ansible-hardening Documentation:

Release 18.1.0.dev157

OpenStack-Ansible Contributors

Sep 27, 2024

CONTENTS


ansible
hardening

CHAPTER

ONE

WHAT DOES THE ROLE DO?

The ansible-hardening Ansible role uses industry-standard security hardening guides to secure Linux hosts. Although the role is designed to work well in OpenStack environments that are deployed with OpenStack-Ansible, it can be used with almost any Linux system.

It all starts with the Security Technical Implementation Guide (STIG) from the Defense Information Systems Agency (DISA), part of the United States Department of Defense. The guide is released with a public domain license and it is commonly used to secure systems at public and private organizations around the world.

Each configuration from the STIG is analyzed to determine what impact it could have on a live production environment and how to implement it in Ansible. Tasks are added to the role that configure a host to meet the configuration requirement. Each task is documented to explain what was changed, why it was changed, and what deployers need to understand about the change.

Deployers have the option to pick and choose which configurations are applied using Ansible variables and tags. Some tasks allow deployers to provide custom configurations to tighten down or relax certain requirements.

CHAPTER

TWO

OPENSTACK SUMMIT BOSTON 2017 TALK

This talk covers the latest updates from the project and a live demo. Slides from the talk are available for download.

CHAPTER

THREE

DOCUMENTATION

The following documentation applies to the Queens release (currently under active development). Documentation for the latest stable and previous stable releases is found within the *Releases* section below.

3.1 Getting started

The ansible-hardening role can be used along with the OpenStack-Ansible project or as a standalone role that can be used along with other Ansible playbooks. This documentation assumes that the reader has completed the steps within the Ansible installation guide.

3.1.1 Installing the ansible-hardening role

The recommended installation methods for the ansible-hardening role are `ansible-galaxy` (recommended) or `git`.

Using `ansible-galaxy`

The easiest installation method is to use the `ansible-galaxy` command that is provided with your Ansible installation:

```
ansible-galaxy install git+https://github.com/openstack/ansible-hardening
```

The `ansible-galaxy` command will install the role into `/etc/ansible/roles/ansible-hardening` and this makes it easy to use with Ansible playbooks.

Using `git`

Start by cloning the role into a directory of your choice:

```
mkdir -p ~/.ansible/roles/
git clone https://github.com/openstack/ansible-hardening ~/.ansible/roles/
↪ansible-hardening
```

Ansible looks for roles in `~/.ansible/roles` by default.

If the role is cloned into a different directory, that directory must be provided with the `roles_path` option in `ansible.cfg`. The following is an example of a `ansible.cfg` file that uses a custom path for roles:

```
[DEFAULTS]
roles_path = /etc/ansible/roles:/home/myuser/custom/roles
```

With this configuration, Ansible looks for roles in `/etc/ansible/roles` and `~/custom/roles`.

3.1.2 Usage

The ansible-hardening role works well with existing playbooks. The following is an example of a basic playbook that uses the ansible-hardening role:

```
---

- name: Harden all systems
  hosts: all
  become: yes
  vars:
    security_enable_firewalld: no
    security_rhel7_initialize_aide: no
    security_ntp_servers:
      - 1.example.com
      - 2.example.com
  roles:
    - ansible-hardening
```

The variables provided in the `vars` section can enable, disable, or alter configuration for various tasks in the ansible-hardening role. For more details on the available variables, refer to the *Hardening Domains (RHEL 7 STIG)* section.

Note: The role must be run as the root user or as a user with `sudo` access. The example above uses the `become` option, which causes Ansible to use sudo before running tasks. If the role is running as root, this option can be changed to `user: root`.

Warning: It is strongly recommended to run the role in check mode (often called a *dry run*) first before making any modifications. This gives the deployer the opportunity to review all of

the proposed changes before applying the role to the system. Use the `--check` parameter with `ansible-playbook` to use check mode.

3.2 Deviations from the Security Technical Implementation Guide (STIG)

The ansible-hardening role deviates from some of the STIGs requirements when a security control could cause significant issues with production systems. The role classifies each control into an implementation status and provides notes on why a certain control is skipped or altered.

The following provides a brief overview of each implementation status:

Exception
: If a control requires manual intervention outside the host, or if it could cause significant harm to a host, it will be skipped and listed as an exception. All controls in this category are not implemented in Ansible.

Configuration Required
: These controls require some type of initial configuration before they can be applied. Review the notes for each control to determine how to configure each of them.

Implemented
: These controls are fully implemented and they may have configurations which can be adjusted. The notes for each control will identify which configuration options are available.

Opt-In
: The controls in the opt-in list are implemented in Ansible, but are disabled by default. They are often disabled because they could cause harm to a subset of systems. Each control has notes that explains the caveats of the control and how to enable it if needed.

Deployers should review the full list of controls sorted by implementation status.

Note: All of the default configurations are found within `defaults/main.yml`.

3.3 Frequently Asked Questions

3.3.1 Does this role work only with OpenStack environments?

No it works on almost any Linux host!

The ansible-hardening role first began as a component of the OpenStack-Ansible project and it was designed to deploy into an existing OpenStack environment without causing disruptions. However, the role now works well in OpenStack and non-OpenStack environments.

See *Which systems are covered?* below for more details.

3.3.2 Why should this role be applied to a system?

There are three main reasons to apply this role to production Linux systems:

Improve security posture
: The configurations from the STIG add security and rigor around multiple components of a Linux system, including user authentication, service configurations, and package management. All of these configurations add up to an environment that is more difficult for an attacker to penetrate and use for lateral movement.

Meet compliance requirements
: Some deployers may be subject to industry compliance programs, such as PCI-DSS, ISO 27001/27002, or NIST 800-53. Many of these programs require hardening standards to be applied to critical systems, such as OpenStack infrastructure components.

Deployment without disruption
: Security is often at odds with usability. The role provides the greatest security benefit without disrupting production systems. Deployers have the option to opt out or opt in for most configurations depending on how their environments are configured.

3.3.3 Which systems are covered?

The ansible-hardening role provides security hardening for physical servers running the following Linux distributions:

- CentOS 7
- Debian 8 Jessie
- Fedora 27
- openSUSE Leap 42.2 and 42.3
- Red Hat Enterprise Linux 7 *(partial automated test coverage)*
- SUSE Linux Enterprise 12 (*experimental*)
- Ubuntu 16.04 Xenial

The OpenStack gating system tests the role against each of these distributions regularly except for Red Hat Enterprise Linux 7, since it is a non-free Linux distribution. CentOS 7 is very similar to Red Hat Enterprise Linux 7 and the existing test coverage for CentOS is very thorough.

3.3.4 Which systems are not covered?

The containers that run various OpenStack services on physical servers in OpenStack-Ansible deployments are currently out of scope and are not changed by the role.

Virtual machines that are created within the OpenStack environment are also not affected by this role, although this role could be applied within those VMs if a deployer chooses to do so.

3.4 Hardening Domains (RHEL 7 STIG)

The STIG divides its hardening requirements into severity levels, but the security role divides the requirements into system domains to make them easier to review.

The documentation provided here includes a brief overview of each hardening domain and the STIG requirements that go along with each.

3.4.1 accounts - User account security controls

Security controls for user accounts on Linux systems are a crucial barrier to prevent unauthorized access.

Overview

Many of the STIG requirements for user account controls are already included in many Linux distributions or they can be applied without disruptions. However, some requirements can cause problems with user authentication without coordination.

Deployers should consider an authentication solution that uses centralized authentication, such as LDAP, Active Directory, or Kerberos, for the best security posture.

STIG requirements

All of the tasks for these STIG requirements are included in `tasks/rhel7stig/accounts.yml`.

V-71903

- **Summary**: When passwords are changed or new passwords are established, the new password must contain at least one upper-case character.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_uppercase: no
```

V-71905

- **Summary**: When passwords are changed or new passwords are established, the new password must contain at least one lower-case character.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_lowercase: no
```

V-71907

- **Summary**: When passwords are changed or new passwords are assigned, the new password must contain at least one numeric character.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_numeric: no
```

V-71909

- **Summary**: When passwords are changed or new passwords are assigned, the new password must contain at least one special character.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_special: no
```

V-71911

- **Summary**: When passwords are changed a minimum of eight of the total number of characters must be changed.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_characters_changed: no
```

V-71913

- **Summary**: When passwords are changed a minimum of four character classes must be changed.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_character_classes_changed: no
```

V-71915

- **Summary**: When passwords are changed the number of repeating consecutive characters must not be more than three characters.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_limit_repeated_characters: no
```

V-71917

- **Summary**: When passwords are changed the number of repeating characters of the same character class must not be more than four characters.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_limit_repeated_character_classes: no
```

V-71919

- **Summary**: The PAM system service must be configured to store only encrypted representations of passwords.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The PAM configuration file for password storage is checked to ensure that `sha512` is found on the `pam_unix.so` line. If `sha512` is not found, a debug message is printed in the Ansible output.

V-71921

- **Summary**: The shadow file must be configured to store only encrypted representations of passwords.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The default password storage mechanism for Ubuntu 16.04, CentOS 7, openSUSE Leap, SUSE Linux Enterprise 12 and Red Hat Enterprise Linux 7 is `SHA512` and the tasks in the security role ensure that the default is maintained.

Deployers can configure a different password storage mechanism by setting the following Ansible variable:

```
security_password_encrypt_method: SHA512
```

> **Warning:** SHA512 is the default on most modern Linux distributions and it meets the requirement of the STIG. Do not change the value unless a system has a specific need for a different password mechanism.

V-71923

- **Summary**: User and group account administration utilities must be configured to store only encrypted representations of passwords.
- **Severity:** Medium
- **Implementation Status:** Implemented - Red Hat Only

Deployer/Auditor notes

The role ensures that `crypt_style` is set to `sha512` in `/etc/libuser.conf`, which is the default for CentOS 7 and Red Hat Enterprise Linux 7.

Ubuntu, openSUSE and SUSE Linux Enterprise 12 do not use `libuser`, so this change is not applicable.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_libuser_crypt_style_sha512: no
```

V-71925

- **Summary**: Passwords for new users must be restricted to a 24 hours/1 day minimum lifetime.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Although the STIG requires that all passwords have a minimum lifetime set, this can cause issue in some production environments. Therefore, deployers must opt in for this change.

Set the following Ansible variable to an integer (in days) to enable this setting:

```
security_password_min_lifetime_days: 1
```

The STIG requires the minimum lifetime for password to be one day.

V-71927

- **Summary**: Passwords must be restricted to a 24 hours/1 day minimum lifetime.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Setting a minimum password lifetime on interactive user accounts provides security benefits by limiting the frequency of password changes. However, this can cause login problems for users without proper communication and coordination.

Deployers can opt-in for this change by setting the following Ansible variable:

```
security_set_minimum_password_lifetime: yes
```

The tasks will examine each interactive user account and set the minimum password age if the existing setting is not equal to one day.

V-71929

- **Summary**: Passwords for new users must be restricted to a 60-day maximum lifetime.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Although the STIG requires that all passwords have a maximum lifetime set, this can cause authentication disruptions in production environments if users are not aware that their password will expire. Therefore, this change is not applied by default.

Deployers can opt in for this change and provide a maximum lifetime for user passwords (in days) by setting the following Ansible variable:

```
security_password_max_lifetime_days: 60
```

The STIG requires that all passwords expire after 60 days.

V-71931

- **Summary**: Existing passwords must be restricted to a 60-day maximum lifetime.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Although the STIG requires that a maximum password lifetime is set for all interactive user accounts, the security benefits of this configuration are debatable. The draft of NIST Publication 800-63B argues that password rotation may reduce overall security in some situations.

Deployers can opt-in for this change by setting the following Ansible variable:

```
security_set_maximum_password_lifetime: yes
```

The tasks will examine each interactive user account and set the maximum password age if the existing setting is not equal to 60 days.

V-71933

- **Summary**: Passwords must be prohibited from reuse for a minimum of five generations.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Although the STIG requires that five passwords are remembered to prevent re- use, this can cause issues in production environment if the change is not communicated well to users. Therefore, the tasks in the security role do not apply this change by default.

Deployers can opt in for the change and specify a number of passwords to remember by setting the following Ansible variable:

```
security_password_remember_password: 5
```

V-71935

- **Summary**: Passwords must be a minimum of 15 characters in length.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Although the STIG requires that passwords have a minimum length of 15 characters, this change might be disruptive to users on a production system without communicating the change first. Therefore, this change is not applied by default.

Deployers can opt in for the change by setting the following Ansible variable:

```
security_pwquality_require_minimum_password_length: yes
```

V-71941

- **Summary**: The operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that user accounts are disabled when their password expires. This might be disruptive for some users or for automated processes. Therefore, the tasks in the security role do not apply this change by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_disable_account_if_password_expires: yes
```

V-71951

- **Summary**: The delay between logon prompts following a failed console logon attempt must be at least four seconds.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks in the Ansible role set a four second delay between failed login attempts. Deployers can configure a different delay (in seconds) by setting the following Ansible variable:

```
security_shadow_utils_fail_delay: 4
```

V-71995

- **Summary**: The operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files.
- **Severity:** Medium
- **Implementation Status:** Opt-In - Ubuntu And Suse Only

Deployer/Auditor notes

The STIG requires that the umask for all authenticated users is `077`. This ensures that all new files and directories created by a user are accessible only by that user.

Although this change has a significant security benefit, it can cause problems for users who are not expecting the change. The security role will not adjust the umask by default.

Deployers can opt-in for the change by setting the default umask with an Ansible variable:

```
security_shadow_utils_umask: 077
```

Note: Ubuntu, openSUSE Leap and SUSE Linux Enterpsise 12 use `pam_umask` and it uses the default umask provided by the `UMASK` line in `/etc/login.defs`. The default setting on Ubuntu, openSUSE Leap and SUSE Linux Enterprise 12 systems is `022`. This allows the users group and other users on the system to read and execute files, but they cannot write to them.

CentOS and Red Hat Enterprise Linux do not use `pam_umask` and instead set a default umask of `0002` for regular users and `0022` for root. This gives the regular users group full access to newly created files, but other users cannot write to those files.

The tasks for this STIG requirement are not currently applied to CentOS and Red Hat Enterprise Linux systems. See Launchpad Bug #1656003 for more details.

V-72003

- **Summary**: All Group Identifiers (GIDs) referenced in the /etc/passwd file must be defined in the /etc/group file.
- **Severity:** Low
- **Implementation Status:** Implemented

Deployer/Auditor notes

If any users are found with invalid GIDs, those users are printed in the Ansible output. Deployers should review the list and ensure all users are assigned to a valid group that is defined in `/etc/group`.

V-72005

- **Summary**: The root account must be the only account having unrestricted access to the system.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

If an account with UID 0 other than `root` exists on the system, the playbook will fail with an error message that includes the other accounts which have a UID of 0.

Deployers are strongly urged to keep only one account with UID 0, `root`, and to use `sudo` any situations where root access is required.

V-72011

- **Summary**: All local interactive users must have a home directory assigned in the /etc/passwd file.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The usernames of all users without home directories assigned are provided in the Ansible console output. Deployers should use this list of usernames to audit each system to ensure every user has a valid home directory.

V-72013

- **Summary**: All local interactive user accounts, upon creation, must be assigned a home directory.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `CREATE_HOME` variable is set to `yes` by the tasks in the security role. This ensures that home directories are created each time a new user account is created.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_shadow_utils_create_home: no
```

Note: On CentOS 7, Red Hat Enterprise Linux 7 systems, openSUSE Leap and SUSE Linux Enterprise 12, home directories are always created with new users by default. Home directories are not created by default on Ubuntu systems.

V-72015

- **Summary**: All local interactive user home directories defined in the /etc/passwd file must exist.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Each interactive user on the system is checked to verify that their assigned home directory exists on the filesystem. If a home directory is missing, the name of the user and their assigned home directory is printed in the Ansible console output.

V-73159

- **Summary**: When passwords are changed or new passwords are established, pwquality must be used.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The security role can require new or changed passwords to follow the pwquality rules, but this change can be disruptive for users without proper communication. Deployers must opt in for this change by setting the following variable:

```
security_enable_pwquality_password_set: yes
```

3.4.2 aide - Advanced Intrusion Detection Environment

AIDE provides integrity monitoring for files on a Linux system and can notify system administrators of changes to critical files and packages.

Overview

By default, AIDE will examine and monitor all of the files on a host unless directories are added to its exclusion list. The security role sets directories to exclude from AIDE monitoring via the `aide_exclude_dirs` variable. this list excludes the most common directories that change very often via automated methods.

The security role skips the AIDE initialization step by default to avoid system disruption or a reduction in performance. Deployers should determine the best time to initialize the database that does not interfere with the systems operations.

To initialize the AIDE database, set the following Ansible variable and re-apply the role:

```
security_rhel7_initialize_aide: true
```

> **Warning:** Even with the excluded directories, the first AIDE initialization can take a long time on some systems. During this time, the CPU and disks are **very busy**.

To avoid installing and initializing AIDE, set the following Ansible variable:

```
security_rhel7_enable_aide: false
```

STIG requirements

All of the tasks for these STIG requirements are included in `tasks/rhel7stig/aide.yml`.

V-71973

- **Summary**: A file integrity tool must verify the baseline operating system configuration at least weekly.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Initializing the AIDE database and completing the first AIDE run causes increased disk I/O and CPU usage for extended periods. Therefore, the AIDE database is not automatically initialized by the tasks in the security role.

Deployers can enable the AIDE database initialization within the security role by setting the following Ansible variable:

```
security_rhel7_initialize_aide: yes
```

V-71975

- **Summary**: Designated personnel must be notified if baseline configurations are changed in an unauthorized manner.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The cron job for AIDE is configured to send emails to the root user after each AIDE run.

V-72069

- **Summary**: The file integrity tool must be configured to verify Access Control Lists (ACLs).
- **Severity:** Low
- **Implementation Status:** Implemented

Deployer/Auditor notes

CentOS 7 and Red Hat Enterprise Linux 7 already deploy a very secure AIDE configuration that checks access control lists (ACLs) and extended attributes by default. No configuration changes are applied on these systems.

However, Ubuntu lacks the rules that include ACL and extended attribute checks. The tasks in the security role will add a small configuration block at the end of the AIDE configuration file to meet the requirements of this STIG, as well as V-72071.

openSUSE Leap and SUSE Linux Enterprise 12 also lack a rule to check ACLs and extended attributes. The default configuration file is adjusted to include those as well.

V-72071

- **Summary**: The file integrity tool must be configured to verify extended attributes.
- **Severity:** Low
- **Implementation Status:** Implemented

Deployer/Auditor notes

CentOS 7 and Red Hat Enterprise Linux 7 already deploy a very secure AIDE configuration that checks access control lists (ACLs) and extended attributes by default. No configuration changes are applied on these systems.

However, Ubuntu lacks the rules that include ACL and extended attribute checks. The tasks in the security role will add a small configuration block at the end of the AIDE configuration file to meet the requirements of this STIG, as well as V-72069.

openSUSE Leap and SUSE Linux Enterprise 12 also lack a rule to check ACLs and extended attributes. The default configuration file is adjusted to include those as well.

V-72073

- **Summary**: The file integrity tool must use FIPS 140-2 approved cryptographic hashes for validating file contents and directories.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The default AIDE configuration in CentOS 7, Red Hat Enterprise Linux 7, openSUSE Leap and SUSE Linux Enterprise 12 already uses SHA512 to validate file contents and directories. No changes are required on these systems.

The tasks in the security role add a rule to end of the AIDE configuration on Ubuntu systems that uses SHA512 for validation.

3.4.3 auditd - audit daemon

The STIG requires all systems to have the audit daemon, `auditd`, running to monitor system calls and other critical events. The daemon has rules that define which events are noteworthy on the system and it can generate alerts based on the events it finds.

Overview

Audit daemon rules

The auditd rules are deployed in a single task via a template (`templates/osas-auditd-rhel7.j2`). Each rule or set of similar rules are controlled by an Ansible variable that starts with `security_audit_rhel7`. Refer to `defaults/main.yml` for a list of these variables.

Example:

```
# Add audit rules for commands/syscalls.
security_rhel7_audit_chsh: yes                                  # V-72167
security_rhel7_audit_chage: yes                                 # V-72155
security_rhel7_audit_chcon: yes                                 # V-72139
security_rhel7_audit_chmod: no                                  # V-72105
security_rhel7_audit_chown: no                                  # V-72097
```

For example, setting `security_rhel7_audit_chown` to `yes` will ensure that the rule for auditing the usage of the `chown` are included on each host. Setting `security_rhel7_audit_chown` to `no` will omit that rule on each host.

Handling audit emergencies

There are several configurations for auditd which are critical for deployers to review in detail. The options beneath the `## Audit daemon (auditd)` comment will change how auditd handles log files and what it should do in case of emergencies.

> **Warning:** Deployers should thoroughly test all changes to auditd emergency configurations. Some of these configuration options can cause serious issues on production systems, ranging from a reduction in security to servers going offline unexpectedly. There is extensive documentation in the developer notes below for each STIG requirement.

STIG requirements

All of the tasks for these STIG requirements are included in `tasks/rhel7stig/auditd.yml`.

V-72079

- **Summary**: Auditing must be configured to produce records containing information to establish what type of events occurred, where the events occurred, the source of the events, and the outcome of the events. These audit records must also identify individual identities of group account users.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks in the security role start the audit daemon immediately and ensure that it starts at boot time.

V-72081

- **Summary**: The operating system must shut down upon audit processing failure, unless availability is an overriding concern. If availability is a concern, the system must alert the designated staff (System Administrator [SA] and Information System Security Officer [ISSO] at a minimum) in the event of an audit processing failure.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The audit daemon takes various actions when there is an auditing failure. There are three options for the `-f` flag for `auditctl`:

- `0`: In the event of an auditing failure, do nothing.
- `1`: In the event of an auditing failure, write messages to the kernel log.
- `2`: In the event of an auditing failure, cause a kernel panic.

Most operating systems set the failure flag to 1 by default, which maximizes system availability while still causing an alert. The tasks in the security role set the flag to 1 by default.

Deployers can adjust the following Ansible variable to customize the failure flag:

```
security_rhel7_audit_failure_flag: 1
```

Warning: Setting the failure flag to 2 is **strongly** discouraged unless the security of the system takes priority over its availability. Any failure in auditing causes a kernel panic and the system requires a hard reboot.

V-72083

- **Summary**: The operating system must off-load audit records onto a different system or media from the system being audited.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The `audispd` service transmits audit logs to other servers. Deployers should specify the address of another server that can receive audit logs by setting the following Ansible variable:

```
security_audisp_remote_server: '10.0.21.1'
```

V-72085

- **Summary**: The operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The `audispd` daemon transmits audit logs without encryption by default. The STIG requires that these logs are encrypted while they are transferred across the network. The encryption is controlled by the `enable_krb5` option in `/etc/audisp/audisp-remote.conf`.

Deployers can opt-in for encrypted audit log transmission by setting the following Ansible variable:

```
security_audisp_enable_krb5: yes
```

Warning: Only enable this setting if kerberos is already configured.

V-72087

- **Summary**: The audit system must take appropriate action when the audit storage volume is full.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks in the security role set the `disk_full_action` and `network_failure_action` to `syslog` in the audispd remote configuration. In the event of a full disk on the remote log server or a network interruption, the local system sends warnings to syslog. This is the safest option since it maximizes the availability of the local system.

Deployers have two other options available:

- `single`: Switch the local server into single-user mode in the event of a logging failure.
- `halt`: Shut off the local server gracefully in the event of a logging failure.

> **Warning:** Choosing `single` or `halt` causes a server to go into a degraded or offline state immediately after a logging failure.

Deployers can adjust these configurations by setting the following Ansible variables (the safe defaults are shown here):

```
security_rhel7_auditd_disk_full_action: syslog
security_rhel7_auditd_network_failure_action: syslog
```

V-72089

- **Summary**: The operating system must immediately notify the System Administrator (SA) and Information System Security Officer ISSO (at a minimum) when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `space_left` configuration is set to 25% of the size of the disk mounted on `/`. This calculation is done automatically.

Deployers can set a custom threshold for the `space_left` configuration (in megabytes) by setting the following Ansible variable:

```
# Example: A setting of 1GB (1024MB)
security_rhel7_auditd_space_left: 1024
```

V-72091

- **Summary**: The operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) via email when the threshold for the repository maximum audit record storage capacity is reached.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `space_left_action` in the audit daemon configuration is set to `email`. This configuration causes the root user to receive an email when the `space_left` threshold is reached.

Deployers can customize this configuration by setting the following Ansible variable:

```
security_rhel7_auditd_space_left_action: email
```

V-72093

- **Summary**: The operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `action_mail_acct` configuration in the audit daemon configuration file is set to `root` to meet the requirements of the STIG. Deployers can customize the recipient of the emails that come from auditd by setting the following Ansible variable:

```
security_rhel7_auditd_action_mail_acct: root
```

V-72095

- **Summary**: All privileged function executions must be audited.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

This STIG is difficult to implement in an automated way because the number of applications on a system with setuid/setgid permissions changes over time. In addition, adding audit rules for some of these automatically could cause a significant increase in logging traffic when these applications are used regularly.

Deployers are urged to do the following instead:

- Minimize the amount of applications with setuid/setgid privileges
- Monitor any new applications that gain setuid/setgid privileges
- Add risky applications with setuid/setgid privileges to auditd for detailed syscall monitoring

---

V-72097

- **Summary**: All uses of the chown command must be audited.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that all `chown` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_chown: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72099

- **Summary**: All uses of the fchown command must be audited.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that all `fchown` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchown: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72101

- **Summary**: All uses of the lchown command must be audited.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that all `lchown` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_lchown: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72103

- **Summary**: All uses of the fchownat command must be audited.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that all `fchownat` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchownat: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72105

- **Summary**: All uses of the chmod command must be audited.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that all `chmod` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_chmod: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72107

- **Summary**: All uses of the fchmod command must be audited.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that all `fchmod` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchmod: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72109

- **Summary**: All uses of the fchmodat command must be audited.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that all `fchmodat` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchmodat: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72111

- **Summary**: All uses of the setxattr command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit all `setxattr` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_setxattr: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72113

- **Summary**: All uses of the fsetxattr command must be audited.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that all `fsetxattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fsetxattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72115

- **Summary**: All uses of the lsetxattr command must be audited.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that all `lsetxattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_lsetxattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72117

- **Summary**: All uses of the removexattr command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit all `removexattr` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_removexattr: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72119

- **Summary**: All uses of the fremovexattr command must be audited.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that all `fremovexattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fremovexattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72121

- **Summary**: All uses of the lremovexattr command must be audited.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that all `lremovexattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_lremovexattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72123

- **Summary**: All uses of the creat command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit all `creat` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_creat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72125

- **Summary**: All uses of the open command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit all `open` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_open: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72127

- **Summary**: All uses of the openat command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit all `openat` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_openat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72129

- **Summary**: All uses of the open_by_handle_at command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit all `open_by_handle_at` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_open_by_handle_at: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72131

- **Summary**: All uses of the truncate command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit all `truncate` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_truncate: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72133

- **Summary**: All uses of the ftruncate command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit all `ftruncate` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_ftruncate: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72135

- **Summary**: All uses of the semanage command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit any time the `semanage` command is used.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_semanage: no
```

V-72137

- **Summary**: All uses of the setsebool command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit any time the `setsebool` command is used.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_setsebool: no
```

V-72139

- **Summary**: All uses of the chcon command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `chcon` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_chcon: no
```

V-72141

- **Summary**: All uses of the setfiles command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `restorecon` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_restorecon: no
```

V-72143

- **Summary**: The operating system must generate audit records for all successful/unsuccessful account access count events.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit all successful and unsuccessful account access events. Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_audit_account_access: no
```

V-72145

- **Summary**: The operating system must generate audit records for all unsuccessful account access events.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all successful/unsuccessful account access count events. (V-72143)*

V-72147

- **Summary**: The operating system must generate audit records for all successful account access events.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time an account is accessed.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_account_access: no
```

V-72149

- **Summary**: All uses of the passwd command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `passwd` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_passwd_command: no
```

V-72151

- **Summary**: All uses of the unix_chkpwd command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `unix_chkpwd` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_unix_chkpwd: no
```

V-72153

- **Summary**: All uses of the gpasswd command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `gpasswd` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_gpasswd: no
```

V-72155

- **Summary**: All uses of the chage command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `chage` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_chage: no
```

V-72157

- **Summary**: All uses of the userhelper command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `userhelper` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_userhelper: no
```

V-72159

- **Summary**: All uses of the su command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `su` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_su: no
```

V-72161

- **Summary**: All uses of the sudo command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `sudo` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_sudo: no
```

V-72163

- **Summary**: All uses of the sudoers command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time a user manages the configuration files for `sudo`.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_sudo_config_changes: no
```

V-72165

- **Summary**: All uses of the newgrp command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `newgrp` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_newgrp: no
```

V-72167

- **Summary**: All uses of the chsh command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `chsh` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_chsh: no
```

V-72169

- **Summary**: All uses of the sudoedit command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `sudoedit` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_sudoedit: no
```

V-72171

- **Summary**: All uses of the mount command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `mount` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_mount: no
```

V-72173

- **Summary**: All uses of the umount command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `umount` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_umount: no
```

V-72175

- **Summary**: All uses of the postdrop command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `postdrop` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_postdrop: no
```

V-72177

- **Summary**: All uses of the postqueue command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `postqueue` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_postqueue: no
```

V-72179

- **Summary**: All uses of the ssh-keysign command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `ssh-keysign` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_ssh_keysign: no
```

V-72183

- **Summary**: All uses of the crontab command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `crontab` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_crontab: no
```

V-72185

- **Summary**: All uses of the pam_timestamp_check command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `pam_timestamp_check` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_pam_timestamp_check: no
```

V-72187

- **Summary**: All uses of the init_module command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit all `init_module` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_init_module: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72189

- **Summary**: All uses of the delete_module command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit all `delete_module` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_delete_module: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72191

- **Summary**: All uses of the insmod command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `insmod` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_insmod: no
```

V-72193

- **Summary**: All uses of the rmmod command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `rmmod` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_rmmod: no
```

V-72195

- **Summary**: All uses of the modprobe command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `modprobe` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_modprobe: no
```

V-72197

- **Summary**: The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time that an account is modified. This includes changes to the following files:

- `/etc/group`
- `/etc/passwd`
- `/etc/gshadow`
- `/etc/shadow`
- `/etc/security/opasswd`

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_account_actions: no
```

V-72199

- **Summary**: All uses of the rename command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit all `rename` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_rename: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72201

- **Summary**: All uses of the renameat command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit all `renameat` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_renameat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72203

- **Summary**: All uses of the rmdir command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Rules are added to audit all `rmdir` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_rmdir: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72205

- **Summary**: All uses of the unlink command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `unlink` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_unlink: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-72207

- **Summary**: All uses of the unlinkat command must be audited.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks add a rule to auditd that logs each time the `unlinkat` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_unlinkat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

V-73163

- **Summary**: The audit system must take appropriate action when there is an error sending audit records to a remote system.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control:

- *The audit system must take appropriate action when the audit storage volume is full. (V-72087)*

V-73165

- **Summary**: The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

V-73167

- **Summary**: The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

V-73171

- **Summary**: The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

V-73173

- **Summary**: The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

3.4.4 auth - Authentication

User or automated authentication to a Linux system must be closely monitored and carefully configured to prevent unauthorized access.

Overview

Most of the STIG requirements for authentication are already included in Linux distributions by default or are easily applied without disruptions. Deployers should review the documentation below and test all changes on a non-production system first.

STIG requirements

All of the tasks for these STIG requirements are included in `tasks/rhel7stig/auth.yml`.

V-71937

- **Summary**: The system must not have accounts configured with blank or null passwords.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

The Ansible tasks will ensure that PAM is configured to disallow logins from accounts with null or blank passwords. This involves removing a single option from one of the PAM configuration files:

- CentOS or RHEL: removes `nullok` from `/etc/pam.d/system-auth`
- Ubuntu: removes `nullok_secure` from `/etc/pam.d/common-auth`
- openSUSE Leap or SLE: remove `nullok` from `/etc/pam.d/common-auth` and `/etc/pam.d/common-password`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_disallow_blank_password_login: no
```

V-71943

- **Summary**: Accounts subject to three unsuccessful logon attempts within 15 minutes must be locked for the maximum configurable period.
- **Severity:** Medium
- **Implementation Status:** Opt-In - Red Hat Only

Deployer/Auditor notes

This STIG control is implemented by:

- *If three unsuccessful root logon attempts within 15 minutes occur the associated account must be locked. (V-71945)*

V-71945

- **Summary**: If three unsuccessful root logon attempts within 15 minutes occur the associated account must be locked.
- **Severity:** Medium
- **Implementation Status:** Opt-In - Red Hat Only

Deployer/Auditor notes

The STIG requires that accounts with excessive failed login attempts are locked. It sets a limit of three failed attempts in a 15 minute interval and these restrictions are applied to all users (including root). Accounts cannot be automatically unlocked for seven days.

This change might cause disruptions in production environments without proper communication to users. Therefore, this change is not applied by default.

Deployers can opt in for the change by setting the following variable:

```
security_pam_faillock_enable: yes
```

There are also three configuration options that can be adjusted by setting Ansible variables:

- `security_pam_faillock_attempts`: This many failed login attempts within the specified time interval with trigger the account to lock. (STIG requirement: `3` attempts)
- `security_pam_faillock_interval`: This is the time interval (in seconds) to use when measuring excessive failed login attempts. (STIG requirement: `900` seconds)
- `security_pam_faillock_deny_root`: Set to `yes` to apply the restriction to the root user or set to `no` to exempt the root user from the account locking restrictions. (STIG requirement: `yes`)
- `security_pam_faillock_unlock_time`: This sets the time delay (in seconds) before a locked account is automatically unlocked. (STIG requirement: `604800` seconds)

Note: Ubuntu, openSUSE Leap and SUSE Linux Enterprise 12 do not provide `pam_faillock`. This change is only applied to CentOS 7 or Red Hat Enterprise Linux 7 systems.

V-71947

- **Summary**: Users must provide a password for privilege escalation.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

The STIG requires all users to authenticate when using `sudo`, but this change can be highly disruptive for automated scripts or applications that cannot perform interactive authentication. Automated edits from Ansible tasks might cause authentication disruptions on some hosts, and deployers are urged to carefully review each use of the `NOPASSWD` directive in their `sudo` configuration files.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_sudoers_nopasswd_check_enable: no
```

V-71949

- **Summary**: Users must re-authenticate for privilege escalation.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

The STIG requires all users to re-authenticate when using `sudo`, but this change can be highly disruptive for automated scripts or applications that cannot perform interactive authentication. Automated edits from Ansible tasks might cause authentication disruptions on some hosts, and deployers are urged to carefully review each use of the `!authenticate` directive in their `sudo` configuration files.

V-71965

- **Summary**: The operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users) using multifactor authentication.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deploying multi-factor authentication methods, including smart cards, is a complicated process that requires preparation and communication. This work is left to deployers to complete manually.

V-71971

- **Summary**: The operating system must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

The tasks in the security role cannot determine the access levels of individual users.

Deployers are strongly encouraged to configure SELinux user confinement on compatible systems using `semanage login`. Refer to the Confining Existing Linux Users documentation from Red Hat for detailed information and command line examples.

V-72001

- **Summary**: The system must not have unnecessary accounts.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deployers are strongly urged to review the list of user accounts on each server regularly. Evaluation of user accounts must be done on a case-by-case basis and the tasks in the security role are unable to determine which user accounts are valid. Deployers must complete this work manually.

V-72217

- **Summary**: The operating system must limit the number of concurrent sessions to 10 for all accounts and/or account types.
- **Severity:** Low
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Although the STIG requires that each account is limited to 10 concurrent connections, this change might be disruptive in some environments. Therefore, this change is not applied by default.

Deployers can opt in for this change by setting a concurrent connection limit with this Ansible variable:

```
security_rhel7_concurrent_session_limit: 10
```

V-72227

- **Summary**: The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) authentication communications.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deployers are strongly urged to utilize `sssd` for systems that authenticate against LDAP or Active Directory (AD) servers.

The ldap connector for `sssd` connects only to LDAP servers over encrypted connections. Review the man page for sssd-ldap for more details on this requirement.

V-72229

- **Summary**: The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deployers are strongly urged to utilize `sssd` for systems that authenticate against LDAP or Active Directory (AD) servers.

To meet this control, deployers must ensure that `ldap_tls_cacert` or `ldap_tls_cacertdir` are set in the `/etc/sssd/sssd.conf` file. The `ldap_tls_cacert` directive specifies a single certificate while `ldap_tls_cacertdir` specifies a directory where `sssd` can find CA certificates.

> **Warning:** Use caution when adjusting these settings. If the correct CA certificates are not already deployed to the servers that perform LDAP authentication, their attempts to authenticate users might fail.
>
> Consult with administrators of the LDAP system and test all changes on a non-production system first.

V-72231

- **Summary**: The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deployers are strongly urged to utilize `sssd` for systems that authenticate against LDAP or Active Directory (AD) servers.

To meet this control, deployers must ensure that `ldap_tls_cacert` or `ldap_tls_cacertdir` are set in the `/etc/sssd/sssd.conf` file. The `ldap_tls_cacert` directive specifies a single certificate while `ldap_tls_cacertdir` specifies a directory where `sssd` can find CA certificates.

> **Warning:** Use caution when adjusting these settings. If the correct CA certificates are not already deployed to the servers that perform LDAP authentication, their attempts to authenticate users might fail.

> Consult with administrators of the LDAP system and test all changes on a non-production system first.

V-72275

- **Summary**: The system must display the date and time of the last successful account logon upon logon.
- **Severity:** Low
- **Implementation Status:** Verification Only

Deployer/Auditor notes

The PAM configuration is checked for the presence of `pam_lastlogin` and a warning message is printed if the directive is not found. The tasks in the security role do not adjust PAM configurations since these changes might be disruptive in some environments.

Deployers should review their PAM configurations and add `pam_lastlogin` to `/etc/pam.d/postlogin` on CentOS and Red Hat Enterprise Linux or to `/etc/pam.d/login` on Ubuntu, openSUSE Leap and SUSE Linux Enterprise.

V-72277

- **Summary**: There must be no .shosts files on the system.
- **Severity:** High
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The tasks in the security role examine the filesystem for any `.shosts` or `shosts.equiv` files. If they are found, they are deleted.

The search for these files will take a very long time on systems with slow disks or systems with a large amount of files. Therefore, this task is skipped by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_remove_shosts_files: yes
```

V-72279

- **Summary**: There must be no shosts.equiv files on the system.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control:

- *There must be no .shosts files on the system. (V-72277)*

V-72427

- **Summary**: The operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules (PAM).
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Although the STIG requires that the `sssd.conf` contains both `nss` and `pam` authentication modules, this change can be disruptive in environments that are already using LDAP or Active Directory for authentication. Deployers should make these changes only if their environment is compatible.

