etc/audit/audit.rules* is compliant** **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-w\s+\/etc\/selinux\/\s+\-p\s+wa\s+\-k\s+MAC\-policy Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file. Add the following lines to /etc/audit/audit.rules -w /etc/selinux/ -p wa -k MAC-policy # Execute the following command to restart auditd # pkill -P 1-HUP auditd Perform the following to determine if events that modify the system's mandatory access controls are recorded # grep MAC-policy /etc/audit/audit.rules -w /etc/selinux/ -p wa -k MAC-policy
	5.2.5 Record Events That Modify User/Group Information	Passed	**Passed: String presence state for */etc/audit/audit.rules* is compliant** **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-w\s+\/etc\/group\s+\-p\s+wa\s+\-k\s+identity Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file. -w /etc/group -p wa -k identity -w /etc/passwd -p wa -k identity -w /etc/gshadow -p wa -k identity -w /etc/shadow -p wa -k identity -w /etc/security/opasswd -p wa -k identity # Execute the following command to restart auditd # pkill -P 1-HUP auditd Perform the following to determine if events that modify user/group information are recorded. # grep identity /etc/audit/audit.rules -w /etc/group -p wa -k identity -w /etc/passwd -p wa -k identity -w /etc/gshadow -p wa -k identity -w /etc/shadow -p wa -k identity -w /etc/security/opasswd -p wa -k identity **Passed: String presence state for */etc/audit/audit.rules* is compliant** **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-w\s+\/etc\/passwd\s+\-p\s+wa\s+\-k\s+identity Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file. -w /etc/passwd -p wa -k identity # Execute the following command to restart auditd # pkill -P 1-HUP auditd

Critical	Rule Violated	Status	Remediation Suggestion
			# pkill -P 1-HUP auditd **Passed: String presence state for */etc/audit/audit.rules* is compliant** **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-w\s+\/etc\/gshadow\s+\-p\s+wa\s+\-k\s+identity Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file. -w /etc/gshadow -p wa -k identity # Execute the following command to restart auditd # pkill -P 1-HUP auditd **Passed: String presence state for */etc/audit/audit.rules* is compliant** **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-w\s+\/etc\/shadow\s+\-p\s+wa\s+\-k\s+identity Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file. -w /etc/shadow -p wa -k identity # Execute the following command to restart auditd # pkill -P 1-HUP auditd **Passed: String presence state for */etc/audit/audit.rules* is compliant** **POLICY SETTINGS** File: **/etc/audit/audit.rules** Expected match: **Contains** ^\-w\s+\/etc\/security\/opasswd\s+\-p\s+wa\s+\-k\s+identity Actual match: **true** **REMEDIATION SUGGESTION** Add the following lines to the /etc/audit/audit.rules file. -w /etc/security/opasswd -p wa -k identity # Execute the following command to restart auditd # pkill -P 1-HUP auditd
	5.2.3 Enable Auditing For Processes That Start Prior To Auditd	Passed	**Passed: String presence state for */etc/grub.conf* is compliant** **POLICY SETTINGS** File: **/etc/grub.conf** Expected match: **Contains** kernel.*audit\s*=\s*1 Actual match: **true** **REMEDIATION SUGGESTION** # ed /etc/grub.conf Perform the following to determine if /etc/grub.conf is configured to log processes that start prior to auditd. # grep "kernel" /etc/grub.conf Make sure each line that starts with kernel has the audit=1 parameter set.
	5.2.2 Enable Auditd Service	Passed	**Passed: process presence state for *auditd* is compliant** **POLICY SETTINGS** Process: **auditd** Expected presence: **true** Actual presence: **true** **REMEDIATION SUGGESTION** # chkconfig auditd on Perform the following to determine if auditd is enabled. # chkconfig --list auditd auditd: 0: off 1: off 2: on 3: on 4: on 5: on 6: off
	5.2.1.3 Keep All Auditing Information	Passed	**Passed : Value for *max_log_file_action* setting in */etc/audit/auditd.conf* is compliant** **POLICY SETTINGS**

Critical	Rule Violated	Status	Information	Remediation Suggestion

			Configuration file: **/etc/audit/auditd.conf**
			Configuration item: **max_log_file_action**
			Expected value: **keep_logs**
			Actual value: **keep_logs**
			
			REMEDIATION SUGGESTION
			
			Add the following line to the /etc/audit/auditd.conf file.
			
			max_log_file_action = keep_logs
			
			Perform the following to determine if audit logs are retained.
			
			# grep max_log_file_action /etc/audit/auditd.conf
			max_log_file_action = keep_logs	

Yes	5.2.1.1 Configure Audit Log Storage Size	Passed	**Passed: String presence state for */etc/audit/auditd.conf* is compliant**
			POLICY SETTINGS
			
			File: **/etc/audit/auditd.conf**
			Expected match: **Contains** ^max_log_file\s+=
			Actual match: **true**
			
			REMEDIATION SUGGESTION
			
			Set the max_log_file parameter in /etc/audit/auditd.conf
			
			max_log_file = <MB>
			
			NOTE: MB is the number of MegaBytes the file can be.
			
			Perform the following to determine the maximum size of the audit log files.
			
			# grep max_log_file /etc/audit/auditd.conf
			max_log_file = <MB>	

	5.1.5 Configure Rsyslog To Send Logs To A Remote Log Host	Passed	**Passed: String presence state for */etc/rsyslog.conf* is compliant** **POLICY SETTINGS** File: **/etc/rsyslog.conf** Expected match: **Contains** ^*\.*\s+@@\S+ Actual match: **true** **REMEDIATION SUGGESTION** Edit the /etc/rsyslog.conf file and add the following line (where _logfile.example.com_ is the name of your central log hos *.* @@loghost.example.com # Execute the following command to restart rsyslogd # pkill -HUP rsyslogd NOTE: The double "at" sign (@@) directs rsyslog to use TCP to send log messages to the server, which is a more reli Review the /etc/rsyslog.conf file and verify that logs are sent to a central host (where _logfile.example.com_ is the name # grep "^*.*[^|][^|]*@" /etc/rsyslog.conf *.* @@loghost.example.com	
	5.1.2 Activate The Rsyslog Service	Passed	**Passed: process presence state for *rsyslogd* is compliant** **POLICY SETTINGS** Process: **rsyslogd** Expected presence: **true** Actual presence: **true** **REMEDIATION SUGGESTION** # chkconfig syslog off # chkconfig rsyslog on # chkconfig --list syslog syslog 0:off 1:off 2:off 3:off 4:off 5:off 6:off # chkconfig --list rsyslog rsyslog 0:off 1:off 2:on 3:on 4:on 5:on 6:off **Passed: process presence state for *syslogd* is compliant** **POLICY SETTINGS** Process: **syslogd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION**	