V-72433

- **Summary**: The operating system must implement certificate status checking for PKI authentication.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Any adjustment to PKI authentication can cause disruptions for users. Deployers should verify that enabling OCSP validation is compatible with their existing configuration.

V-72435

- **Summary**: The operating system must implement smart card logons for multifactor authentication for access to privileged accounts.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Any adjustment to PKI authentication can cause disruptions for users. Deployers should verify that their environment is compatible with smart cards before requiring them for authentication.

V-77823

- **Summary**: The operating system must require authentication upon booting into single-user and maintenance modes.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Modifying sensitive systemd unit files directly or via overrides could cause a system to have issues during the boot process. The role does not make any adjustments to the `rescue.service` because this service is critical during emergencies.

All of the distributions supported by the role already require authentication for single user mode.

3.4.5 file_perms - Filesystem permissions

One of the first layers of defense against attacks on a Linux system is Discretionary Access Control (DAC), which is managed through filesystem permissions.

Overview

Some of the STIG requirements for file permissions could cause disruptions on production systems if the permissions were adjusted to meet the needs of a particular application. These configurations are applied on an opt-in basis. Deployers must verify that these changes work well with their systems before applying the changes.

STIG requirements

All of the tasks for these STIG requirements are included in `tasks/rhel7stig/file_perms.yml`.

V-71849

- **Summary**: The file permissions, ownership, and group membership of system files and commands must match the vendor values.
- **Severity:** High
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Note: Ubuntus `debsums` command does not support verification of permissions and ownership for files that were installed by packages. This STIG requirement will be skipped on Ubuntu.

The STIG requires that all files owned by an installed package must have their permissions, user ownership, and group ownership set back to the vendor defaults.

Although this is a good practice, it can cause issues if permissions or ownership were intentionally set after the packages were installed. It also causes significant delays in deployments. Therefore, this STIG is not applied by default.

Deployers may opt in for the change by setting the following Ansible variable:

```
security_reset_perm_ownership: yes
```

V-72007

- **Summary**: All files and directories must have a valid owner.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Searching an entire filesystem with `find` reduces system performance and might impact certain applications negatively. Therefore, the search for files and directories with an invalid owner is **disabled by default**.

Deployers can opt in for this search by setting the following Ansible variable:

```
security_search_for_invalid_owner: yes
```

Any files or directories without a valid user owner are displayed in the Ansible output.

V-72009

- **Summary**: All files and directories must have a valid group owner.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Searching an entire filesystem with `find` reduces system performance and might impact certain applications negatively. Therefore, the search for files and directories with an invalid group owner is **disabled by default**.

Deployers can opt in for this search by setting the following Ansible variable:

```
security_search_for_invalid_group_owner: yes
```

Any files or directories without a valid group owner are displayed in the Ansible output.

V-72017

- **Summary**: All local interactive user home directories must have mode 0750 or less permissive.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Although the STIG requires that all home directories have the proper owner, group owner, and permissions, these changes might be disruptive in some environments. These tasks are not executed by default.

Deployers can opt in for the following changes to each home directory:

- Permissions are set to `0750` at a maximum. If permissions are already more restrictive than `0750`, the permissions are left unchanged.
- User ownership is set to the `UID` of the user.
- Group ownership is set to the `GID` of the user.

Deployers can opt in for these changes by setting the following Ansible variable:

```
security_set_home_directory_permissions_and_owners: yes
```

V-72019

- **Summary**: All local interactive user home directories must be owned by their respective users.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *All local interactive user home directories must have mode 0750 or less permissive. (V-72017)*

V-72021

- **Summary**: All local interactive user home directories must be group-owned by the home directory owners primary group.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *All local interactive user home directories must have mode 0750 or less permissive. (V-72017)*

V-72023

- **Summary**: All files and directories contained in local interactive user home directories must be owned by the owner of the home directory.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Although the STIG has requirements for ownership and permissions of files and directories in each users home directory, broad changes to these settings might cause disruptions to users on a system. Therefore, these changes are left to deployers to examine and adjust manually.

V-72025

- **Summary**: All files and directories contained in local interactive user home directories must be group-owned by a group of which the home directory owner is a member.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Although the STIG has requirements for ownership and permissions of files and directories in each users home directory, broad changes to these settings might cause disruptions to users on a system. Therefore, these changes are left to deployers to examine and adjust manually.

V-72027

- **Summary**: All files and directories contained in local interactive user home directories must have mode 0750 or less permissive.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Although the STIG has requirements for ownership and permissions of files and directories in each users home directory, broad changes to these settings might cause disruptions to users on a system. Therefore, these changes are left to deployers to examine and adjust manually.

V-72029

- **Summary**: All local initialization files for interactive users must be owned by the home directory user or root.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Although the STIG requires that all initialization files for interactive users have proper owners, group owners, and permissions, these changes are often disruptive for users. The tasks in the security role do not make any changes to user initialization files.

Deployers should review the content and discretionary access controls applied to each users initialization files in their home directory.

V-72031

- **Summary**: Local initialization files for local interactive users must be group-owned by the users primary group or root.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Although the STIG requires that all initialization files for interactive users have proper owners, group owners, and permissions, these changes are often disruptive for users. The tasks in the security role do not make any changes to user initialization files.

Deployers should review the content and discretionary access controls applied to each users initialization files in their home directory.

V-72033

- **Summary**: All local initialization files must have mode 0740 or less permissive.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Although the STIG requires that all initialization files for interactive users have proper owners, group owners, and permissions, these changes are often disruptive for users. The tasks in the security role do not make any changes to user initialization files.

Deployers should review the content and discretionary access controls applied to each users initialization files in their home directory.

V-72037

- **Summary**: Local initialization files must not execute world-writable programs.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deployers should manually search their system for world-writable programs and change the permissions on those programs. They are easily found with this command:

```
find / -perm -002 -type f
```

World-writable executables should not be needed under almost all circumstances.

V-72047

- **Summary**: All world-writable directories must be group-owned by root, sys, bin, or an application group.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The tasks in the security role examine the world-writable directories on the system and report any directories that are not group-owned by the `root` user. Those directories appear in the Ansible output.

Deployers should review the list of directories and group owners to ensure that they are appropriate for the directory. Unauthorized group ownership could allow certain users to modify files from other users.

Searching the entire filesystem for world-writable directories will consume a significant amount of disk I/O and could impact the performance of a production system. It can also delay the playbooks completion. Therefore, the search is disabled by default.

Deployers can enable the search by setting the following Ansible variable:

```
security_find_world_writable_dirs: yes
```

V-72049

- **Summary**: The umask must be set to 077 for all local interactive user accounts.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Although the STIG requires that all local interactive user accounts have a umask of `077`, this change can be disruptive for users and the applications they run. This change cannot be applied in an automated way.

Deployers should review user initialization files regularly to ensure that the umask is not specified. This allows the system-wide setting of `077` to be applied to all user sessions.

V-72053

- **Summary**: If the cron.allow file exists it must be owned by root.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks in the security role check for the existence of `/etc/cron.allow` and set both the user and group ownership to `root`. This is the default on Ubuntu, CentOS, Red Hat Enterprise Linux systems, openSUSE Leap and SUSE Linux Enterprise 12 already.

3.4.6 graphical - Graphical login security controls

Although most Linux servers only have text-based interfaces, graphical environments are required for certain applications. Security controls must be applied to these graphical environments to prevent unauthorized access.

Overview

The STIG requirements for graphical interfaces are focused on ensuring proper authentication for new sessions and enforcing re-authentication after idle periods.

These controls will be skipped on systems without a graphical login interface.

STIG requirements

All of the tasks for these STIG requirements are included in `tasks/rhel7stig/graphical.yml`.

V-71859

- **Summary**: The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks in the security role configure `dconf` to display a login banner each time a graphical session starts on the system. The default banner message set by the role is:

> You are accessing a secured system and your actions will be logged along with identifying information. Disconnect immediately if you are not an authorized user of this system.

Deployers can customize this message by setting an Ansible variable:

```
security_enable_graphical_login_message_text: >
    This is a customized banner message.
```

> **Warning:** The dconf configuration does not support multi-line strings. Ensure that `security_enable_graphical_login_message_text` contains a single line of text.

In addition, deployers can opt out of displaying a login banner message by changing `security_enable_graphical_login_message` to `no`.

V-71861

- **Summary**: The operating system must display the approved Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The security role configures a login banner for graphical logins using `dconf`. Deployers can opt out of this change by setting the following Ansible variable:

```
security_enable_graphical_login_message: no
```

The message is customized by setting another Ansible variable:

```
security_enable_graphical_login_message_text: >
    You are accessing a secured system and your actions will be logged along
    with identifying information. Disconnect immediately if you are not an
    authorized user of this system.
```

Note: The space available for the graphical banner is relatively short. Deployers should limit the length of their graphical login banners to the shortest length possible.

V-71891

- **Summary**: The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The STIG requires that graphical sessions are locked when the screensaver starts and that users must re-enter credentials to restore access to the system. The screensaver lock is enabled by default if `dconf` is present on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_lock_session: no
```

V-71893

- **Summary**: The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The STIG requires that the screensaver appears when a session reaches a certain period of inactivity. The tasks will enable the screensaver for inactive sessions by default.

Deployers can opt out of this change by setting an Ansible variable:

```
security_lock_session_when_inactive: no
```

V-71895

- **Summary**: The operating system must set the idle delay setting for all connection types.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces. (V-71893)*

V-71899

- **Summary**: The operating system must initiate a session lock for the screensaver after a period of inactivity for graphical user interfaces.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces. (V-71893)*

V-71901

- **Summary**: The operating system must initiate a session lock for graphical user interfaces when the screensaver is activated.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The STIG requires that a graphical session is locked when the screensaver starts. This requires a user to re-enter their credentials to regain access to the system.

The tasks will set a timeout of 5 seconds after the screensaver has started before the session is locked. This gives a user a few seconds to press a key or wiggle their mouse after the screensaver appears without needing to re-enter their credentials.

Deployers can adjust this timeout by setting an Ansible variable:

```
security_lock_session_screensaver_lock_delay: 5
```

V-71953

- **Summary**: The operating system must not allow an unattended or automatic logon to the system via a graphical user interface.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

If `AutomaticLoginEnable=true` exists in the gdm configuration file, `/etc/gdm/custom.conf`, the configuration will removed. This disallows automatic logins for gdm and requires a user to complete the username and password prompts.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_disable_gdm_automatic_login: no
```

V-71955

- **Summary**: The operating system must not allow an unrestricted logon to the system.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

If `TimedLoginEnable=true` exists in the gdm configuration file, `/etc/gdm/custom.conf`, the configuration will removed. This disallows timed logins for guest users in gdm.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_disable_gdm_timed_login: no
```

V-73155

- **Summary**: The operating system must set the lock delay setting for all connection types.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control:

- *The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. (V-71891)*

V-73157

- **Summary**: The operating system must set the session idle delay setting for all connection types.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control:

- *The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. (V-71891)*

3.4.7 kernel - Kernel parameters

The Linux kernel has many parameters that can improve overall system security and most of these parameters can be changed while a system is running.

Overview

The security role applies several changes to kernel parameters and each of these changes are controlled by Ansible variables. Review the `## Kernel settings` section within `defaults/main.yml` file for more information on these changes.

One deviation appears in this section for IP forwarding. Review the documentation for `V-72309` below for more details.

STIG requirements

All of the tasks for these STIG requirements are included in `tasks/rhel7stig/kernel.yml`.

V-71983

- **Summary**: USB mass storage must be disabled.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The tasks in the security role disable the `usb-storage` module and the change is applied the next time the server is rebooted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_disable_usb_storage: no
```

V-72057

- **Summary**: Kernel core dumps must be disabled unless needed.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `kdump` service is disabled if it exists on the system. Deployers can opt out of this change by setting the following Ansible variable:

```
security_disable_kdump: no
```

V-72283

- **Summary**: The system must not forward Internet Protocol version 4 (IPv4) source-routed packets.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks in this role set `net.ipv4.conf.all.accept_source_route` and `net.ipv4.conf.default.accept_source_route` to `0` by default. This prevents the system from forwarding source-routed IPv4 packets on all new and existing interfaces.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_source_routed_packet_forward_ipv4: no
```

For more details on source routed packets, refer to the Red Hat documentation.

V-72285

- **Summary**: The system must not forward Internet Protocol version 4 (IPv4) source-routed packets by default.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control:

- *The system must not forward Internet Protocol version 4 (IPv4) source-routed packets. (V-72283)*

V-72287

- **Summary**: The system must not respond to Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) echoes sent to a broadcast address.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks in this role set `net.ipv4.icmp_echo_ignore_broadcasts` to 1 by default. This prevents the system from responding to IPv4 ICMP echoes sent to the broadcast address.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_echoes_broadcast_address: no
```

V-72291

- **Summary**: The system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks in this role set `net.ipv4.conf.default.send_redirects` and `net.ipv4.conf.all.send_redirects` to `0` by default. This prevents a system from sending IPv4 ICMP redirect packets on all new and existing interfaces.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_icmp_redirects: no
```

V-72293

- **Summary**: The system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control:

- *The system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default. (V-72291)*

V-72309

- **Summary**: The system must not be performing packet forwarding unless the system is a router.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Disabling IP forwarding on a system that routes packets or host virtual machines might cause network interruptions. The tasks in this role do not adjust the `net.ipv4.ip_forward` configuration by default.

Deployers can opt in for this change and disable IP forwarding by setting the following Ansible variable:

```
security_disallow_ip_forwarding: yes
```

> **Warning:** IP forwarding is required in some environments. Always test in a non-production environment before changing this setting on a production system.

V-72319

- **Summary**: The system must not forward IPv6 source-routed packets.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks in this role set `net.ipv6.conf.all.accept_source_route` to `0` by default. This prevents the system from forwarding source-routed IPv6 packets.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_source_routed_packet_forward_ipv6: no
```

Refer to IPv6 source routing: history repeats itself for more details on IPv6 source routed packets.

V-73175

- **Summary**: The system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control:

- *The system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects. (V-72293)*

V-77821

- **Summary**: The Datagram Congestion Control Protocol (DCCP) kernel module must be disabled unless required.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The ansible-hardening role disables the DCCP kernel module by default. Each system must be rebooted to fully apply the change.

Deployers can opt out of the change by setting the following Ansible variable:

```
security_rhel7_disable_dccp: no
```

V-77825

- **Summary**: The operating system must implement virtual address space randomization.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

Most modern systems enable Address Space Layout Randomization (ASLR) by default (with a setting of 2), and the role ensures that the secure default is maintained.

Deployers can opt out of the change by setting the following Ansible variable:

```
security_enable_aslr: no
```

For more details on the ASLR settings, review the sysctl documentation.

3.4.8 lsm - Linux Security Modules

Linux Security Modules, such as AppArmor and SELinux, provide an extra level of security controls on a Linux system. They provide Mandatory Access Control (MAC) that checks system activities against security policy. These policies apply to all users, including root.

Overview

The STIG requires that SELinux is in enforcing mode to provide additional security against attacks. The security role will enable SELinux on CentOS systems and enable AppArmor on Ubuntu and Debian systems.

STIG requirements

All of the tasks for these STIG requirements are included in `tasks/rhel7stig/lsm.yml`.

V-71989

- **Summary**: The operating system must enable SELinux.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks in the security role enable the appropriate Linux Security Module (LSM) for the operating system.

For Ubuntu, openSUSE and SUSE Linux Enterprise 12 systems, AppArmor is installed and enabled. This change takes effect immediately.

For CentOS or Red Hat Enterprise Linux systems, SELinux is enabled (in enforcing mode) and its user tools are automatically installed. If SELinux is not in enforcing mode already, a reboot is required to enable SELinux and relabel the filesystem.

> **Warning:** Relabeling a filesystem takes time and the server must be offline for the relabeling to complete. Filesystems with large amounts of files and filesystems on slow disks will cause the relabeling process to take more time.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_enable_linux_security_module: no
```

V-72039

- **Summary**: All system device files must be correctly labeled to prevent unauthorized modification.
- **Severity:** Medium
- **Implementation Status:** Implemented - Red Hat Only

Deployer/Auditor notes

The tasks in the security role examine the SELinux contexts on each device file found on the system. Any devices without appropriate labels are printed in the Ansible output.

Deployers should investigate the unlabeled devices and ensure that the correct labels are applied for the class of device.

Note: This change applies only to CentOS or Red Hat Enterprise Linux systems since they rely on SELinux as their default Linux Security Module (LSM). Ubuntu, openSUSE Leap and SUSE Linux Enterprise systems use AppArmor, which uses policy files rather than labels applied to individual files.

3.4.9 misc - Miscellaneous security controls

Some of the security controls provided by the STIG are difficult to group together. The following documentation includes STIG requirements which do not easily fit into one of the other hardening domains.

Overview

Reliable time synchronization is a requirement in the STIG and the `chrony` package will be installed to handle NTP for systems secured with the openstack- ansible-security role. The default settings will work for most environments, but some deployers may prefer to use NTP servers which are geographically closer to their servers.

The role configures the chrony daemon to listen only on `localhost`. To allow chrony to listen on all addresses (the upstream default for chrony), set the `security_ntp_bind_local_interfaces_only` variable to `False`.

The default configuration allows RFC1918 addresses to reach the NTP server running on each host. That could be changed by using the `security_allowed_ntp_subnets` parameter.

STIG requirements

All of the tasks for these STIG requirements are included in `tasks/rhel7stig/misc.yml`.

V-71863

- **Summary**: The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a command line user logon.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The security role already deploys a login banner for console logins with tasks from another STIG:

- *The Standard Mandatory DoD Notice and Consent Banner must be displayed immediately prior to, or as part of, remote access logon prompts. (V-72225)*

V-71961

- **Summary**: Systems with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes.
- **Severity:** High
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Although the STIG requires that GRUB 2 asks for a password whenever a user attempts to enter single-user or maintenance mode, this change might be disruptive in an emergency situation. Therefore, this change is not applied by default.

Deployers that wish to opt in for this change should set two Ansible variables:

```
security_require_grub_authentication: yes
security_grub_password_hash: grub.pbkdf2.sha512.10000.7B21785BEAFEE3AC...
```

The default password set in the security role is secrete, but deployers should set a much more secure password for production environments. Use the `grub2-mkpasswd-pbkdf2` command to create a password hash string and use it as the value for the Ansible variable `security_grub_password_hash`.

Warning: This change must be tested in a non-production environment first. Requiring authentication in GRUB 2 without proper communication to users could cause extensive delays in emergency situations.

V-71963

- **Summary**: Systems using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes.
- **Severity:** High
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The tasks in the security role for V-71961 will also apply changes to systems that use UEFI. For more details, refer to the following documentation:

- *Systems with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes. (V-71961)*

V-71985

- **Summary**: File system automounter must be disabled unless required.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `autofs` service is stopped and disabled if it is found on the system. Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_disable_autofs: no
```

V-71991

- **Summary**: The operating system must enable the SELinux targeted policy.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

The SELinux targeted policy is enabled on CentOS 7 and Red Hat systems. AppArmor only has one set of policies, so this change has no effect on Ubuntu, openSUSE Leap and SUSE systems running AppArmor.

For more information on this change and how to opt out, refer to *The operating system must enable SELinux. (V-71989)*.

V-71993

- **Summary**: The x86 Ctrl-Alt-Delete key sequence must be disabled.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks in the security role disable the control-alt-delete key sequence by masking its systemd service unit.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_disable_ctrl_alt_delete: no
```

V-72035

- **Summary**: All local interactive user initialization files executable search paths must contain only paths that resolve to the users home directory.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Although the STIG requires that all initialization files must contain executable search paths that resolve to the users home directory, this change be disruptive for most users. The tasks in the security role do not make any changes to user initialization files.

V-72041

- **Summary**: File systems that contain user home directories must be mounted to prevent files with the setuid and setgid bit set from being executed.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deployers should examine any filesystem mounts that contain home directories to ensure that the `nosetuid` option is set.

V-72043

- **Summary**: File systems that are used with removable media must be mounted to prevent files with the setuid and setgid bit set from being executed.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deployers should examine any filesystem mounts of removable media to ensure that the `nosetuid` option is set.

V-72045

- **Summary**: File systems that are being imported via Network File System (NFS) must be mounted to prevent files with the setuid and setgid bit set from being executed.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deployers should examine any filesystem mounts of NFS imports to ensure that the `nosetuid` option is set.

V-72051

- **Summary**: Cron logging must be implemented.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Ubuntu, CentOS, Red Hat Enterprise Linux, openSUSE Leap and SUSE Linux Enterprise already capture the logs from cron.

Ubuntu systems collect cron job logs into the main syslog file (`/var/log/syslog`) rather than separate them into their own log file. CentOS and Red Hat Enterprise Linux systems collect cron logs in `/var/log/cron`. openSUSE Leap and SUSE Linux Enterprise collect cron job in `/var/log/messages`.

Deployers should not need to adjust these configurations unless a specific environment requires it. The tasks in the security role do not make changes to the `rsyslog` configuration.

V-72055

- **Summary**: If the cron.allow file exists it must be group-owned by root.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The group ownership for `/etc/cron.allow` is already set by the task for the following STIG control:

If the cron.allow file exists it must be owned by root. (V-72053)

V-72059

- **Summary**: A separate file system must be used for user home directories (such as /home or an equivalent).
- **Severity:** Low
- **Implementation Status:** Exception - Initial Provisioning

Deployer/Auditor notes

Deployers should consider using filesystem mounts for home directories during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/home` as a separate filesystem, a warning is printed in the Ansible output.

V-72061

- **Summary**: The system must use a separate file system for /var.
- **Severity:** Low
- **Implementation Status:** Exception - Initial Provisioning

Deployer/Auditor notes

Deployers should consider using filesystem mounts for `/var` during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/var` as a separate filesystem, a warning is printed in the Ansible output.

V-72063

- **Summary**: The system must use a separate file system for the system audit data path.
- **Severity:** Low
- **Implementation Status:** Exception - Initial Provisioning

Deployer/Auditor notes

Deployers should consider using filesystem mounts for `/var/log/audit` during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/var/log/audit` as a separate filesystem, a warning is printed in the Ansible output.

V-72065

- **Summary**: The system must use a separate file system for /tmp (or equivalent).
- **Severity:** Low
- **Implementation Status:** Exception - Initial Provisioning

Deployer/Auditor notes

Deployers should consider using filesystem mounts for `/tmp` during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/tmp` as a separate filesystem, a warning is printed in the Ansible output.

V-72067

- **Summary**: The operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
- **Severity:** High
- **Implementation Status:** Implemented - Red Hat And Suse Only

Deployer/Auditor notes

The tasks in the Ansible role install the `dracut-fips` (RHEL and SLE) and `dracut-fips-aesni` (RHEL) packages and check to see if FIPS is enabled on the system. If it is not enabled, a warning message is printed in the Ansible output.

Enabling FIPS at boot time requires additional manual configuration. Refer to Chapter 7. Federal Standards and Regulations in the Red Hat documentation for more details. Section 7.1.1 contains the steps required for updating the bootloader configuration and regenerating the initramfs.

Note: This change only applies to CentOS, Red Hat Enterprise Linux, openSUSE Leap and SUSE Linux Enterprise. Ubuntu does not use dracut by default and the process for enabling the FIPS functionality at boot time is more complex.

V-72075

- **Summary**: The system must not allow removable media to be used as the boot loader unless approved.
- **Severity:** Medium
- **Implementation Status:** Exception - Initial Provisioning

Deployer/Auditor notes

When a server is initially provisioned, deployers should avoid storing the boot loader on removable media. It is not possible to change this via automated tasks.

V-72209

- **Summary**: The system must send rsyslog output to a log aggregation server.
- **Severity:** Medium
- **Implementation Status:** Verification Only

Deployer/Auditor notes

The tasks in the security role check for uncommented lines in the rsyslog configuration that contain `@` or `@@`, which signifies that a remote logging configuration is in place. If these lines are not found, a warning message is printed in the Ansible output.

V-72211

- **Summary**: The rsyslog daemon must not accept log messages from other servers unless the server is being used for log aggregation.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deployers must take manual steps to add or remove syslog reception configuration lines depending on a servers role:

- If the server is a log aggregation server, deployers must configure the server to receive syslog output from the other servers via TCP connections.
- If the server is not a log aggregation server, deployers must configure the server so that it does not accept syslog output from other servers.

V-72213

- **Summary**: The system must use a virus scan program.
- **Severity:** High
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that a virus scanner is installed and running, but the value of a virus scanner within an OpenStack control plane or on a hypervisor is negligible in many cases. In addition, the disk I/O impact of a virus scanner can impact a production environment negatively.

The security role has tasks to deploy ClamAV with automatic updates, but the tasks are disabled by default.

Deployers can enable the ClamAV virus scanner by setting the following Ansible variable:

```
security_enable_virus_scanner: yes
```

> **Warning:** The ClamAV packages are provided in the EPEL repository. Setting the `security_enable_virus_scanner` will also cause the EPEL repository to be installed by the role.

V-72215

- **Summary**: The system must update the virus scan program every seven days or more frequently.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

By default, CentOS 7, Red Hat Enterprise Linux 7, openSUSE Leap and SUSE Linux Enterprise 12 check for virus database updates 12 times a day. Ubuntu servers have a default of 24 checks per day.

The tasks in the security role do not adjust these defaults as they are more secure than the STIGs requirement.

V-72219

- **Summary**: The host must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management Component Local Service Assessment (PPSM CLSA) and vulnerability assessments.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deployers should review each firewall rule on a regular basis to ensure that each port is open for a valid reason.

V-72223

- **Summary**: All network connections associated with a communication session must be terminated at the end of the session or after 10 minutes of inactivity from the user at a command prompt, except to fulfill documented and validated mission requirements.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks in the security role set a 600 second (10 minute) timeout for network connections associated with a communication session. Deployers can change the timeout value by setting the following Ansible variable:

```
# Example: shorten the timeout to 5 minutes (300 seconds)
security_rhel7_session_timeout: 300
```

V-72269

- **Summary**: The operating system must, for networked systems, synchronize clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks in the security role make the following changes on each host:

- The `chrony` package is installed.
- The service (`chronyd` on Red Hat, CentOS, SLE and openSUSE Leap, `chrony` on Ubuntu) is started and enabled at boot time.
- A configuration file template is deployed that includes `maxpoll 10` on each server line.

Deployers can opt out of these changes by setting the following Ansible variable:

```
security_rhel7_enable_chrony: no
```

Note: Although the STIG mentions the traditional `ntpd` service, this role uses `chrony`, which is a more modern implementation.

V-72271

- **Summary**: The operating system must protect against or limit the effects of Denial of Service (DoS) attacks by validating the operating system is implementing rate-limiting measures on impacted network interfaces.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Although the STIG requires that incoming TCP connections are rate limited with `firewalld`, this setting can cause problems with certain applications which handle large amounts of TCP connections. Therefore, the tasks in the security role do not apply the rate limit by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_enable_firewalld_rate_limit: yes
```

The STIG recommends a limit of 25 connection per minute and allowing bursts up to 100 connections. Both of these options are adjustable with the following Ansible variables:

```
security_enable_firewalld_rate_limit_per_minute: 25
security_enable_firewalld_rate_limit_burst: 100
```

Warning: Deployers should test rate limiting in a non-production environment first before applying it to production systems. Ensure that the application running on the system is receiving a large volume of requests so that the rule can be thoroughly tested.

V-72273

- **Summary**: The operating system must enable an application firewall, if available.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that a firewall is configured on each server. This might be disruptive to some environments since the default firewall policy for `firewalld` is very restrictive. Therefore, the tasks in the security role do not install or enable the `firewalld` daemon by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_enable_firewalld: yes
```

Warning: Deployers must pre-configure `firewalld` or copy over a working XML file in `/etc/firewalld/zones/` from another server. The default firewalld restrictions on Ubuntu, CentOS, Red Hat Enterprise Linux and openSUSE Leap are highly restrictive.

V-72281

- **Summary**: For systems using DNS resolution, at least two name servers must be configured.
- **Severity:** Low
- **Implementation Status:** Implemented

Deployer/Auditor notes

If a server has fewer than two nameservers configured in `/etc/resolv.conf`, a warning is printed in the Ansible output.

V-72295

- **Summary**: Network interfaces must not be in promiscuous mode.
- **Severity:** Medium
- **Implementation Status:** Verification Only

Deployer/Auditor notes

All interfaces are examined to ensure they are not in promiscuous mode. A warning message is printed in the Ansible output if any promiscuous interfaces are found.

V-72297

- **Summary**: The system must be configured to prevent unrestricted mail relaying.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `smtpd_client_restrictions` configuration in postfix is set to `permit_mynetworks, reject` to meet the STIGs requirements.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_restrict_mail_relaying: no
```

V-72305

- **Summary**: If the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon must be configured to operate in secure mode.
- **Severity:** Medium
- **Implementation Status:** Verification Only

Deployer/Auditor notes

The tasks in the security role examine the TFTP server configuration file (if it exists) to verify that the secure operation flag (`-s`) is listed on the `server_args` line. If it is missing, a warning message is printed in the Ansible output.

V-72311

- **Summary**: The Network File System (NFS) must be configured to use RPCSEC_GSS.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deployers using NFS should examine their mounts to ensure `krb5:krb5i:krb5p` is provided with the `sec` option. Kerberos must be installed and configured before making the change.

V-72313

- **Summary**: SNMP community strings must be changed from the default.
- **Severity:** High
- **Implementation Status:** Verification Only

Deployer/Auditor notes

The tasks in the security role examine the contents of the `/etc/snmp/snmpd.conf` file (if it exists) and search for the default community strings: `public` and `private`. If either default string is found, a message is printed in the Ansible output.

V-72315

- **Summary**: The system access control program must be configured to grant or deny system access to specific hosts and services.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

The `firewalld` service is optionally enabled and configured in the tasks for another STIG control:

- *The operating system must enable an application firewall, if available. (V-72273)*

Deployers should review their `firewalld` ruleset regularly to ensure that each firewall rule is specific as possible. Each rule should allow the smallest number of hosts to access the smallest number of services.

V-72317

- **Summary**: The system must not have unauthorized IP tunnels configured.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deployers should review all tunneled connections on a regular basis to ensure each is valid and properly secured. This requires careful verification that cannot be done with automated Ansible tasks.

V-73161

- **Summary**: File systems that are being imported via Network File System (NFS) must be mounted to prevent binary files from being executed.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deployers should review their NFS mounts to ensure they are mounted with the `noexec` option. Deployers should skip this change if they execute applications from NFS mounts.

V-73177

- **Summary**: Wireless network adapters must be disabled.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

Deployers should review the configuration of any wireless networking device connected to the system to ensure it must be enabled. The STIG requires that all wireless network devices are enabled unless required.

V-77819

- **Summary**: The operating system must uniquely identify and must authenticate users using multifactor authentication via a graphical user logon.
- **Severity:** Medium
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

The STIG requires that multifactor authentication is used for graphical user logon, but this change requires custom configuration based on the authentication solution that is used.

Deployers should review the available options, such as traditional smartcards, USB devices (such as Yubikeys), or software token systems, and use one of these solutions on each system.

3.4.10 packages - Package managers

Package managers provide a convenient, secure method for installing and upgrading applications on a system. They must be configured properly to ensure that software is carefully verified before it is installed.

Overview

Lorem ipsum

STIG requirements

All of the tasks for these STIG requirements are included in `tasks/rhel7stig/packages.yml`.

V-71855

- **Summary**: The cryptographic hash of system files and commands must match vendor values.
- **Severity:** High
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Ansible tasks will check the `rpm -Va` output (on CentOS, RHEL, openSUSE and SLE) or the output of `debsums` (on Ubuntu) to see if any files installed from packages have been altered. The tasks will print a list of files that have changed since their package was installed.

Deployers should be most concerned with any checksum failures for binaries and their libraries. These are most often a sign of system compromise or poor system administration practices.

Configuration files may appear in the list as well, but these are often less concerning since some of these files are adjusted by the security role itself.

Generating and validating checksums of all files installed by packages consume a significant amount of disk I/O and could impact the performance of a production system. It can also delay the playbooks completion. Therefore, the check is disabled by default.

Deployers can enable the check by setting the following Ansible variable:

```
security_check_package_checksums: yes
```

V-71897

- **Summary**: The operating system must have the screen package installed.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The role will ensure that the `screen` package is installed.

V-71967

- **Summary**: The rsh-server package must not be installed.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

The role will remove the `rsh-server` package from the system if it is installed. Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_rsh_server: no
```

V-71969

- **Summary**: The ypserv package must not be installed.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

The role will remove the NIS server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `ypserv`
- Ubuntu: `nis`
- openSUSE Leap: `ypserv`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_ypserv: no
```

V-71977

- **Summary**: The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components from a repository without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

On Ubuntu systems, the tasks check for the `AllowUnauthenticated` string anywhere in the apt configuration files found within `/etc/apt/apt.conf.d/`. If the string is found, a warning is printed on the console.

On CentOS 7 systems, the tasks set the `gpgcheck` option to 1 in the `/etc/yum.conf` file. This enables GPG checks for all packages installed with `yum`.

On openSUSE Leap systems, the tasks set the `gpgcheck` option to 1 in the `/etc/zypp/zypp.conf` file. This enables GPG checks for all packages installed with `zypper`.

Setting `security_enable_gpgcheck_packages` to `no` will skip the `AllowUnauthenticated` string check on Ubuntu and it will set `gpgcheck=0` in `/etc/yum.conf` or `/etc/zypp/zypp.conf` on CentOS and openSUSE Leap systems respectively.

V-71979

- **Summary**: The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

On Ubuntu systems, the tasks comment out the `no-debsig` configuration line in `/etc/dpkg/dpkg.cfg`. This causes `dpkg` to verify GPG signatures for all packages that are installed locally.

On CentOS 7 systems, the tasks set the `localpkg_gpgcheck` option to 1 in the `/etc/yum.conf` file. This enables GPG checks for all packages installed locally with `yum`.

On openSUSE Leap systems, the tasks set the `gpgcheck` option to 1 in the `/etc/zypp/zypp.conf` file. This enables GPG checks for all packages installed with `zypper`.

Setting `security_enable_gpgcheck_packages_local` to `no` will skip the `no-debsig` adjustment on Ubuntu and it will set `local_gpgcheck=0` in `/etc/yum.conf` on CentOS systems. Similarly, on openSUSE Leap systems, it will set `gpgcheck=0` in `/etc/zypp/zypp.conf`.