Critical	Rule Violated	Status	Remediation Suggestion
			# chkconfig rsyslog on # chconfig syslog off
	5.1.1 Install The Rsyslog Package	Passed	**Passed : package presence state for package *rsyslog* is compliant** **POLICY SETTINGS** Package: **rsyslog** Expected presence: **true** Actual presence: **true** **REMEDIATION SUGGESTION** # yum install rsyslog Perform the following command to verify that rsyslog is installed. # rpm -q rsyslog rsyslog..
	4.5.5 Verify Permissions On /Etc/Hosts.Deny	Passed	**Passed: ACL *644* for file */etc/hosts.deny* is compliant** **POLICY SETTINGS** File: **/etc/hosts.deny** Expected ACL: **644** Actual ACL: **644** **REMEDIATION SUGGESTION** If the permissions of the /etc/hosts.deny file are incorrect, run the following command to correct them: # /bin/chmod 644 /etc/hosts.deny Run the following command to determine the permissions on the /etc/hosts.deny file. # /bin/ls -l /etc/hosts.deny -rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/hosts.deny
	4.5.3 Verify Permissions On /Etc/Hosts.Allow	Passed	**Passed: ACL *644* for file */etc/hosts.allow* is compliant** **POLICY SETTINGS** File: **/etc/hosts.allow** Expected ACL: **644** Actual ACL: **644** **REMEDIATION SUGGESTION** If the permissions of the /etc/hosts.allow file are incorrect, run the following command to correct them: # /bin/chmod 644 /etc/hosts.allow Run the following command to determine the permissions on the /etc/hosts.allow file. # /bin/ls -l /etc/hosts.allow -rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/hosts.allow
	4.5.2 Create /Etc/Hosts.Allow	Passed	**Passed: File presence state for */etc/hosts.allow* is compliant** **POLICY SETTINGS** File: **/etc/hosts.allow** Expected presence: **true** Actual presence: **true** **REMEDIATION SUGGESTION** Create /etc/hosts.allow: # echo "ALL: <net>/<mask>, <net>/<mask>, " >/etc/hosts.allow where each <net>/<mask> combination (for example, "192.168.1.0/255.255.255.0") represents one network block in us Run the following command to verify the contents of the /etc/hosts.allow file. # cat /etc/hosts.allow [contents will vary, depending on your network configuration]
	4.2.8 Enable Tcp Syn Cookies	Passed	**Passed : Value for *net.ipv4.tcp_syncookies* setting in */etc/sysctl.conf* is compliant** **POLICY SETTINGS** Configuration file: **/etc/sysctl.conf** Configuration item: **net.ipv4.tcp_syncookies** Expected value: **1** Actual value: **1**

Critical	Rule Violated	Status	Remediation Suggestion
			REMEDIATION SUGGESTION Set the net.ipv4.tcp_syncookies parameter to 1 in /etc/sysctl.conf: net.ipv4.tcp_syncookies=1 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.tcp_syncookies=1 # /sbin/sysctl -w net.ipv4.route.flush=1 Perform the following to determine if TCP SYN Cookies is enabled. # /sbin/sysctl net.ipv4.tcp_syncookies net.ipv4.tcp_syncookies = 1
	4.2.7 Enable Rfc Recommended Source Route Validation	Passed	**Passed : Value for setting in *<u>/proc/sys/net/ipv4/conf/all/rp_filter</u>* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv4/conf/all/rp_filter** Configuration item: Expected value: **1** Actual value: **1** **REMEDIATION SUGGESTION** Set the net.ipv4.conf.all.rp_filter and net.ipv4.conf.default.rp_filter parameters to 1 in /etc/sysctl.conf: net.ipv4.conf.all.rp_filter=1 net.ipv4.conf.default.rp_filter=1 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.conf.all.rp_filter=1 # /sbin/sysctl -w net.ipv4.conf.default.rp_filter=1 # /sbin/sysctl -w net.ipv4.route.flush=1 Perform the following to determine if RFC-recommended source route validation is enabled. # /sbin/sysctl net.ipv4.conf.all.rp_filter net.ipv4.conf.all.rp_filter = 1 # /sbin/sysctl net.ipv4.conf.default.rp_filter net.ipv4.conf.default.rp_filter = 1 **Passed : Value for setting in *<u>/proc/sys/net/ipv4/conf/default/rp_filter</u>* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv4/conf/default/rp_filter** Configuration item: Expected value: **1** Actual value: **1** **REMEDIATION SUGGESTION** Set the net.ipv4.conf.all.rp_filter and net.ipv4.conf.default.rp_filter parameters to 1 in /etc/sysctl.conf: net.ipv4.conf.all.rp_filter=1 net.ipv4.conf.default.rp_filter=1 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.conf.all.rp_filter=1 # /sbin/sysctl -w net.ipv4.conf.default.rp_filter=1 # /sbin/sysctl -w net.ipv4.route.flush=1
	4.2.6 Enable Bad Error Message Protection	Passed	**Passed : Value for setting in *<u>/proc/sys/net/ipv4/icmp_ignore_bogus_error_responses</u>* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv4/icmp_ignore_bogus_error_responses** Configuration item: Expected value: **1** Actual value: **1** **REMEDIATION SUGGESTION** Set the net.ipv4.icmp_ignore_bogus_error_responses parameter to 1 in /etc/sysctl.conf: net.ipv4.icmp_ignore_bogus_error_responses=1 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1 # /sbin/sysctl -w net.ipv4.route.flush=1 Perform the following to determine if bogus messages will be ignored.

Critical	Rule Violated	Status	Remediation Suggestion
			# /sbin/sysctl net.ipv4.icmp_ignore_bogus_error_responses net.ipv4.icmp_ignore_bogus_error_responses = 1
	4.2.5 Enable Ignore Broadcast Requests	Passed	**Passed : Value for setting in *<u>/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts</u>* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts** Configuration item: Expected value: **1** Actual value: **1** **REMEDIATION SUGGESTION** Set the net.ipv4.icmp_echo_ignore_broadcasts parameter to 1 in /etc/sysctl.conf: net.ipv4.icmp_echo_ignore_broadcasts=1 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1 # /sbin/sysctl -w net.ipv4.route.flush=1 Perform the following to determine if all ICMP echo and timestamp requests to broadcast and multicast addresses will b # /sbin/sysctl net.ipv4.icmp_echo_ignore_broadcasts net.ipv4.icmp_echo_ignore_broadcasts = 1
	4.2.4 Log Suspicious Packets	Passed	**Passed : Value for setting in *<u>/proc/sys/net/ipv4/conf/all/log_martians</u>* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv4/conf/all/log_martians** Configuration item: Expected value: **1** Actual value: **1** **REMEDIATION SUGGESTION** Set the net.ipv4.conf.all.log_martians and net.ipv4.conf.default.log_martians parameters to 1 in /etc/sysctl.conf: net.ipv4.conf.all.log_martians=1 net.ipv4.conf.default.log_martians=1 net.ipv4.route.flush=1 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.conf.all.log_martians=1 # /sbin/sysctl -w net.ipv4.conf.default.log_martians=1 # /sbin/sysctl -w net.ipv4.route.flush=1 Perform the following to determine if suspicious packets are logged. # /sbin/sysctl net.ipv4.conf.all.log_martians net.ipv4.conf.all.log_martians = 1 # /sbin/sysctl net.ipv4.conf.default.log_martians net.ipv4.conf.default.log_martians = 1 **Passed : Value for setting in *<u>/proc/sys/net/ipv4/conf/default/log_martians</u>* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv4/conf/default/log_martians** Configuration item: Expected value: **1** Actual value: **1** **REMEDIATION SUGGESTION** Set the net.ipv4.conf.all.log_martians and net.ipv4.conf.default.log_martians parameters to 1 in /etc/sysctl.conf: net.ipv4.conf.all.log_martians=1 net.ipv4.conf.default.log_martians=1 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.conf.all.log_martians=1 # /sbin/sysctl -w net.ipv4.conf.default.log_martians=1 # /sbin/sysctl -w net.ipv4.route.flush=1
	4.2.3 Disable Secure Icmp Redirect Acceptance	Passed	**Passed : Value for setting in *<u>/proc/sys/net/ipv4/conf/all/secure_redirects</u>* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv4/conf/all/secure_redirects** Configuration item: Expected value: **0** Actual value: **0** **REMEDIATION SUGGESTION**