V-71981

- **Summary**: The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of packages without verification of the repository metadata.
- **Severity:** High
- **Implementation Status:** Opt-In

Deployer/Auditor notes

The STIG requires that repository XML files are verified during `yum` runs.

> **Warning:** This setting is disabled by default because it can cause issues with CentOS systems and prevent them from retrieving repository information. Deployers who choose to enable this setting should test it thoroughly on non-production environments before applying it to production systems.

Deployers can override this default and opt in for the change by setting the following Ansible variable:

```
security_enable_gpgcheck_repo: yes
```

V-71987

- **Summary**: The operating system must remove all software components after updated versions have been installed.
- **Severity:** Low
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Although the STIG requires that dependent packages are removed automatically when a package is removed, this can cause problems with certain packages, especially kernels. Deployers must opt in to meet the requirements of this STIG control.

Deployers should set the following variable to enable automatic dependent package removal:

```
security_package_clean_on_remove: yes
```

V-71997

- **Summary**: The operating system must be a vendor supported release.
- **Severity:** High
- **Implementation Status:** Exception - Manual Intervention

Deployer/Auditor notes

The STIG requires that the current release of the operating system is still supported and is actively receiving security updates. Deployers are urged to stay current with the latest releases from Ubuntu, SUSE, CentOS and Red Hat.

The following links provide more details on end of life (EOL) dates for the distributions supported by this role:

- Ubuntu releases
- CentOS EOL dates
- Red Hat Enterprise Linux Life Cycle
- openSUSE EOL dates
- SUSE Linux Enterprise

V-71999

- **Summary**: Vendor packaged system security patches and updates must be installed and up to date.
- **Severity:** Medium
- **Implementation Status:** Opt-In

Deployer/Auditor notes

Although the STIG requires that security patches and updates are applied when they are made available, this might be disruptive to some systems. Therefore, the tasks in the security role will not configure automatic updates by default.

Deployers can opt in for automatic package updates by setting the following Ansible variable:

```
security_rhel7_automatic_package_updates: yes
```

When enabled, the tasks install and configure `yum-cron` on CentOS and Red Hat Enterprise Linux. On Ubuntu systems, the `unattended-upgrades` package is installed and configured. On openSUSE Leap and SUSE Linux Enterprise systems, a daily cronjob is installed.

V-72077

- **Summary**: The telnet-server package must not be installed.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

The role will remove the telnet server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `telnet-server`
- Ubuntu: `telnetd`
- openSUSE Leap: `telnet-server`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_telnet_server: no
```

V-72233

- **Summary**: All networked systems must have SSH installed.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The STIG requires that every system has an ssh client and server installed. The role installs the following packages:

- CentOS: `openssh-clients`, `openssh-server`
- Ubuntu: `openssh-client`, `openssh-server`
- openSUSE Leap: `openssh`

V-72299

- **Summary**: A File Transfer Protocol (FTP) server package must not be installed unless needed.
- **Severity:** High
- **Implementation Status:** Not Implemented

Deployer/Auditor notes

This STIG is not yet implemented.

V-72301

- **Summary**: The Trivial File Transfer Protocol (TFTP) server package must not be installed if not required for operational support.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

The role will remove the TFTP server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `tftp-server`
- Ubuntu: `tftpd`
- openSUSE Leap: `tftp`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_tftp_server: no
```

V-72307

- **Summary**: An X Windows display manager must not be installed unless approved.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The role will remove the xorg server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `xorg-x11-server-Xorg`
- Ubuntu: `xorg-xserver`
- openSUSE Leap: `xorg-x11-server`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_xorg: no
```

V-72417

- **Summary**: The operating system must have the required packages for multifactor authentication installed.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The STIG requires that the following multifactor authentication packages are installed:

- authconfig
- authconfig-gtk
- esc
- pam_pkcs11

These packages are benign if they are not needed on a system, but `authconfig-gtk` may cause some graphical dependencies to be installed which may not be needed on some systems. The security role installs these packages, but it skips the installation of `authconfig-gtk`. Deployers can install the graphical package manually if needed.

3.4.11 sshd - SSH daemon

The SSH daemon, `sshd`, provides secure, encrypted access to Linux servers.

Overview

The STIG has several requirements for ssh server configuration and these requirements are applied by default by the role. To opt-out or change these requirements, see the section under the `## ssh server (sshd)` comment in `defaults/main.yml`.

Deviation for PermitRootLogin

There is one deviation from the STIG for the `PermitRootLogin` configuration option. The STIG requires that direct root logins are disabled, and this is the recommended setting for secure production environments.

However, this can cause problems in some existing environments and the default for the role is to set it to `yes` (direct root logins allowed).

STIG requirements

All of the tasks for these STIG requirements are included in `tasks/rhel7stig/sshd.yml`.

V-71939

- **Summary**: The SSH daemon must not allow authentication using an empty password.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `PermitEmptyPasswords` configuration will be set to `no` in `/etc/ssh/sshd_config` and sshd will be restarted. This disallows logins over ssh for users with a empty or null password set.

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_sshd_disallow_empty_password: no
```

V-71957

- **Summary**: The operating system must not allow users to override SSH environment variables.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `PermitUserEnvironment` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_environment_override: no
```

V-71959

- **Summary**: The operating system must not allow a non-certificate trusted host SSH logon to the system.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `HostbasedAuthentication` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_host_based_auth: no
```

V-72221

- **Summary**: A FIPS 140-2 approved cryptographic algorithm must be used for SSH communications.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `Ciphers` configuration is set to `aes128-ctr,aes192-ctr,aes256-ctr` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can change the list of ciphers by setting the following Ansible variable:

```
security_sshd_cipher_list: 'cipher1,cipher2,cipher3'
```

V-72225

- **Summary**: The Standard Mandatory DoD Notice and Consent Banner must be displayed immediately prior to, or as part of, remote access logon prompts.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The tasks in the security role deploy a standard notice and consent banner into `/etc/motd` on each server. Ubuntu, CentOS, Red Hat Enterprise Linux, openSUSE Leap and SUSE Linux Enterprise display this banner after each successful login via ssh or the console.

Deployers can choose a different destination for the banner by setting the following Ansible variable:

```
security_sshd_banner_file: /etc/motd
```

The message is customized with the following Ansible variable:

```
security_login_banner_text: |
  ------------------------------------------------------------------------
↪--
  * WARNING                                                              ␣
↪ *
  * You are accessing a secured system and your actions will be logged along ␣
↪ *
  * with identifying information. Disconnect immediately if you are not an   ␣
↪ *
  * authorized user of this system.                                       ␣
↪ *
  ------------------------------------------------------------------------
↪--
```

V-72235

- **Summary**: All networked systems must use SSH for confidentiality and integrity of transmitted and received information as well as information during preparation for transmission.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The STIG has a requirement that the `sshd` daemon is running and enabled at boot time. The tasks in the security role ensure that these requirements are met.

Some deployers may not have `sshd` enabled on highly specialized systems and those deployers should opt out of this change by setting the following Ansible variable:

```
security_enable_sshd: no
```

Note: Setting `security_enable_sshd` to `no` causes the tasks to ignore the state of the service entirely. A setting of `no` does not stop or alter the `sshd` service.

V-72237

- **Summary**: All network connections associated with SSH traffic must terminate at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `ClientAliveInterval` configuration is set to `600` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can adjust the length of the interval by changing the following Ansible variable:

```
security_sshd_client_alive_interval: 600
```

Note: The STIG requires that `ClientAliveInterval` is set to 600 and `ClientAliveCountMax` is set to zero, which sets a 10 minute session timeout. If no data is transferred in a 10 minute period, the session is disconnected.

The `ClientAliveInterval` specifies how long the ssh daemon waits before it sends a message to the client to see if it is still alive. The `ClientAliveCountMax` specifies how many of these messages are sent without receiving a response.

Deployers should refer to *All network connections associated with SSH traffic must terminate after a period of inactivity. (V-72241)* to customize the `ClientAliveCountMax` setting.

V-72239

- **Summary**: The SSH daemon must not allow authentication using RSA rhosts authentication.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This STIG is already applied by the changes for *The SSH daemon must not allow authentication using known hosts authentication. (V-72249)*.

V-72241

- **Summary**: All network connections associated with SSH traffic must terminate after a period of inactivity.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `ClientAliveCountMax` configuration is set to `0` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can adjust the maximum amount of client alive intervals by changing the following Ansible variable.

```
security_sshd_client_alive_count_max: 0
```

Note: The STIG requires that `ClientAliveInterval` is set to 600 and `ClientAliveCountMax` is set to zero, which sets a 10 minute session timeout. If no data is transferred in a 10 minute period, the session is disconnected.

The `ClientAliveInterval` specifies how long the ssh daemon waits before it sends a message to the client to see if it is still alive. The `ClientAliveCountMax` specifies how many of these messages are sent without receiving a response.

Deployers should refer to *All network connections associated with SSH traffic must terminate at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements. (V-72237)* to customize the `ClientAliveInterval` setting.

V-72243

- **Summary**: The SSH daemon must not allow authentication using rhosts authentication.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `IgnoreRhosts` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_rhosts_auth: no
```

V-72245

- **Summary**: The system must display the date and time of the last successful account logon upon an SSH logon.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `PrintLastLog` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_print_last_log: no
```

V-72247

- **Summary**: The system must not permit direct logons to the root account using remote access via SSH.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `PermitRootLogin` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can select another setting for PermitRootLogin, from the available options `without-password`, `prohibit-password`, `forced-commands-only`, `yes`, or `no` by setting the following variable:

```
security_sshd_permit_root_login: no
```

> **Warning:** Ensure that a regular user account exists with a pathway to root access (preferably via `sudo`) before applying the security role. This configuration change disallows any direct logins with the `root` user.

V-72249

- **Summary**: The SSH daemon must not allow authentication using known hosts authentication.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `IgnoreUserKnownHosts` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_known_hosts_auth: no
```

V-72251

- **Summary**: The SSH daemon must be configured to only use the SSHv2 protocol.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `Protocol` configuration is set to `2` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_protocol: 2
```

> **Warning:** There is no reason to enable any other protocol than SSHv2. SSHv1 has multiple vulnerabilities, and it is no longer widely used.

V-72253

- **Summary**: The SSH daemon must be configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `MACs` configuration is set to `hmac-sha2-256,hmac-sha2-512` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can adjust the allowed Message Authentication Codes (MACs) by setting the following Ansible variable:

```
security_sshd_allowed_macs: 'hmac-sha2-256,hmac-sha2-512'
```

V-72255

- **Summary**: The SSH public host key files must have mode 0644 or less permissive.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The permissions on ssh public host keys is set to `0644`. If the existing permissions are more restrictive than `0644`, the tasks do not make changes to the files.

V-72257

- **Summary**: The SSH private host key files must have mode 0600 or less permissive.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The permissions on ssh private host keys is set to `0600`. If the existing permissions are more restrictive than `0600`, the tasks do not make changes to the files.

V-72259

- **Summary**: The SSH daemon must not permit Generic Security Service Application Program Interface (GSSAPI) authentication unless needed.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `GSSAPIAuthentication` setting is set to `no` to meet the requirements of the STIG.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_gssapi: no
```

V-72261

- **Summary**: The SSH daemon must not permit Kerberos authentication unless needed.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `KerberosAuthentication` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disable_kerberos_auth: no
```

V-72263

- **Summary**: The SSH daemon must perform strict mode checking of home directory configuration files.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `StrictModes` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_enable_strict_modes: no
```

V-72265

- **Summary**: The SSH daemon must use privilege separation.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `UsePrivilegeSeparation` configuration is set to `sandbox` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_enable_privilege_separation: no
```

Note: Although the STIG requires this setting to be `yes`, the `sandbox` setting actually provides more security because it enables privilege separation during the early authentication process.

V-72267

- **Summary**: The SSH daemon must not allow compression or must only allow compression after successful authentication.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `Compression` configuration is set to `delayed` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can choose another option by setting the following Ansible variable:

```
security_sshd_compression: 'no'
```

Note: The following are the available settings for `Compression` in the ssh configuration file:

- `delayed`: Compression is enabled after authentication.
- `no`: Compression is disabled.
- `yes`: Compression is enabled during authentication and during the session (not allowed by the STIG).

The `delayed` option balances security with performance and is an approved option in the STIG.

V-72289

- **Summary**: The system must prevent Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages from being accepted.
- **Severity:** Medium
- **Implementation Status:** Implemented

Deployer/Auditor notes

This control is implemented by the tasks for another control:

- *The system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages. (V-73175)*

V-72303

- **Summary**: Remote X connections for interactive users must be encrypted.
- **Severity:** High
- **Implementation Status:** Implemented

Deployer/Auditor notes

The `X11Forwarding` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_enable_x11_forwarding: no
```

3.5 Security hardening controls in detail (RHEL 7 STIG)

The ansible-hardening role follows the Red Hat Enteprise Linux 7 Security Technical Implementation Guide (STIG). The guide has over 200 controls that apply to various parts of a Linux system, and it is updated regularly by the Defense Information Systems Agency (DISA). DISA is part of the United States Department of Defense. The current version of the openstack- ansible-security role is based on release 1, version 0.2 of the Red Hat Enterprise Linux 7 STIG.

Controls are divided into groups based on the following properties:

- **Severity:**
  - *High severity* controls have a large impact on the security of a system. They also have the largest operational impact to a system and deployers should test them thoroughly in non-production environments.
  - *Low severity* controls have a smaller impact on overall security, but they are generally easier to implement with a much lower operational impact.
- **Implementation Status:**
  - *Implemented* controls are automatically implemented with automated tasks. Deployers can often opt out of these controls by adjusting Ansible variables. These variables are documented with each control below.
  - *Exceptions* denote controls that cannot be completed via automated tasks. Some of these controls must be applied during the initial provisioning process for new servers while others require manual inspection of the system.
  - *Opt in* controls have automated tasks written, but these tasks are disabled by default. These controls are often disabled because they could cause disruptions on a production system, or they do not provide a significant security benefit. Each control can be enabled with Ansible variables and these variables are documented with each control below.
  - *Verification only* controls have tasks that verify that a control is met. These tasks do not take any action on the system, but they often display debug output with additional instructions for deployers.
- **Tag:**

  - Each control has a tag applied, and the tags allow deployers to select specific groups of controls to apply. For example, deployers can apply the controls for the ssh daemon by using `--tags sshd` on the Ansible command line.
  - Tags also make it easier to navigate through the Ansible tasks in the code itself. For example, all tasks tagged with `auditd` are found within `tasks/rhel7stig/auditd.yml`.

Although the STIG is specific to Red Hat Enterprise Linux 7, it also applies to CentOS 7 systems. In addition, almost all of the controls are easily translated for Ubuntu 16.04, openSUSE Leap and SUSE Linux Enterprise 12. Any deviations during translation are noted within the documentation below.

3.5.1 STIG Controls by Severity

Contents

High (29 controls)

The file permissions, ownership, and group membership of system files and commands must match the vendor values. (V-71849)

STIG Description

Severity: High

Discretionary access control is weakened if a user or group has access permissions to system files and directories greater than the default.

Satisfies: SRG-OS-000257-GPOS-00098, SRG-OS-000278-GPOS-00108

Deployer/Auditor notes

Implementation Status: Opt-In

Note: Ubuntus `debsums` command does not support verification of permissions and ownership for files that were installed by packages. This STIG requirement will be skipped on Ubuntu.

The STIG requires that all files owned by an installed package must have their permissions, user ownership, and group ownership set back to the vendor defaults.

Although this is a good practice, it can cause issues if permissions or ownership were intentionally set after the packages were installed. It also causes significant delays in deployments. Therefore, this STIG is not applied by default.

Deployers may opt in for the change by setting the following Ansible variable:

```
security_reset_perm_ownership: yes
```

The cryptographic hash of system files and commands must match vendor values. (V-71855)

STIG Description

Severity: High

Without cryptographic integrity protections, system command and files can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Deployer/Auditor notes

Implementation Status: Opt-In

Ansible tasks will check the `rpm -Va` output (on CentOS, RHEL, openSUSE and SLE) or the output of `debsums` (on Ubuntu) to see if any files installed from packages have been altered. The tasks will print a list of files that have changed since their package was installed.

Deployers should be most concerned with any checksum failures for binaries and their libraries. These are most often a sign of system compromise or poor system administration practices.

Configuration files may appear in the list as well, but these are often less concerning since some of these files are adjusted by the security role itself.

Generating and validating checksums of all files installed by packages consume a significant amount of disk I/O and could impact the performance of a production system. It can also delay the playbooks completion. Therefore, the check is disabled by default.

Deployers can enable the check by setting the following Ansible variable:

```
security_check_package_checksums: yes
```

The system must not have accounts configured with blank or null passwords. (V-71937)

STIG Description

Severity: High

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Deployer/Auditor notes

Implementation Status: Implemented

The Ansible tasks will ensure that PAM is configured to disallow logins from accounts with null or blank passwords. This involves removing a single option from one of the PAM configuration files:

- CentOS or RHEL: removes `nullok` from `/etc/pam.d/system-auth`
- Ubuntu: removes `nullok_secure` from `/etc/pam.d/common-auth`
- openSUSE Leap or SLE: remove `nullok` from `/etc/pam.d/common-auth` and `/etc/pam.d/common-password`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_disallow_blank_password_login: no
```

The SSH daemon must not allow authentication using an empty password. (V-71939)

STIG Description

Severity: High

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Deployer/Auditor notes

Implementation Status: Implemented

The `PermitEmptyPasswords` configuration will be set to `no` in `/etc/ssh/sshd_config` and sshd will be restarted. This disallows logins over ssh for users with a empty or null password set.

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_sshd_disallow_empty_password: no
```

The operating system must not allow an unattended or automatic logon to the system via a graphical user interface. (V-71953)

STIG Description

Severity: High

Failure to restrict system access to authenticated users negatively impacts operating system security.

Deployer/Auditor notes

Implementation Status: Implemented

If `AutomaticLoginEnable=true` exists in the gdm configuration file, `/etc/gdm/custom.conf`, the configuration will removed. This disallows automatic logins for gdm and requires a user to complete the username and password prompts.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_disable_gdm_automatic_login: no
```

The operating system must not allow an unrestricted logon to the system. (V-71955)

STIG Description

Severity: High

Failure to restrict system access to authenticated users negatively impacts operating system security.

Deployer/Auditor notes

Implementation Status: Implemented

If `TimedLoginEnable=true` exists in the gdm configuration file, `/etc/gdm/custom.conf`, the configuration will removed. This disallows timed logins for guest users in gdm.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_disable_gdm_timed_login: no
```

Systems with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes. (V-71961)

STIG Description

Severity: High

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that GRUB 2 asks for a password whenever a user attempts to enter single-user or maintenance mode, this change might be disruptive in an emergency situation. Therefore, this change is not applied by default.

Deployers that wish to opt in for this change should set two Ansible variables:

```
security_require_grub_authentication: yes
security_grub_password_hash: grub.pbkdf2.sha512.10000.7B21785BEAFEE3AC...
```

The default password set in the security role is secrete, but deployers should set a much more secure password for production environments. Use the `grub2-mkpasswd-pbkdf2` command to create a password hash string and use it as the value for the Ansible variable `security_grub_password_hash`.

> **Warning:** This change must be tested in a non-production environment first. Requiring authentication in GRUB 2 without proper communication to users could cause extensive delays in emergency situations.

Systems using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes. (V-71963)

STIG Description

Severity: High

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Deployer/Auditor notes

Implementation Status: Opt-In

The tasks in the security role for V-71961 will also apply changes to systems that use UEFI. For more details, refer to the following documentation:

- *Systems with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes. (V-71961)*

The rsh-server package must not be installed. (V-71967)

STIG Description

Severity: High

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The rsh-server service provides an unencrypted remote access service that does not provide for the confidentiality and integrity of user passwords or the remote session and has very weak authentication.

If a privileged user were to log on using this service, the privileged user password could be compromised.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the `rsh-server` package from the system if it is installed. Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_rsh_server: no
```

The ypserv package must not be installed. (V-71969)

STIG Description

Severity: High

Removing the ypserv package decreases the risk of the accidental (or intentional) activation of NIS or NIS+ services.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the NIS server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `ypserv`
- Ubuntu: `nis`
- openSUSE Leap: `ypserv`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_ypserv: no
```

The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components from a repository without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization. (V-71977)

STIG Description

Severity: High

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Deployer/Auditor notes

Implementation Status: Implemented

On Ubuntu systems, the tasks check for the `AllowUnauthenticated` string anywhere in the apt configuration files found within `/etc/apt/apt.conf.d/`. If the string is found, a warning is printed on the console.

On CentOS 7 systems, the tasks set the `gpgcheck` option to 1 in the `/etc/yum.conf` file. This enables GPG checks for all packages installed with `yum`.

On openSUSE Leap systems, the tasks set the `gpgcheck` option to 1 in the `/etc/zypp/zypp.conf` file. This enables GPG checks for all packages installed with `zypper`.

Setting `security_enable_gpgcheck_packages` to `no` will skip the `AllowUnauthenticated` string check on Ubuntu and it will set `gpgcheck=0` in `/etc/yum.conf` or `/etc/zypp/zypp.conf` on CentOS and openSUSE Leap systems respectively.

The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization. (V-71979)

STIG Description

Severity: High

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Deployer/Auditor notes

Implementation Status: Implemented

On Ubuntu systems, the tasks comment out the `no-debsig` configuration line in `/etc/dpkg/dpkg.cfg`. This causes `dpkg` to verify GPG signatures for all packages that are installed locally.

On CentOS 7 systems, the tasks set the `localpkg_gpgcheck` option to `1` in the `/etc/yum.conf` file. This enables GPG checks for all packages installed locally with `yum`.

On openSUSE Leap systems, the tasks set the `gpgcheck` option to `1` in the `/etc/zypp/zypp.conf` file. This enables GPG checks for all packages installed with `zypper`.

Setting `security_enable_gpgcheck_packages_local` to `no` will skip the `no-debsig` adjustment on Ubuntu and it will set `local_gpgcheck=0` in `/etc/yum.conf` on CentOS systems. Similarly, on openSUSE Leap systems, it will set `gpgcheck=0` in `/etc/zypp/zypp.conf`.

The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of packages without verification of the repository metadata. (V-71981)

STIG Description

Severity: High

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This ensures the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved Certificate Authority.

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that repository XML files are verified during `yum` runs.

> **Warning:** This setting is disabled by default because it can cause issues with CentOS systems and prevent them from retrieving repository information. Deployers who choose to enable this setting should test it thoroughly on non-production environments before applying it to production systems.

Deployers can override this default and opt in for the change by setting the following Ansible variable:

```
security_enable_gpgcheck_repo: yes
```

The operating system must enable SELinux. (V-71989)

STIG Description

Severity: High

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role enable the appropriate Linux Security Module (LSM) for the operating system.

For Ubuntu, openSUSE and SUSE Linux Enterprise 12 systems, AppArmor is installed and enabled. This change takes effect immediately.

For CentOS or Red Hat Enterprise Linux systems, SELinux is enabled (in enforcing mode) and its user tools are automatically installed. If SELinux is not in enforcing mode already, a reboot is required to enable SELinux and relabel the filesystem.

> **Warning:** Relabeling a filesystem takes time and the server must be offline for the relabeling to complete. Filesystems with large amounts of files and filesystems on slow disks will cause the relabeling process to take more time.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_enable_linux_security_module: no
```

The operating system must enable the SELinux targeted policy. (V-71991)

STIG Description

Severity: High

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Deployer/Auditor notes

Implementation Status: Implemented

The SELinux targeted policy is enabled on CentOS 7 and Red Hat systems. AppArmor only has one set of policies, so this change has no effect on Ubuntu, openSUSE Leap and SUSE systems running AppArmor.

For more information on this change and how to opt out, refer to *The operating system must enable SELinux. (V-71989)*.

The x86 Ctrl-Alt-Delete key sequence must be disabled. (V-71993)

STIG Description

Severity: High

A locally logged-on user who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In the GNOME graphical environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role disable the control-alt-delete key sequence by masking its systemd service unit.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_disable_ctrl_alt_delete: no
```

The operating system must be a vendor supported release. (V-71997)

STIG Description

Severity: High

An operating system release is considered supported if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The STIG requires that the current release of the operating system is still supported and is actively receiving security updates. Deployers are urged to stay current with the latest releases from Ubuntu, SUSE, CentOS and Red Hat.

The following links provide more details on end of life (EOL) dates for the distributions supported by this role:

- Ubuntu releases
- CentOS EOL dates
- Red Hat Enterprise Linux Life Cycle
- openSUSE EOL dates

- SUSE Linux Enterprise

The root account must be the only account having unrestricted access to the system. (V-72005)

STIG Description

Severity: High

If an account other than root also has a User Identifier (UID) of 0, it has root authority, giving that account unrestricted access to the entire operating system. Multiple accounts with a UID of 0 afford an opportunity for potential intruders to guess a password for a privileged account.

Deployer/Auditor notes

Implementation Status: Implemented

If an account with UID 0 other than `root` exists on the system, the playbook will fail with an error message that includes the other accounts which have a UID of 0.

Deployers are strongly urged to keep only one account with UID 0, `root`, and to use `sudo` any situations where root access is required.

The operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. (V-72067)

STIG Description

Severity: High

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000185-GPOS-00079, SRG-OS-000396-GPOS-00176, SRG-OS-000405-GPOS-00184, SRG-OS-000478-GPOS-00223

Deployer/Auditor notes

Implementation Status: Implemented - Red Hat And Suse Only

The tasks in the Ansible role install the `dracut-fips` (RHEL and SLE) and `dracut-fips-aesni` (RHEL) packages and check to see if FIPS is enabled on the system. If it is not enabled, a warning message is printed in the Ansible output.

Enabling FIPS at boot time requires additional manual configuration. Refer to Chapter 7. Federal Standards and Regulations in the Red Hat documentation for more details. Section 7.1.1 contains the steps required for updating the bootloader configuration and regenerating the initramfs.

Note: This change only applies to CentOS, Red Hat Enterprise Linux, openSUSE Leap and SUSE Linux Enterprise. Ubuntu does not use dracut by default and the process for enabling the FIPS functionality at boot time is more complex.

The telnet-server package must not be installed. (V-72077)

STIG Description

Severity: High

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the telnet server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `telnet-server`
- Ubuntu: `telnetd`
- openSUSE Leap: `telnet-server`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_telnet_server: no
```

Auditing must be configured to produce records containing information to establish what type of events occurred, where the events occurred, the source of the events, and the outcome of the events.

These audit records must also identify individual identities of group account users. (V-72079)

STIG Description

Severity: High

Without establishing what type of events occurred, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in the operating system audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured operating system.

Satisfies: SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000042-GPOS-00021, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role start the audit daemon immediately and ensure that it starts at boot time.

The system must use a virus scan program. (V-72213)

STIG Description

Severity: High

Virus scanning software can be used to protect a system from penetration from computer viruses and to limit their spread through intermediate systems.

The virus scanning software should be configured to perform scans dynamically on accessed files. If this capability is not available, the system must be configured to scan, at a minimum, all altered files on the system on a daily basis.

If the system processes inbound SMTP mail, the virus scanner must be configured to scan all received mail.

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that a virus scanner is installed and running, but the value of a virus scanner within an OpenStack control plane or on a hypervisor is negligible in many cases. In addition, the disk I/O impact of a virus scanner can impact a production environment negatively.

The security role has tasks to deploy ClamAV with automatic updates, but the tasks are disabled by default.

Deployers can enable the ClamAV virus scanner by setting the following Ansible variable:

```
security_enable_virus_scanner: yes
```

> **Warning:** The ClamAV packages are provided in the EPEL repository. Setting the `security_enable_virus_scanner` will also cause the EPEL repository to be installed by the role.

The SSH daemon must be configured to only use the SSHv2 protocol. (V-72251)

STIG Description

Severity: High

SSHv1 is an insecure implementation of the SSH protocol and has many well-known vulnerability exploits. Exploits of the SSH daemon could provide immediate root access to the system.

Satisfies: SRG-OS-000074-GPOS-00042, SRG-OS-000480-GPOS-00227

Deployer/Auditor notes

Implementation Status: Implemented

The `Protocol` configuration is set to `2` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_protocol: 2
```

> **Warning:** There is no reason to enable any other protocol than SSHv2. SSHv1 has multiple vulnerabilities, and it is no longer widely used.

There must be no .shosts files on the system. (V-72277)

STIG Description

Severity: High

The .shosts files are used to configure host-based authentication for individual users or the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Deployer/Auditor notes

Implementation Status: Opt-In

The tasks in the security role examine the filesystem for any `.shosts` or `shosts.equiv` files. If they are found, they are deleted.

The search for these files will take a very long time on systems with slow disks or systems with a large amount of files. Therefore, this task is skipped by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_remove_shosts_files: yes
```

There must be no shosts.equiv files on the system. (V-72279)

STIG Description

Severity: High

The shosts.equiv files are used to configure host-based authentication for the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *There must be no .shosts files on the system. (V-72277)*

A File Transfer Protocol (FTP) server package must not be installed unless needed. (V-72299)

STIG Description

Severity: High

The FTP service provides an unencrypted remote access that does not provide for the confidentiality and integrity of user passwords or the remote session. If a privileged user were to log on using this service, the privileged user password could be compromised. SSH or other encrypted file transfer methods must be used in place of this service.

Deployer/Auditor notes

Implementation Status: Not Implemented

This STIG is not yet implemented.

The Trivial File Transfer Protocol (TFTP) server package must not be installed if not required for operational support. (V-72301)

STIG Description

Severity: High

If TFTP is required for operational support (such as the transmission of router configurations) its use must be documented with the Information System Security Officer (ISSO), restricted to only authorized personnel, and have access control rules established.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the TFTP server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `tftp-server`
- Ubuntu: `tftpd`
- openSUSE Leap: `tftp`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_tftp_server: no
```

Remote X connections for interactive users must be encrypted. (V-72303)

STIG Description

Severity: High

Open X displays allow an attacker to capture keystrokes and execute commands remotely.

Deployer/Auditor notes

Implementation Status: Implemented

The `X11Forwarding` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_enable_x11_forwarding: no
```

SNMP community strings must be changed from the default. (V-72313)

STIG Description

Severity: High

Whether active or not, default Simple Network Management Protocol (SNMP) community strings must be changed to maintain security. If the service is running with the default authenticators, anyone can gather data about the system and the network and use the information to potentially compromise the integrity of the system or network(s). It is highly recommended that SNMP version 3 user authentication and message encryption be used in place of the version 2 community strings.

Deployer/Auditor notes

Implementation Status: Verification Only

The tasks in the security role examine the contents of the `/etc/snmp/snmpd.conf` file (if it exists) and search for the default community strings: `public` and `private`. If either default string is found, a message is printed in the Ansible output.

Medium (198 controls)

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon. (V-71859)

STIG Description

Severity: Medium

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is␣
↪provided for USG-authorized use only.
```

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

```
-The USG routinely intercepts and monitors communications on this IS for␣
↪purposes including, but not limited to, penetration testing, COMSEC␣
↪monitoring, network operations and defense, personnel misconduct (PM), law␣
↪enforcement (LE), and counterintelligence (CI) investigations.
```

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interestsnot for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
"I've read  consent to terms in IS user agreem't."
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role configure `dconf` to display a login banner each time a graphical session starts on the system. The default banner message set by the role is:

> You are accessing a secured system and your actions will be logged along with identifying information. Disconnect immediately if you are not an authorized user of this system.

Deployers can customize this message by setting an Ansible variable:

```
security_enable_graphical_login_message_text: >
    This is a customized banner message.
```

Warning: The dconf configuration does not support multi-line strings. Ensure that `security_enable_graphical_login_message_text` contains a single line of text.

In addition, deployers can opt out of displaying a login banner message by changing `security_enable_graphical_login_message` to `no`.

The operating system must display the approved Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon. (V-71861)

STIG Description

Severity: Medium

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is␣
↪provided for USG-authorized use only.
```

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

```
-The USG routinely intercepts and monitors communications on this IS for␣
↪purposes including, but not limited to, penetration testing, COMSEC␣
↪monitoring, network operations and defense, personnel misconduct (PM), law␣
↪enforcement (LE), and counterintelligence (CI) investigations.
```

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interestsnot for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Deployer/Auditor notes

Implementation Status: Implemented

The security role configures a login banner for graphical logins using `dconf`. Deployers can opt out of this change by setting the following Ansible variable:

```
security_enable_graphical_login_message: no
```

The message is customized by setting another Ansible variable:

```
security_enable_graphical_login_message_text: >
    You are accessing a secured system and your actions will be logged along
    with identifying information. Disconnect immediately if you are not an
    authorized user of this system.
```

Note: The space available for the graphical banner is relatively short. Deployers should limit the length of their graphical login banners to the shortest length possible.

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a command line user logon. (V-71863)

STIG Description

Severity: Medium

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is␣
↪provided for USG-authorized use only.
```

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

```
-The USG routinely intercepts and monitors communications on this IS for␣
↪purposes including, but not limited to, penetration testing, COMSEC␣
↪monitoring, network operations and defense, personnel misconduct (PM), law␣
↪enforcement (LE), and counterintelligence (CI) investigations.
```

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interestsnot for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
"I've read  consent to terms in IS user agreem't."
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007

Deployer/Auditor notes

Implementation Status: Implemented

The security role already deploys a login banner for console logins with tasks from another STIG:

- *The Standard Mandatory DoD Notice and Consent Banner must be displayed immediately prior to, or as part of, remote access logon prompts. (V-72225)*

The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. (V-71891)

STIG Description

Severity: Medium

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

Regardless of where the session lock is determined and implemented, once invoked, the session lock must remain in place until the user reauthenticates. No other activity aside from reauthentication must unlock the system.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that graphical sessions are locked when the screensaver starts and that users must re-enter credentials to restore access to the system. The screensaver lock is enabled by default if `dconf` is present on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_lock_session: no
```

The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces. (V-71893)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that the screensaver appears when a session reaches a certain period of inactivity. The tasks will enable the screensaver for inactive sessions by default.

Deployers can opt out of this change by setting an Ansible variable:

```
security_lock_session_when_inactive: no
```

The operating system must set the idle delay setting for all connection types. (V-71895)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session

prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces. (V-71893)*

The operating system must have the screen package installed. (V-71897)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The screen package allows for a session lock to be implemented and configured.

Deployer/Auditor notes

Implementation Status: Implemented

The role will ensure that the `screen` package is installed.

The operating system must initiate a session lock for the screensaver after a period of inactivity for graphical user interfaces. (V-71899)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces. (V-71893)*

The operating system must initiate a session lock for graphical user interfaces when the screensaver is activated. (V-71901)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that a graphical session is locked when the screensaver starts. This requires a user to re-enter their credentials to regain access to the system.

The tasks will set a timeout of 5 seconds after the screensaver has started before the session is locked. This gives a user a few seconds to press a key or wiggle their mouse after the screensaver appears without needing to re-enter their credentials.

Deployers can adjust this timeout by setting an Ansible variable:

```
security_lock_session_screensaver_lock_delay: 5
```

When passwords are changed or new passwords are established, the new password must contain at least one upper-case character. (V-71903)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_uppercase: no
```

When passwords are changed or new passwords are established, the new password must contain at least one lower-case character. (V-71905)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_lowercase: no
```

When passwords are changed or new passwords are assigned, the new password must contain at least one numeric character. (V-71907)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_numeric: no
```

When passwords are changed or new passwords are assigned, the new password must contain at least one special character. (V-71909)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_special: no
```

When passwords are changed a minimum of eight of the total number of characters must be changed. (V-71911)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_characters_changed: no
```

When passwords are changed a minimum of four character classes must be changed. (V-71913)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_character_classes_changed: no
```

When passwords are changed the number of repeating consecutive characters must not be more than three characters. (V-71915)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_limit_repeated_characters: no
```

When passwords are changed the number of repeating characters of the same character class must not be more than four characters. (V-71917)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_limit_repeated_character_classes: no
```

The PAM system service must be configured to store only encrypted representations of passwords. (V-71919)

STIG Description

Severity: Medium

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Deployer/Auditor notes

Implementation Status: Implemented

The PAM configuration file for password storage is checked to ensure that `sha512` is found on the `pam_unix.so` line. If `sha512` is not found, a debug message is printed in the Ansible output.

The shadow file must be configured to store only encrypted representations of passwords. (V-71921)

STIG Description

Severity: Medium

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Deployer/Auditor notes

Implementation Status: Implemented

The default password storage mechanism for Ubuntu 16.04, CentOS 7, openSUSE Leap, SUSE Linux Enterprise 12 and Red Hat Enterprise Linux 7 is `SHA512` and the tasks in the security role ensure that the default is maintained.