Critical	Rule Violated	Status	Remediation Suggestion
			Set the net.ipv4.conf.all.secure_redirects and net.ipv4.conf.default.secure_redirects parameters to 0 in /etc/sysctl.conf: net.ipv4.conf.all.secure_redirects=0 net.ipv4.conf.default.secure_redirects=0 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.conf.all.secure_redirects=0 # /sbin/sysctl -w net.ipv4.conf.default.secure_redirects=0 # /sbin/sysctl -w net.ipv4.route.flush=1 Perform the following to determine if ICMP redirect messages will be rejected from known gateways. # /sbin/sysctl net.ipv4.conf.all.secure_redirects net.ipv4.conf.all.secure_redirects = 0 # /sbin/sysctl net.ipv4.conf.default.secure_redirects net.ipv4.conf.default.secure_redirects = 0 **Passed : Value for setting in */proc/sys/net/ipv4/conf/default/secure_redirects* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv4/conf/default/secure_redirects** Configuration item: Expected value: **0** Actual value: **0** **REMEDIATION SUGGESTION** Set the net.ipv4.conf.all.secure_redirects and net.ipv4.conf.default.secure_redirects parameters to 0 in /etc/sysctl.conf: net.ipv4.conf.all.secure_redirects=0 net.ipv4.conf.default.secure_redirects=0 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.conf.all.secure_redirects=0 # /sbin/sysctl -w net.ipv4.conf.default.secure_redirects=0 # /sbin/sysctl -w net.ipv4.route.flush=1
4.2.2 Disable Icmp Redirect Acceptance		Passed	**Passed : Value for setting in */proc/sys/net/ipv4/conf/all/accept_redirects* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv4/conf/all/accept_redirects** Configuration item: Expected value: **0** Actual value: **0** **REMEDIATION SUGGESTION** Set the net.ipv4.conf.all.accept_redirects and net.ipv4.conf.default.accept_redirects parameters to 0 in /etc/sysctl.conf: net.ipv4.conf.all.accept_redirects=0 net.ipv4.conf.default.accept_redirects=0 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.conf.all.accept_redirects=0 # /sbin/sysctl -w net.ipv4.conf.default.accept_redirects=0 # /sbin/sysctl -w net.ipv4.route.flush=1 Perform the following to determine if ICMP redirect messages will be rejected. # /sbin/sysctl net.ipv4.conf.all.accept_redirects net.ipv4.conf.all.accept_redirects = 0 # /sbin/sysctl net.ipv4.conf.default.accept_redirects net.ipv4.conf.default.accept_redirects = 0 **Passed : Value for setting in */proc/sys/net/ipv4/conf/default/accept_redirects* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv4/conf/default/accept_redirects** Configuration item: Expected value: **0** Actual value: **0** **REMEDIATION SUGGESTION** Set the net.ipv4.conf.all.accept_redirects and net.ipv4.conf.default.accept_redirects parameters to 0 in /etc/sysctl.conf: net.ipv4.conf.all.accept_redirects=0 net.ipv4.conf.default.accept_redirects=0 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.conf.all.accept_redirects=0 # /sbin/sysctl -w net.ipv4.conf.default.accept_redirects=0

Critical	Rule Violated	Status	Remediation Suggestion
	4.2.1 Disable Source Routed Packet Acceptance	Passed	# /sbin/sysctl -w net.ipv4.route.flush=1 **Passed : Value for setting in *<u>/proc/sys/net/ipv4/conf/all/accept_source_route</u>* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv4/conf/all/accept_source_route** Configuration item: Expected value: **0** Actual value: **0** **REMEDIATION SUGGESTION** Set the net.ipv4.conf.all.accept_source_route and net.ipv4.conf.default.accept_source_route parameters to 0 in /etc/sys net.ipv4.conf.all.accept_source_route=0 net.ipv4.conf.default.accept_source_route=0 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.conf.all.accept_source_route=0 # /sbin/sysctl -w net.ipv4.conf.default.accept_source_route=0 # /sbin/sysctl -w net.ipv4.route.flush=1 Perform the following to determine if accepting source routed packets is disabled. # /sbin/sysctl net.ipv4.conf.all.accept_source_route net.ipv4.conf.all.accept_source_route = 0 # /sbin/sysctl net.ipv4.conf.default.accept_source_route net.ipv4.conf.default.accept_source_route = 0 **Passed : Value for setting in *<u>/proc/sys/net/ipv4/conf/default/accept_source_route</u>* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv4/conf/default/accept_source_route** Configuration item: Expected value: **0** Actual value: **0** **REMEDIATION SUGGESTION** Set the net.ipv4.conf.all.accept_source_route and net.ipv4.conf.default.accept_source_route parameters to 0 in /etc/sysctl.conf: net.ipv4.conf.all.accept_source_route=0 net.ipv4. conf.default.accept_source_route=0 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.conf.all.accept_source_route=0 # /sbin/sysctl -w net.ipv4.conf.default.accept_source_route=0 # /sbin/sysctl -w net.ipv4.route.flush=1
	4.1.2 Disable Send Packet Redirects	Passed	**Passed : Value for setting in *<u>/proc/sys/net/ipv4/conf/all/send_redirects</u>* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv4/conf/all/send_redirects** Configuration item: Expected value: **0** Actual value: **0** **REMEDIATION SUGGESTION** Set the net.ipv4.conf.all.send_redirects and net.ipv4.conf.default.send_redirects parameters to 0 in /etc/sysctl.conf: net.ipv4.conf.all.send_redirects=0 net.ipv4.conf.default.send_redirects=0 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.conf.all.send_redirects=0 # /sbin/sysctl -w net.ipv4.conf.default.send_redirects=0 # /sbin/sysctl -w net.ipv4.route.flush=1 Perform the following to determine if send packet redirects is disabled. # /sbin/sysctl net.ipv4.conf.all.send_redirects net.ipv4.conf.all.send_redirects = 0 # /sbin/sysctl net.ipv4.conf.default.send_redirects net.ipv4.conf.default.send_redirects = 0 **Passed : Value for setting in *<u>/proc/sys/net/ipv4/conf/default/send_redirects</u>* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/net/ipv4/conf/default/send_redirects** Configuration item: Expected value: **0** Actual value: **0**

Critical	Rule Violated	Status	REMEDIATION SUGGESTION	Remediation Suggestion
			Set the net.ipv4.conf.all.send_redirects and net.ipv4.conf.default.send_redirects parameters to 0 in /etc/sysctl.conf: net.ipv4.conf.all.send_redirects=0 net.ipv4.conf.default.send_redirects=0 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.conf.all.send_redirects=0 # /sbin/sysctl -w net.ipv4.default.all.send_redirects=0 # /sbin/sysctl -w net.ipv4.route.flush=1	
	4.1.1 Disable Ip Forwarding	Passed	**Passed : Value for *net.ipv4.ip_forward* setting in */etc/sysctl.conf* is compliant** **POLICY SETTINGS** Configuration file: **/etc/sysctl.conf** Configuration item: **net.ipv4.ip_forward** Expected value: **0** Actual value: **0** **REMEDIATION SUGGESTION** Set the net.ipv4.ip_forward parameter to 0 in /etc/sysctl.conf: net.ipv4.ip_forward=0 Modify active kernel parameters to match: # /sbin/sysctl -w net.ipv4.ip_forward=0 # /sbin/sysctl -w net.ipv4.route.flush=1 Perform the following to determine if net.ipv4.ip_forward is enabled on the system. # /sbin/sysctl net.ipv4.ip_forward net.ipv4.ip_forward = 0	
	3.15 Remove Snmp Server	Passed	**Passed : package presence state for package *net-snmp* is compliant** **POLICY SETTINGS** Package: **net-snmp** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase net-snmp Perform the following to determine if net-snmp is installed on the system. # rpm -q net-snmp package net-snmp is not installed	
	3.14 Remove Http Proxy Server	Passed	**Passed : package presence state for package *squid* is compliant** **POLICY SETTINGS** Package: **squid** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase squid Perform the following to determine if squid is installed on the system. # rpm -q squid package squid is not installed	
	3.13 Remove Samba	Passed	**Passed : package presence state for package *samba* is compliant** **POLICY SETTINGS** Package: **samba** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase samba Perform the following to determine if samba is installed on the system. # rpm -q samba package samba is not installed	

Critical	Rule Violated	Status	Remediation Suggestion
	3.12 Remove Dovecot (Imap And Pop3 Services)	Passed	**Passed : package presence state for package *dovecot* is compliant** **POLICY SETTINGS** Package: **dovecot** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase dovecot Perform the following to determine if dovecot is installed on the system. # rpm -q dovecot package dovecot is not installed
	3.9 Remove Dns Server	Passed	**Passed : package presence state for package *bind* is compliant** **POLICY SETTINGS** Package: **bind** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase bind Perform the following to determine if DNS is disabled on the system. # rpm -q bind package bind is not installed
	3.8 Disable Nfs And Rpc	Passed	**Passed: process presence state for *nfslock* is compliant** **POLICY SETTINGS** Process: **nfslock** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # chkconfig nfslock off # chkconfig rpcgssd off # chkconfig rpcbind off # chkconfig rpcidmapd off # chkconfig rpcsvcgssd off Perform the following to determine if NFS is disabled. # chkconfig --list nfslock nfslock: 0:off 1:off 2:off 3:off 4:off 5:off 6:off # chkconfig --list rpcgssd rpcgssd: 0:off 1:off 2:off 3:off 4:off 5:off 6:off # chkconfig --list rpcbind rpcbind: 0:off 1:off 2:off 3:off 4:off 5:off 6:off # chkconfig --list rpcidmapd rpcidmapd: 0:off 1:off 2:off 3:off 4:off 5:off 6:off # chkconfig --list rpcsvcgssd rpcsvcgssd: 0:off 1:off 2:off 3:off 4:off 5:off 6:off **Passed: process presence state for *rpcgssd* is compliant** **POLICY SETTINGS** Process: **rpcgssd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # chkconfig rpcgssd off **Passed: process presence state for *rpcbind* is compliant** **POLICY SETTINGS** Process: **rpcbind** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # chkconfig rpcbind off

Critical	Rule Violated	Status	Passed: process presence state for *rpcidmapd* is compliant **POLICY SETTINGS**	Remediation Suggestion
			Process: **rpcidmapd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # chkconfig rpcidmapd off	
			Passed: process presence state for *rpcsvcgssd* is compliant **POLICY SETTINGS** Process: **rpcsvcgssd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # chkconfig rpcsvcgssd off	
	3.7 Remove Ldap	Passed	**Passed : package presence state for package *openldap-servers* is compliant** **POLICY SETTINGS** Package: **openldap-servers** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** If LDAP is running on the system and is not needed, remove it as follows: # yum erase openldap-servers # yum erase openldap-clients Perform the following to determine if LDAP is running. # rpm -q openldap-servers package openldap-servers is not installed # rpm -q openldap-clients package openldap-clients is not installed	
			Passed : package presence state for package *openldap-clients* is compliant **POLICY SETTINGS** Package: **openldap-clients** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** If LDAP is running on the system and is not needed, remove it as follows: # yum erase openldap-servers # yum erase openldap-clients	
	3.6 Configure Network Time Protocol (Ntp)	Passed	**Passed: String presence state for */etc/ntp.conf* is compliant** **POLICY SETTINGS** File: **/etc/ntp.conf** Expected match: **Contains** ^restrict\s*default Actual match: **true** **REMEDIATION SUGGESTION** NTP is configured by default in RHEL6. If for some reason, it is not configured on your system, set the following restrict restrict default kod nomodify notrap nopeer noquery restrict -6 default kod nomodify notrap nopeer noquery Also, make sure /etc/ntp.conf has an NTP server specified: server <ntp-server> NOTE: <ntp-server> is the IP address or hostname of a trusted time server. Configuring an NTP server is outside the s The following script checks for the correct parameters on restrict default and restrict -6 default: # grep "restrict default" /etc/ntp.conf restrict default kod nomodify notrap nopeer noquery # grep "restrict -6 default" /etc/ntp.conf restrict -6 default kod nomodify notrap nopeer noquery	

Critical	Rule Violated	Status	Remediation Suggestion

			Perform the following to determine if the system is configured to use an NTP Server and that the ntp daemon is running
			# grep "^server" /etc/ntp.conf
			server
			# grep "ntp:ntp" /etc/sysconfig/ntpd
			OPTIONS="-u ntp:ntp -p /var/run/ntpd.pid"
			Passed: String presence state for */etc/ntp.conf* is compliant
			POLICY SETTINGS
			File: **/etc/ntp.conf**
			Expected match: **Contains** ^restrict\s*\-6\s*default
			Actual match: **true**
			REMEDIATION SUGGESTION
			NTP is configured by default in CentOS 6. If for some reason, it is not configured on your system, set the following restri
			restrict default kod nomodify notrap nopeer noquery
			restrict -6 default kod nomodify notrap nopeer noquery
			Passed: String presence state for */etc/ntp.conf* is compliant
			POLICY SETTINGS
			File: **/etc/ntp.conf**
			Expected match: **Contains** ^server
			Actual match: **true**
			REMEDIATION SUGGESTION
			Also, make sure /etc/ntp.conf has an NTP server specified:
			server <ntp-server>
			Note: <ntp-server> is the IP address or hostname of a trusted time server. Configuring an NTP server is outside the sc