Deployers can configure a different password storage mechanism by setting the following Ansible variable:

```
security_password_encrypt_method: SHA512
```

> **Warning:** SHA512 is the default on most modern Linux distributions and it meets the requirement of the STIG. Do not change the value unless a system has a specific need for a different password mechanism.

User and group account administration utilities must be configured to store only encrypted representations of passwords. (V-71923)

STIG Description

Severity: Medium

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Deployer/Auditor notes

Implementation Status: Implemented - Red Hat Only

The role ensures that `crypt_style` is set to `sha512` in `/etc/libuser.conf`, which is the default for CentOS 7 and Red Hat Enterprise Linux 7.

Ubuntu, openSUSE and SUSE Linux Enterprise 12 do not use `libuser`, so this change is not applicable.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_libuser_crypt_style_sha512: no
```

Passwords for new users must be restricted to a 24 hours/1 day minimum lifetime. (V-71925)

STIG Description

Severity: Medium

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organizations policy regarding password reuse.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that all passwords have a minimum lifetime set, this can cause issue in some production environments. Therefore, deployers must opt in for this change.

Set the following Ansible variable to an integer (in days) to enable this setting:

```
security_password_min_lifetime_days: 1
```

The STIG requires the minimum lifetime for password to be one day.

Passwords must be restricted to a 24 hours/1 day minimum lifetime. (V-71927)

STIG Description

Severity: Medium

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organizations policy regarding password reuse.

Deployer/Auditor notes

Implementation Status: Opt-In

Setting a minimum password lifetime on interactive user accounts provides security benefits by limiting the frequency of password changes. However, this can cause login problems for users without proper communication and coordination.

Deployers can opt-in for this change by setting the following Ansible variable:

```
security_set_minimum_password_lifetime: yes
```

The tasks will examine each interactive user account and set the minimum password age if the existing setting is not equal to one day.

Passwords for new users must be restricted to a 60-day maximum lifetime. (V-71929)

STIG Description

Severity: Medium

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that all passwords have a maximum lifetime set, this can cause authentication disruptions in production environments if users are not aware that their password will expire. Therefore, this change is not applied by default.

Deployers can opt in for this change and provide a maximum lifetime for user passwords (in days) by setting the following Ansible variable:

```
security_password_max_lifetime_days: 60
```

The STIG requires that all passwords expire after 60 days.

Existing passwords must be restricted to a 60-day maximum lifetime. (V-71931)

STIG Description

Severity: Medium

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that a maximum password lifetime is set for all interactive user accounts, the security benefits of this configuration are debatable. The draft of NIST Publication 800-63B argues that password rotation may reduce overall security in some situations.

Deployers can opt-in for this change by setting the following Ansible variable:

```
security_set_maximum_password_lifetime: yes
```

The tasks will examine each interactive user account and set the maximum password age if the existing setting is not equal to 60 days.

Passwords must be prohibited from reuse for a minimum of five generations. (V-71933)

STIG Description

Severity: Medium

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed per policy requirements.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that five passwords are remembered to prevent re- use, this can cause issues in production environment if the change is not communicated well to users. Therefore, the tasks in the security role do not apply this change by default.

Deployers can opt in for the change and specify a number of passwords to remember by setting the following Ansible variable:

```
security_password_remember_password: 5
```

Passwords must be a minimum of 15 characters in length. (V-71935)

STIG Description

Severity: Medium

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that passwords have a minimum length of 15 characters, this change might be disruptive to users on a production system without communicating the change first. Therefore, this change is not applied by default.

Deployers can opt in for the change by setting the following Ansible variable:

```
security_pwquality_require_minimum_password_length: yes
```

The operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires. (V-71941)

STIG Description

Severity: Medium

Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Operating systems need to track periods of inactivity and disable application identifiers after zero days of inactivity.

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that user accounts are disabled when their password expires. This might be disruptive for some users or for automated processes. Therefore, the tasks in the security role do not apply this change by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_disable_account_if_password_expires: yes
```

Accounts subject to three unsuccessful logon attempts within 15 minutes must be locked for the maximum configurable period. (V-71943)

STIG Description

Severity: Medium

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Deployer/Auditor notes

Implementation Status: Opt-In - Red Hat Only

This STIG control is implemented by:

- *If three unsuccessful root logon attempts within 15 minutes occur the associated account must be locked. (V-71945)*

If three unsuccessful root logon attempts within 15 minutes occur the associated account must be locked. (V-71945)

STIG Description

Severity: Medium

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Deployer/Auditor notes

Implementation Status: Opt-In - Red Hat Only

The STIG requires that accounts with excessive failed login attempts are locked. It sets a limit of three failed attempts in a 15 minute interval and these restrictions are applied to all users (including root). Accounts cannot be automatically unlocked for seven days.

This change might cause disruptions in production environments without proper communication to users. Therefore, this change is not applied by default.

Deployers can opt in for the change by setting the following variable:

```
security_pam_faillock_enable: yes
```

There are also three configuration options that can be adjusted by setting Ansible variables:

- `security_pam_faillock_attempts`: This many failed login attempts within the specified time interval with trigger the account to lock. (STIG requirement: `3` attempts)
- `security_pam_faillock_interval`: This is the time interval (in seconds) to use when measuring excessive failed login attempts. (STIG requirement: `900` seconds)
- `security_pam_faillock_deny_root`: Set to `yes` to apply the restriction to the root user or set to `no` to exempt the root user from the account locking restrictions. (STIG requirement: `yes`)
- `security_pam_faillock_unlock_time`: This sets the time delay (in seconds) before a locked account is automatically unlocked. (STIG requirement: `604800` seconds)

Note: Ubuntu, openSUSE Leap and SUSE Linux Enterprise 12 do not provide `pam_faillock`. This change is only applied to CentOS 7 or Red Hat Enterprise Linux 7 systems.

Users must provide a password for privilege escalation. (V-71947)

STIG Description

Severity: Medium

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The STIG requires all users to authenticate when using `sudo`, but this change can be highly disruptive for automated scripts or applications that cannot perform interactive authentication. Automated edits from Ansible tasks might cause authentication disruptions on some hosts, and deployers are urged to carefully review each use of the `NOPASSWD` directive in their `sudo` configuration files.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_sudoers_nopasswd_check_enable: no
```

Users must re-authenticate for privilege escalation. (V-71949)

STIG Description

Severity: Medium

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The STIG requires all users to re-authenticate when using `sudo`, but this change can be highly disruptive for automated scripts or applications that cannot perform interactive authentication. Automated edits from Ansible tasks might cause authentication disruptions on some hosts, and deployers are urged to carefully review each use of the `!authenticate` directive in their `sudo` configuration files.

The delay between logon prompts following a failed console logon attempt must be at least four seconds. (V-71951)

STIG Description

Severity: Medium

Configuring the operating system to implement organization-wide security implementation guides and security checklists verifies compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the Ansible role set a four second delay between failed login attempts. Deployers can configure a different delay (in seconds) by setting the following Ansible variable:

```
security_shadow_utils_fail_delay: 4
```

The operating system must not allow users to override SSH environment variables. (V-71957)

STIG Description

Severity: Medium

Failure to restrict system access to authenticated users negatively impacts operating system security.

Deployer/Auditor notes

Implementation Status: Implemented

The `PermitUserEnvironment` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_environment_override: no
```

The operating system must not allow a non-certificate trusted host SSH logon to the system. (V-71959)

STIG Description

Severity: Medium

Failure to restrict system access to authenticated users negatively impacts operating system security.

Deployer/Auditor notes

Implementation Status: Implemented

The `HostbasedAuthentication` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_host_based_auth: no
```

The operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users) using multifactor authentication. (V-71965)

STIG Description

Severity: Medium

To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

```
1) Accesses explicitly identified and documented by the organization.␣
↪Organizations document specific user actions that can be performed on the␣
↪information system without identification or authentication;
```

and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000109-GPOS-00056, SRG-OS-000108-GPOS-00055, SRG-OS-000108-GPOS-00057, SRG-OS-000108-GPOS-00058

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deploying multi-factor authentication methods, including smart cards, is a complicated process that requires preparation and communication. This work is left to deployers to complete manually.

The operating system must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. (V-71971)

STIG Description

Severity: Medium

Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The tasks in the security role cannot determine the access levels of individual users.

Deployers are strongly encouraged to configure SELinux user confinement on compatible systems using `semanage login`. Refer to the Confining Existing Linux Users documentation from Red Hat for detailed information and command line examples.

A file integrity tool must verify the baseline operating system configuration at least weekly. (V-71973)

STIG Description

Severity: Medium

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating systems Information Management Officer (IMO)/Information System Security Officer (ISSO) and System Administrators (SAs) must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Deployer/Auditor notes

Implementation Status: Opt-In

Initializing the AIDE database and completing the first AIDE run causes increased disk I/O and CPU usage for extended periods. Therefore, the AIDE database is not automatically initialized by the tasks in the security role.

Deployers can enable the AIDE database initialization within the security role by setting the following Ansible variable:

```
security_rhel7_initialize_aide: yes
```

Designated personnel must be notified if baseline configurations are changed in an unauthorized manner. (V-71975)

STIG Description

Severity: Medium

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating systems Information Management Officer (IMO)/Information System Security Officer (ISSO) and System Administrators (SAs) must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Deployer/Auditor notes

Implementation Status: Implemented

The cron job for AIDE is configured to send emails to the root user after each AIDE run.

USB mass storage must be disabled. (V-71983)

STIG Description

Severity: Medium

USB mass storage permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Deployer/Auditor notes

Implementation Status: Opt-In

The tasks in the security role disable the `usb-storage` module and the change is applied the next time the server is rebooted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_disable_usb_storage: no
```

File system automounter must be disabled unless required. (V-71985)

STIG Description

Severity: Medium

Automatically mounting file systems permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Deployer/Auditor notes

Implementation Status: Implemented

The `autofs` service is stopped and disabled if it is found on the system. Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_disable_autofs: no
```

The operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files. (V-71995)

STIG Description

Severity: Medium

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Deployer/Auditor notes

Implementation Status: Opt-In - Ubuntu And Suse Only

The STIG requires that the umask for all authenticated users is `077`. This ensures that all new files and directories created by a user are accessible only by that user.

Although this change has a significant security benefit, it can cause problems for users who are not expecting the change. The security role will not adjust the umask by default.

Deployers can opt-in for the change by setting the default umask with an Ansible variable:

```
security_shadow_utils_umask: 077
```

Note: Ubuntu, openSUSE Leap and SUSE Linux Enterpsise 12 use `pam_umask` and it uses the default umask provided by the `UMASK` line in `/etc/login.defs`. The default setting on Ubuntu, openSUSE Leap and SUSE Linux Enterprise 12 systems is `022`. This allows the users group and other users on the system to read and execute files, but they cannot write to them.

CentOS and Red Hat Enterprise Linux do not use `pam_umask` and instead set a default umask of `0002` for regular users and `0022` for root. This gives the regular users group full access to newly created files, but other users cannot write to those files.

The tasks for this STIG requirement are not currently applied to CentOS and Red Hat Enterprise Linux systems. See Launchpad Bug #1656003 for more details.

Vendor packaged system security patches and updates must be installed and up to date. (V-71999)

STIG Description

Severity: Medium

Timely patching is critical for maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. However, failure to keep operating system and application software patched is a common mistake made by IT professionals. New patches are released daily, and it is often difficult for even experienced System Administrators to keep abreast of all the new patches. When new weaknesses in an operating system exist, patches are usually made available by the vendor to resolve the problems. If the most recent security patches and updates are not installed, unauthorized users may take advantage of weaknesses in the unpatched software. The lack of prompt attention to patching could result in a system compromise.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that security patches and updates are applied when they are made available, this might be disruptive to some systems. Therefore, the tasks in the security role will not configure automatic updates by default.

Deployers can opt in for automatic package updates by setting the following Ansible variable:

```
security_rhel7_automatic_package_updates: yes
```

When enabled, the tasks install and configure `yum-cron` on CentOS and Red Hat Enterprise Linux. On Ubuntu systems, the `unattended-upgrades` package is installed and configured. On openSUSE Leap and SUSE Linux Enterprise systems, a daily cronjob is installed.

The system must not have unnecessary accounts. (V-72001)

STIG Description

Severity: Medium

Accounts providing no operational purpose provide additional opportunities for system compromise. Unnecessary accounts include user accounts for individuals not requiring access to the system and application accounts for applications not installed on the system.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers are strongly urged to review the list of user accounts on each server regularly. Evaluation of user accounts must be done on a case-by-case basis and the tasks in the security role are unable to determine which user accounts are valid. Deployers must complete this work manually.

All files and directories must have a valid owner. (V-72007)

STIG Description

Severity: Medium

Unowned files and directories may be unintentionally inherited if a user is assigned the same User Identifier UID as the UID of the un-owned files.

Deployer/Auditor notes

Implementation Status: Opt-In

Searching an entire filesystem with `find` reduces system performance and might impact certain applications negatively. Therefore, the search for files and directories with an invalid owner is **disabled by default**.

Deployers can opt in for this search by setting the following Ansible variable:

```
security_search_for_invalid_owner: yes
```

Any files or directories without a valid user owner are displayed in the Ansible output.

All files and directories must have a valid group owner. (V-72009)

STIG Description

Severity: Medium

Files without a valid group owner may be unintentionally inherited if a group is assigned the same Group Identifier (GID) as the GID of the files without a valid group owner.

Deployer/Auditor notes

Implementation Status: Opt-In

Searching an entire filesystem with `find` reduces system performance and might impact certain applications negatively. Therefore, the search for files and directories with an invalid group owner is **disabled by default**.

Deployers can opt in for this search by setting the following Ansible variable:

```
security_search_for_invalid_group_owner: yes
```

Any files or directories without a valid group owner are displayed in the Ansible output.

All local interactive users must have a home directory assigned in the /etc/passwd file. (V-72011)

STIG Description

Severity: Medium

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Deployer/Auditor notes

Implementation Status: Implemented

The usernames of all users without home directories assigned are provided in the Ansible console output. Deployers should use this list of usernames to audit each system to ensure every user has a valid home directory.

All local interactive user accounts, upon creation, must be assigned a home directory. (V-72013)

STIG Description

Severity: Medium

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Deployer/Auditor notes

Implementation Status: Implemented

The `CREATE_HOME` variable is set to `yes` by the tasks in the security role. This ensures that home directories are created each time a new user account is created.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_shadow_utils_create_home: no
```

Note: On CentOS 7, Red Hat Enterprise Linux 7 systems, openSUSE Leap and SUSE Linux Enterprise 12, home directories are always created with new users by default. Home directories are not created by default on Ubuntu systems.

All local interactive user home directories defined in the /etc/passwd file must exist. (V-72015)

STIG Description

Severity: Medium

If a local interactive user has a home directory defined that does not exist, the user may be given access to the / directory as the current working directory upon logon. This could create a Denial of Service because the user would not be able to access their logon configuration files, and it may give them visibility to system files they normally would not be able to access.

Deployer/Auditor notes

Implementation Status: Implemented

Each interactive user on the system is checked to verify that their assigned home directory exists on the filesystem. If a home directory is missing, the name of the user and their assigned home directory is printed in the Ansible console output.

All local interactive user home directories must have mode 0750 or less permissive. (V-72017)

STIG Description

Severity: Medium

Excessive permissions on local interactive user home directories may allow unauthorized access to user files by other users.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that all home directories have the proper owner, group owner, and permissions, these changes might be disruptive in some environments. These tasks are not executed by default.

Deployers can opt in for the following changes to each home directory:

- Permissions are set to `0750` at a maximum. If permissions are already more restrictive than `0750`, the permissions are left unchanged.
- User ownership is set to the `UID` of the user.
- Group ownership is set to the `GID` of the user.

Deployers can opt in for these changes by setting the following Ansible variable:

```
security_set_home_directory_permissions_and_owners: yes
```

All local interactive user home directories must be owned by their respective users. (V-72019)

STIG Description

Severity: Medium

If a local interactive user does not own their home directory, unauthorized users could access or modify the users files, and the users may not be able to access their own files.

Deployer/Auditor notes

Implementation Status: Opt-In

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *All local interactive user home directories must have mode 0750 or less permissive. (V-72017)*

All local interactive user home directories must be group-owned by the home directory owners primary group. (V-72021)

STIG Description

Severity: Medium

If the Group Identifier (GID) of a local interactive users home directory is not the same as the primary GID of the user, this would allow unauthorized access to the users files, and users that share the same group may not be able to access files that they legitimately should.

Deployer/Auditor notes

Implementation Status: Opt-In

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *All local interactive user home directories must have mode 0750 or less permissive. (V-72017)*

All files and directories contained in local interactive user home directories must be owned by the owner of the home directory. (V-72023)

STIG Description

Severity: Medium

If local interactive users do not own the files in their directories, unauthorized users may be able to access them. Additionally, if files are not owned by the user, this could be an indication of system compromise.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG has requirements for ownership and permissions of files and directories in each users home directory, broad changes to these settings might cause disruptions to users on a system. Therefore, these changes are left to deployers to examine and adjust manually.

All files and directories contained in local interactive user home directories must be group-owned by a group of which the home directory owner is a member. (V-72025)

STIG Description

Severity: Medium

If a local interactive users files are group-owned by a group of which the user is not a member, unintended users may be able to access them.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG has requirements for ownership and permissions of files and directories in each users home directory, broad changes to these settings might cause disruptions to users on a system. Therefore, these changes are left to deployers to examine and adjust manually.

All files and directories contained in local interactive user home directories must have mode 0750 or less permissive. (V-72027)

STIG Description

Severity: Medium

If a local interactive user files have excessive permissions, unintended users may be able to access or modify them.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG has requirements for ownership and permissions of files and directories in each users home directory, broad changes to these settings might cause disruptions to users on a system. Therefore, these changes are left to deployers to examine and adjust manually.

All local initialization files for interactive users must be owned by the home directory user or root. (V-72029)

STIG Description

Severity: Medium

Local initialization files are used to configure the users shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all initialization files for interactive users have proper owners, group owners, and permissions, these changes are often disruptive for users. The tasks in the security role do not make any changes to user initialization files.

Deployers should review the content and discretionary access controls applied to each users initialization files in their home directory.

Local initialization files for local interactive users must be group-owned by the users primary group or root. (V-72031)

STIG Description

Severity: Medium

Local initialization files for interactive users are used to configure the users shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all initialization files for interactive users have proper owners, group owners, and permissions, these changes are often disruptive for users. The tasks in the security role do not make any changes to user initialization files.

Deployers should review the content and discretionary access controls applied to each users initialization files in their home directory.

All local initialization files must have mode 0740 or less permissive. (V-72033)

STIG Description

Severity: Medium

Local initialization files are used to configure the users shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all initialization files for interactive users have proper owners, group owners, and permissions, these changes are often disruptive for users. The tasks in the security role do not make any changes to user initialization files.

Deployers should review the content and discretionary access controls applied to each users initialization files in their home directory.

All local interactive user initialization files executable search paths must contain only paths that resolve to the users home directory. (V-72035)

STIG Description

Severity: Medium

The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory (other than the users home directory), executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. If deviations from the default system search path for the local interactive user are required, they must be documented with the Information System Security Officer (ISSO).

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all initialization files must contain executable search paths that resolve to the users home directory, this change be disruptive for most users. The tasks in the security role do not make any changes to user initialization files.

Local initialization files must not execute world-writable programs. (V-72037)

STIG Description

Severity: Medium

If user start-up files execute world-writable programs, especially in unprotected directories, they could be maliciously modified to destroy user files or otherwise compromise the system at the user level. If the system is compromised at the user level, it is easier to elevate privileges to eventually compromise the system at the root and network level.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should manually search their system for world-writable programs and change the permissions on those programs. They are easily found with this command:

```
find / -perm -002 -type f
```

World-writable executables should not be needed under almost all circumstances.

All system device files must be correctly labeled to prevent unauthorized modification. (V-72039)

STIG Description

Severity: Medium

If an unauthorized or modified device is allowed to exist on the system, there is the possibility the system may perform unintended or unauthorized operations.

Deployer/Auditor notes

Implementation Status: Implemented - Red Hat Only

The tasks in the security role examine the SELinux contexts on each device file found on the system. Any devices without appropriate labels are printed in the Ansible output.

Deployers should investigate the unlabeled devices and ensure that the correct labels are applied for the class of device.

Note: This change applies only to CentOS or Red Hat Enterprise Linux systems since they rely on SELinux as their default Linux Security Module (LSM). Ubuntu, openSUSE Leap and SUSE Linux Enterprise systems use AppArmor, which uses policy files rather than labels applied to individual files.

File systems that contain user home directories must be mounted to prevent files with the setuid and setgid bit set from being executed. (V-72041)

STIG Description

Severity: Medium

The nosuid mount option causes the system to not execute setuid and setgid files with owner privileges. This option must be used for mounting any file system not containing approved setuid and setguid files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should examine any filesystem mounts that contain home directories to ensure that the `nosetuid` option is set.

File systems that are used with removable media must be mounted to prevent files with the setuid and setgid bit set from being executed. (V-72043)

STIG Description

Severity: Medium

The nosuid mount option causes the system to not execute setuid and setgid files with owner privileges. This option must be used for mounting any file system not containing approved setuid and setguid files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should examine any filesystem mounts of removable media to ensure that the `nosetuid` option is set.

File systems that are being imported via Network File System (NFS) must be mounted to prevent files with the setuid and setgid bit set from being executed. (V-72045)

STIG Description

Severity: Medium

The nosuid mount option causes the system to not execute setuid and setgid files with owner privileges. This option must be used for mounting any file system not containing approved setuid and setguid files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should examine any filesystem mounts of NFS imports to ensure that the `nosetuid` option is set.

All world-writable directories must be group-owned by root, sys, bin, or an application group. (V-72047)

STIG Description

Severity: Medium

If a world-writable directory has the sticky bit set and is not group-owned by a privileged Group Identifier (GID), unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

Deployer/Auditor notes

Implementation Status: Opt-In

The tasks in the security role examine the world-writable directories on the system and report any directories that are not group-owned by the `root` user. Those directories appear in the Ansible output.

Deployers should review the list of directories and group owners to ensure that they are appropriate for the directory. Unauthorized group ownership could allow certain users to modify files from other users.

Searching the entire filesystem for world-writable directories will consume a significant amount of disk I/O and could impact the performance of a production system. It can also delay the playbooks completion. Therefore, the search is disabled by default.

Deployers can enable the search by setting the following Ansible variable:

```
security_find_world_writable_dirs: yes
```

The umask must be set to 077 for all local interactive user accounts. (V-72049)

STIG Description

Severity: Medium

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 700 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be 0. This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all local interactive user accounts have a umask of `077`, this change can be disruptive for users and the applications they run. This change cannot be applied in an automated way.

Deployers should review user initialization files regularly to ensure that the umask is not specified. This allows the system-wide setting of `077` to be applied to all user sessions.

Cron logging must be implemented. (V-72051)

STIG Description

Severity: Medium

Cron logging can be used to trace the successful or unsuccessful execution of cron jobs. It can also be used to spot intrusions into the use of the cron facility by unauthorized and malicious users.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Ubuntu, CentOS, Red Hat Enterprise Linux, openSUSE Leap and SUSE Linux Enterprise already capture the logs from cron.

Ubuntu systems collect cron job logs into the main syslog file (`/var/log/syslog`) rather than separate them into their own log file. CentOS and Red Hat Enterprise Linux systems collect cron logs in `/var/log/cron`. openSUSE Leap and SUSE Linux Enterprise collect cron job in `/var/log/messages`.

Deployers should not need to adjust these configurations unless a specific environment requires it. The tasks in the security role do not make changes to the `rsyslog` configuration.

If the cron.allow file exists it must be owned by root. (V-72053)

STIG Description

Severity: Medium

If the owner of the cron.allow file is not set to root, the possibility exists for an unauthorized user to view or to edit sensitive information.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role check for the existence of `/etc/cron.allow` and set both the user and group ownership to `root`. This is the default on Ubuntu, CentOS, Red Hat Enterprise Linux systems, openSUSE Leap and SUSE Linux Enterprise 12 already.

If the cron.allow file exists it must be group-owned by root. (V-72055)

STIG Description

Severity: Medium

If the group owner of the cron.allow file is not set to root, sensitive information could be viewed or edited by unauthorized users.

Deployer/Auditor notes

Implementation Status: Implemented

The group ownership for `/etc/cron.allow` is already set by the task for the following STIG control:

If the cron.allow file exists it must be owned by root. (V-72053)

Kernel core dumps must be disabled unless needed. (V-72057)

STIG Description

Severity: Medium

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in denial of service by exhausting the available space on the target file system partition.

Deployer/Auditor notes

Implementation Status: Implemented

The `kdump` service is disabled if it exists on the system. Deployers can opt out of this change by setting the following Ansible variable:

```
security_disable_kdump: no
```

The file integrity tool must use FIPS 140-2 approved cryptographic hashes for validating file contents and directories. (V-72073)

STIG Description

Severity: Medium

File integrity tools use cryptographic hashes for verifying file contents and directories have not been altered. These hashes must be FIPS 140-2 approved cryptographic hashes.

Deployer/Auditor notes

Implementation Status: Implemented

The default AIDE configuration in CentOS 7, Red Hat Enterprise Linux 7, openSUSE Leap and SUSE Linux Enterprise 12 already uses SHA512 to validate file contents and directories. No changes are required on these systems.

The tasks in the security role add a rule to end of the AIDE configuration on Ubuntu systems that uses SHA512 for validation.

The system must not allow removable media to be used as the boot loader unless approved. (V-72075)

STIG Description

Severity: Medium

Malicious users with removable boot media can gain access to a system configured to use removable media as the boot loader. If removable media is designed to be used as the boot loader, the requirement must be documented with the Information System Security Officer (ISSO).

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

When a server is initially provisioned, deployers should avoid storing the boot loader on removable media. It is not possible to change this via automated tasks.

The operating system must shut down upon audit processing failure, unless availability is an overriding concern. If availability is a concern, the system must alert the designated staff (System Administrator [SA] and Information System Security Officer [ISSO] at a minimum) in the event of an audit processing failure. (V-72081)

STIG Description

Severity: Medium

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Satisfies: SRG-OS-000046-GPOS-00022, SRG-OS-000047-GPOS-00023

Deployer/Auditor notes

Implementation Status: Implemented

The audit daemon takes various actions when there is an auditing failure. There are three options for the `-f` flag for `auditctl`:

- `0`: In the event of an auditing failure, do nothing.
- `1`: In the event of an auditing failure, write messages to the kernel log.
- `2`: In the event of an auditing failure, cause a kernel panic.

Most operating systems set the failure flag to 1 by default, which maximizes system availability while still causing an alert. The tasks in the security role set the flag to 1 by default.

Deployers can adjust the following Ansible variable to customize the failure flag:

```
security_rhel7_audit_failure_flag: 1
```

> **Warning:** Setting the failure flag to 2 is **strongly** discouraged unless the security of the system takes priority over its availability. Any failure in auditing causes a kernel panic and the system requires a hard reboot.

The operating system must off-load audit records onto a different system or media from the system being audited. (V-72083)

STIG Description

Severity: Medium

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Deployer/Auditor notes

Implementation Status: Opt-In

The `audispd` service transmits audit logs to other servers. Deployers should specify the address of another server that can receive audit logs by setting the following Ansible variable:

```
security_audisp_remote_server: '10.0.21.1'
```

The operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited. (V-72085)

STIG Description

Severity: Medium

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Deployer/Auditor notes

Implementation Status: Opt-In

The `audispd` daemon transmits audit logs without encryption by default. The STIG requires that these logs are encrypted while they are transferred across the network. The encryption is controlled by the `enable_krb5` option in `/etc/audisp/audisp-remote.conf`.

Deployers can opt-in for encrypted audit log transmission by setting the following Ansible variable:

```
security_audisp_enable_krb5: yes
```

> **Warning:** Only enable this setting if kerberos is already configured.

The audit system must take appropriate action when the audit storage volume is full. (V-72087)

STIG Description

Severity: Medium

Taking appropriate action in case of a filled audit storage volume will minimize the possibility of losing audit records.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role set the `disk_full_action` and `network_failure_action` to `syslog` in the audispd remote configuration. In the event of a full disk on the remote log server or a network interruption, the local system sends warnings to syslog. This is the safest option since it maximizes the availability of the local system.

Deployers have two other options available:

- `single`: Switch the local server into single-user mode in the event of a logging failure.
- `halt`: Shut off the local server gracefully in the event of a logging failure.

> **Warning:** Choosing `single` or `halt` causes a server to go into a degraded or offline state immediately after a logging failure.

Deployers can adjust these configurations by setting the following Ansible variables (the safe defaults are shown here):

```
security_rhel7_auditd_disk_full_action: syslog
security_rhel7_auditd_network_failure_action: syslog
```

The operating system must immediately notify the System Administrator (SA) and Information System Security Officer ISSO (at a minimum) when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity. (V-72089)

STIG Description

Severity: Medium

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

Deployer/Auditor notes

Implementation Status: Implemented

The `space_left` configuration is set to 25% of the size of the disk mounted on `/`. This calculation is done automatically.

Deployers can set a custom threshold for the `space_left` configuration (in megabytes) by setting the following Ansible variable:

```
# Example: A setting of 1GB (1024MB)
security_rhel7_auditd_space_left: 1024
```

The operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) via email when the threshold for the repository maximum audit record storage capacity is reached. (V-72091)

STIG Description

Severity: Medium

If security personnel are not notified immediately when the threshold for the repository maximum audit record storage capacity is reached, they are unable to expand the audit record storage capacity before records are lost.

Deployer/Auditor notes

Implementation Status: Implemented

The `space_left_action` in the audit daemon configuration is set to `email`. This configuration causes the root user to receive an email when the `space_left` threshold is reached.

Deployers can customize this configuration by setting the following Ansible variable:

```
security_rhel7_auditd_space_left_action: email
```

The operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached. (V-72093)

STIG Description

Severity: Medium

If security personnel are not notified immediately when the threshold for the repository maximum audit record storage capacity is reached, they are unable to expand the audit record storage capacity before records are lost.

Deployer/Auditor notes

Implementation Status: Implemented

The `action_mail_acct` configuration in the audit daemon configuration file is set to `root` to meet the requirements of the STIG. Deployers can customize the recipient of the emails that come from auditd by setting the following Ansible variable:

```
security_rhel7_auditd_action_mail_acct: root
```

All privileged function executions must be audited. (V-72095)

STIG Description

Severity: Medium

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

This STIG is difficult to implement in an automated way because the number of applications on a system with setuid/setgid permissions changes over time. In addition, adding audit rules for some of these automatically could cause a significant increase in logging traffic when these applications are used regularly.

Deployers are urged to do the following instead:

- Minimize the amount of applications with setuid/setgid privileges
- Monitor any new applications that gain setuid/setgid privileges
- Add risky applications with setuid/setgid privileges to auditd for detailed syscall monitoring

---

All uses of the chown command must be audited. (V-72097)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `chown` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_chown: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fchown command must be audited. (V-72099)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fchown` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchown: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the lchown command must be audited. (V-72101)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `lchown` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_lchown: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fchownat command must be audited. (V-72103)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fchownat` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchownat: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the chmod command must be audited. (V-72105)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `chmod` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_chmod: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fchmod command must be audited. (V-72107)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fchmod` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchmod: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fchmodat command must be audited. (V-72109)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fchmodat` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchmodat: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the setxattr command must be audited. (V-72111)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `setxattr` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_setxattr: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fsetxattr command must be audited. (V-72113)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fsetxattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fsetxattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the lsetxattr command must be audited. (V-72115)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `lsetxattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_lsetxattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the removexattr command must be audited. (V-72117)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `removexattr` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_removexattr: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fremovexattr command must be audited. (V-72119)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fremovexattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fremovexattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the lremovexattr command must be audited. (V-72121)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `lremovexattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_lremovexattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the creat command must be audited. (V-72123)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `creat` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_creat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the open command must be audited. (V-72125)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `open` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_open: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the openat command must be audited. (V-72127)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `openat` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_openat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the open_by_handle_at command must be audited. (V-72129)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `open_by_handle_at` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_open_by_handle_at: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the truncate command must be audited. (V-72131)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `truncate` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_truncate: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the ftruncate command must be audited. (V-72133)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `ftruncate` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_ftruncate: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the semanage command must be audited. (V-72135)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit any time the `semanage` command is used.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_semanage: no
```

All uses of the setsebool command must be audited. (V-72137)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit any time the `setsebool` command is used.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_setsebool: no
```

All uses of the chcon command must be audited. (V-72139)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `chcon` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_chcon: no
```

All uses of the setfiles command must be audited. (V-72141)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `restorecon` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_restorecon: no
```

The operating system must generate audit records for all successful/unsuccessful account access count events. (V-72143)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all successful and unsuccessful account access events. Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_audit_account_access: no
```

The operating system must generate audit records for all unsuccessful account access events. (V-72145)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all successful/unsuccessful account access count events. (V-72143)*

The operating system must generate audit records for all successful account access events. (V-72147)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time an account is accessed.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_account_access: no
```

All uses of the passwd command must be audited. (V-72149)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `passwd` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_passwd_command: no
```

All uses of the unix_chkpwd command must be audited. (V-72151)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `unix_chkpwd` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_unix_chkpwd: no
```

All uses of the gpasswd command must be audited. (V-72153)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `gpasswd` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_gpasswd: no
```

All uses of the chage command must be audited. (V-72155)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `chage` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_chage: no
```

All uses of the userhelper command must be audited. (V-72157)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `userhelper` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_userhelper: no
```

All uses of the su command must be audited. (V-72159)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `su` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_su: no
```

All uses of the sudo command must be audited. (V-72161)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the sudo command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_sudo: no
```

All uses of the sudoers command must be audited. (V-72163)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time a user manages the configuration files for sudo.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_sudo_config_changes: no
```

All uses of the newgrp command must be audited. (V-72165)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `newgrp` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_newgrp: no
```

All uses of the chsh command must be audited. (V-72167)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `chsh` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_chsh: no
```

All uses of the sudoedit command must be audited. (V-72169)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `sudoedit` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_sudoedit: no
```

All uses of the mount command must be audited. (V-72171)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `mount` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_mount: no
```

All uses of the umount command must be audited. (V-72173)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `umount` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_umount: no
```

All uses of the postdrop command must be audited. (V-72175)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `postdrop` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_postdrop: no
```

All uses of the postqueue command must be audited. (V-72177)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `postqueue` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_postqueue: no
```

All uses of the ssh-keysign command must be audited. (V-72179)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged ssh commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `ssh-keysign` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_ssh_keysign: no
```

All uses of the crontab command must be audited. (V-72183)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `crontab` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_crontab: no
```

All uses of the pam_timestamp_check command must be audited. (V-72185)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `pam_timestamp_check` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_pam_timestamp_check: no
```

All uses of the init_module command must be audited. (V-72187)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `init_module` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_init_module: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the delete_module command must be audited. (V-72189)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `delete_module` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_delete_module: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the insmod command must be audited. (V-72191)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `insmod` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_insmod: no
```

All uses of the rmmod command must be audited. (V-72193)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `rmmod` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_rmmod: no
```

All uses of the modprobe command must be audited. (V-72195)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `modprobe` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_modprobe: no
```

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000476-GPOS-00221

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time that an account is modified. This includes changes to the following files:

- `/etc/group`
- `/etc/passwd`
- `/etc/gshadow`
- `/etc/shadow`
- `/etc/security/opasswd`

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_account_actions: no
```

All uses of the rename command must be audited. (V-72199)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `rename` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_rename: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the renameat command must be audited. (V-72201)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `renameat` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_renameat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the rmdir command must be audited. (V-72203)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `rmdir` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_rmdir: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the unlink command must be audited. (V-72205)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `unlink` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_unlink: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the unlinkat command must be audited. (V-72207)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `unlinkat` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_unlinkat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

The system must send rsyslog output to a log aggregation server. (V-72209)

STIG Description

Severity: Medium

Sending rsyslog output to another system ensures that the logs cannot be removed or modified in the event that the system is compromised or has a hardware failure.

Deployer/Auditor notes

Implementation Status: Verification Only

The tasks in the security role check for uncommented lines in the rsyslog configuration that contain `@` or `@@`, which signifies that a remote logging configuration is in place. If these lines are not found, a warning message is printed in the Ansible output.

The rsyslog daemon must not accept log messages from other servers unless the server is being used for log aggregation. (V-72211)

STIG Description

Severity: Medium

Unintentionally running a rsyslog server accepting remote messages puts the system at increased risk. Malicious rsyslog messages sent to the server could exploit vulnerabilities in the server software itself, could introduce misleading information in to the systems logs, or could fill the systems storage leading to a Denial of Service. If the system is intended to be a log aggregation server its use must be documented with the ISSO.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers must take manual steps to add or remove syslog reception configuration lines depending on a servers role:

- If the server is a log aggregation server, deployers must configure the server to receive syslog output from the other servers via TCP connections.
- If the server is not a log aggregation server, deployers must configure the server so that it does not accept syslog output from other servers.

The system must update the virus scan program every seven days or more frequently. (V-72215)

STIG Description

Severity: Medium

Virus scanning software can be used to protect a system from penetration from computer viruses and to limit their spread through intermediate systems.

The virus scanning software should be configured to check for software and virus definition updates with a frequency no longer than seven days. If a manual process is required to update the virus scan software or definitions, it must be documented with the Information System Security Officer (ISSO).

Deployer/Auditor notes

Implementation Status: Implemented

By default, CentOS 7, Red Hat Enterprise Linux 7, openSUSE Leap and SUSE Linux Enterprise 12 check for virus database updates 12 times a day. Ubuntu servers have a default of 24 checks per day.

The tasks in the security role do not adjust these defaults as they are more secure than the STIGs requirement.

The host must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management Component Local Service Assessment (PPSM CLSA) and vulnerability assessments. (V-72219)

STIG Description

Severity: Medium

In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000297-GPOS-00115

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should review each firewall rule on a regular basis to ensure that each port is open for a valid reason.

A FIPS 140-2 approved cryptographic algorithm must be used for SSH communications. (V-72221)

STIG Description

Severity: Medium

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

Operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general purpose computing system.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173

Deployer/Auditor notes

Implementation Status: Implemented

The `Ciphers` configuration is set to `aes128-ctr,aes192-ctr,aes256-ctr` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can change the list of ciphers by setting the following Ansible variable:

```
security_sshd_cipher_list: 'cipher1,cipher2,cipher3'
```

All network connections associated with a communication session must be terminated at the end of the session or after 10 minutes of inactivity from the user at a command prompt, except to fulfill documented and validated mission requirements. (V-72223)

STIG Description

Severity: Medium

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that

has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role set a 600 second (10 minute) timeout for network connections associated with a communication session. Deployers can change the timeout value by setting the following Ansible variable:

```
# Example: shorten the timeout to 5 minutes (300 seconds)
security_rhel7_session_timeout: 300
```

The Standard Mandatory DoD Notice and Consent Banner must be displayed immediately prior to, or as part of, remote access logon prompts. (V-72225)

STIG Description

Severity: Medium

Display of a standardized and approved use notification before granting access to the publicly accessible operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is␣
↪provided for USG-authorized use only.
```

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

```
-The USG routinely intercepts and monitors communications on this IS for␣
↪purposes including, but not limited to, penetration testing, COMSEC␣
↪monitoring, network operations and defense, personnel misconduct (PM), law␣
↪enforcement (LE), and counterintelligence (CI) investigations.
```

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interestsnot for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007 , SRG-OS-000228-GPOS-00088

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role deploy a standard notice and consent banner into `/etc/motd` on each server. Ubuntu, CentOS, Red Hat Enterprise Linux, openSUSE Leap and SUSE Linux Enterprise display this banner after each successful login via ssh or the console.

Deployers can choose a different destination for the banner by setting the following Ansible variable:

```
security_sshd_banner_file: /etc/motd
```

The message is customized with the following Ansible variable:

```
security_login_banner_text: |
  ------------------------------------------------------------------------
↪--
  * WARNING                                                              ␣
↪ *
  * You are accessing a secured system and your actions will be logged along ␣
↪ *
  * with identifying information. Disconnect immediately if you are not an   ␣
↪ *
  * authorized user of this system.                                       ␣
↪ *
  ------------------------------------------------------------------------
↪--
```

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) authentication communications. (V-72227)

STIG Description

Severity: Medium

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers are strongly urged to utilize `sssd` for systems that authenticate against LDAP or Active Directory (AD) servers.

The ldap connector for `sssd` connects only to LDAP servers over encrypted connections. Review the man page for sssd-ldap for more details on this requirement.

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications. (V-72229)

STIG Description

Severity: Medium

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers are strongly urged to utilize `sssd` for systems that authenticate against LDAP or Active Directory (AD) servers.

To meet this control, deployers must ensure that `ldap_tls_cacert` or `ldap_tls_cacertdir` are set in the `/etc/sssd/sssd.conf` file. The `ldap_tls_cacert` directive specifies a single certificate while `ldap_tls_cacertdir` specifies a directory where `sssd` can find CA certificates.

> **Warning:** Use caution when adjusting these settings. If the correct CA certificates are not already deployed to the servers that perform LDAP authentication, their attempts to authenticate users might fail.
>
> Consult with administrators of the LDAP system and test all changes on a non-production system first.

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications. (V-72231)

STIG Description

Severity: Medium

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers are strongly urged to utilize `sssd` for systems that authenticate against LDAP or Active Directory (AD) servers.

To meet this control, deployers must ensure that `ldap_tls_cacert` or `ldap_tls_cacertdir` are set in the `/etc/sssd/sssd.conf` file. The `ldap_tls_cacert` directive specifies a single certificate while `ldap_tls_cacertdir` specifies a directory where `sssd` can find CA certificates.

> **Warning:** Use caution when adjusting these settings. If the correct CA certificates are not already deployed to the servers that perform LDAP authentication, their attempts to authenticate users might fail.
>
> Consult with administrators of the LDAP system and test all changes on a non-production system first.

All networked systems must have SSH installed. (V-72233)

STIG Description

Severity: Medium

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that every system has an ssh client and server installed. The role installs the following packages:

- CentOS: `openssh-clients`, `openssh-server`
- Ubuntu: `openssh-client`, `openssh-server`
- openSUSE Leap: `openssh`

All networked systems must use SSH for confidentiality and integrity of transmitted and received information as well as information during preparation for transmission. (V-72235)

STIG Description

Severity: Medium

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000423-GPOS-00188, SRG-OS-000423-GPOS-00189, SRG-OS-000423-GPOS-00190

Deployer/Auditor notes

Implementation Status: Implemented

The STIG has a requirement that the `sshd` daemon is running and enabled at boot time. The tasks in the security role ensure that these requirements are met.

Some deployers may not have `sshd` enabled on highly specialized systems and those deployers should opt out of this change by setting the following Ansible variable:

```
security_enable_sshd: no
```

Note: Setting `security_enable_sshd` to `no` causes the tasks to ignore the state of the service entirely. A setting of `no` does not stop or alter the `sshd` service.

All network connections associated with SSH traffic must terminate at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements. (V-72237)

STIG Description

Severity: Medium

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Deployer/Auditor notes

Implementation Status: Implemented

The `ClientAliveInterval` configuration is set to `600` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can adjust the length of the interval by changing the following Ansible variable:

```
security_sshd_client_alive_interval: 600
```

Note: The STIG requires that `ClientAliveInterval` is set to 600 and `ClientAliveCountMax` is set to zero, which sets a 10 minute session timeout. If no data is transferred in a 10 minute period, the session is disconnected.

The `ClientAliveInterval` specifies how long the ssh daemon waits before it sends a message to the client to see if it is still alive. The `ClientAliveCountMax` specifies how many of these messages are sent without receiving a response.

Deployers should refer to *All network connections associated with SSH traffic must terminate after a period of inactivity. (V-72241)* to customize the `ClientAliveCountMax` setting.

The SSH daemon must not allow authentication using RSA rhosts authentication. (V-72239)

STIG Description

Severity: Medium

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Deployer/Auditor notes

Implementation Status: Implemented

This STIG is already applied by the changes for *The SSH daemon must not allow authentication using known hosts authentication. (V-72249)*.

All network connections associated with SSH traffic must terminate after a period of inactivity. (V-72241)

STIG Description

Severity: Medium

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Deployer/Auditor notes

Implementation Status: Implemented

The `ClientAliveCountMax` configuration is set to `0` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can adjust the maximum amount of client alive intervals by changing the following Ansible variable.

```
security_sshd_client_alive_count_max: 0
```

Note: The STIG requires that `ClientAliveInterval` is set to 600 and `ClientAliveCountMax` is set to zero, which sets a 10 minute session timeout. If no data is transferred in a 10 minute period, the session is disconnected.

The `ClientAliveInterval` specifies how long the ssh daemon waits before it sends a message to the client to see if it is still alive. The `ClientAliveCountMax` specifies how many of these messages are sent without receiving a response.

Deployers should refer to *All network connections associated with SSH traffic must terminate at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements. (V-72237)* to customize the `ClientAliveInterval` setting.

The SSH daemon must not allow authentication using rhosts authentication. (V-72243)

STIG Description

Severity: Medium

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Deployer/Auditor notes

Implementation Status: Implemented

The `IgnoreRhosts` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_rhosts_auth: no
```

The system must display the date and time of the last successful account logon upon an SSH logon. (V-72245)

STIG Description

Severity: Medium

Providing users with feedback on when account accesses via SSH last occurred facilitates user recognition and reporting of unauthorized account use.

Deployer/Auditor notes

Implementation Status: Implemented

The `PrintLastLog` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_print_last_log: no
```

The system must not permit direct logons to the root account using remote access via SSH. (V-72247)

STIG Description

Severity: Medium

Even though the communications channel may be encrypted, an additional layer of security is gained by extending the policy of not logging on directly as root. In addition, logging on with a user-specific account provides individual accountability of actions performed on the system.

Deployer/Auditor notes

Implementation Status: Implemented

The `PermitRootLogin` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can select another setting for PermitRootLogin, from the available options `without-password`, `prohibit-password`, `forced-commands-only`, `yes`, or `no` by setting the following variable:

```
security_sshd_permit_root_login: no
```

> **Warning:** Ensure that a regular user account exists with a pathway to root access (preferably via `sudo`) before applying the security role. This configuration change disallows any direct logins with the `root` user.

The SSH daemon must not allow authentication using known hosts authentication. (V-72249)

STIG Description

Severity: Medium

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Deployer/Auditor notes

Implementation Status: Implemented

The `IgnoreUserKnownHosts` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_known_hosts_auth: no
```

The SSH daemon must be configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms. (V-72253)

STIG Description

Severity: Medium

DoD information systems are required to use FIPS 140-2 approved cryptographic hash functions. The only SSHv2 hash algorithm meeting this requirement is SHA.

Deployer/Auditor notes

Implementation Status: Implemented

The `MACs` configuration is set to `hmac-sha2-256,hmac-sha2-512` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can adjust the allowed Message Authentication Codes (MACs) by setting the following Ansible variable:

```
security_sshd_allowed_macs: 'hmac-sha2-256,hmac-sha2-512'
```

The SSH public host key files must have mode 0644 or less permissive. (V-72255)

STIG Description

Severity: Medium

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Deployer/Auditor notes

Implementation Status: Implemented

The permissions on ssh public host keys is set to `0644`. If the existing permissions are more restrictive than `0644`, the tasks do not make changes to the files.

The SSH private host key files must have mode 0600 or less permissive. (V-72257)

STIG Description

Severity: Medium

If an unauthorized user obtains the private SSH host key file, the host could be impersonated.

Deployer/Auditor notes

Implementation Status: Implemented

The permissions on ssh private host keys is set to `0600`. If the existing permissions are more restrictive than `0600`, the tasks do not make changes to the files.

The SSH daemon must not permit Generic Security Service Application Program Interface (GSSAPI) authentication unless needed. (V-72259)

STIG Description

Severity: Medium

GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through SSH exposes the systems GSSAPI to remote hosts, increasing the attack surface of the system. GSSAPI authentication must be disabled unless needed.

Deployer/Auditor notes

Implementation Status: Implemented

The `GSSAPIAuthentication` setting is set to `no` to meet the requirements of the STIG.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_gssapi: no
```

The SSH daemon must not permit Kerberos authentication unless needed. (V-72261)

STIG Description

Severity: Medium

Kerberos authentication for SSH is often implemented using Generic Security Service Application Program Interface (GSSAPI). If Kerberos is enabled through SSH, the SSH daemon provides a means of access to the systems Kerberos implementation. Vulnerabilities in the systems Kerberos implementation may then be subject to exploitation. To reduce the attack surface of the system, the Kerberos authentication mechanism within SSH must be disabled for systems not using this capability.

Deployer/Auditor notes

Implementation Status: Implemented

The `KerberosAuthentication` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disable_kerberos_auth: no
```

The SSH daemon must perform strict mode checking of home directory configuration files. (V-72263)

STIG Description

Severity: Medium

If other users have access to modify user-specific SSH configuration files, they may be able to log on to the system as another user.

Deployer/Auditor notes

Implementation Status: Implemented

The `StrictModes` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_enable_strict_modes: no
```

The SSH daemon must use privilege separation. (V-72265)

STIG Description

Severity: Medium

SSH daemon privilege separation causes the SSH process to drop root privileges when not needed, which would decrease the impact of software vulnerabilities in the unprivileged section.

Deployer/Auditor notes

Implementation Status: Implemented

The `UsePrivilegeSeparation` configuration is set to `sandbox` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_enable_privilege_separation: no
```

Note: Although the STIG requires this setting to be `yes`, the `sandbox` setting actually provides more security because it enables privilege separation during the early authentication process.

The SSH daemon must not allow compression or must only allow compression after successful authentication. (V-72267)

STIG Description

Severity: Medium

If compression is allowed in an SSH connection prior to authentication, vulnerabilities in the compression software could result in compromise of the system from an unauthenticated connection, potentially with root privileges.

Deployer/Auditor notes

Implementation Status: Implemented

The `Compression` configuration is set to `delayed` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can choose another option by setting the following Ansible variable:

```
security_sshd_compression: 'no'
```

Note: The following are the available settings for `Compression` in the ssh configuration file:

- `delayed`: Compression is enabled after authentication.

- `no`: Compression is disabled.
- `yes`: Compression is enabled during authentication and during the session (not allowed by the STIG).

The `delayed` option balances security with performance and is an approved option in the STIG.

The operating system must, for networked systems, synchronize clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS). (V-72269)

STIG Description

Severity: Medium

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Satisfies: SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role make the following changes on each host:

- The `chrony` package is installed.
- The service (`chronyd` on Red Hat, CentOS, SLE and openSUSE Leap, `chrony` on Ubuntu) is started and enabled at boot time.
- A configuration file template is deployed that includes `maxpoll 10` on each server line.

Deployers can opt out of these changes by setting the following Ansible variable:

```
security_rhel7_enable_chrony: no
```

Note: Although the STIG mentions the traditional `ntpd` service, this role uses `chrony`, which is a more modern implementation.

The operating system must protect against or limit the effects of Denial of Service (DoS) attacks by validating the operating system is implementing rate-limiting measures on impacted network interfaces. (V-72271)

STIG Description

Severity: Medium

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of the operating system to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that incoming TCP connections are rate limited with `firewalld`, this setting can cause problems with certain applications which handle large amounts of TCP connections. Therefore, the tasks in the security role do not apply the rate limit by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_enable_firewalld_rate_limit: yes
```

The STIG recommends a limit of 25 connection per minute and allowing bursts up to 100 connections. Both of these options are adjustable with the following Ansible variables:

```
security_enable_firewalld_rate_limit_per_minute: 25
security_enable_firewalld_rate_limit_burst: 100
```

> **Warning:** Deployers should test rate limiting in a non-production environment first before applying it to production systems. Ensure that the application running on the system is receiving a large volume of requests so that the rule can be thoroughly tested.

The operating system must enable an application firewall, if available. (V-72273)

STIG Description

Severity: Medium

Firewalls protect computers from network attacks by blocking or limiting access to open network ports. Application firewalls limit which applications are allowed to communicate over the network.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000480-GPOS-00231, SRG-OS-000480-GPOS-00232

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that a firewall is configured on each server. This might be disruptive to some environments since the default firewall policy for `firewalld` is very restrictive. Therefore, the tasks in the security role do not install or enable the `firewalld` daemon by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_enable_firewalld: yes
```

> **Warning:** Deployers must pre-configure `firewalld` or copy over a working XML file in `/etc/firewalld/zones/` from another server. The default firewalld restrictions on Ubuntu, CentOS, Red Hat Enterprise Linux and openSUSE Leap are highly restrictive.

The system must not forward Internet Protocol version 4 (IPv4) source-routed packets. (V-72283)

STIG Description

Severity: Medium

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in this role set `net.ipv4.conf.all.accept_source_route` and `net.ipv4.conf.default.accept_source_route` to `0` by default. This prevents the system from forwarding source-routed IPv4 packets on all new and existing interfaces.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_source_routed_packet_forward_ipv4: no
```

For more details on source routed packets, refer to the Red Hat documentation.

The system must not forward Internet Protocol version 4 (IPv4) source-routed packets by default. (V-72285)

STIG Description

Severity: Medium

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The system must not forward Internet Protocol version 4 (IPv4) source-routed packets. (V-72283)*

The system must not respond to Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) echoes sent to a broadcast address. (V-72287)

STIG Description

Severity: Medium

Responding to broadcast (ICMP) echoes facilitates network mapping and provides a vector for amplification attacks.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in this role set `net.ipv4.icmp_echo_ignore_broadcasts` to 1 by default. This prevents the system from responding to IPv4 ICMP echoes sent to the broadcast address.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_echoes_broadcast_address: no
```

The system must prevent Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages from being accepted. (V-72289)

STIG Description

Severity: Medium

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the hosts route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages. (V-73175)*

The system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default. (V-72291)

STIG Description

Severity: Medium

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the systems route table, possibly revealing portions of the network topology.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in this role set `net.ipv4.conf.default.send_redirects` and `net.ipv4.conf.all.send_redirects` to `0` by default. This prevents a system from sending IPv4 ICMP redirect packets on all new and existing interfaces.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_icmp_redirects: no
```

The system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects. (V-72293)

STIG Description

Severity: Medium

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the systems route table, possibly revealing portions of the network topology.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default. (V-72291)*

Network interfaces must not be in promiscuous mode. (V-72295)

STIG Description

Severity: Medium

Network interfaces in promiscuous mode allow for the capture of all network traffic visible to the system. If unauthorized individuals can access these applications, it may allow then to collect information such as logon IDs, passwords, and key exchanges between systems.

If the system is being used to perform a network troubleshooting function, the use of these tools must be documented with the Information System Security Officer (ISSO) and restricted to only authorized personnel.

Deployer/Auditor notes

Implementation Status: Verification Only

All interfaces are examined to ensure they are not in promiscuous mode. A warning message is printed in the Ansible output if any promiscuous interfaces are found.

The system must be configured to prevent unrestricted mail relaying. (V-72297)

STIG Description

Severity: Medium

If unrestricted mail relaying is permitted, unauthorized senders could use this host as a mail relay for the purpose of sending spam or other unauthorized activity.

Deployer/Auditor notes

Implementation Status: Implemented

The `smtpd_client_restrictions` configuration in postfix is set to `permit_mynetworks, reject` to meet the STIGs requirements.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_restrict_mail_relaying: no
```

If the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon must be configured to operate in secure mode. (V-72305)

STIG Description

Severity: Medium

Restricting TFTP to a specific directory prevents remote users from copying, transferring, or overwriting system files.

Deployer/Auditor notes

Implementation Status: Verification Only

The tasks in the security role examine the TFTP server configuration file (if it exists) to verify that the secure operation flag (`-s`) is listed on the `server_args` line. If it is missing, a warning message is printed in the Ansible output.

An X Windows display manager must not be installed unless approved. (V-72307)

STIG Description

Severity: Medium

Internet services that are not required for system or application processes must not be active to decrease the attack surface of the system. X Windows has a long history of security vulnerabilities and will not be used unless approved and documented.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the xorg server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `xorg-x11-server-Xorg`
- Ubuntu: `xorg-xserver`
- openSUSE Leap: `xorg-x11-server`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_xorg: no
```

The system must not be performing packet forwarding unless the system is a router. (V-72309)

STIG Description

Severity: Medium

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

Deployer/Auditor notes

Implementation Status: Opt-In

Disabling IP forwarding on a system that routes packets or host virtual machines might cause network interruptions. The tasks in this role do not adjust the `net.ipv4.ip_forward` configuration by default.

Deployers can opt in for this change and disable IP forwarding by setting the following Ansible variable:

```
security_disallow_ip_forwarding: yes
```

Warning: IP forwarding is required in some environments. Always test in a non-production environment before changing this setting on a production system.

The Network File System (NFS) must be configured to use RPCSEC_GSS. (V-72311)

STIG Description

Severity: Medium

When an NFS server is configured to use RPCSEC_SYS, a selected userid and groupid are used to handle requests from the remote user. The userid and groupid could mistakenly or maliciously be set incorrectly. The RPCSEC_GSS method of authentication uses certificates on the server and client systems to more securely authenticate the remote mount request.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers using NFS should examine their mounts to ensure `krb5:krb5i:krb5p` is provided with the `sec` option. Kerberos must be installed and configured before making the change.

The system access control program must be configured to grant or deny system access to specific hosts and services. (V-72315)

STIG Description

Severity: Medium

If the systems access control program is not configured with appropriate rules for allowing and denying access to system network resources, services may be accessible to unauthorized hosts.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The `firewalld` service is optionally enabled and configured in the tasks for another STIG control:

- *The operating system must enable an application firewall, if available. (V-72273)*

Deployers should review their `firewalld` ruleset regularly to ensure that each firewall rule is specific as possible. Each rule should allow the smallest number of hosts to access the smallest number of services.

The system must not have unauthorized IP tunnels configured. (V-72317)

STIG Description

Severity: Medium

IP tunneling mechanisms can be used to bypass network filtering. If tunneling is required, it must be documented with the Information System Security Officer (ISSO).

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should review all tunneled connections on a regular basis to ensure each is valid and properly secured. This requires careful verification that cannot be done with automated Ansible tasks.

The system must not forward IPv6 source-routed packets. (V-72319)

STIG Description

Severity: Medium

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv6 forwarding is enabled and the system is functioning as a router.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in this role set `net.ipv6.conf.all.accept_source_route` to `0` by default. This prevents the system from forwarding source-routed IPv6 packets.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_source_routed_packet_forward_ipv6: no
```

Refer to IPv6 source routing: history repeats itself for more details on IPv6 source routed packets.

The operating system must have the required packages for multifactor authentication installed. (V-72417)

STIG Description

Severity: Medium

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that the following multifactor authentication packages are installed:

- authconfig
- authconfig-gtk
- esc
- pam_pkcs11

These packages are benign if they are not needed on a system, but `authconfig-gtk` may cause some graphical dependencies to be installed which may not be needed on some systems. The security role installs these packages, but it skips the installation of `authconfig-gtk`. Deployers can install the graphical package manually if needed.

The operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules (PAM). (V-72427)

STIG Description

Severity: Medium

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that the `sssd.conf` contains both `nss` and `pam` authentication modules, this change can be disruptive in environments that are already using LDAP or Active Directory for authentication. Deployers should make these changes only if their environment is compatible.

The operating system must implement certificate status checking for PKI authentication. (V-72433)

STIG Description

Severity: Medium

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Any adjustment to PKI authentication can cause disruptions for users. Deployers should verify that enabling OCSP validation is compatible with their existing configuration.

The operating system must implement smart card logons for multifactor authentication for access to privileged accounts. (V-72435)

STIG Description

Severity: Medium

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Any adjustment to PKI authentication can cause disruptions for users. Deployers should verify that their environment is compatible with smart cards before requiring them for authentication.

The operating system must set the lock delay setting for all connection types. (V-73155)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. (V-71891)*

The operating system must set the session idle delay setting for all connection types. (V-73157)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. (V-71891)*

When passwords are changed or new passwords are established, pwquality must be used. (V-73159)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Pwquality enforces complex password construction configuration on the system.

Deployer/Auditor notes

Implementation Status: Opt-In

The security role can require new or changed passwords to follow the pwquality rules, but this change can be disruptive for users without proper communication. Deployers must opt in for this change by setting the following variable:

```
security_enable_pwquality_password_set: yes
```

File systems that are being imported via Network File System (NFS) must be mounted to prevent binary files from being executed. (V-73161)

STIG Description

Severity: Medium

The noexec mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should review their NFS mounts to ensure they are mounted with the `noexec` option. Deployers should skip this change if they execute applications from NFS mounts.

The audit system must take appropriate action when there is an error sending audit records to a remote system. (V-73163)

STIG Description

Severity: Medium

Taking appropriate action when there is an error sending audit records to a remote system will minimize the possibility of losing audit records.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The audit system must take appropriate action when the audit storage volume is full. (V-72087)*

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group. (V-73165)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow. (V-73167)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow. (V-73171)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd. (V-73173)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

The system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages. (V-73175)

STIG Description

Severity: Medium

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the hosts route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects. (V-72293)*

Wireless network adapters must be disabled. (V-73177)

STIG Description

Severity: Medium

The use of wireless networking can introduce many different attack vectors into the organizations network. Common attack vectors such as malicious association and ad hoc networks will allow an attacker to spoof a wireless access point (AP), allowing validated systems to connect to the malicious AP and enabling the attacker to monitor and record network traffic. These malicious APs can also serve to create a man-in-the-middle attack or be used to create a denial of service to valid network resources.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should review the configuration of any wireless networking device connected to the system to ensure it must be enabled. The STIG requires that all wireless network devices are enabled unless required.

The operating system must uniquely identify and must authenticate users using multifactor authentication via a graphical user logon. (V-77819)

STIG Description

Severity: Medium

To assure accountability and prevent unauthenticated access, users must be identified and authenticated to prevent potential misuse and compromise of the system.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

Satisfies: SRG-OS-000375-GPOS-00161,SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The STIG requires that multifactor authentication is used for graphical user logon, but this change requires custom configuration based on the authentication solution that is used.

Deployers should review the available options, such as traditional smartcards, USB devices (such as Yubikeys), or software token systems, and use one of these solutions on each system.

The Datagram Congestion Control Protocol (DCCP) kernel module must be disabled unless required. (V-77821)

STIG Description

Severity: Medium

Disabling DCCP protects the system against exploitation of any flaws in the protocol implementation.

Deployer/Auditor notes

Implementation Status: Implemented

The ansible-hardening role disables the DCCP kernel module by default. Each system must be rebooted to fully apply the change.

Deployers can opt out of the change by setting the following Ansible variable:

```
security_rhel7_disable_dccp: no
```

The operating system must require authentication upon booting into single-user and maintenance modes. (V-77823)

STIG Description

Severity: Medium

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Modifying sensitive systemd unit files directly or via overrides could cause a system to have issues during the boot process. The role does not make any adjustments to the `rescue.service` because this service is critical during emergencies.

All of the distributions supported by the role already require authentication for single user mode.

The operating system must implement virtual address space randomization. (V-77825)

STIG Description

Severity: Medium

Address space layout randomization (ASLR) makes it more difficult for an attacker to predict the location of attack code he or she has introduced into a processs address space during an attempt at exploitation. Additionally, ASLR also makes it more difficult for an attacker to know the location of existing code in order to repurpose it using return-oriented programming (ROP) techniques.

Deployer/Auditor notes

Implementation Status: Implemented

Most modern systems enable Address Space Layout Randomization (ASLR) by default (with a setting of 2), and the role ensures that the secure default is maintained.

Deployers can opt out of the change by setting the following Ansible variable:

```
security_enable_aslr: no
```

For more details on the ASLR settings, review the sysctl documentation.

Low (11 controls)

The operating system must remove all software components after updated versions have been installed. (V-71987)

STIG Description

Severity: Low

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that dependent packages are removed automatically when a package is removed, this can cause problems with certain packages, especially kernels. Deployers must opt in to meet the requirements of this STIG control.

Deployers should set the following variable to enable automatic dependent package removal:

```
security_package_clean_on_remove: yes
```

All Group Identifiers (GIDs) referenced in the /etc/passwd file must be defined in the /etc/group file. (V-72003)

STIG Description

Severity: Low

If a user is assigned the GID of a group not existing on the system, and a group with the GID is subsequently created, the user may have unintended rights to any files associated with the group.

Deployer/Auditor notes

Implementation Status: Implemented

If any users are found with invalid GIDs, those users are printed in the Ansible output. Deployers should review the list and ensure all users are assigned to a valid group that is defined in `/etc/group`.

A separate file system must be used for user home directories (such as /home or an equivalent). (V-72059)

STIG Description

Severity: Low

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

Deployers should consider using filesystem mounts for home directories during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/home` as a separate filesystem, a warning is printed in the Ansible output.

The system must use a separate file system for /var. (V-72061)

STIG Description

Severity: Low

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

Deployers should consider using filesystem mounts for `/var` during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/var` as a separate filesystem, a warning is printed in the Ansible output.

The system must use a separate file system for the system audit data path. (V-72063)

STIG Description

Severity: Low

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

Deployers should consider using filesystem mounts for `/var/log/audit` during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/var/log/audit` as a separate filesystem, a warning is printed in the Ansible output.

The system must use a separate file system for /tmp (or equivalent). (V-72065)

STIG Description

Severity: Low

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

Deployers should consider using filesystem mounts for `/tmp` during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/tmp` as a separate filesystem, a warning is printed in the Ansible output.

The file integrity tool must be configured to verify Access Control Lists (ACLs). (V-72069)

STIG Description

Severity: Low

ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.

Deployer/Auditor notes

Implementation Status: Implemented

CentOS 7 and Red Hat Enterprise Linux 7 already deploy a very secure AIDE configuration that checks access control lists (ACLs) and extended attributes by default. No configuration changes are applied on these systems.

However, Ubuntu lacks the rules that include ACL and extended attribute checks. The tasks in the security role will add a small configuration block at the end of the AIDE configuration file to meet the requirements of this STIG, as well as V-72071.

openSUSE Leap and SUSE Linux Enterprise 12 also lack a rule to check ACLs and extended attributes. The default configuration file is adjusted to include those as well.

The file integrity tool must be configured to verify extended attributes. (V-72071)

STIG Description

Severity: Low

Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.

Deployer/Auditor notes

Implementation Status: Implemented

CentOS 7 and Red Hat Enterprise Linux 7 already deploy a very secure AIDE configuration that checks access control lists (ACLs) and extended attributes by default. No configuration changes are applied on these systems.

However, Ubuntu lacks the rules that include ACL and extended attribute checks. The tasks in the security role will add a small configuration block at the end of the AIDE configuration file to meet the requirements of this STIG, as well as V-72069.

openSUSE Leap and SUSE Linux Enterprise 12 also lack a rule to check ACLs and extended attributes. The default configuration file is adjusted to include those as well.

The operating system must limit the number of concurrent sessions to 10 for all accounts and/or account types. (V-72217)

STIG Description

Severity: Low

Operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to DoS attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that each account is limited to 10 concurrent connections, this change might be disruptive in some environments. Therefore, this change is not applied by default.

Deployers can opt in for this change by setting a concurrent connection limit with this Ansible variable:

```
security_rhel7_concurrent_session_limit: 10
```

The system must display the date and time of the last successful account logon upon logon. (V-72275)

STIG Description

Severity: Low

Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.

Deployer/Auditor notes

Implementation Status: Verification Only

The PAM configuration is checked for the presence of `pam_lastlogin` and a warning message is printed if the directive is not found. The tasks in the security role do not adjust PAM configurations since these changes might be disruptive in some environments.

Deployers should review their PAM configurations and add `pam_lastlogin` to `/etc/pam.d/postlogin` on CentOS and Red Hat Enterprise Linux or to `/etc/pam.d/login` on Ubuntu, openSUSE Leap and SUSE Linux Enterprise.

For systems using DNS resolution, at least two name servers must be configured. (V-72281)

STIG Description

Severity: Low

To provide availability for name resolution services, multiple redundant name servers are mandated. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.

Deployer/Auditor notes

Implementation Status: Implemented

If a server has fewer than two nameservers configured in `/etc/resolv.conf`, a warning is printed in the Ansible output.

3.5.2 STIG Controls by Implementation Status

Contents

Exception - Initial Provisioning (5 controls)

A separate file system must be used for user home directories (such as /home or an equivalent). (V-72059)

STIG Description

Severity: Low

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

Deployers should consider using filesystem mounts for home directories during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/home` as a separate filesystem, a warning is printed in the Ansible output.

The system must use a separate file system for /var. (V-72061)

STIG Description

Severity: Low

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

Deployers should consider using filesystem mounts for `/var` during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/var` as a separate filesystem, a warning is printed in the Ansible output.

The system must use a separate file system for the system audit data path. (V-72063)

STIG Description

Severity: Low

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

Deployers should consider using filesystem mounts for `/var/log/audit` during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/var/log/audit` as a separate filesystem, a warning is printed in the Ansible output.

The system must use a separate file system for /tmp (or equivalent). (V-72065)

STIG Description

Severity: Low

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

Deployers should consider using filesystem mounts for `/tmp` during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/tmp` as a separate filesystem, a warning is printed in the Ansible output.

The system must not allow removable media to be used as the boot loader unless approved. (V-72075)

STIG Description

Severity: Medium

Malicious users with removable boot media can gain access to a system configured to use removable media as the boot loader. If removable media is designed to be used as the boot loader, the requirement must be documented with the Information System Security Officer (ISSO).

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

When a server is initially provisioned, deployers should avoid storing the boot loader on removable media. It is not possible to change this via automated tasks.