	3.5 Remove Dhcp Server	Passed	**Passed : package presence state for package *dhcp* is compliant** **POLICY SETTINGS** Package: **dhcp** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase dhcp Perform the following to determine if DHCP is disabled. # rpm -q dhcp package dhcp is not installed
	3.4 Disable Print Server Cups	Passed	**Passed: process presence state for *cupsd* is compliant** **POLICY SETTINGS** Process: **cupsd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # chkconfig cups off Perform the following to determine if CUPS is disabled. # chkconfig --list cups chkconfig: 0:off 1:off 2:off 3:off 4:off 5:off 6:off
	3.3 Disable Avahi Server	Passed	**Passed: process presence state for *avahi-daemon* is compliant** **POLICY SETTINGS** Process: **avahi-daemon** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # chkconfig avahi-daemon off In addition, edit the /etc/sysconfig/network file and remove zeroconf. Perform the following to determine if Avahi is disabled. # chkconfig --list avahi-daemon

Critical	Rule Violated	Status	Remediation Suggestion
			avahi-daemon: 0:off 1:off 2:off 3:off 4:off 5:off 6:off
	3.2 Remove The X Window System	Passed	**Passed : package presence state for package *xorg-x11-server-common* is compliant** **POLICY SETTINGS** Package: **xorg-x11-server-common** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** Edit the /etc/inittab file to set the default runlevel as follows: id:3:initdefault Uninstall the X Window Server: # yum remove xorg-x11-server-common Perform the following to determine if the X Window server is installed on the system: # grep "^id:" /etc/inittab id:3:initdefault # rpm -q xorg-x11-server-common
	3.10 Remove Ftp Server	Passed	**Passed : package presence state for package *vsftpd* is compliant** **POLICY SETTINGS** Package: **vsftpd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase vsftpd Perform the following to determine if FTP is disabled. # rpm -q vsftpd package vsftpd is not installed
	3.1 Set Daemon Umask	Passed	**Passed : Value for *umask* setting in */etc/sysconfig/init* is compliant** **POLICY SETTINGS** Configuration file: **/etc/sysconfig/init** Configuration item: **umask** Expected value: **027** Actual value: **027** **REMEDIATION SUGGESTION** Add the following line to the /etc/sysconfig/init file. umask 027 Perform the following to determine if the daemon umask is set. # grep umask /etc/sysconfig/init umask 027
	2.1.18 Disable Tcpmux Server	Passed	**Passed : package presence state for package *xinetd* is compliant** **POLICY SETTINGS** Package: **xinetd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** Disable the tcpmux-server service by running the following command: # chkconfig tcpmux-server off # chkconfig --list tcpmux-server tcpmux-server: off **Indeterminate: presence */etc/xinetd.d/tcpmux-server* could not be found** **POLICY SETTINGS** File: **/etc/xinetd.d/tcpmux-server** Expected match: **Contains** disable\s*=\s*yes Actual match: **false** **REMEDIATION SUGGESTION**

Critical	Rule Violated	Status	Remediation Suggestion
			REMEDIATION SUGGESTION No remediation suggestion is available for this check.
	2.1.17 Disable Echo Stream	Passed	**Passed : package presence state for package *xinetd* is compliant** **POLICY SETTINGS** Package: **xinetd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** Disable the echo-stream service by running the following command: # chkconfig echo-stream off # chkconfig --list echo-stream echo-stream: off **Indeterminate: presence */etc/xinetd.d/echo-stream* could not be found** **POLICY SETTINGS** File: **/etc/xinetd.d/echo-stream** Expected match: **Contains** disable\s*=\s*yes Actual match: **false** **REMEDIATION SUGGESTION** No remediation suggestion is available for this check.
	2.1.16 Disable Echo Dgram	Passed	**Passed : package presence state for package *xinetd* is compliant** **POLICY SETTINGS** Package: **xinetd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** Disable the echo-dgram service by running the following command: # chkconfig echo-dgram off # chkconfig --list echo-dgram echo-dgram: off **Indeterminate: presence */etc/xinetd.d/echo-dgram* could not be found** **POLICY SETTINGS** File: **/etc/xinetd.d/echo-dgram** Expected match: **Contains** disable\s*=\s*yes Actual match: **false** **REMEDIATION SUGGESTION** No remediation suggestion is available for this check.
	2.1.15 Disable Daytime Stream	Passed	**Passed : package presence state for package *xinetd* is compliant** **POLICY SETTINGS** Package: **xinetd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** Disable the daytime-stream service by running the following command: # chkconfig daytime-stream off # chkconfig --list daytime-stream daytime-stream: off **Indeterminate: presence */etc/xinetd.d/daytime-stream* could not be found** **POLICY SETTINGS** File: **/etc/xinetd.d/daytime-stream** Expected match: **Contains** disable\s*=\s*yes Actual match: **false** **REMEDIATION SUGGESTION** No remediation suggestion is available for this check.

Critical	Rule Violated	Status	Remediation Suggestion
	2.1.14 Disable Daytime Dgram	Passed	**Passed : package presence state for package *xinetd* is compliant** **POLICY SETTINGS** Package: **xinetd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** Disable the daytime-dgram service by running the following command: # chkconfig daytime-dgram off # chkconfig --list daytime-dgram daytime-dgram: off **Indeterminate: presence */etc/xinetd.d/daytime-dgram* could not be found** **POLICY SETTINGS** File: **/etc/xinetd.d/daytime-dgram** Expected match: **Contains** disable\s*=\s*yes Actual match: **false** **REMEDIATION SUGGESTION** No remediation suggestion is available for this check.
	2.1.13 Disable Chargen Stream	Passed	**Passed : package presence state for package *xinetd* is compliant** **POLICY SETTINGS** Package: **xinetd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** Disable the chargen-stream service by running the following command: # chkconfig chargen-stream off # chkconfig --list chargen-stream chargen-stream: off **Indeterminate: presence */etc/xinetd.d/chargen-stream* could not be found** **POLICY SETTINGS** File: **/etc/xinetd.d/chargen-stream** Expected match: **Contains** disable\s*=\s*yes Actual match: **false** **REMEDIATION SUGGESTION** No remediation suggestion is available for this check.
	2.1.12 Disable Chargen Dgram	Passed	**Passed : package presence state for package *xinetd* is compliant** **POLICY SETTINGS** Package: **xinetd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** Disable the chargen-dgram service by running the following command: # chkconfig chargen-dgram off # chkconfig --list chargen-dgram chargen-dgram: off **Indeterminate: presence */etc/xinetd.d/chargen-dgram* could not be found** **POLICY SETTINGS** File: **/etc/xinetd.d/chargen-dgram** Expected match: **Contains** disable\s*=\s*yes Actual match: **false** **REMEDIATION SUGGESTION** No remediation suggestion is available for this check.