Exception - Manual Intervention (35 controls)

Users must provide a password for privilege escalation. (V-71947)

STIG Description

Severity: Medium

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The STIG requires all users to authenticate when using `sudo`, but this change can be highly disruptive for automated scripts or applications that cannot perform interactive authentication. Automated edits from Ansible tasks might cause authentication disruptions on some hosts, and deployers are urged to carefully review each use of the `NOPASSWD` directive in their `sudo` configuration files.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_sudoers_nopasswd_check_enable: no
```

Users must re-authenticate for privilege escalation. (V-71949)

STIG Description

Severity: Medium

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The STIG requires all users to re-authenticate when using `sudo`, but this change can be highly disruptive for automated scripts or applications that cannot perform interactive authentication. Automated edits from Ansible tasks might cause authentication disruptions on some hosts, and deployers are urged to carefully review each use of the `!authenticate` directive in their `sudo` configuration files.

The operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users) using multifactor authentication. (V-71965)

STIG Description

Severity: Medium

To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

```
1) Accesses explicitly identified and documented by the organization.␣
↪Organizations document specific user actions that can be performed on the␣
↪information system without identification or authentication;
```

and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000109-GPOS-00056, SRG-OS-000108-GPOS-00055, SRG-OS-000108-GPOS-00057, SRG-OS-000108-GPOS-00058

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deploying multi-factor authentication methods, including smart cards, is a complicated process that requires preparation and communication. This work is left to deployers to complete manually.

The operating system must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. (V-71971)

STIG Description

Severity: Medium

Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The tasks in the security role cannot determine the access levels of individual users.

Deployers are strongly encouraged to configure SELinux user confinement on compatible systems using `semanage login`. Refer to the Confining Existing Linux Users documentation from Red Hat for detailed information and command line examples.

The operating system must be a vendor supported release. (V-71997)

STIG Description

Severity: High

An operating system release is considered supported if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The STIG requires that the current release of the operating system is still supported and is actively receiving security updates. Deployers are urged to stay current with the latest releases from Ubuntu, SUSE, CentOS and Red Hat.

The following links provide more details on end of life (EOL) dates for the distributions supported by this role:

- Ubuntu releases
- CentOS EOL dates
- Red Hat Enterprise Linux Life Cycle
- openSUSE EOL dates
- SUSE Linux Enterprise

The system must not have unnecessary accounts. (V-72001)

STIG Description

Severity: Medium

Accounts providing no operational purpose provide additional opportunities for system compromise. Unnecessary accounts include user accounts for individuals not requiring access to the system and application accounts for applications not installed on the system.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers are strongly urged to review the list of user accounts on each server regularly. Evaluation of user accounts must be done on a case-by-case basis and the tasks in the security role are unable to determine which user accounts are valid. Deployers must complete this work manually.

All files and directories contained in local interactive user home directories must be owned by the owner of the home directory. (V-72023)

STIG Description

Severity: Medium

If local interactive users do not own the files in their directories, unauthorized users may be able to access them. Additionally, if files are not owned by the user, this could be an indication of system compromise.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG has requirements for ownership and permissions of files and directories in each users home directory, broad changes to these settings might cause disruptions to users on a system. Therefore, these changes are left to deployers to examine and adjust manually.

All files and directories contained in local interactive user home directories must be group-owned by a group of which the home directory owner is a member. (V-72025)

STIG Description

Severity: Medium

If a local interactive users files are group-owned by a group of which the user is not a member, unintended users may be able to access them.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG has requirements for ownership and permissions of files and directories in each users home directory, broad changes to these settings might cause disruptions to users on a system. Therefore, these changes are left to deployers to examine and adjust manually.

All files and directories contained in local interactive user home directories must have mode 0750 or less permissive. (V-72027)

STIG Description

Severity: Medium

If a local interactive user files have excessive permissions, unintended users may be able to access or modify them.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG has requirements for ownership and permissions of files and directories in each users home directory, broad changes to these settings might cause disruptions to users on a system. Therefore, these changes are left to deployers to examine and adjust manually.

All local initialization files for interactive users must be owned by the home directory user or root. (V-72029)

STIG Description

Severity: Medium

Local initialization files are used to configure the users shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all initialization files for interactive users have proper owners, group owners, and permissions, these changes are often disruptive for users. The tasks in the security role do not make any changes to user initialization files.

Deployers should review the content and discretionary access controls applied to each users initialization files in their home directory.

Local initialization files for local interactive users must be group-owned by the users primary group or root. (V-72031)

STIG Description

Severity: Medium

Local initialization files for interactive users are used to configure the users shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all initialization files for interactive users have proper owners, group owners, and permissions, these changes are often disruptive for users. The tasks in the security role do not make any changes to user initialization files.

Deployers should review the content and discretionary access controls applied to each users initialization files in their home directory.

All local initialization files must have mode 0740 or less permissive. (V-72033)

STIG Description

Severity: Medium

Local initialization files are used to configure the users shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all initialization files for interactive users have proper owners, group owners, and permissions, these changes are often disruptive for users. The tasks in the security role do not make any changes to user initialization files.

Deployers should review the content and discretionary access controls applied to each users initialization files in their home directory.

All local interactive user initialization files executable search paths must contain only paths that resolve to the users home directory. (V-72035)

STIG Description

Severity: Medium

The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory (other than the users home directory), executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. If deviations from the default system search path for the local interactive user are required, they must be documented with the Information System Security Officer (ISSO).

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all initialization files must contain executable search paths that resolve to the users home directory, this change be disruptive for most users. The tasks in the security role do not make any changes to user initialization files.

Local initialization files must not execute world-writable programs. (V-72037)

STIG Description

Severity: Medium

If user start-up files execute world-writable programs, especially in unprotected directories, they could be maliciously modified to destroy user files or otherwise compromise the system at the user level. If the system is compromised at the user level, it is easier to elevate privileges to eventually compromise the system at the root and network level.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should manually search their system for world-writable programs and change the permissions on those programs. They are easily found with this command:

```
find / -perm -002 -type f
```

World-writable executables should not be needed under almost all circumstances.

File systems that contain user home directories must be mounted to prevent files with the setuid and setgid bit set from being executed. (V-72041)

STIG Description

Severity: Medium

The nosuid mount option causes the system to not execute setuid and setgid files with owner privileges. This option must be used for mounting any file system not containing approved setuid and setguid files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should examine any filesystem mounts that contain home directories to ensure that the `nosetuid` option is set.

File systems that are used with removable media must be mounted to prevent files with the setuid and setgid bit set from being executed. (V-72043)

STIG Description

Severity: Medium

The nosuid mount option causes the system to not execute setuid and setgid files with owner privileges. This option must be used for mounting any file system not containing approved setuid and setguid files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should examine any filesystem mounts of removable media to ensure that the `nosetuid` option is set.

File systems that are being imported via Network File System (NFS) must be mounted to prevent files with the setuid and setgid bit set from being executed. (V-72045)

STIG Description

Severity: Medium

The nosuid mount option causes the system to not execute setuid and setgid files with owner privileges. This option must be used for mounting any file system not containing approved setuid and setguid files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should examine any filesystem mounts of NFS imports to ensure that the `nosetuid` option is set.

The umask must be set to 077 for all local interactive user accounts. (V-72049)

STIG Description

Severity: Medium

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 700 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be 0. This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all local interactive user accounts have a umask of `077`, this change can be disruptive for users and the applications they run. This change cannot be applied in an automated way.

Deployers should review user initialization files regularly to ensure that the umask is not specified. This allows the system-wide setting of `077` to be applied to all user sessions.

Cron logging must be implemented. (V-72051)

STIG Description

Severity: Medium

Cron logging can be used to trace the successful or unsuccessful execution of cron jobs. It can also be used to spot intrusions into the use of the cron facility by unauthorized and malicious users.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Ubuntu, CentOS, Red Hat Enterprise Linux, openSUSE Leap and SUSE Linux Enterprise already capture the logs from cron.

Ubuntu systems collect cron job logs into the main syslog file (`/var/log/syslog`) rather than separate them into their own log file. CentOS and Red Hat Enterprise Linux systems collect cron logs in `/var/log/cron`. openSUSE Leap and SUSE Linux Enterprise collect cron job in `/var/log/messages`.

Deployers should not need to adjust these configurations unless a specific environment requires it. The tasks in the security role do not make changes to the `rsyslog` configuration.

All privileged function executions must be audited. (V-72095)

STIG Description

Severity: Medium

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

This STIG is difficult to implement in an automated way because the number of applications on a system with setuid/setgid permissions changes over time. In addition, adding audit rules for some of these automatically could cause a significant increase in logging traffic when these applications are used regularly.

Deployers are urged to do the following instead:

- Minimize the amount of applications with setuid/setgid privileges
- Monitor any new applications that gain setuid/setgid privileges
- Add risky applications with setuid/setgid privileges to auditd for detailed syscall monitoring

---

The rsyslog daemon must not accept log messages from other servers unless the server is being used for log aggregation. (V-72211)

STIG Description

Severity: Medium

Unintentionally running a rsyslog server accepting remote messages puts the system at increased risk. Malicious rsyslog messages sent to the server could exploit vulnerabilities in the server software itself, could introduce misleading information in to the systems logs, or could fill the systems storage leading to a Denial of Service. If the system is intended to be a log aggregation server its use must be documented with the ISSO.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers must take manual steps to add or remove syslog reception configuration lines depending on a servers role:

- If the server is a log aggregation server, deployers must configure the server to receive syslog output from the other servers via TCP connections.
- If the server is not a log aggregation server, deployers must configure the server so that it does not accept syslog output from other servers.

The host must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management Component Local Service Assessment (PPSM CLSA) and vulnerability assessments. (V-72219)

STIG Description

Severity: Medium

In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000297-GPOS-00115

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should review each firewall rule on a regular basis to ensure that each port is open for a valid reason.

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) authentication communications. (V-72227)

STIG Description

Severity: Medium

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers are strongly urged to utilize `sssd` for systems that authenticate against LDAP or Active Directory (AD) servers.

The ldap connector for `sssd` connects only to LDAP servers over encrypted connections. Review the man page for sssd-ldap for more details on this requirement.

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications. (V-72229)

STIG Description

Severity: Medium

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers are strongly urged to utilize `sssd` for systems that authenticate against LDAP or Active Directory (AD) servers.

To meet this control, deployers must ensure that `ldap_tls_cacert` or `ldap_tls_cacertdir` are set in the `/etc/sssd/sssd.conf` file. The `ldap_tls_cacert` directive specifies a single certificate while `ldap_tls_cacertdir` specifies a directory where `sssd` can find CA certificates.

> **Warning:** Use caution when adjusting these settings. If the correct CA certificates are not already deployed to the servers that perform LDAP authentication, their attempts to authenticate users might fail.
>
> Consult with administrators of the LDAP system and test all changes on a non-production system first.

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications. (V-72231)

STIG Description

Severity: Medium

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers are strongly urged to utilize `sssd` for systems that authenticate against LDAP or Active Directory (AD) servers.

To meet this control, deployers must ensure that `ldap_tls_cacert` or `ldap_tls_cacertdir` are set in the `/etc/sssd/sssd.conf` file. The `ldap_tls_cacert` directive specifies a single certificate while `ldap_tls_cacertdir` specifies a directory where `sssd` can find CA certificates.

> **Warning:** Use caution when adjusting these settings. If the correct CA certificates are not already deployed to the servers that perform LDAP authentication, their attempts to authenticate users might fail.
>
> Consult with administrators of the LDAP system and test all changes on a non-production system first.

The Network File System (NFS) must be configured to use RPCSEC_GSS. (V-72311)

STIG Description

Severity: Medium

When an NFS server is configured to use RPCSEC_SYS, a selected userid and groupid are used to handle requests from the remote user. The userid and groupid could mistakenly or maliciously be set incorrectly. The RPCSEC_GSS method of authentication uses certificates on the server and client systems to more securely authenticate the remote mount request.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers using NFS should examine their mounts to ensure `krb5:krb5i:krb5p` is provided with the `sec` option. Kerberos must be installed and configured before making the change.

The system access control program must be configured to grant or deny system access to specific hosts and services. (V-72315)

STIG Description

Severity: Medium

If the systems access control program is not configured with appropriate rules for allowing and denying access to system network resources, services may be accessible to unauthorized hosts.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The `firewalld` service is optionally enabled and configured in the tasks for another STIG control:

- *The operating system must enable an application firewall, if available. (V-72273)*

Deployers should review their `firewalld` ruleset regularly to ensure that each firewall rule is specific as possible. Each rule should allow the smallest number of hosts to access the smallest number of services.

The system must not have unauthorized IP tunnels configured. (V-72317)

STIG Description

Severity: Medium

IP tunneling mechanisms can be used to bypass network filtering. If tunneling is required, it must be documented with the Information System Security Officer (ISSO).

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should review all tunneled connections on a regular basis to ensure each is valid and properly secured. This requires careful verification that cannot be done with automated Ansible tasks.

The operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules (PAM). (V-72427)

STIG Description

Severity: Medium

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that the `sssd.conf` contains both `nss` and `pam` authentication modules, this change can be disruptive in environments that are already using LDAP or Active Directory for authentication. Deployers should make these changes only if their environment is compatible.

The operating system must implement certificate status checking for PKI authentication. (V-72433)

STIG Description

Severity: Medium

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Any adjustment to PKI authentication can cause disruptions for users. Deployers should verify that enabling OCSP validation is compatible with their existing configuration.

The operating system must implement smart card logons for multifactor authentication for access to privileged accounts. (V-72435)

STIG Description

Severity: Medium

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Any adjustment to PKI authentication can cause disruptions for users. Deployers should verify that their environment is compatible with smart cards before requiring them for authentication.

File systems that are being imported via Network File System (NFS) must be mounted to prevent binary files from being executed. (V-73161)

STIG Description

Severity: Medium

The noexec mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should review their NFS mounts to ensure they are mounted with the `noexec` option. Deployers should skip this change if they execute applications from NFS mounts.

Wireless network adapters must be disabled. (V-73177)

STIG Description

Severity: Medium

The use of wireless networking can introduce many different attack vectors into the organizations network. Common attack vectors such as malicious association and ad hoc networks will allow an attacker to spoof a wireless access point (AP), allowing validated systems to connect to the malicious AP and enabling the attacker to monitor and record network traffic. These malicious APs can also serve to create a man-in-the-middle attack or be used to create a denial of service to valid network resources.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should review the configuration of any wireless networking device connected to the system to ensure it must be enabled. The STIG requires that all wireless network devices are enabled unless required.

The operating system must uniquely identify and must authenticate users using multifactor authentication via a graphical user logon. (V-77819)

STIG Description

Severity: Medium

To assure accountability and prevent unauthenticated access, users must be identified and authenticated to prevent potential misuse and compromise of the system.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

Satisfies: SRG-OS-000375-GPOS-00161,SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The STIG requires that multifactor authentication is used for graphical user logon, but this change requires custom configuration based on the authentication solution that is used.

Deployers should review the available options, such as traditional smartcards, USB devices (such as Yubikeys), or software token systems, and use one of these solutions on each system.

The operating system must require authentication upon booting into single-user and maintenance modes. (V-77823)

STIG Description

Severity: Medium

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Modifying sensitive systemd unit files directly or via overrides could cause a system to have issues during the boot process. The role does not make any adjustments to the `rescue.service` because this service is critical during emergencies.

All of the distributions supported by the role already require authentication for single user mode.

Implemented (136 controls)

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon. (V-71859)

STIG Description

Severity: Medium

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is␣
↪provided for USG-authorized use only.
```

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

```
-The USG routinely intercepts and monitors communications on this IS for␣
↪purposes including, but not limited to, penetration testing, COMSEC␣
↪monitoring, network operations and defense, personnel misconduct (PM), law␣
↪enforcement (LE), and counterintelligence (CI) investigations.
```

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interestsnot for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
"I've read  consent to terms in IS user agreem't."
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role configure `dconf` to display a login banner each time a graphical session starts on the system. The default banner message set by the role is:

> You are accessing a secured system and your actions will be logged along with identifying information. Disconnect immediately if you are not an authorized user of this system.

Deployers can customize this message by setting an Ansible variable:

```
security_enable_graphical_login_message_text: >
    This is a customized banner message.
```

> **Warning:** The dconf configuration does not support multi-line strings. Ensure that `security_enable_graphical_login_message_text` contains a single line of text.

In addition, deployers can opt out of displaying a login banner message by changing `security_enable_graphical_login_message` to `no`.

The operating system must display the approved Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon. (V-71861)

STIG Description

Severity: Medium

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is␣
↪provided for USG-authorized use only.
```

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

```
-The USG routinely intercepts and monitors communications on this IS for␣
↪purposes including, but not limited to, penetration testing, COMSEC␣
↪monitoring, network operations and defense, personnel misconduct (PM), law␣
↪enforcement (LE), and counterintelligence (CI) investigations.
```

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interestsnot for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Deployer/Auditor notes

Implementation Status: Implemented

The security role configures a login banner for graphical logins using `dconf`. Deployers can opt out of this change by setting the following Ansible variable:

```
security_enable_graphical_login_message: no
```

The message is customized by setting another Ansible variable:

```
security_enable_graphical_login_message_text: >
    You are accessing a secured system and your actions will be logged along
    with identifying information. Disconnect immediately if you are not an
    authorized user of this system.
```

Note: The space available for the graphical banner is relatively short. Deployers should limit the length of their graphical login banners to the shortest length possible.

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a command line user logon. (V-71863)

STIG Description

Severity: Medium

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is␣
↪provided for USG-authorized use only.
```

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

```
-The USG routinely intercepts and monitors communications on this IS for␣
↪purposes including, but not limited to, penetration testing, COMSEC␣
↪monitoring, network operations and defense, personnel misconduct (PM), law␣
↪enforcement (LE), and counterintelligence (CI) investigations.
```

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interestsnot for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
"I've read  consent to terms in IS user agreem't."
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007

Deployer/Auditor notes

Implementation Status: Implemented

The security role already deploys a login banner for console logins with tasks from another STIG:

- *The Standard Mandatory DoD Notice and Consent Banner must be displayed immediately prior to, or as part of, remote access logon prompts. (V-72225)*

The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. (V-71891)

STIG Description

Severity: Medium

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

Regardless of where the session lock is determined and implemented, once invoked, the session lock must remain in place until the user reauthenticates. No other activity aside from reauthentication must unlock the system.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that graphical sessions are locked when the screensaver starts and that users must re-enter credentials to restore access to the system. The screensaver lock is enabled by default if `dconf` is present on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_lock_session: no
```

The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces. (V-71893)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that the screensaver appears when a session reaches a certain period of inactivity. The tasks will enable the screensaver for inactive sessions by default.

Deployers can opt out of this change by setting an Ansible variable:

```
security_lock_session_when_inactive: no
```

The operating system must set the idle delay setting for all connection types. (V-71895)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces. (V-71893)*

The operating system must have the screen package installed. (V-71897)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The screen package allows for a session lock to be implemented and configured.

Deployer/Auditor notes

Implementation Status: Implemented

The role will ensure that the `screen` package is installed.

The operating system must initiate a session lock for the screensaver after a period of inactivity for graphical user interfaces. (V-71899)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces. (V-71893)*

The operating system must initiate a session lock for graphical user interfaces when the screensaver is activated. (V-71901)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that a graphical session is locked when the screensaver starts. This requires a user to re-enter their credentials to regain access to the system.

The tasks will set a timeout of 5 seconds after the screensaver has started before the session is locked. This gives a user a few seconds to press a key or wiggle their mouse after the screensaver appears without needing to re-enter their credentials.

Deployers can adjust this timeout by setting an Ansible variable:

```
security_lock_session_screensaver_lock_delay: 5
```

The PAM system service must be configured to store only encrypted representations of passwords. (V-71919)

STIG Description

Severity: Medium

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Deployer/Auditor notes

Implementation Status: Implemented

The PAM configuration file for password storage is checked to ensure that `sha512` is found on the `pam_unix.so` line. If `sha512` is not found, a debug message is printed in the Ansible output.

The shadow file must be configured to store only encrypted representations of passwords. (V-71921)

STIG Description

Severity: Medium

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Deployer/Auditor notes

Implementation Status: Implemented

The default password storage mechanism for Ubuntu 16.04, CentOS 7, openSUSE Leap, SUSE Linux Enterprise 12 and Red Hat Enterprise Linux 7 is `SHA512` and the tasks in the security role ensure that the default is maintained.

Deployers can configure a different password storage mechanism by setting the following Ansible variable:

```
security_password_encrypt_method: SHA512
```

> **Warning:** SHA512 is the default on most modern Linux distributions and it meets the requirement of the STIG. Do not change the value unless a system has a specific need for a different password mechanism.

The system must not have accounts configured with blank or null passwords. (V-71937)

STIG Description

Severity: High

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Deployer/Auditor notes

Implementation Status: Implemented

The Ansible tasks will ensure that PAM is configured to disallow logins from accounts with null or blank passwords. This involves removing a single option from one of the PAM configuration files:

- CentOS or RHEL: removes `nullok` from `/etc/pam.d/system-auth`
- Ubuntu: removes `nullok_secure` from `/etc/pam.d/common-auth`
- openSUSE Leap or SLE: remove `nullok` from `/etc/pam.d/common-auth` and `/etc/pam.d/common-password`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_disallow_blank_password_login: no
```

The SSH daemon must not allow authentication using an empty password. (V-71939)

STIG Description

Severity: High

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Deployer/Auditor notes

Implementation Status: Implemented

The `PermitEmptyPasswords` configuration will be set to `no` in `/etc/ssh/sshd_config` and sshd will be restarted. This disallows logins over ssh for users with a empty or null password set.

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_sshd_disallow_empty_password: no
```

The delay between logon prompts following a failed console logon attempt must be at least four seconds. (V-71951)

STIG Description

Severity: Medium

Configuring the operating system to implement organization-wide security implementation guides and security checklists verifies compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the Ansible role set a four second delay between failed login attempts. Deployers can configure a different delay (in seconds) by setting the following Ansible variable:

```
security_shadow_utils_fail_delay: 4
```

The operating system must not allow an unattended or automatic logon to the system via a graphical user interface. (V-71953)

STIG Description

Severity: High

Failure to restrict system access to authenticated users negatively impacts operating system security.

Deployer/Auditor notes

Implementation Status: Implemented

If `AutomaticLoginEnable=true` exists in the gdm configuration file, `/etc/gdm/custom.conf`, the configuration will removed. This disallows automatic logins for gdm and requires a user to complete the username and password prompts.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_disable_gdm_automatic_login: no
```

The operating system must not allow an unrestricted logon to the system. (V-71955)

STIG Description

Severity: High

Failure to restrict system access to authenticated users negatively impacts operating system security.

Deployer/Auditor notes

Implementation Status: Implemented

If `TimedLoginEnable=true` exists in the gdm configuration file, `/etc/gdm/custom.conf`, the configuration will removed. This disallows timed logins for guest users in gdm.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_disable_gdm_timed_login: no
```

The operating system must not allow users to override SSH environment variables. (V-71957)

STIG Description

Severity: Medium

Failure to restrict system access to authenticated users negatively impacts operating system security.

Deployer/Auditor notes

Implementation Status: Implemented

The `PermitUserEnvironment` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_environment_override: no
```

The operating system must not allow a non-certificate trusted host SSH logon to the system. (V-71959)

STIG Description

Severity: Medium

Failure to restrict system access to authenticated users negatively impacts operating system security.

Deployer/Auditor notes

Implementation Status: Implemented

The `HostbasedAuthentication` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_host_based_auth: no
```

The rsh-server package must not be installed. (V-71967)

STIG Description

Severity: High

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The rsh-server service provides an unencrypted remote access service that does not provide for the confidentiality and integrity of user passwords or the remote session and has very weak authentication.

If a privileged user were to log on using this service, the privileged user password could be compromised.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the `rsh-server` package from the system if it is installed. Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_rsh_server: no
```

The ypserv package must not be installed. (V-71969)

STIG Description

Severity: High

Removing the ypserv package decreases the risk of the accidental (or intentional) activation of NIS or NIS+ services.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the NIS server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `ypserv`
- Ubuntu: `nis`
- openSUSE Leap: `ypserv`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_ypserv: no
```

Designated personnel must be notified if baseline configurations are changed in an unauthorized manner. (V-71975)

STIG Description

Severity: Medium

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating systems Information Management Officer (IMO)/Information System Security Officer (ISSO) and System Administrators (SAs) must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Deployer/Auditor notes

Implementation Status: Implemented

The cron job for AIDE is configured to send emails to the root user after each AIDE run.

The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components from a repository without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization. (V-71977)

STIG Description

Severity: High

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Deployer/Auditor notes

Implementation Status: Implemented

On Ubuntu systems, the tasks check for the `AllowUnauthenticated` string anywhere in the apt configuration files found within `/etc/apt/apt.conf.d/`. If the string is found, a warning is printed on the console.

On CentOS 7 systems, the tasks set the `gpgcheck` option to `1` in the `/etc/yum.conf` file. This enables GPG checks for all packages installed with `yum`.

On openSUSE Leap systems, the tasks set the `gpgcheck` option to `1` in the `/etc/zypp/zypp.conf` file. This enables GPG checks for all packages installed with `zypper`.

Setting `security_enable_gpgcheck_packages` to `no` will skip the `AllowUnauthenticated` string check on Ubuntu and it will set `gpgcheck=0` in `/etc/yum.conf` or `/etc/zypp/zypp.conf` on CentOS and openSUSE Leap systems respectively.

The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization. (V-71979)

STIG Description

Severity: High

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Deployer/Auditor notes

Implementation Status: Implemented

On Ubuntu systems, the tasks comment out the `no-debsig` configuration line in `/etc/dpkg/dpkg.cfg`. This causes `dpkg` to verify GPG signatures for all packages that are installed locally.

On CentOS 7 systems, the tasks set the `localpkg_gpgcheck` option to 1 in the `/etc/yum.conf` file. This enables GPG checks for all packages installed locally with `yum`.

On openSUSE Leap systems, the tasks set the `gpgcheck` option to 1 in the `/etc/zypp/zypp.conf` file. This enables GPG checks for all packages installed with `zypper`.

Setting `security_enable_gpgcheck_packages_local` to `no` will skip the `no-debsig` adjustment on Ubuntu and it will set `local_gpgcheck=0` in `/etc/yum.conf` on CentOS systems. Similarly, on openSUSE Leap systems, it will set `gpgcheck=0` in `/etc/zypp/zypp.conf`.

File system automounter must be disabled unless required. (V-71985)

STIG Description

Severity: Medium

Automatically mounting file systems permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Deployer/Auditor notes

Implementation Status: Implemented

The `autofs` service is stopped and disabled if it is found on the system. Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_disable_autofs: no
```

The operating system must enable SELinux. (V-71989)

STIG Description

Severity: High

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to,

establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role enable the appropriate Linux Security Module (LSM) for the operating system.

For Ubuntu, openSUSE and SUSE Linux Enterprise 12 systems, AppArmor is installed and enabled. This change takes effect immediately.

For CentOS or Red Hat Enterprise Linux systems, SELinux is enabled (in enforcing mode) and its user tools are automatically installed. If SELinux is not in enforcing mode already, a reboot is required to enable SELinux and relabel the filesystem.

> **Warning:** Relabeling a filesystem takes time and the server must be offline for the relabeling to complete. Filesystems with large amounts of files and filesystems on slow disks will cause the relabeling process to take more time.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_enable_linux_security_module: no
```

The operating system must enable the SELinux targeted policy. (V-71991)

STIG Description

Severity: High

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Deployer/Auditor notes

Implementation Status: Implemented

The SELinux targeted policy is enabled on CentOS 7 and Red Hat systems. AppArmor only has one set of policies, so this change has no effect on Ubuntu, openSUSE Leap and SUSE systems running AppArmor.

For more information on this change and how to opt out, refer to *The operating system must enable SELinux. (V-71989)*.

The x86 Ctrl-Alt-Delete key sequence must be disabled. (V-71993)

STIG Description

Severity: High

A locally logged-on user who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In the GNOME graphical environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role disable the control-alt-delete key sequence by masking its systemd service unit.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_disable_ctrl_alt_delete: no
```

All Group Identifiers (GIDs) referenced in the /etc/passwd file must be defined in the /etc/group file. (V-72003)

STIG Description

Severity: Low

If a user is assigned the GID of a group not existing on the system, and a group with the GID is subsequently created, the user may have unintended rights to any files associated with the group.

Deployer/Auditor notes

Implementation Status: Implemented

If any users are found with invalid GIDs, those users are printed in the Ansible output. Deployers should review the list and ensure all users are assigned to a valid group that is defined in `/etc/group`.

The root account must be the only account having unrestricted access to the system. (V-72005)

STIG Description

Severity: High

If an account other than root also has a User Identifier (UID) of 0, it has root authority, giving that account unrestricted access to the entire operating system. Multiple accounts with a UID of 0 afford an opportunity for potential intruders to guess a password for a privileged account.

Deployer/Auditor notes

Implementation Status: Implemented

If an account with UID 0 other than `root` exists on the system, the playbook will fail with an error message that includes the other accounts which have a UID of 0.

Deployers are strongly urged to keep only one account with UID 0, `root`, and to use `sudo` any situations where root access is required.

All local interactive users must have a home directory assigned in the /etc/passwd file. (V-72011)

STIG Description

Severity: Medium

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Deployer/Auditor notes

Implementation Status: Implemented

The usernames of all users without home directories assigned are provided in the Ansible console output. Deployers should use this list of usernames to audit each system to ensure every user has a valid home directory.

All local interactive user accounts, upon creation, must be assigned a home directory. (V-72013)

STIG Description

Severity: Medium

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Deployer/Auditor notes

Implementation Status: Implemented

The `CREATE_HOME` variable is set to `yes` by the tasks in the security role. This ensures that home directories are created each time a new user account is created.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_shadow_utils_create_home: no
```

Note: On CentOS 7, Red Hat Enterprise Linux 7 systems, openSUSE Leap and SUSE Linux Enterprise 12, home directories are always created with new users by default. Home directories are not created by default on Ubuntu systems.

All local interactive user home directories defined in the /etc/passwd file must exist. (V-72015)

STIG Description

Severity: Medium

If a local interactive user has a home directory defined that does not exist, the user may be given access to the / directory as the current working directory upon logon. This could create a Denial of Service because the user would not be able to access their logon configuration files, and it may give them visibility to system files they normally would not be able to access.

Deployer/Auditor notes

Implementation Status: Implemented

Each interactive user on the system is checked to verify that their assigned home directory exists on the filesystem. If a home directory is missing, the name of the user and their assigned home directory is printed in the Ansible console output.

If the cron.allow file exists it must be owned by root. (V-72053)

STIG Description

Severity: Medium

If the owner of the cron.allow file is not set to root, the possibility exists for an unauthorized user to view or to edit sensitive information.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role check for the existence of `/etc/cron.allow` and set both the user and group ownership to `root`. This is the default on Ubuntu, CentOS, Red Hat Enterprise Linux systems, openSUSE Leap and SUSE Linux Enterprise 12 already.

If the cron.allow file exists it must be group-owned by root. (V-72055)

STIG Description

Severity: Medium

If the group owner of the cron.allow file is not set to root, sensitive information could be viewed or edited by unauthorized users.

Deployer/Auditor notes

Implementation Status: Implemented

The group ownership for `/etc/cron.allow` is already set by the task for the following STIG control:

If the cron.allow file exists it must be owned by root. (V-72053)

Kernel core dumps must be disabled unless needed. (V-72057)

STIG Description

Severity: Medium

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in denial of service by exhausting the available space on the target file system partition.

Deployer/Auditor notes

Implementation Status: Implemented

The `kdump` service is disabled if it exists on the system. Deployers can opt out of this change by setting the following Ansible variable:

```
security_disable_kdump: no
```

The file integrity tool must be configured to verify Access Control Lists (ACLs). (V-72069)

STIG Description

Severity: Low

ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.

Deployer/Auditor notes

Implementation Status: Implemented

CentOS 7 and Red Hat Enterprise Linux 7 already deploy a very secure AIDE configuration that checks access control lists (ACLs) and extended attributes by default. No configuration changes are applied on these systems.

However, Ubuntu lacks the rules that include ACL and extended attribute checks. The tasks in the security role will add a small configuration block at the end of the AIDE configuration file to meet the requirements of this STIG, as well as V-72071.

openSUSE Leap and SUSE Linux Enterprise 12 also lack a rule to check ACLs and extended attributes. The default configuration file is adjusted to include those as well.

The file integrity tool must be configured to verify extended attributes. (V-72071)

STIG Description

Severity: Low

Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.

Deployer/Auditor notes

Implementation Status: Implemented

CentOS 7 and Red Hat Enterprise Linux 7 already deploy a very secure AIDE configuration that checks access control lists (ACLs) and extended attributes by default. No configuration changes are applied on these systems.

However, Ubuntu lacks the rules that include ACL and extended attribute checks. The tasks in the security role will add a small configuration block at the end of the AIDE configuration file to meet the requirements of this STIG, as well as V-72069.

openSUSE Leap and SUSE Linux Enterprise 12 also lack a rule to check ACLs and extended attributes. The default configuration file is adjusted to include those as well.

The file integrity tool must use FIPS 140-2 approved cryptographic hashes for validating file contents and directories. (V-72073)

STIG Description

Severity: Medium

File integrity tools use cryptographic hashes for verifying file contents and directories have not been altered. These hashes must be FIPS 140-2 approved cryptographic hashes.

Deployer/Auditor notes

Implementation Status: Implemented

The default AIDE configuration in CentOS 7, Red Hat Enterprise Linux 7, openSUSE Leap and SUSE Linux Enterprise 12 already uses SHA512 to validate file contents and directories. No changes are required on these systems.

The tasks in the security role add a rule to end of the AIDE configuration on Ubuntu systems that uses SHA512 for validation.

The telnet-server package must not be installed. (V-72077)

STIG Description

Severity: High

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the telnet server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `telnet-server`
- Ubuntu: `telnetd`
- openSUSE Leap: `telnet-server`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_telnet_server: no
```

Auditing must be configured to produce records containing information to establish what type of events occurred, where the events occurred, the source of the events, and the outcome of the events.

These audit records must also identify individual identities of group account users. (V-72079)

STIG Description

Severity: High

Without establishing what type of events occurred, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in the operating system audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured operating system.

Satisfies: SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000042-GPOS-00021, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role start the audit daemon immediately and ensure that it starts at boot time.

The operating system must shut down upon audit processing failure, unless availability is an overriding concern. If availability is a concern, the system must alert the designated staff (System Administrator [SA] and Information System Security Officer [ISSO] at a minimum) in the event of an audit processing failure. (V-72081)

STIG Description

Severity: Medium

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Satisfies: SRG-OS-000046-GPOS-00022, SRG-OS-000047-GPOS-00023

Deployer/Auditor notes

Implementation Status: Implemented

The audit daemon takes various actions when there is an auditing failure. There are three options for the `-f` flag for `auditctl`:

- `0`: In the event of an auditing failure, do nothing.
- `1`: In the event of an auditing failure, write messages to the kernel log.
- `2`: In the event of an auditing failure, cause a kernel panic.

Most operating systems set the failure flag to `1` by default, which maximizes system availability while still causing an alert. The tasks in the security role set the flag to `1` by default.

Deployers can adjust the following Ansible variable to customize the failure flag:

```
security_rhel7_audit_failure_flag: 1
```

> **Warning:** Setting the failure flag to `2` is **strongly** discouraged unless the security of the system takes priority over its availability. Any failure in auditing causes a kernel panic and the system requires a hard reboot.

The audit system must take appropriate action when the audit storage volume is full. (V-72087)

STIG Description

Severity: Medium

Taking appropriate action in case of a filled audit storage volume will minimize the possibility of losing audit records.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role set the `disk_full_action` and `network_failure_action` to `syslog` in the audispd remote configuration. In the event of a full disk on the remote log server or a network interruption, the local system sends warnings to syslog. This is the safest option since it maximizes the availability of the local system.

Deployers have two other options available:

- `single`: Switch the local server into single-user mode in the event of a logging failure.
- `halt`: Shut off the local server gracefully in the event of a logging failure.

> **Warning:** Choosing `single` or `halt` causes a server to go into a degraded or offline state immediately after a logging failure.

Deployers can adjust these configurations by setting the following Ansible variables (the safe defaults are shown here):

```
security_rhel7_auditd_disk_full_action: syslog
security_rhel7_auditd_network_failure_action: syslog
```

The operating system must immediately notify the System Administrator (SA) and Information System Security Officer ISSO (at a minimum) when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity. (V-72089)

STIG Description

Severity: Medium

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

Deployer/Auditor notes

Implementation Status: Implemented

The `space_left` configuration is set to 25% of the size of the disk mounted on `/`. This calculation is done automatically.

Deployers can set a custom threshold for the `space_left` configuration (in megabytes) by setting the following Ansible variable:

```
# Example: A setting of 1GB (1024MB)
security_rhel7_auditd_space_left: 1024
```

The operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) via email when the threshold for the repository maximum audit record storage capacity is reached. (V-72091)

STIG Description

Severity: Medium

If security personnel are not notified immediately when the threshold for the repository maximum audit record storage capacity is reached, they are unable to expand the audit record storage capacity before records are lost.

Deployer/Auditor notes

Implementation Status: Implemented

The `space_left_action` in the audit daemon configuration is set to `email`. This configuration causes the root user to receive an email when the `space_left` threshold is reached.

Deployers can customize this configuration by setting the following Ansible variable:

```
security_rhel7_auditd_space_left_action: email
```

The operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached. (V-72093)

STIG Description

Severity: Medium

If security personnel are not notified immediately when the threshold for the repository maximum audit record storage capacity is reached, they are unable to expand the audit record storage capacity before records are lost.

Deployer/Auditor notes

Implementation Status: Implemented

The `action_mail_acct` configuration in the audit daemon configuration file is set to `root` to meet the requirements of the STIG. Deployers can customize the recipient of the emails that come from auditd by setting the following Ansible variable:

```
security_rhel7_auditd_action_mail_acct: root
```

All uses of the setxattr command must be audited. (V-72111)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `setxattr` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_setxattr: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the removexattr command must be audited. (V-72117)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `removexattr` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_removexattr: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the creat command must be audited. (V-72123)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `creat` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_creat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the open command must be audited. (V-72125)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `open` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_open: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the openat command must be audited. (V-72127)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `openat` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_openat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the open_by_handle_at command must be audited. (V-72129)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `open_by_handle_at` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_open_by_handle_at: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the truncate command must be audited. (V-72131)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `truncate` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_truncate: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the ftruncate command must be audited. (V-72133)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `ftruncate` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_ftruncate: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the semanage command must be audited. (V-72135)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit any time the `semanage` command is used.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_semanage: no
```

All uses of the setsebool command must be audited. (V-72137)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit any time the `setsebool` command is used.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_setsebool: no
```

All uses of the chcon command must be audited. (V-72139)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `chcon` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_chcon: no
```

All uses of the setfiles command must be audited. (V-72141)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `restorecon` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_restorecon: no
```

The operating system must generate audit records for all successful/unsuccessful account access count events. (V-72143)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all successful and unsuccessful account access events. Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_audit_account_access: no
```

The operating system must generate audit records for all unsuccessful account access events. (V-72145)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all successful/unsuccessful account access count events. (V-72143)*

The operating system must generate audit records for all successful account access events. (V-72147)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time an account is accessed.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_account_access: no
```

All uses of the passwd command must be audited. (V-72149)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `passwd` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_passwd_command: no
```

All uses of the unix_chkpwd command must be audited. (V-72151)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `unix_chkpwd` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_unix_chkpwd: no
```

All uses of the gpasswd command must be audited. (V-72153)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `gpasswd` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_gpasswd: no
```

All uses of the chage command must be audited. (V-72155)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `chage` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_chage: no
```

All uses of the userhelper command must be audited. (V-72157)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `userhelper` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_userhelper: no
```

All uses of the su command must be audited. (V-72159)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `su` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_su: no
```

All uses of the sudo command must be audited. (V-72161)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `sudo` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_sudo: no
```

All uses of the sudoers command must be audited. (V-72163)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time a user manages the configuration files for `sudo`.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_sudo_config_changes: no
```

All uses of the newgrp command must be audited. (V-72165)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `newgrp` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_newgrp: no
```

All uses of the chsh command must be audited. (V-72167)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `chsh` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_chsh: no
```

All uses of the sudoedit command must be audited. (V-72169)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `sudoedit` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_sudoedit: no
```

All uses of the mount command must be audited. (V-72171)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `mount` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_mount: no
```

All uses of the umount command must be audited. (V-72173)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `umount` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_umount: no
```

All uses of the postdrop command must be audited. (V-72175)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `postdrop` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_postdrop: no
```

All uses of the postqueue command must be audited. (V-72177)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `postqueue` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_postqueue: no
```

All uses of the ssh-keysign command must be audited. (V-72179)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged ssh commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `ssh-keysign` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_ssh_keysign: no
```

All uses of the crontab command must be audited. (V-72183)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `crontab` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_crontab: no
```

All uses of the pam_timestamp_check command must be audited. (V-72185)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `pam_timestamp_check` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_pam_timestamp_check: no
```

All uses of the init_module command must be audited. (V-72187)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `init_module` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_init_module: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the delete_module command must be audited. (V-72189)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `delete_module` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_delete_module: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the insmod command must be audited. (V-72191)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `insmod` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_insmod: no
```

All uses of the rmmod command must be audited. (V-72193)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `rmmod` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_rmmod: no
```

All uses of the modprobe command must be audited. (V-72195)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `modprobe` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_modprobe: no
```

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000476-GPOS-00221

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time that an account is modified. This includes changes to the following files:

- `/etc/group`
- `/etc/passwd`
- `/etc/gshadow`
- `/etc/shadow`
- `/etc/security/opasswd`

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_account_actions: no
```

All uses of the rename command must be audited. (V-72199)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `rename` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_rename: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the renameat command must be audited. (V-72201)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `renameat` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_renameat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the rmdir command must be audited. (V-72203)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `rmdir` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_rmdir: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the unlink command must be audited. (V-72205)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `unlink` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_unlink: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the unlinkat command must be audited. (V-72207)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `unlinkat` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_unlinkat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

The system must update the virus scan program every seven days or more frequently. (V-72215)

STIG Description

Severity: Medium

Virus scanning software can be used to protect a system from penetration from computer viruses and to limit their spread through intermediate systems.