Critical	Rule Violated	Status	Remediation Suggestion
	2.1.11 Remove Xinetd	Passed	**Passed : package presence state for package *xinetd* is compliant** **POLICY SETTINGS** Package: **xinetd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase xinetd Perform the following to determine if xinetd is installed on the system. # rpm -q xinetd package xinetd is not installed
	2.1.10 Remove Talk Server	Passed	**Passed : package presence state for package *talk-server* is compliant** **POLICY SETTINGS** Package: **talk-server** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase talk-server Perform the following to determine if talk-server is installed on the system: # rpm -q talk-server package talk-server is not installed
	2.1.9 Remove Talk	Passed	**Passed : package presence state for package *talk* is compliant** **POLICY SETTINGS** Package: **talk** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase talk Perform the following to determine if talk is installed on the system. # rpm -q talk package talk is not installed
	2.1.8 Remove Tftp Server	Passed	**Passed : package presence state for package *tftp-server* is compliant** **POLICY SETTINGS** Package: **tftp-server** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase tftp-server Perform the following to determine if tftp-server is installed on the system. # rpm -q tftp-server package tftp-server is not installed
	2.1.7 Remove Tftp	Passed	**Passed : package presence state for package *tftp* is compliant** **POLICY SETTINGS** Package: **tftp** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase tftp Perform the following to determine if tftp is installed on the system. # rpm -q tftp package tftp is not installed
	2.1.6 Remove Nis Server	Passed	**Passed : package presence state for package *ypserv* is compliant** **POLICY SETTINGS**

Critical	Rule Violated	Status	Remediation Suggestion
			Package: **ypserv** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase ypserv Perform the following to determine if ypserv is installed on the system. # rpm -q ypserv package ypserv is not installed
	2.1.5 Remove Nis Client	Passed	**Passed : package presence state for package *ypbind* is compliant** **POLICY SETTINGS** Package: **ypbind** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase ypbind Perform the following to determine if ypbind is installed on the system. # rpm -q ypbind package ypbind is not installed
	2.1.4 Remove Rsh	Passed	**Passed : package presence state for package *rsh* is compliant** **POLICY SETTINGS** Package: **rsh** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase rsh Perform the following to determine if rsh is installed on the system. # rpm -q rsh package rsh is not installed
	2.1.3 Remove Rsh Server	Passed	**Passed : package presence state for package *rsh-server* is compliant** **POLICY SETTINGS** Package: **rsh-server** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase rsh-server Perform the following to determine if rsh-server is installed on the system. # rpm -q rsh-server package rsh-server is not installed
	2.1.2 Remove Telnet Clients	Passed	**Passed : package presence state for package *telnet* is compliant** **POLICY SETTINGS** Package: **telnet** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** # yum erase telnet Perform the following to determine if the telnet package is on the system. # rpm -q telnet package telnet is not installed
	2.1.1 Remove Telnet Server	Passed	**Passed : package presence state for package *telnet-server* is compliant** **POLICY SETTINGS** Package: **telnet-server**

Critical	Rule Violated	Status	Expected presence: **false** Actual presence: **false**	Remediation Suggestion
			REMEDIATION SUGGESTION # yum erase telnet-server Perform the following to determine if the telnet-server package is on the system. # rpm -q telnet-server package telnet-server is not installed	

	1.6.3 Enable Randomized Virtual Memory Region Placement	Passed	**Passed : Value for setting in *proc/sys/kernel/randomize_va_space* is compliant**
			POLICY SETTINGS
			Configuration file: **/proc/sys/kernel/randomize_va_space**
			Configuration item:
			Expected value: **2**
			Actual value: **2**
			
			REMEDIATION SUGGESTION
			Add the following line to the /etc/sysctl.conf file.
			
			kernel.randomize_va_space = 2
			
			Perform the following to determine if virtual memory is randomized.
			
			# sysctl kernel.randomize_va_space
			kernel.randomize_va_space = 2	

	1.6.2 Configure Exec Shield	Passed	**Passed : Value for setting in *proc/sys/kernel/exec-shield* is compliant** **POLICY SETTINGS** Configuration file: **/proc/sys/kernel/exec-shield** Configuration item: Expected value: **1** Actual value: **1** **REMEDIATION SUGGESTION** Add the following line to the /etc/sysctl.conf file. kernel.exec-shield = 1 Perform the following to determine if ExecShield is enabled. # sysctl kernel.exec-shield kernel.exec-shield = 1	

	1.6.1 Restrict Core Dumps	Passed	**Passed: String presence state for *etc/security/limits.conf* is compliant**
			POLICY SETTINGS
			File: **/etc/security/limits.conf**
			Expected match: **Contains** ^*\s*hard\s+core\s+0
			Actual match: **true**
			
			REMEDIATION SUGGESTION
			Add the following line to the /etc/security/limits.conf file.
			
			* hard core 0
			
			Add the following line to the /etc/sysctl.conf file.
			
			fs.suid_dumpable = 0
			
			Perform the following to determine if core dumps are restricted.
			
			# grep "hard core" /etc/security/limits.conf
			* hard core 0
			# sysctl fs.suid_dumpable
			fs.suid_dumpable = 0
			
			Passed : Value for setting in *proc/sys/fs/suid_dumpable* is compliant
			POLICY SETTINGS
			Configuration file: **/proc/sys/fs/suid_dumpable**
			Configuration item:
			Expected value: **0**
			Actual value: **0**
			
			REMEDIATION SUGGESTION	

Critical	Rule Violated	Status	Remediation Suggestion
			Add the following line to the /etc/sysctl.conf file: fs.suid_dumpable = 0

	1.5.5 Disable Interactive Boot	Passed	**Passed : Value for *PROMPT* setting in */etc/sysconfig/init* is compliant**
			POLICY SETTINGS
			Configuration file: **/etc/sysconfig/init**
			Configuration item: **PROMPT**
			Expected value: **no**
			Actual value: **no**
			
			REMEDIATION SUGGESTION
			Set the PROMPT parameter in /etc/sysconfig/init to no.
			
			PROMPT=no
			
			Perform the following to determine if PROMPT is disabled:
			
			# grep "^PROMPT=" /etc/sysconfig/init
			PROMPT=no

	1.5.4 Require Authentication For Single User Mode	Passed	**Passed : Value for *SINGLE* setting in */etc/sysconfig/init* is compliant**
			POLICY SETTINGS
			Configuration file: **/etc/sysconfig/init**
			Configuration item: **SINGLE**
			Expected value: **/sbin/sulogin**
			Actual value: **/sbin/sulogin**
			
			REMEDIATION SUGGESTION
			Run the following to edit /etc/sysconfig/init:
			
			sed -i "/SINGLE/s/sushell/sulogin/" /etc/sysconfig/init
			
			Perform the following to determine if /etc/sysconfig/init is configured correctly:
			
			# grep SINGLE /etc/sysconfig/init
			SINGLE=/sbin/sulogin

	1.5.3 Set Boot Loader Password	Passed	**Passed: String presence state for */etc/grub.conf* is compliant** **POLICY SETTINGS** File: **/etc/grub.conf** Expected match: **Contains** ^password Actual match: **true** **REMEDIATION SUGGESTION** Use grub-md5-crypt to produce an encrypted password: # grub-md5-crypt Password: Retype password: _[Encrypted Password]_ Set the password parameter to_[Encrypted Password]_ in /etc/grub.conf: password --md5 _[Encrypted Password]_ Perform the following to determine if a password is required to set command line boot parameters: # grep "^password" /etc/grub.conf password --md5 _[Encrypted Password]_ NOTE: Requirement is only that a password is set, other encryption options are available.
	1.5.2 Set Permissions On /Etc/Grub.Conf	Passed	**Passed: ACL *600* for file */etc/grub.conf* is compliant** **POLICY SETTINGS** File: **/etc/grub.conf** Expected ACL: ***00** Actual ACL: **600** **REMEDIATION SUGGESTION** # chmod og-rwx /etc/grub.conf Perform the following to determine if the /etc/grub.conf file permissions are correct: # stat -L -c "%a" /etc/grub.conf | egrep ".00" If the above command emits no output then the system is not configured as recommended

Critical	Rule Violated	Status	Remediation Suggestion
			# the above command emits no output then the system is not configured as recommended.
	1.5.1 Set User/Group Owner On /Etc/Grub.Conf	Passed	**Passed: User owner *root* for file */etc/grub.conf* is compliant** **POLICY SETTINGS** File: **/etc/grub.conf** Expected owner: **root** Actual owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/grub.conf Perform the following to determine if the /etc/grub.conf file has the correct ownership: # stat -L -c "%u %g" /etc/grub.conf | egrep "0 0" If the above command emits no output then the system is not configured as recommended. **Passed: Group owner *root* for file */etc/grub.conf* is compliant** **POLICY SETTINGS** File: **/etc/grub.conf** Expected group owner: **root** Actual group owner: **root** **REMEDIATION SUGGESTION** # chown root:root /etc/grub.conf

	1.4.3 Set The Se Linux Policy	Passed	**Passed : Value for *SELINUXTYPE* setting in */etc/selinux/config* is compliant**
			POLICY SETTINGS
			Configuration file: **/etc/selinux/config**
			Configuration item: **SELINUXTYPE**
			Expected value: **targeted**
			Actual value: **targeted**
			REMEDIATION SUGGESTION
			Edit the /etc/selinux/config file to set the SELINUXTYPE parameter:
			SELINUXTYPE=targeted
			NOTE: If your organization requires stricter policies, make sure they are added to the /etc/selinux/config file.
			Perform the following to determine if the targeted policy is selected in the /etc/selinux/config file.
			# grep SELINUXTYPE=targeted /etc/selinux/config
			SELINUXTYPE=targeted
			# /usr/sbin/sestatus
			SELinux status: enabled
			Current mode: enforcing
			Mode from config file: enforcing
			Policy from config file: targeted
			Note: If your organization requires stricter policies, verify that they are selected by using the "grep" command on the /et

	1.4.2 Set The Se Linux State	Passed	**Passed : Value for *SELINUX* setting in */etc/selinux/config* is compliant**
			POLICY SETTINGS
			Configuration file: **/etc/selinux/config**
			Configuration item: **SELINUX**
			Expected value: **enforcing**
			Actual value: **enforcing**
			REMEDIATION SUGGESTION
			Edit the /etc/selinux/config file to set the SELINUX parameter:
			SELINUX=enforcing
			Perform the following to determine if SELinux is enabled at boot time.
			# grep SELINUX=enforcing /etc/selinux/config
			SELINUX=enforcing
			# /usr/sbin/sestatus
			SELinux status: enabled
			Current mode: enforcing
			Mode from config file: enforcing
			Policy from config file: targeted

	1.4.1 Enable Se	Passed	**Passed: String presence state for */etc/grub.conf* is compliant**

Critical	Rule Violated	Status	Remediation Suggestion
	linux In /Etc/Grub.Conf		**POLICY SETTINGS** File: **/etc/grub.conf** Expected match: **Does not contain** selinux\s*=\s*0 Actual match: **false** **REMEDIATION SUGGESTION** Remove all instances of selinux=0 and enforcing=0 from /etc/grub.conf. Perform the following to verify that SELinux is enabled at boot time: # grep selinux=0 /etc/grub.conf [no output produced] # grep enforcing=0 /etc/grub.conf [no output produced]
			Passed: String presence state for */etc/grub.conf* is compliant **POLICY SETTINGS** File: **/etc/grub.conf** Expected match: **Does not contain** enforcing\s*=\s*0 Actual match: **false** **REMEDIATION SUGGESTION** Remove all instances of enforcing=0 from /etc/grub.conf.
	1.2.4 Disable The Rhnsd Daemon	Passed	**Passed: process presence state for *rhnsd* is compliant** **POLICY SETTINGS** Process: **rhnsd** Expected presence: **false** Actual presence: **false** **REMEDIATION SUGGESTION** Disable the rhnsd daemon by running the following command: # chkconfig rhnsd off # chkconfig --list rhnsd rhnsd: 0:off 1:off 2:off 3:off 4:off 5:off 6:off

	1.2.3 Verify That Gpgcheck Is Globally Activated	Passed	**Passed : Value for *gpgcheck* setting in */etc/yum.conf* is compliant**
			POLICY SETTINGS
			Configuration file: **/etc/yum.conf**
			Configuration item: **gpgcheck**
			Expected value: **1**
			Actual value: **1**
			
			REMEDIATION SUGGESTION
			Edit the /etc/yum.conf file and set the gpgcheck to 1 as follows:
			
			gpgcheck=1
			
			Run the following command to verify that gpgcheck is set to 1 in all occurrences of the /etc/yum.conf file:
			
			# grep gpgcheck /etc/yum.conf
			gpgcheck=1

	1.1.16 Add Noexec Option To /Dev/Shm Partition	Passed	**Passed: String presence state for */etc/fstab* is compliant** **POLICY SETTINGS** File: **/etc/fstab** Expected match: **Contains** \/dev\/shm.*noexec Actual match: **true** **REMEDIATION SUGGESTION** Edit the /etc/fstab file and add noexec to the fourth field (mounting options). Look for entries that have mount points that information. # mount -o remount,noexec /dev/shm Run the following commands to determine if the system is in configured as recommended: # grep /dev/shm /etc/fstab | grep noexec # mount | grep /dev/shm | grep noexec If either command emits no output then the system is not configured as recommended.
	1.1.15 Add	Passed	