The virus scanning software should be configured to check for software and virus definition updates with a frequency no longer than seven days. If a manual process is required to update the virus scan software or definitions, it must be documented with the Information System Security Officer (ISSO).

Deployer/Auditor notes

Implementation Status: Implemented

By default, CentOS 7, Red Hat Enterprise Linux 7, openSUSE Leap and SUSE Linux Enterprise 12 check for virus database updates 12 times a day. Ubuntu servers have a default of 24 checks per day.

The tasks in the security role do not adjust these defaults as they are more secure than the STIGs requirement.

A FIPS 140-2 approved cryptographic algorithm must be used for SSH communications. (V-72221)

STIG Description

Severity: Medium

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

Operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general purpose computing system.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173

Deployer/Auditor notes

Implementation Status: Implemented

The `Ciphers` configuration is set to `aes128-ctr,aes192-ctr,aes256-ctr` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can change the list of ciphers by setting the following Ansible variable:

```
security_sshd_cipher_list: 'cipher1,cipher2,cipher3'
```

All network connections associated with a communication session must be terminated at the end of the session or after 10 minutes of inactivity from the user at a command prompt, except to fulfill documented and validated mission requirements. (V-72223)

STIG Description

Severity: Medium

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role set a 600 second (10 minute) timeout for network connections associated with a communication session. Deployers can change the timeout value by setting the following Ansible variable:

```
# Example: shorten the timeout to 5 minutes (300 seconds)
security_rhel7_session_timeout: 300
```

The Standard Mandatory DoD Notice and Consent Banner must be displayed immediately prior to, or as part of, remote access logon prompts. (V-72225)

STIG Description

Severity: Medium

Display of a standardized and approved use notification before granting access to the publicly accessible operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is␣
↪provided for USG-authorized use only.
```

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

```
-The USG routinely intercepts and monitors communications on this IS for␣
↪purposes including, but not limited to, penetration testing, COMSEC␣
↪monitoring, network operations and defense, personnel misconduct (PM), law␣
↪enforcement (LE), and counterintelligence (CI) investigations.
```

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interestsnot for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007 , SRG-OS-000228-GPOS-00088

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role deploy a standard notice and consent banner into `/etc/motd` on each server. Ubuntu, CentOS, Red Hat Enterprise Linux, openSUSE Leap and SUSE Linux Enterprise display this banner after each successful login via ssh or the console.

Deployers can choose a different destination for the banner by setting the following Ansible variable:

```
security_sshd_banner_file: /etc/motd
```

The message is customized with the following Ansible variable:

```
security_login_banner_text: |
  ------------------------------------------------------------------------
↪--
  * WARNING                                                              ␣
↪ *
  * You are accessing a secured system and your actions will be logged along ␣
↪ *
  * with identifying information. Disconnect immediately if you are not an ␣
↪ *
  * authorized user of this system.                                       ␣
↪ *
  ------------------------------------------------------------------------
↪--
```

All networked systems must have SSH installed. (V-72233)

STIG Description

Severity: Medium

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that every system has an ssh client and server installed. The role installs the following packages:

- CentOS: `openssh-clients`, `openssh-server`
- Ubuntu: `openssh-client`, `openssh-server`
- openSUSE Leap: `openssh`

All networked systems must use SSH for confidentiality and integrity of transmitted and received information as well as information during preparation for transmission. (V-72235)

STIG Description

Severity: Medium

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000423-GPOS-00188, SRG-OS-000423-GPOS-00189, SRG-OS-000423-GPOS-00190

Deployer/Auditor notes

Implementation Status: Implemented

The STIG has a requirement that the `sshd` daemon is running and enabled at boot time. The tasks in the security role ensure that these requirements are met.

Some deployers may not have `sshd` enabled on highly specialized systems and those deployers should opt out of this change by setting the following Ansible variable:

```
security_enable_sshd: no
```

Note: Setting `security_enable_sshd` to `no` causes the tasks to ignore the state of the service entirely. A setting of `no` does not stop or alter the `sshd` service.

All network connections associated with SSH traffic must terminate at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements. (V-72237)

STIG Description

Severity: Medium

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that

has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Deployer/Auditor notes

Implementation Status: Implemented

The `ClientAliveInterval` configuration is set to `600` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can adjust the length of the interval by changing the following Ansible variable:

```
security_sshd_client_alive_interval: 600
```

Note: The STIG requires that `ClientAliveInterval` is set to 600 and `ClientAliveCountMax` is set to zero, which sets a 10 minute session timeout. If no data is transferred in a 10 minute period, the session is disconnected.

The `ClientAliveInterval` specifies how long the ssh daemon waits before it sends a message to the client to see if it is still alive. The `ClientAliveCountMax` specifies how many of these messages are sent without receiving a response.

Deployers should refer to *All network connections associated with SSH traffic must terminate after a period of inactivity. (V-72241)* to customize the `ClientAliveCountMax` setting.

The SSH daemon must not allow authentication using RSA rhosts authentication. (V-72239)

STIG Description

Severity: Medium

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Deployer/Auditor notes

Implementation Status: Implemented

This STIG is already applied by the changes for *The SSH daemon must not allow authentication using known hosts authentication. (V-72249)*.

All network connections associated with SSH traffic must terminate after a period of inactivity. (V-72241)

STIG Description

Severity: Medium

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Deployer/Auditor notes

Implementation Status: Implemented

The `ClientAliveCountMax` configuration is set to `0` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can adjust the maximum amount of client alive intervals by changing the following Ansible variable.

```
security_sshd_client_alive_count_max: 0
```

Note: The STIG requires that `ClientAliveInterval` is set to 600 and `ClientAliveCountMax` is set to zero, which sets a 10 minute session timeout. If no data is transferred in a 10 minute period, the session is disconnected.

The `ClientAliveInterval` specifies how long the ssh daemon waits before it sends a message to the client to see if it is still alive. The `ClientAliveCountMax` specifies how many of these messages are sent without receiving a response.

Deployers should refer to *All network connections associated with SSH traffic must terminate at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements. (V-72237)* to customize the `ClientAliveInterval` setting.

The SSH daemon must not allow authentication using rhosts authentication. (V-72243)

STIG Description

Severity: Medium

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Deployer/Auditor notes

Implementation Status: Implemented

The `IgnoreRhosts` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_rhosts_auth: no
```

The system must display the date and time of the last successful account logon upon an SSH logon. (V-72245)

STIG Description

Severity: Medium

Providing users with feedback on when account accesses via SSH last occurred facilitates user recognition and reporting of unauthorized account use.

Deployer/Auditor notes

Implementation Status: Implemented

The `PrintLastLog` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_print_last_log: no
```

The system must not permit direct logons to the root account using remote access via SSH. (V-72247)

STIG Description

Severity: Medium

Even though the communications channel may be encrypted, an additional layer of security is gained by extending the policy of not logging on directly as root. In addition, logging on with a user-specific account provides individual accountability of actions performed on the system.

Deployer/Auditor notes

Implementation Status: Implemented

The `PermitRootLogin` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can select another setting for PermitRootLogin, from the available options `without-password`, `prohibit-password`, `forced-commands-only`, `yes`, or `no` by setting the following variable:

```
security_sshd_permit_root_login: no
```

> **Warning:** Ensure that a regular user account exists with a pathway to root access (preferably via `sudo`) before applying the security role. This configuration change disallows any direct logins with the `root` user.

The SSH daemon must not allow authentication using known hosts authentication. (V-72249)

STIG Description

Severity: Medium

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Deployer/Auditor notes

Implementation Status: Implemented

The `IgnoreUserKnownHosts` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_known_hosts_auth: no
```

The SSH daemon must be configured to only use the SSHv2 protocol. (V-72251)

STIG Description

Severity: High

SSHv1 is an insecure implementation of the SSH protocol and has many well-known vulnerability exploits. Exploits of the SSH daemon could provide immediate root access to the system.

Satisfies: SRG-OS-000074-GPOS-00042, SRG-OS-000480-GPOS-00227

Deployer/Auditor notes

Implementation Status: Implemented

The `Protocol` configuration is set to `2` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_protocol: 2
```

> **Warning:** There is no reason to enable any other protocol than SSHv2. SSHv1 has multiple vulnerabilities, and it is no longer widely used.

The SSH daemon must be configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms. (V-72253)

STIG Description

Severity: Medium

DoD information systems are required to use FIPS 140-2 approved cryptographic hash functions. The only SSHv2 hash algorithm meeting this requirement is SHA.

Deployer/Auditor notes

Implementation Status: Implemented

The `MACs` configuration is set to `hmac-sha2-256,hmac-sha2-512` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can adjust the allowed Message Authentication Codes (MACs) by setting the following Ansible variable:

```
security_sshd_allowed_macs: 'hmac-sha2-256,hmac-sha2-512'
```

The SSH public host key files must have mode 0644 or less permissive. (V-72255)

STIG Description

Severity: Medium

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Deployer/Auditor notes

Implementation Status: Implemented

The permissions on ssh public host keys is set to `0644`. If the existing permissions are more restrictive than `0644`, the tasks do not make changes to the files.

The SSH private host key files must have mode 0600 or less permissive. (V-72257)

STIG Description

Severity: Medium

If an unauthorized user obtains the private SSH host key file, the host could be impersonated.

Deployer/Auditor notes

Implementation Status: Implemented

The permissions on ssh private host keys is set to `0600`. If the existing permissions are more restrictive than `0600`, the tasks do not make changes to the files.

The SSH daemon must not permit Generic Security Service Application Program Interface (GSSAPI) authentication unless needed. (V-72259)

STIG Description

Severity: Medium

GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through SSH exposes the systems GSSAPI to remote hosts, increasing the attack surface of the system. GSSAPI authentication must be disabled unless needed.

Deployer/Auditor notes

Implementation Status: Implemented

The `GSSAPIAuthentication` setting is set to `no` to meet the requirements of the STIG.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_gssapi: no
```

The SSH daemon must not permit Kerberos authentication unless needed. (V-72261)

STIG Description

Severity: Medium

Kerberos authentication for SSH is often implemented using Generic Security Service Application Program Interface (GSSAPI). If Kerberos is enabled through SSH, the SSH daemon provides a means of access to the systems Kerberos implementation. Vulnerabilities in the systems Kerberos implementation may then be subject to exploitation. To reduce the attack surface of the system, the Kerberos authentication mechanism within SSH must be disabled for systems not using this capability.

Deployer/Auditor notes

Implementation Status: Implemented

The `KerberosAuthentication` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disable_kerberos_auth: no
```

The SSH daemon must perform strict mode checking of home directory configuration files. (V-72263)

STIG Description

Severity: Medium

If other users have access to modify user-specific SSH configuration files, they may be able to log on to the system as another user.

Deployer/Auditor notes

Implementation Status: Implemented

The `StrictModes` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_enable_strict_modes: no
```

The SSH daemon must use privilege separation. (V-72265)

STIG Description

Severity: Medium

SSH daemon privilege separation causes the SSH process to drop root privileges when not needed, which would decrease the impact of software vulnerabilities in the unprivileged section.

Deployer/Auditor notes

Implementation Status: Implemented

The `UsePrivilegeSeparation` configuration is set to `sandbox` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_enable_privilege_separation: no
```

Note: Although the STIG requires this setting to be `yes`, the `sandbox` setting actually provides more security because it enables privilege separation during the early authentication process.

The SSH daemon must not allow compression or must only allow compression after successful authentication. (V-72267)

STIG Description

Severity: Medium

If compression is allowed in an SSH connection prior to authentication, vulnerabilities in the compression software could result in compromise of the system from an unauthenticated connection, potentially with root privileges.

Deployer/Auditor notes

Implementation Status: Implemented

The `Compression` configuration is set to `delayed` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can choose another option by setting the following Ansible variable:

```
security_sshd_compression: 'no'
```

Note: The following are the available settings for `Compression` in the ssh configuration file:

- `delayed`: Compression is enabled after authentication.
- `no`: Compression is disabled.
- `yes`: Compression is enabled during authentication and during the session (not allowed by the STIG).

The `delayed` option balances security with performance and is an approved option in the STIG.

The operating system must, for networked systems, synchronize clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS). (V-72269)

STIG Description

Severity: Medium

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Satisfies: SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role make the following changes on each host:

- The `chrony` package is installed.
- The service (`chronyd` on Red Hat, CentOS, SLE and openSUSE Leap, `chrony` on Ubuntu) is started and enabled at boot time.
- A configuration file template is deployed that includes `maxpoll 10` on each server line.

Deployers can opt out of these changes by setting the following Ansible variable:

```
security_rhel7_enable_chrony: no
```

Note: Although the STIG mentions the traditional `ntpd` service, this role uses `chrony`, which is a more modern implementation.

There must be no shosts.equiv files on the system. (V-72279)

STIG Description

Severity: High

The shosts.equiv files are used to configure host-based authentication for the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *There must be no .shosts files on the system. (V-72277)*

For systems using DNS resolution, at least two name servers must be configured. (V-72281)

STIG Description

Severity: Low

To provide availability for name resolution services, multiple redundant name servers are mandated. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.

Deployer/Auditor notes

Implementation Status: Implemented

If a server has fewer than two nameservers configured in `/etc/resolv.conf`, a warning is printed in the Ansible output.

The system must not forward Internet Protocol version 4 (IPv4) source-routed packets. (V-72283)

STIG Description

Severity: Medium

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in this role set `net.ipv4.conf.all.accept_source_route` and `net.ipv4.conf.default.accept_source_route` to `0` by default. This prevents the system from forwarding source-routed IPv4 packets on all new and existing interfaces.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_source_routed_packet_forward_ipv4: no
```

For more details on source routed packets, refer to the Red Hat documentation.

The system must not forward Internet Protocol version 4 (IPv4) source-routed packets by default. (V-72285)

STIG Description

Severity: Medium

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The system must not forward Internet Protocol version 4 (IPv4) source-routed packets. (V-72283)*

The system must not respond to Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) echoes sent to a broadcast address. (V-72287)

STIG Description

Severity: Medium

Responding to broadcast (ICMP) echoes facilitates network mapping and provides a vector for amplification attacks.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in this role set `net.ipv4.icmp_echo_ignore_broadcasts` to 1 by default. This prevents the system from responding to IPv4 ICMP echoes sent to the broadcast address.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_echoes_broadcast_address: no
```

The system must prevent Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages from being accepted. (V-72289)

STIG Description

Severity: Medium

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the hosts route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages. (V-73175)*

The system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default. (V-72291)

STIG Description

Severity: Medium

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the systems route table, possibly revealing portions of the network topology.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in this role set `net.ipv4.conf.default.send_redirects` and `net.ipv4.conf.all.send_redirects` to `0` by default. This prevents a system from sending IPv4 ICMP redirect packets on all new and existing interfaces.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_icmp_redirects: no
```

The system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects. (V-72293)

STIG Description

Severity: Medium

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the systems route table, possibly revealing portions of the network topology.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default. (V-72291)*

The system must be configured to prevent unrestricted mail relaying. (V-72297)

STIG Description

Severity: Medium

If unrestricted mail relaying is permitted, unauthorized senders could use this host as a mail relay for the purpose of sending spam or other unauthorized activity.

Deployer/Auditor notes

Implementation Status: Implemented

The `smtpd_client_restrictions` configuration in postfix is set to `permit_mynetworks, reject` to meet the STIGs requirements.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_restrict_mail_relaying: no
```

The Trivial File Transfer Protocol (TFTP) server package must not be installed if not required for operational support. (V-72301)

STIG Description

Severity: High

If TFTP is required for operational support (such as the transmission of router configurations) its use must be documented with the Information System Security Officer (ISSO), restricted to only authorized personnel, and have access control rules established.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the TFTP server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `tftp-server`
- Ubuntu: `tftpd`
- openSUSE Leap: `tftp`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_tftp_server: no
```

Remote X connections for interactive users must be encrypted. (V-72303)

STIG Description

Severity: High

Open X displays allow an attacker to capture keystrokes and execute commands remotely.

Deployer/Auditor notes

Implementation Status: Implemented

The `X11Forwarding` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_enable_x11_forwarding: no
```

An X Windows display manager must not be installed unless approved. (V-72307)

STIG Description

Severity: Medium

Internet services that are not required for system or application processes must not be active to decrease the attack surface of the system. X Windows has a long history of security vulnerabilities and will not be used unless approved and documented.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the xorg server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `xorg-x11-server-Xorg`
- Ubuntu: `xorg-xserver`
- openSUSE Leap: `xorg-x11-server`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_xorg: no
```

The system must not forward IPv6 source-routed packets. (V-72319)

STIG Description

Severity: Medium

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv6 forwarding is enabled and the system is functioning as a router.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in this role set `net.ipv6.conf.all.accept_source_route` to `0` by default. This prevents the system from forwarding source-routed IPv6 packets.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_source_routed_packet_forward_ipv6: no
```

Refer to IPv6 source routing: history repeats itself for more details on IPv6 source routed packets.

The operating system must have the required packages for multifactor authentication installed. (V-72417)

STIG Description

Severity: Medium

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that the following multifactor authentication packages are installed:

- authconfig
- authconfig-gtk
- esc
- pam_pkcs11

These packages are benign if they are not needed on a system, but `authconfig-gtk` may cause some graphical dependencies to be installed which may not be needed on some systems. The security role installs these packages, but it skips the installation of `authconfig-gtk`. Deployers can install the graphical package manually if needed.

The operating system must set the lock delay setting for all connection types. (V-73155)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. (V-71891)*

The operating system must set the session idle delay setting for all connection types. (V-73157)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. (V-71891)*

The audit system must take appropriate action when there is an error sending audit records to a remote system. (V-73163)

STIG Description

Severity: Medium

Taking appropriate action when there is an error sending audit records to a remote system will minimize the possibility of losing audit records.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The audit system must take appropriate action when the audit storage volume is full. (V-72087)*

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group. (V-73165)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow. (V-73167)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow. (V-73171)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd. (V-73173)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

The system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages. (V-73175)

STIG Description

Severity: Medium

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the hosts route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects. (V-72293)*

The Datagram Congestion Control Protocol (DCCP) kernel module must be disabled unless required. (V-77821)

STIG Description

Severity: Medium

Disabling DCCP protects the system against exploitation of any flaws in the protocol implementation.

Deployer/Auditor notes

Implementation Status: Implemented

The ansible-hardening role disables the DCCP kernel module by default. Each system must be rebooted to fully apply the change.

Deployers can opt out of the change by setting the following Ansible variable:

```
security_rhel7_disable_dccp: no
```

The operating system must implement virtual address space randomization. (V-77825)

STIG Description

Severity: Medium

Address space layout randomization (ASLR) makes it more difficult for an attacker to predict the location of attack code he or she has introduced into a processs address space during an attempt at exploitation. Additionally, ASLR also makes it more difficult for an attacker to know the location of existing code in order to repurpose it using return-oriented programming (ROP) techniques.

Deployer/Auditor notes

Implementation Status: Implemented

Most modern systems enable Address Space Layout Randomization (ASLR) by default (with a setting of 2), and the role ensures that the secure default is maintained.

Deployers can opt out of the change by setting the following Ansible variable:

```
security_enable_aslr: no
```

For more details on the ASLR settings, review the sysctl documentation.

Implemented - Red Hat And Suse Only (1 controls)

The operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. (V-72067)

STIG Description

Severity: High

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000185-GPOS-00079, SRG-OS-000396-GPOS-00176, SRG-OS-000405-GPOS-00184, SRG-OS-000478-GPOS-00223

Deployer/Auditor notes

Implementation Status: Implemented - Red Hat And Suse Only

The tasks in the Ansible role install the `dracut-fips` (RHEL and SLE) and `dracut-fips-aesni` (RHEL) packages and check to see if FIPS is enabled on the system. If it is not enabled, a warning message is printed in the Ansible output.

Enabling FIPS at boot time requires additional manual configuration. Refer to Chapter 7. Federal Standards and Regulations in the Red Hat documentation for more details. Section 7.1.1 contains the steps required for updating the bootloader configuration and regenerating the initramfs.

Note: This change only applies to CentOS, Red Hat Enterprise Linux, openSUSE Leap and SUSE Linux Enterprise. Ubuntu does not use dracut by default and the process for enabling the FIPS functionality at boot time is more complex.

Implemented - Red Hat Only (2 controls)

User and group account administration utilities must be configured to store only encrypted representations of passwords. (V-71923)

STIG Description

Severity: Medium

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Deployer/Auditor notes

Implementation Status: Implemented - Red Hat Only

The role ensures that `crypt_style` is set to `sha512` in `/etc/libuser.conf`, which is the default for CentOS 7 and Red Hat Enterprise Linux 7.

Ubuntu, openSUSE and SUSE Linux Enterprise 12 do not use `libuser`, so this change is not applicable.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_libuser_crypt_style_sha512: no
```

All system device files must be correctly labeled to prevent unauthorized modification. (V-72039)

STIG Description

Severity: Medium

If an unauthorized or modified device is allowed to exist on the system, there is the possibility the system may perform unintended or unauthorized operations.

Deployer/Auditor notes

Implementation Status: Implemented - Red Hat Only

The tasks in the security role examine the SELinux contexts on each device file found on the system. Any devices without appropriate labels are printed in the Ansible output.

Deployers should investigate the unlabeled devices and ensure that the correct labels are applied for the class of device.

Note: This change applies only to CentOS or Red Hat Enterprise Linux systems since they rely on SELinux as their default Linux Security Module (LSM). Ubuntu, openSUSE Leap and SUSE Linux Enterprise systems use AppArmor, which uses policy files rather than labels applied to individual files.

Not Implemented (1 controls)

A File Transfer Protocol (FTP) server package must not be installed unless needed. (V-72299)

STIG Description

Severity: High

The FTP service provides an unencrypted remote access that does not provide for the confidentiality and integrity of user passwords or the remote session. If a privileged user were to log on using this service,

the privileged user password could be compromised. SSH or other encrypted file transfer methods must be used in place of this service.

Deployer/Auditor notes

Implementation Status: Not Implemented

This STIG is not yet implemented.

Opt-In (50 controls)

The file permissions, ownership, and group membership of system files and commands must match the vendor values. (V-71849)

STIG Description

Severity: High

Discretionary access control is weakened if a user or group has access permissions to system files and directories greater than the default.

Satisfies: SRG-OS-000257-GPOS-00098, SRG-OS-000278-GPOS-00108

Deployer/Auditor notes

Implementation Status: Opt-In

Note: Ubuntus `debsums` command does not support verification of permissions and ownership for files that were installed by packages. This STIG requirement will be skipped on Ubuntu.

The STIG requires that all files owned by an installed package must have their permissions, user ownership, and group ownership set back to the vendor defaults.

Although this is a good practice, it can cause issues if permissions or ownership were intentionally set after the packages were installed. It also causes significant delays in deployments. Therefore, this STIG is not applied by default.

Deployers may opt in for the change by setting the following Ansible variable:

```
security_reset_perm_ownership: yes
```

The cryptographic hash of system files and commands must match vendor values. (V-71855)

STIG Description

Severity: High

Without cryptographic integrity protections, system command and files can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Deployer/Auditor notes

Implementation Status: Opt-In

Ansible tasks will check the `rpm -Va` output (on CentOS, RHEL, openSUSE and SLE) or the output of `debsums` (on Ubuntu) to see if any files installed from packages have been altered. The tasks will print a list of files that have changed since their package was installed.

Deployers should be most concerned with any checksum failures for binaries and their libraries. These are most often a sign of system compromise or poor system administration practices.

Configuration files may appear in the list as well, but these are often less concerning since some of these files are adjusted by the security role itself.

Generating and validating checksums of all files installed by packages consume a significant amount of disk I/O and could impact the performance of a production system. It can also delay the playbooks completion. Therefore, the check is disabled by default.

Deployers can enable the check by setting the following Ansible variable:

```
security_check_package_checksums: yes
```

When passwords are changed or new passwords are established, the new password must contain at least one upper-case character. (V-71903)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_uppercase: no
```

When passwords are changed or new passwords are established, the new password must contain at least one lower-case character. (V-71905)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_lowercase: no
```

When passwords are changed or new passwords are assigned, the new password must contain at least one numeric character. (V-71907)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_numeric: no
```

When passwords are changed or new passwords are assigned, the new password must contain at least one special character. (V-71909)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_special: no
```

When passwords are changed a minimum of eight of the total number of characters must be changed. (V-71911)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_characters_changed: no
```

When passwords are changed a minimum of four character classes must be changed. (V-71913)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_character_classes_changed: no
```

When passwords are changed the number of repeating consecutive characters must not be more than three characters. (V-71915)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_limit_repeated_characters: no
```

When passwords are changed the number of repeating characters of the same character class must not be more than four characters. (V-71917)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_limit_repeated_character_classes: no
```

Passwords for new users must be restricted to a 24 hours/1 day minimum lifetime. (V-71925)

STIG Description

Severity: Medium

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organizations policy regarding password reuse.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that all passwords have a minimum lifetime set, this can cause issue in some production environments. Therefore, deployers must opt in for this change.

Set the following Ansible variable to an integer (in days) to enable this setting:

```
security_password_min_lifetime_days: 1
```

The STIG requires the minimum lifetime for password to be one day.

Passwords must be restricted to a 24 hours/1 day minimum lifetime. (V-71927)

STIG Description

Severity: Medium

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organizations policy regarding password reuse.

Deployer/Auditor notes

Implementation Status: Opt-In

Setting a minimum password lifetime on interactive user accounts provides security benefits by limiting the frequency of password changes. However, this can cause login problems for users without proper communication and coordination.

Deployers can opt-in for this change by setting the following Ansible variable:

```
security_set_minimum_password_lifetime: yes
```

The tasks will examine each interactive user account and set the minimum password age if the existing setting is not equal to one day.

Passwords for new users must be restricted to a 60-day maximum lifetime. (V-71929)

STIG Description

Severity: Medium

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that all passwords have a maximum lifetime set, this can cause authentication disruptions in production environments if users are not aware that their password will expire. Therefore, this change is not applied by default.

Deployers can opt in for this change and provide a maximum lifetime for user passwords (in days) by setting the following Ansible variable:

```
security_password_max_lifetime_days: 60
```

The STIG requires that all passwords expire after 60 days.

Existing passwords must be restricted to a 60-day maximum lifetime. (V-71931)

STIG Description

Severity: Medium

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that a maximum password lifetime is set for all interactive user accounts, the security benefits of this configuration are debatable. The draft of NIST Publication 800-63B argues that password rotation may reduce overall security in some situations.

Deployers can opt-in for this change by setting the following Ansible variable:

```
security_set_maximum_password_lifetime: yes
```

The tasks will examine each interactive user account and set the maximum password age if the existing setting is not equal to 60 days.

Passwords must be prohibited from reuse for a minimum of five generations. (V-71933)

STIG Description

Severity: Medium

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed per policy requirements.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that five passwords are remembered to prevent re- use, this can cause issues in production environment if the change is not communicated well to users. Therefore, the tasks in the security role do not apply this change by default.

Deployers can opt in for the change and specify a number of passwords to remember by setting the following Ansible variable:

```
security_password_remember_password: 5
```

Passwords must be a minimum of 15 characters in length. (V-71935)

STIG Description

Severity: Medium

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that passwords have a minimum length of 15 characters, this change might be disruptive to users on a production system without communicating the change first. Therefore, this change is not applied by default.

Deployers can opt in for the change by setting the following Ansible variable:

```
security_pwquality_require_minimum_password_length: yes
```

The operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires. (V-71941)

STIG Description

Severity: Medium

Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Operating systems need to track periods of inactivity and disable application identifiers after zero days of inactivity.

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that user accounts are disabled when their password expires. This might be disruptive for some users or for automated processes. Therefore, the tasks in the security role do not apply this change by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_disable_account_if_password_expires: yes
```

Systems with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes. (V-71961)

STIG Description

Severity: High

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that GRUB 2 asks for a password whenever a user attempts to enter single-user or maintenance mode, this change might be disruptive in an emergency situation. Therefore, this change is not applied by default.

Deployers that wish to opt in for this change should set two Ansible variables:

```
security_require_grub_authentication: yes
security_grub_password_hash: grub.pbkdf2.sha512.10000.7B21785BEAFEE3AC...
```

The default password set in the security role is secrete, but deployers should set a much more secure password for production environments. Use the `grub2-mkpasswd-pbkdf2` command to create a password hash string and use it as the value for the Ansible variable `security_grub_password_hash`.

> **Warning:** This change must be tested in a non-production environment first. Requiring authentication in GRUB 2 without proper communication to users could cause extensive delays in emergency situations.

Systems using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes. (V-71963)

STIG Description

Severity: High

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Deployer/Auditor notes

Implementation Status: Opt-In

The tasks in the security role for V-71961 will also apply changes to systems that use UEFI. For more details, refer to the following documentation:

- *Systems with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes. (V-71961)*

A file integrity tool must verify the baseline operating system configuration at least weekly. (V-71973)

STIG Description

Severity: Medium

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating systems Information Management Officer (IMO)/Information System Security Officer (ISSO) and System Administrators (SAs) must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Deployer/Auditor notes

Implementation Status: Opt-In

Initializing the AIDE database and completing the first AIDE run causes increased disk I/O and CPU usage for extended periods. Therefore, the AIDE database is not automatically initialized by the tasks in the security role.

Deployers can enable the AIDE database initialization within the security role by setting the following Ansible variable:

```
security_rhel7_initialize_aide: yes
```

The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of packages without verification of the repository metadata. (V-71981)

STIG Description

Severity: High

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This ensures the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved Certificate Authority.

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that repository XML files are verified during `yum` runs.

> **Warning:** This setting is disabled by default because it can cause issues with CentOS systems and prevent them from retrieving repository information. Deployers who choose to enable this setting should test it thoroughly on non-production environments before applying it to production systems.

Deployers can override this default and opt in for the change by setting the following Ansible variable:

```
security_enable_gpgcheck_repo: yes
```

USB mass storage must be disabled. (V-71983)

STIG Description

Severity: Medium

USB mass storage permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Deployer/Auditor notes

Implementation Status: Opt-In

The tasks in the security role disable the `usb-storage` module and the change is applied the next time the server is rebooted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_disable_usb_storage: no
```

The operating system must remove all software components after updated versions have been installed. (V-71987)

STIG Description

Severity: Low

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that dependent packages are removed automatically when a package is removed, this can cause problems with certain packages, especially kernels. Deployers must opt in to meet the requirements of this STIG control.

Deployers should set the following variable to enable automatic dependent package removal:

```
security_package_clean_on_remove: yes
```

Vendor packaged system security patches and updates must be installed and up to date. (V-71999)

STIG Description

Severity: Medium

Timely patching is critical for maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. However, failure to keep operating system and application software patched is a common mistake made by IT professionals. New patches are released daily, and it is often difficult for even experienced System Administrators to keep abreast of all the new patches. When new weaknesses in an operating system exist, patches are usually made available by the vendor to resolve the problems. If the most recent security patches and updates are not installed, unauthorized users may take advantage of weaknesses in the unpatched software. The lack of prompt attention to patching could result in a system compromise.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that security patches and updates are applied when they are made available, this might be disruptive to some systems. Therefore, the tasks in the security role will not configure automatic updates by default.

Deployers can opt in for automatic package updates by setting the following Ansible variable:

```
security_rhel7_automatic_package_updates: yes
```

When enabled, the tasks install and configure `yum-cron` on CentOS and Red Hat Enterprise Linux. On Ubuntu systems, the `unattended-upgrades` package is installed and configured. On openSUSE Leap and SUSE Linux Enterprise systems, a daily cronjob is installed.

All files and directories must have a valid owner. (V-72007)

STIG Description

Severity: Medium

Unowned files and directories may be unintentionally inherited if a user is assigned the same User Identifier UID as the UID of the un-owned files.

Deployer/Auditor notes

Implementation Status: Opt-In

Searching an entire filesystem with `find` reduces system performance and might impact certain applications negatively. Therefore, the search for files and directories with an invalid owner is **disabled by default**.

Deployers can opt in for this search by setting the following Ansible variable:

```
security_search_for_invalid_owner: yes
```

Any files or directories without a valid user owner are displayed in the Ansible output.

All files and directories must have a valid group owner. (V-72009)

STIG Description

Severity: Medium

Files without a valid group owner may be unintentionally inherited if a group is assigned the same Group Identifier (GID) as the GID of the files without a valid group owner.

Deployer/Auditor notes

Implementation Status: Opt-In

Searching an entire filesystem with `find` reduces system performance and might impact certain applications negatively. Therefore, the search for files and directories with an invalid group owner is **disabled by default**.

Deployers can opt in for this search by setting the following Ansible variable:

```
security_search_for_invalid_group_owner: yes
```

Any files or directories without a valid group owner are displayed in the Ansible output.

All local interactive user home directories must have mode 0750 or less permissive. (V-72017)

STIG Description

Severity: Medium

Excessive permissions on local interactive user home directories may allow unauthorized access to user files by other users.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that all home directories have the proper owner, group owner, and permissions, these changes might be disruptive in some environments. These tasks are not executed by default.

Deployers can opt in for the following changes to each home directory:

- Permissions are set to `0750` at a maximum. If permissions are already more restrictive than `0750`, the permissions are left unchanged.
- User ownership is set to the `UID` of the user.
- Group ownership is set to the `GID` of the user.

Deployers can opt in for these changes by setting the following Ansible variable:

```
security_set_home_directory_permissions_and_owners: yes
```

All local interactive user home directories must be owned by their respective users. (V-72019)

STIG Description

Severity: Medium

If a local interactive user does not own their home directory, unauthorized users could access or modify the users files, and the users may not be able to access their own files.

Deployer/Auditor notes

Implementation Status: Opt-In

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *All local interactive user home directories must have mode 0750 or less permissive. (V-72017)*

All local interactive user home directories must be group-owned by the home directory owners primary group. (V-72021)

STIG Description

Severity: Medium

If the Group Identifier (GID) of a local interactive users home directory is not the same as the primary GID of the user, this would allow unauthorized access to the users files, and users that share the same group may not be able to access files that they legitimately should.

Deployer/Auditor notes

Implementation Status: Opt-In

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *All local interactive user home directories must have mode 0750 or less permissive. (V-72017)*

All world-writable directories must be group-owned by root, sys, bin, or an application group. (V-72047)

STIG Description

Severity: Medium

If a world-writable directory has the sticky bit set and is not group-owned by a privileged Group Identifier (GID), unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

Deployer/Auditor notes

Implementation Status: Opt-In

The tasks in the security role examine the world-writable directories on the system and report any directories that are not group-owned by the `root` user. Those directories appear in the Ansible output.