Critical	Rule Violated	Status	Remediation Suggestion
	1.1.15 Add Nosuid Option To /Dev/Shm Partition	Passed	**Passed: String presence state for *<u>/etc/fstab</u>* is compliant** **POLICY SETTINGS** File: **/etc/fstab** Expected match: **Contains** \/dev\/shm.*nosuid Actual match: **true** **REMEDIATION SUGGESTION** Edit the /etc/fstab file and add nosuid to the fourth field (mounting options). Look for entries that have mount points that information. # mount -o remount,nosuid /dev/shm Run the following commands to determine if the system is in configured as recommended: # grep /dev/shm /etc/fstab | grep nosuid # mount | grep /dev/shm | grep nosuid If either command emits no output then the system is not configured as recommended.
	1.1.14 Add Nodev Option To /Dev/Shm Partition	Passed	**Passed: String presence state for *<u>/etc/fstab</u>* is compliant** **POLICY SETTINGS** File: **/etc/fstab** Expected match: **Contains** \/dev\/shm.*nodev Actual match: **true** **REMEDIATION SUGGESTION** Edit the /etc/fstab file and add nodev to the fourth field (mounting options of entries that have mount points that contain # mount -o remount,nodev /dev/shm Run the following commands to determine if the system is in configured as recommended: # grep /dev/shm /etc/fstab | grep nodev # mount | grep /dev/shm | grep nodev If either command emits no output then the system is not configured as recommended.
	1.1.10 Add Nodev Option To /Home	Passed	**Passed: String presence state for *<u>/etc/fstab</u>* is compliant** **POLICY SETTINGS** File: **/etc/fstab** Expected match: **Contains** \/home.*nodev Actual match: **true** **REMEDIATION SUGGESTION** Edit the /etc/fstab file and add nodev to the fourth field (mounting options). See the fstab(5) manual page for more inforn # mount -o remount,nodev /home Run the following commands to determine if the system is configured as recommended. # grep /home /etc/fstab | grep noexec # mount | grep /home | grep noexec If either command emits no output then the system is not configured as recommended.
	1.1.9 Create Separate Partition For /Home	Passed	**Passed: String presence state for *<u>/etc/fstab</u>* is compliant** **POLICY SETTINGS** File: **/etc/fstab** Expected match: **Contains** \s\/home\s Actual match: **true** **REMEDIATION SUGGESTION** For new installations, check the box to "Review and modify partitioning" and create a separate partition for /home. For systems that were previously installed, use the Logical Volume Manager (LVM) to create partitions. # grep /home /etc/fstab /home ext3
	1.1.8 Create Separate Partition For /Var/Log/Audit	Passed	**Passed: String presence state for *<u>/etc/fstab</u>* is compliant** **POLICY SETTINGS** File: **/etc/fstab** Expected match: **Contains** \/var\/log\/audit\s Actual match: **true**

Critical	Rule Violated	Status	Remediation Suggestion
			REMEDIATION SUGGESTION For new installations, check the box to "Review and modify partitioning" and create a separate partition for /var/log/audit Volume Manager (LVM) to create partitions. # grep /var/log/audit /etc/fstab /var/log/audit ext3
	1.1.7 Create Separate Partition For /Var/Log	Passed	**Passed: String presence state for *<u>/etc/fstab</u>* is compliant** **POLICY SETTINGS** File: **/etc/fstab** Expected match: **Contains** \/var\/log\s Actual match: **true** **REMEDIATION SUGGESTION** For new installations, check the box to "Review and modify partitioning" and create a separate partition for /var/log. For systems that were previously installed, use the Logical Volume Manager (LVM) to create partitions. # grep /var/log /etc/fstab /var/log ext3
	1.1.6 Bind Mount The /Var/Tmp Directory To /Tmp	Passed	**Passed: String presence state for *<u>/etc/fstab</u>* is compliant** **POLICY SETTINGS** File: **/etc/fstab** Expected match: **Contains** ^\/tmp.*\/var\/tmp.*none.*bind\s+0\s+0 Actual match: **true** **REMEDIATION SUGGESTION** # mount --bind /tmp /var/tmp and edit the /etc/fstab file to contain the following line: /tmp /var/tmp none bind 0 0 Perform the following to determine if the system is configured as recommended: # grep -e "^/tmp" /etc/fstab | grep /var/tmp /tmp /var/tmp none none 0 0 # mount | grep -e "^/tmp" | grep /var/tmp /tmp on /var/tmp type none (rw,bind) If the above commands emit no output then the system is not configured as recommended.
	1.1.5 Create Separate Partition For /Var	Passed	**Passed: String presence state for *<u>/etc/fstab</u>* is compliant** **POLICY SETTINGS** File: **/etc/fstab** Expected match: **Contains** \/var\s Actual match: **true** **REMEDIATION SUGGESTION** For new installations, check the box to "Review and modify partitioning" and create a separate partition for /var. For systems that were previously installed, use the Logical Volume Manager (LVM) to create partitions. #grep /var /etc/fstab /var ext3
	1.1.4 Set Noexec Option For /Tmp Partition	Passed	**Passed: String presence state for *<u>/etc/fstab</u>* is compliant** **POLICY SETTINGS** File: **/etc/fstab** Expected match: **Contains** \/tmp.*noexec Actual match: **true** **REMEDIATION SUGGESTION** Edit the /etc/fstab file and add noexec to the fourth field (mounting options). See the fstab(5) manual page for more infor # mount -o remount,noexec /tmp Run the following commands to determine if the system is configured as recommended. # grep /tmp /etc/fstab | grep noexec # mount | grep /tmp | grep noexec If either command emits no output then the system is not configured as recommended.

Critical	Rule Violated	Status	Remediation Suggestion
	1.1.3 Set Nosuid Option For /Tmp Partition	Passed	**Passed: String presence state for *~~/etc/fstab~~* is compliant** **POLICY SETTINGS** File: **/etc/fstab** Expected match: **Contains** \/tmp.*nosuid Actual match: **true** **REMEDIATION SUGGESTION** Edit the /etc/fstab file and add nosuid to the fourth field (mounting options). See the fstab(5) manual page for more infor Run the following commands to determine if the system is configured as recommended. # grep /tmp /etc/fstab | grep nosuid # mount | grep /tmp | grep nosuid If either command emits no output then the system is not configured as recommended.
	1.1.2 Set Nodev Option For /Tmp Partition	Passed	**Passed: String presence state for *~~/etc/fstab~~* is compliant** **POLICY SETTINGS** File: **/etc/fstab** Expected match: **Contains** \/tmp.*nodev Actual match: **true** **REMEDIATION SUGGESTION** Edit the /etc/fstab file and add nodev to the fourth field (mounting options). See the fstab(5) manual page for more inform # mount -o remount,nodev /tmp Run the following commands to determine if the system is configured as recommended. # grep /tmp /etc/fstab | grep nodev # mount | grep /tmp | grep nodev If either command emits no output then the system is not configured as recommended.
	1.1.1 Create Separate Partition For /Tmp	Passed	**Passed: String presence state for *~~/etc/fstab~~* is compliant** **POLICY SETTINGS** File: **/etc/fstab** Expected match: **Contains** \s\/tmp\s Actual match: **true** **REMEDIATION SUGGESTION** For new installations, check the box to "Review and modify partitioning" and create a separate partition for /tmp. For systems that were previously installed, use the Logical Volume Manager (LVM) to create partitions. Verify that there is a /tmp file partition in the /etc/fstab file. # grep "[[:space:]]/tmp[[:space:]]" /etc/fstab

This report was generated at 2016-06-09 21:13:53.