Deployers should review the list of directories and group owners to ensure that they are appropriate for the directory. Unauthorized group ownership could allow certain users to modify files from other users.

Searching the entire filesystem for world-writable directories will consume a significant amount of disk I/O and could impact the performance of a production system. It can also delay the playbooks completion. Therefore, the search is disabled by default.

Deployers can enable the search by setting the following Ansible variable:

```
security_find_world_writable_dirs: yes
```

The operating system must off-load audit records onto a different system or media from the system being audited. (V-72083)

STIG Description

Severity: Medium

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Deployer/Auditor notes

Implementation Status: Opt-In

The `audispd` service transmits audit logs to other servers. Deployers should specify the address of another server that can receive audit logs by setting the following Ansible variable:

```
security_audisp_remote_server: '10.0.21.1'
```

The operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited. (V-72085)

STIG Description

Severity: Medium

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Deployer/Auditor notes

Implementation Status: Opt-In

The `audispd` daemon transmits audit logs without encryption by default. The STIG requires that these logs are encrypted while they are transferred across the network. The encryption is controlled by the `enable_krb5` option in `/etc/audisp/audisp-remote.conf`.

Deployers can opt-in for encrypted audit log transmission by setting the following Ansible variable:

```
security_audisp_enable_krb5: yes
```

Warning: Only enable this setting if kerberos is already configured.

All uses of the chown command must be audited. (V-72097)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `chown` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

Warning: This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_chown: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fchown command must be audited. (V-72099)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fchown` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchown: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the lchown command must be audited. (V-72101)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `lchown` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_lchown: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fchownat command must be audited. (V-72103)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fchownat` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchownat: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the chmod command must be audited. (V-72105)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `chmod` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_chmod: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fchmod command must be audited. (V-72107)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fchmod` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchmod: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fchmodat command must be audited. (V-72109)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fchmodat` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchmodat: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fsetxattr command must be audited. (V-72113)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fsetxattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fsetxattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the lsetxattr command must be audited. (V-72115)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `lsetxattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_lsetxattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fremovexattr command must be audited. (V-72119)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fremovexattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fremovexattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the lremovexattr command must be audited. (V-72121)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `lremovexattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_lremovexattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

The system must use a virus scan program. (V-72213)

STIG Description

Severity: High

Virus scanning software can be used to protect a system from penetration from computer viruses and to limit their spread through intermediate systems.

The virus scanning software should be configured to perform scans dynamically on accessed files. If this capability is not available, the system must be configured to scan, at a minimum, all altered files on the system on a daily basis.

If the system processes inbound SMTP mail, the virus scanner must be configured to scan all received mail.

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that a virus scanner is installed and running, but the value of a virus scanner within an OpenStack control plane or on a hypervisor is negligible in many cases. In addition, the disk I/O impact of a virus scanner can impact a production environment negatively.

The security role has tasks to deploy ClamAV with automatic updates, but the tasks are disabled by default.

Deployers can enable the ClamAV virus scanner by setting the following Ansible variable:

```
security_enable_virus_scanner: yes
```

> **Warning:** The ClamAV packages are provided in the EPEL repository. Setting the `security_enable_virus_scanner` will also cause the EPEL repository to be installed by the role.

The operating system must limit the number of concurrent sessions to 10 for all accounts and/or account types. (V-72217)

STIG Description

Severity: Low

Operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to DoS attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that each account is limited to 10 concurrent connections, this change might be disruptive in some environments. Therefore, this change is not applied by default.

Deployers can opt in for this change by setting a concurrent connection limit with this Ansible variable:

```
security_rhel7_concurrent_session_limit: 10
```

The operating system must protect against or limit the effects of Denial of Service (DoS) attacks by validating the operating system is implementing rate-limiting measures on impacted network interfaces. (V-72271)

STIG Description

Severity: Medium

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of the operating system to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that incoming TCP connections are rate limited with `firewalld`, this setting can cause problems with certain applications which handle large amounts of TCP connections. Therefore, the tasks in the security role do not apply the rate limit by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_enable_firewalld_rate_limit: yes
```

The STIG recommends a limit of 25 connection per minute and allowing bursts up to 100 connections. Both of these options are adjustable with the following Ansible variables:

```
security_enable_firewalld_rate_limit_per_minute: 25
security_enable_firewalld_rate_limit_burst: 100
```

> **Warning:** Deployers should test rate limiting in a non-production environment first before applying it to production systems. Ensure that the application running on the system is receiving a large volume of requests so that the rule can be thoroughly tested.

The operating system must enable an application firewall, if available. (V-72273)

STIG Description

Severity: Medium

Firewalls protect computers from network attacks by blocking or limiting access to open network ports. Application firewalls limit which applications are allowed to communicate over the network.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000480-GPOS-00231, SRG-OS-000480-GPOS-00232

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that a firewall is configured on each server. This might be disruptive to some environments since the default firewall policy for `firewalld` is very restrictive. Therefore, the tasks in the security role do not install or enable the `firewalld` daemon by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_enable_firewalld: yes
```

Warning: Deployers must pre-configure `firewalld` or copy over a working XML file in `/etc/firewalld/zones/` from another server. The default firewalld restrictions on Ubuntu, CentOS, Red Hat Enterprise Linux and openSUSE Leap are highly restrictive.

There must be no .shosts files on the system. (V-72277)

STIG Description

Severity: High

The .shosts files are used to configure host-based authentication for individual users or the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Deployer/Auditor notes

Implementation Status: Opt-In

The tasks in the security role examine the filesystem for any `.shosts` or `shosts.equiv` files. If they are found, they are deleted.

The search for these files will take a very long time on systems with slow disks or systems with a large amount of files. Therefore, this task is skipped by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_remove_shosts_files: yes
```

The system must not be performing packet forwarding unless the system is a router. (V-72309)

STIG Description

Severity: Medium

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

Deployer/Auditor notes

Implementation Status: Opt-In

Disabling IP forwarding on a system that routes packets or host virtual machines might cause network interruptions. The tasks in this role do not adjust the `net.ipv4.ip_forward` configuration by default.

Deployers can opt in for this change and disable IP forwarding by setting the following Ansible variable:

```
security_disallow_ip_forwarding: yes
```

> **Warning:** IP forwarding is required in some environments. Always test in a non-production environment before changing this setting on a production system.

When passwords are changed or new passwords are established, pwquality must be used. (V-73159)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Pwquality enforces complex password construction configuration on the system.

Deployer/Auditor notes

Implementation Status: Opt-In

The security role can require new or changed passwords to follow the pwquality rules, but this change can be disruptive for users without proper communication. Deployers must opt in for this change by setting the following variable:

```
security_enable_pwquality_password_set: yes
```

Opt-In - Red Hat Only (2 controls)

Accounts subject to three unsuccessful logon attempts within 15 minutes must be locked for the maximum configurable period. (V-71943)

STIG Description

Severity: Medium

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Deployer/Auditor notes

Implementation Status: Opt-In - Red Hat Only

This STIG control is implemented by:

- *If three unsuccessful root logon attempts within 15 minutes occur the associated account must be locked. (V-71945)*

If three unsuccessful root logon attempts within 15 minutes occur the associated account must be locked. (V-71945)

STIG Description

Severity: Medium

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Deployer/Auditor notes

Implementation Status: Opt-In - Red Hat Only

The STIG requires that accounts with excessive failed login attempts are locked. It sets a limit of three failed attempts in a 15 minute interval and these restrictions are applied to all users (including root). Accounts cannot be automatically unlocked for seven days.

This change might cause disruptions in production environments without proper communication to users. Therefore, this change is not applied by default.

Deployers can opt in for the change by setting the following variable:

```
security_pam_faillock_enable: yes
```

There are also three configuration options that can be adjusted by setting Ansible variables:

- `security_pam_faillock_attempts`: This many failed login attempts within the specified time interval with trigger the account to lock. (STIG requirement: `3` attempts)
- `security_pam_faillock_interval`: This is the time interval (in seconds) to use when measuring excessive failed login attempts. (STIG requirement: `900` seconds)
- `security_pam_faillock_deny_root`: Set to `yes` to apply the restriction to the root user or set to `no` to exempt the root user from the account locking restrictions. (STIG requirement: `yes`)
- `security_pam_faillock_unlock_time`: This sets the time delay (in seconds) before a locked account is automatically unlocked. (STIG requirement: `604800` seconds)

Note: Ubuntu, openSUSE Leap and SUSE Linux Enterprise 12 do not provide `pam_faillock`. This change is only applied to CentOS 7 or Red Hat Enterprise Linux 7 systems.

Opt-In - Ubuntu And Suse Only (1 controls)

The operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files. (V-71995)

STIG Description

Severity: Medium

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Deployer/Auditor notes

Implementation Status: Opt-In - Ubuntu And Suse Only

The STIG requires that the umask for all authenticated users is `077`. This ensures that all new files and directories created by a user are accessible only by that user.

Although this change has a significant security benefit, it can cause problems for users who are not expecting the change. The security role will not adjust the umask by default.

Deployers can opt-in for the change by setting the default umask with an Ansible variable:

```
security_shadow_utils_umask: 077
```

Note: Ubuntu, openSUSE Leap and SUSE Linux Enterpsise 12 use `pam_umask` and it uses the default umask provided by the `UMASK` line in `/etc/login.defs`. The default setting on Ubuntu, openSUSE Leap and SUSE Linux Enterprise 12 systems is `022`. This allows the users group and other users on the system to read and execute files, but they cannot write to them.

CentOS and Red Hat Enterprise Linux do not use `pam_umask` and instead set a default umask of `0002` for regular users and `0022` for root. This gives the regular users group full access to newly created files, but other users cannot write to those files.

The tasks for this STIG requirement are not currently applied to CentOS and Red Hat Enterprise Linux systems. See Launchpad Bug #1656003 for more details.

Verification Only (5 controls)

The system must send rsyslog output to a log aggregation server. (V-72209)

STIG Description

Severity: Medium

Sending rsyslog output to another system ensures that the logs cannot be removed or modified in the event that the system is compromised or has a hardware failure.

Deployer/Auditor notes

Implementation Status: Verification Only

The tasks in the security role check for uncommented lines in the rsyslog configuration that contain `@` or `@@`, which signifies that a remote logging configuration is in place. If these lines are not found, a warning message is printed in the Ansible output.

The system must display the date and time of the last successful account logon upon logon. (V-72275)

STIG Description

Severity: Low

Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.

Deployer/Auditor notes

Implementation Status: Verification Only

The PAM configuration is checked for the presence of `pam_lastlogin` and a warning message is printed if the directive is not found. The tasks in the security role do not adjust PAM configurations since these changes might be disruptive in some environments.

Deployers should review their PAM configurations and add `pam_lastlogin` to `/etc/pam.d/postlogin` on CentOS and Red Hat Enterprise Linux or to `/etc/pam.d/login` on Ubuntu, openSUSE Leap and SUSE Linux Enterprise.

Network interfaces must not be in promiscuous mode. (V-72295)

STIG Description

Severity: Medium

Network interfaces in promiscuous mode allow for the capture of all network traffic visible to the system. If unauthorized individuals can access these applications, it may allow then to collect information such as logon IDs, passwords, and key exchanges between systems.

If the system is being used to perform a network troubleshooting function, the use of these tools must be documented with the Information System Security Officer (ISSO) and restricted to only authorized personnel.

Deployer/Auditor notes

Implementation Status: Verification Only

All interfaces are examined to ensure they are not in promiscuous mode. A warning message is printed in the Ansible output if any promiscuous interfaces are found.

If the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon must be configured to operate in secure mode. (V-72305)

STIG Description

Severity: Medium

Restricting TFTP to a specific directory prevents remote users from copying, transferring, or overwriting system files.

Deployer/Auditor notes

Implementation Status: Verification Only

The tasks in the security role examine the TFTP server configuration file (if it exists) to verify that the secure operation flag (`-s`) is listed on the `server_args` line. If it is missing, a warning message is printed in the Ansible output.

SNMP community strings must be changed from the default. (V-72313)

STIG Description

Severity: High

Whether active or not, default Simple Network Management Protocol (SNMP) community strings must be changed to maintain security. If the service is running with the default authenticators, anyone can gather data about the system and the network and use the information to potentially compromise the integrity of the system or network(s). It is highly recommended that SNMP version 3 user authentication and message encryption be used in place of the version 2 community strings.

Deployer/Auditor notes

Implementation Status: Verification Only

The tasks in the security role examine the contents of the `/etc/snmp/snmpd.conf` file (if it exists) and search for the default community strings: `public` and `private`. If either default string is found, a message is printed in the Ansible output.

3.5.3 Review All STIG Controls

Navigating the list

Use your browsers search function (usually CTRL-f) to find the security configuration in the full list shown here. You can search for STIG ID numbers, such as `V-38463`, or for particular topics, like `audit`.

The file permissions, ownership, and group membership of system files and commands must match the vendor values. (V-71849)

STIG Description

Severity: High

Discretionary access control is weakened if a user or group has access permissions to system files and directories greater than the default.

Satisfies: SRG-OS-000257-GPOS-00098, SRG-OS-000278-GPOS-00108

Deployer/Auditor notes

Implementation Status: Opt-In

Note: Ubuntus `debsums` command does not support verification of permissions and ownership for files that were installed by packages. This STIG requirement will be skipped on Ubuntu.

The STIG requires that all files owned by an installed package must have their permissions, user ownership, and group ownership set back to the vendor defaults.

Although this is a good practice, it can cause issues if permissions or ownership were intentionally set after the packages were installed. It also causes significant delays in deployments. Therefore, this STIG is not applied by default.

Deployers may opt in for the change by setting the following Ansible variable:

```
security_reset_perm_ownership: yes
```

The cryptographic hash of system files and commands must match vendor values. (V-71855)

STIG Description

Severity: High

Without cryptographic integrity protections, system command and files can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Deployer/Auditor notes

Implementation Status: Opt-In

Ansible tasks will check the `rpm -Va` output (on CentOS, RHEL, openSUSE and SLE) or the output of `debsums` (on Ubuntu) to see if any files installed from packages have been altered. The tasks will print a list of files that have changed since their package was installed.

Deployers should be most concerned with any checksum failures for binaries and their libraries. These are most often a sign of system compromise or poor system administration practices.

Configuration files may appear in the list as well, but these are often less concerning since some of these files are adjusted by the security role itself.

Generating and validating checksums of all files installed by packages consume a significant amount of disk I/O and could impact the performance of a production system. It can also delay the playbooks completion. Therefore, the check is disabled by default.

Deployers can enable the check by setting the following Ansible variable:

```
security_check_package_checksums: yes
```

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon. (V-71859)

STIG Description

Severity: Medium

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is␣
↪provided for USG-authorized use only.
```

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

```
-The USG routinely intercepts and monitors communications on this IS for␣
↪purposes including, but not limited to, penetration testing, COMSEC␣
↪monitoring, network operations and defense, personnel misconduct (PM), law␣
↪enforcement (LE), and counterintelligence (CI) investigations.
```

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interestsnot for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
"I've read  consent to terms in IS user agreem't."
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role configure `dconf` to display a login banner each time a graphical session starts on the system. The default banner message set by the role is:

> You are accessing a secured system and your actions will be logged along with identifying information. Disconnect immediately if you are not an authorized user of this system.

Deployers can customize this message by setting an Ansible variable:

```
security_enable_graphical_login_message_text: >
    This is a customized banner message.
```

> **Warning:** The dconf configuration does not support multi-line strings. Ensure that `security_enable_graphical_login_message_text` contains a single line of text.

In addition, deployers can opt out of displaying a login banner message by changing `security_enable_graphical_login_message` to `no`.

The operating system must display the approved Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon. (V-71861)

STIG Description

Severity: Medium

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is␣
↪provided for USG-authorized use only.
```

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

```
-The USG routinely intercepts and monitors communications on this IS for␣
↪purposes including, but not limited to, penetration testing, COMSEC␣
↪monitoring, network operations and defense, personnel misconduct (PM), law␣
↪enforcement (LE), and counterintelligence (CI) investigations.
```

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interestsnot for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Deployer/Auditor notes

Implementation Status: Implemented

The security role configures a login banner for graphical logins using `dconf`. Deployers can opt out of this change by setting the following Ansible variable:

```
security_enable_graphical_login_message: no
```

The message is customized by setting another Ansible variable:

```
security_enable_graphical_login_message_text: >
    You are accessing a secured system and your actions will be logged along
    with identifying information. Disconnect immediately if you are not an
    authorized user of this system.
```

Note: The space available for the graphical banner is relatively short. Deployers should limit the length of their graphical login banners to the shortest length possible.

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a command line user logon. (V-71863)

STIG Description

Severity: Medium

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is␣
↪provided for USG-authorized use only.
```

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

```
-The USG routinely intercepts and monitors communications on this IS for␣
↪purposes including, but not limited to, penetration testing, COMSEC␣
↪monitoring, network operations and defense, personnel misconduct (PM), law␣
↪enforcement (LE), and counterintelligence (CI) investigations.
```

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interestsnot for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
"I've read  consent to terms in IS user agreem't."
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007

Deployer/Auditor notes

Implementation Status: Implemented

The security role already deploys a login banner for console logins with tasks from another STIG:

- *The Standard Mandatory DoD Notice and Consent Banner must be displayed immediately prior to, or as part of, remote access logon prompts. (V-72225)*

The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. (V-71891)

STIG Description

Severity: Medium

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

Regardless of where the session lock is determined and implemented, once invoked, the session lock must remain in place until the user reauthenticates. No other activity aside from reauthentication must unlock the system.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that graphical sessions are locked when the screensaver starts and that users must re-enter credentials to restore access to the system. The screensaver lock is enabled by default if `dconf` is present on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_lock_session: no
```

The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces. (V-71893)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that the screensaver appears when a session reaches a certain period of inactivity. The tasks will enable the screensaver for inactive sessions by default.

Deployers can opt out of this change by setting an Ansible variable:

```
security_lock_session_when_inactive: no
```

The operating system must set the idle delay setting for all connection types. (V-71895)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces. (V-71893)*

The operating system must have the screen package installed. (V-71897)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The screen package allows for a session lock to be implemented and configured.

Deployer/Auditor notes

Implementation Status: Implemented

The role will ensure that the `screen` package is installed.

The operating system must initiate a session lock for the screensaver after a period of inactivity for graphical user interfaces. (V-71899)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces. (V-71893)*

The operating system must initiate a session lock for graphical user interfaces when the screensaver is activated. (V-71901)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that a graphical session is locked when the screensaver starts. This requires a user to re-enter their credentials to regain access to the system.

The tasks will set a timeout of 5 seconds after the screensaver has started before the session is locked. This gives a user a few seconds to press a key or wiggle their mouse after the screensaver appears without needing to re-enter their credentials.

Deployers can adjust this timeout by setting an Ansible variable:

```
security_lock_session_screensaver_lock_delay: 5
```

When passwords are changed or new passwords are established, the new password must contain at least one upper-case character. (V-71903)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_uppercase: no
```

When passwords are changed or new passwords are established, the new password must contain at least one lower-case character. (V-71905)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_lowercase: no
```

When passwords are changed or new passwords are assigned, the new password must contain at least one numeric character. (V-71907)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_numeric: no
```

When passwords are changed or new passwords are assigned, the new password must contain at least one special character. (V-71909)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_special: no
```

When passwords are changed a minimum of eight of the total number of characters must be changed. (V-71911)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_characters_changed: no
```

When passwords are changed a minimum of four character classes must be changed. (V-71913)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_require_character_classes_changed: no
```

When passwords are changed the number of repeating consecutive characters must not be more than three characters. (V-71915)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_limit_repeated_characters: no
```

When passwords are changed the number of repeating characters of the same character class must not be more than four characters. (V-71917)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

The password quality requirements from the STIG are examples of good security practice, but deployers are strongly encouraged to use centralized authentication for administrative server access whenever possible.

Password quality requirements are controlled by two Ansible variables: one for each individual password requirement and one master switch variable. The master switch variable controls all password requirements and it is **disabled by default**.

Deployers can enable all password quality requirements by setting the master switch variable to `yes`:

```
security_pwquality_apply_rules: yes
```

When the master switch variable is enabled, each individual password quality requirement can be disabled by a variable. To disable the fix for this STIG control, set the following Ansible variable:

```
security_pwquality_limit_repeated_character_classes: no
```

The PAM system service must be configured to store only encrypted representations of passwords. (V-71919)

STIG Description

Severity: Medium

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Deployer/Auditor notes

Implementation Status: Implemented

The PAM configuration file for password storage is checked to ensure that `sha512` is found on the `pam_unix.so` line. If `sha512` is not found, a debug message is printed in the Ansible output.

The shadow file must be configured to store only encrypted representations of passwords. (V-71921)

STIG Description

Severity: Medium

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Deployer/Auditor notes

Implementation Status: Implemented

The default password storage mechanism for Ubuntu 16.04, CentOS 7, openSUSE Leap, SUSE Linux Enterprise 12 and Red Hat Enterprise Linux 7 is `SHA512` and the tasks in the security role ensure that the default is maintained.

Deployers can configure a different password storage mechanism by setting the following Ansible variable:

```
security_password_encrypt_method: SHA512
```

Warning: SHA512 is the default on most modern Linux distributions and it meets the requirement of the STIG. Do not change the value unless a system has a specific need for a different password mechanism.

User and group account administration utilities must be configured to store only encrypted representations of passwords. (V-71923)

STIG Description

Severity: Medium

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Deployer/Auditor notes

Implementation Status: Implemented - Red Hat Only

The role ensures that `crypt_style` is set to `sha512` in `/etc/libuser.conf`, which is the default for CentOS 7 and Red Hat Enterprise Linux 7.

Ubuntu, openSUSE and SUSE Linux Enterprise 12 do not use `libuser`, so this change is not applicable.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_libuser_crypt_style_sha512: no
```

Passwords for new users must be restricted to a 24 hours/1 day minimum lifetime. (V-71925)

STIG Description

Severity: Medium

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organizations policy regarding password reuse.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that all passwords have a minimum lifetime set, this can cause issue in some production environments. Therefore, deployers must opt in for this change.

Set the following Ansible variable to an integer (in days) to enable this setting:

```
security_password_min_lifetime_days: 1
```

The STIG requires the minimum lifetime for password to be one day.

Passwords must be restricted to a 24 hours/1 day minimum lifetime. (V-71927)

STIG Description

Severity: Medium

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organizations policy regarding password reuse.

Deployer/Auditor notes

Implementation Status: Opt-In

Setting a minimum password lifetime on interactive user accounts provides security benefits by limiting the frequency of password changes. However, this can cause login problems for users without proper communication and coordination.

Deployers can opt-in for this change by setting the following Ansible variable:

```
security_set_minimum_password_lifetime: yes
```

The tasks will examine each interactive user account and set the minimum password age if the existing setting is not equal to one day.

Passwords for new users must be restricted to a 60-day maximum lifetime. (V-71929)

STIG Description

Severity: Medium

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that all passwords have a maximum lifetime set, this can cause authentication disruptions in production environments if users are not aware that their password will expire. Therefore, this change is not applied by default.

Deployers can opt in for this change and provide a maximum lifetime for user passwords (in days) by setting the following Ansible variable:

```
security_password_max_lifetime_days: 60
```

The STIG requires that all passwords expire after 60 days.

Existing passwords must be restricted to a 60-day maximum lifetime. (V-71931)

STIG Description

Severity: Medium

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that a maximum password lifetime is set for all interactive user accounts, the security benefits of this configuration are debatable. The draft of NIST Publication 800-63B argues that password rotation may reduce overall security in some situations.

Deployers can opt-in for this change by setting the following Ansible variable:

```
security_set_maximum_password_lifetime: yes
```

The tasks will examine each interactive user account and set the maximum password age if the existing setting is not equal to 60 days.

Passwords must be prohibited from reuse for a minimum of five generations. (V-71933)

STIG Description

Severity: Medium

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed per policy requirements.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that five passwords are remembered to prevent re- use, this can cause issues in production environment if the change is not communicated well to users. Therefore, the tasks in the security role do not apply this change by default.

Deployers can opt in for the change and specify a number of passwords to remember by setting the following Ansible variable:

```
security_password_remember_password: 5
```

Passwords must be a minimum of 15 characters in length. (V-71935)

STIG Description

Severity: Medium

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that passwords have a minimum length of 15 characters, this change might be disruptive to users on a production system without communicating the change first. Therefore, this change is not applied by default.

Deployers can opt in for the change by setting the following Ansible variable:

```
security_pwquality_require_minimum_password_length: yes
```

The system must not have accounts configured with blank or null passwords. (V-71937)

STIG Description

Severity: High

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Deployer/Auditor notes

Implementation Status: Implemented

The Ansible tasks will ensure that PAM is configured to disallow logins from accounts with null or blank passwords. This involves removing a single option from one of the PAM configuration files:

- CentOS or RHEL: removes `nullok` from `/etc/pam.d/system-auth`
- Ubuntu: removes `nullok_secure` from `/etc/pam.d/common-auth`
- openSUSE Leap or SLE: remove `nullok` from `/etc/pam.d/common-auth` and `/etc/pam.d/common-password`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_disallow_blank_password_login: no
```

The SSH daemon must not allow authentication using an empty password. (V-71939)

STIG Description

Severity: High

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Deployer/Auditor notes

Implementation Status: Implemented

The `PermitEmptyPasswords` configuration will be set to `no` in `/etc/ssh/sshd_config` and sshd will be restarted. This disallows logins over ssh for users with a empty or null password set.

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_sshd_disallow_empty_password: no
```

The operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires. (V-71941)

STIG Description

Severity: Medium

Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Operating systems need to track periods of inactivity and disable application identifiers after zero days of inactivity.

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that user accounts are disabled when their password expires. This might be disruptive for some users or for automated processes. Therefore, the tasks in the security role do not apply this change by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_disable_account_if_password_expires: yes
```

Accounts subject to three unsuccessful logon attempts within 15 minutes must be locked for the maximum configurable period. (V-71943)

STIG Description

Severity: Medium

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Deployer/Auditor notes

Implementation Status: Opt-In - Red Hat Only

This STIG control is implemented by:

- *If three unsuccessful root logon attempts within 15 minutes occur the associated account must be locked. (V-71945)*

If three unsuccessful root logon attempts within 15 minutes occur the associated account must be locked. (V-71945)

STIG Description

Severity: Medium

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Deployer/Auditor notes

Implementation Status: Opt-In - Red Hat Only

The STIG requires that accounts with excessive failed login attempts are locked. It sets a limit of three failed attempts in a 15 minute interval and these restrictions are applied to all users (including root). Accounts cannot be automatically unlocked for seven days.

This change might cause disruptions in production environments without proper communication to users. Therefore, this change is not applied by default.

Deployers can opt in for the change by setting the following variable:

```
security_pam_faillock_enable: yes
```

There are also three configuration options that can be adjusted by setting Ansible variables:

- `security_pam_faillock_attempts`: This many failed login attempts within the specified time interval with trigger the account to lock. (STIG requirement: `3` attempts)
- `security_pam_faillock_interval`: This is the time interval (in seconds) to use when measuring excessive failed login attempts. (STIG requirement: `900` seconds)
- `security_pam_faillock_deny_root`: Set to `yes` to apply the restriction to the root user or set to `no` to exempt the root user from the account locking restrictions. (STIG requirement: `yes`)
- `security_pam_faillock_unlock_time`: This sets the time delay (in seconds) before a locked account is automatically unlocked. (STIG requirement: `604800` seconds)

Note: Ubuntu, openSUSE Leap and SUSE Linux Enterprise 12 do not provide `pam_faillock`. This change is only applied to CentOS 7 or Red Hat Enterprise Linux 7 systems.

Users must provide a password for privilege escalation. (V-71947)

STIG Description

Severity: Medium

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The STIG requires all users to authenticate when using `sudo`, but this change can be highly disruptive for automated scripts or applications that cannot perform interactive authentication. Automated edits from Ansible tasks might cause authentication disruptions on some hosts, and deployers are urged to carefully review each use of the `NOPASSWD` directive in their `sudo` configuration files.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_sudoers_nopasswd_check_enable: no
```

Users must re-authenticate for privilege escalation. (V-71949)

STIG Description

Severity: Medium

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The STIG requires all users to re-authenticate when using `sudo`, but this change can be highly disruptive for automated scripts or applications that cannot perform interactive authentication. Automated edits from Ansible tasks might cause authentication disruptions on some hosts, and deployers are urged to carefully review each use of the `!authenticate` directive in their `sudo` configuration files.

The delay between logon prompts following a failed console logon attempt must be at least four seconds. (V-71951)

STIG Description

Severity: Medium

Configuring the operating system to implement organization-wide security implementation guides and security checklists verifies compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the Ansible role set a four second delay between failed login attempts. Deployers can configure a different delay (in seconds) by setting the following Ansible variable:

```
security_shadow_utils_fail_delay: 4
```

The operating system must not allow an unattended or automatic logon to the system via a graphical user interface. (V-71953)

STIG Description

Severity: High

Failure to restrict system access to authenticated users negatively impacts operating system security.

Deployer/Auditor notes

Implementation Status: Implemented

If `AutomaticLoginEnable=true` exists in the gdm configuration file, `/etc/gdm/custom.conf`, the configuration will removed. This disallows automatic logins for gdm and requires a user to complete the username and password prompts.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_disable_gdm_automatic_login: no
```

The operating system must not allow an unrestricted logon to the system. (V-71955)

STIG Description

Severity: High

Failure to restrict system access to authenticated users negatively impacts operating system security.

Deployer/Auditor notes

Implementation Status: Implemented

If `TimedLoginEnable=true` exists in the gdm configuration file, `/etc/gdm/custom.conf`, the configuration will removed. This disallows timed logins for guest users in gdm.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_disable_gdm_timed_login: no
```

The operating system must not allow users to override SSH environment variables. (V-71957)

STIG Description

Severity: Medium

Failure to restrict system access to authenticated users negatively impacts operating system security.

Deployer/Auditor notes

Implementation Status: Implemented

The `PermitUserEnvironment` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_environment_override: no
```

The operating system must not allow a non-certificate trusted host SSH logon to the system. (V-71959)

STIG Description

Severity: Medium

Failure to restrict system access to authenticated users negatively impacts operating system security.

Deployer/Auditor notes

Implementation Status: Implemented

The `HostbasedAuthentication` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_host_based_auth: no
```

Systems with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes. (V-71961)

STIG Description

Severity: High

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that GRUB 2 asks for a password whenever a user attempts to enter single-user or maintenance mode, this change might be disruptive in an emergency situation. Therefore, this change is not applied by default.

Deployers that wish to opt in for this change should set two Ansible variables:

```
security_require_grub_authentication: yes
security_grub_password_hash: grub.pbkdf2.sha512.10000.7B21785BEAFEE3AC...
```

The default password set in the security role is secrete, but deployers should set a much more secure password for production environments. Use the `grub2-mkpasswd-pbkdf2` command to create a password hash string and use it as the value for the Ansible variable `security_grub_password_hash`.

> **Warning:** This change must be tested in a non-production environment first. Requiring authentication in GRUB 2 without proper communication to users could cause extensive delays in emergency situations.

Systems using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes. (V-71963)

STIG Description

Severity: High

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Deployer/Auditor notes

Implementation Status: Opt-In

The tasks in the security role for V-71961 will also apply changes to systems that use UEFI. For more details, refer to the following documentation:

- *Systems with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes. (V-71961)*

The operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users) using multifactor authentication. (V-71965)

STIG Description

Severity: Medium

To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

```
1) Accesses explicitly identified and documented by the organization.␣
↪Organizations document specific user actions that can be performed on the␣
↪information system without identification or authentication;
```

and

2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000109-GPOS-00056, SRG-OS-000108-GPOS-00055, SRG-OS-000108-GPOS-00057, SRG-OS-000108-GPOS-00058

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deploying multi-factor authentication methods, including smart cards, is a complicated process that requires preparation and communication. This work is left to deployers to complete manually.

The rsh-server package must not be installed. (V-71967)

STIG Description

Severity: High

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The rsh-server service provides an unencrypted remote access service that does not provide for the confidentiality and integrity of user passwords or the remote session and has very weak authentication.

If a privileged user were to log on using this service, the privileged user password could be compromised.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the `rsh-server` package from the system if it is installed. Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_rsh_server: no
```

The ypserv package must not be installed. (V-71969)

STIG Description

Severity: High

Removing the ypserv package decreases the risk of the accidental (or intentional) activation of NIS or NIS+ services.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the NIS server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `ypserv`
- Ubuntu: `nis`
- openSUSE Leap: `ypserv`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_ypserv: no
```

The operating system must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. (V-71971)

STIG Description

Severity: Medium

Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The tasks in the security role cannot determine the access levels of individual users.

Deployers are strongly encouraged to configure SELinux user confinement on compatible systems using `semanage login`. Refer to the Confining Existing Linux Users documentation from Red Hat for detailed information and command line examples.

A file integrity tool must verify the baseline operating system configuration at least weekly. (V-71973)

STIG Description

Severity: Medium

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating systems Information Management Officer (IMO)/Information System Security Officer (ISSO) and System Administrators (SAs) must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Deployer/Auditor notes

Implementation Status: Opt-In

Initializing the AIDE database and completing the first AIDE run causes increased disk I/O and CPU usage for extended periods. Therefore, the AIDE database is not automatically initialized by the tasks in the security role.

Deployers can enable the AIDE database initialization within the security role by setting the following Ansible variable:

```
security_rhel7_initialize_aide: yes
```

Designated personnel must be notified if baseline configurations are changed in an unauthorized manner. (V-71975)

STIG Description

Severity: Medium

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating systems Information Management Officer (IMO)/Information System Security Officer (ISSO) and System Administrators (SAs) must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Deployer/Auditor notes

Implementation Status: Implemented

The cron job for AIDE is configured to send emails to the root user after each AIDE run.

The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components from a repository without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization. (V-71977)

STIG Description

Severity: High

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Deployer/Auditor notes

Implementation Status: Implemented

On Ubuntu systems, the tasks check for the `AllowUnauthenticated` string anywhere in the apt configuration files found within `/etc/apt/apt.conf.d/`. If the string is found, a warning is printed on the console.

On CentOS 7 systems, the tasks set the `gpgcheck` option to 1 in the `/etc/yum.conf` file. This enables GPG checks for all packages installed with `yum`.

On openSUSE Leap systems, the tasks set the `gpgcheck` option to 1 in the `/etc/zypp/zypp.conf` file. This enables GPG checks for all packages installed with `zypper`.

Setting `security_enable_gpgcheck_packages` to `no` will skip the `AllowUnauthenticated` string check on Ubuntu and it will set `gpgcheck=0` in `/etc/yum.conf` or `/etc/zypp/zypp.conf` on CentOS and openSUSE Leap systems respectively.

The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization. (V-71979)

STIG Description

Severity: High

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Deployer/Auditor notes

Implementation Status: Implemented

On Ubuntu systems, the tasks comment out the `no-debsig` configuration line in `/etc/dpkg/dpkg.cfg`. This causes `dpkg` to verify GPG signatures for all packages that are installed locally.

On CentOS 7 systems, the tasks set the `localpkg_gpgcheck` option to `1` in the `/etc/yum.conf` file. This enables GPG checks for all packages installed locally with `yum`.

On openSUSE Leap systems, the tasks set the `gpgcheck` option to `1` in the `/etc/zypp/zypp.conf` file. This enables GPG checks for all packages installed with `zypper`.

Setting `security_enable_gpgcheck_packages_local` to `no` will skip the `no-debsig` adjustment on Ubuntu and it will set `local_gpgcheck=0` in `/etc/yum.conf` on CentOS systems. Similarly, on openSUSE Leap systems, it will set `gpgcheck=0` in `/etc/zypp/zypp.conf`.

The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of packages without verification of the repository metadata. (V-71981)

STIG Description

Severity: High

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This ensures the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved Certificate Authority.

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that repository XML files are verified during `yum` runs.

> **Warning:** This setting is disabled by default because it can cause issues with CentOS systems and prevent them from retrieving repository information. Deployers who choose to enable this setting should test it thoroughly on non-production environments before applying it to production systems.

Deployers can override this default and opt in for the change by setting the following Ansible variable:

```
security_enable_gpgcheck_repo: yes
```

USB mass storage must be disabled. (V-71983)

STIG Description

Severity: Medium

USB mass storage permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Deployer/Auditor notes

Implementation Status: Opt-In

The tasks in the security role disable the `usb-storage` module and the change is applied the next time the server is rebooted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_disable_usb_storage: no
```

File system automounter must be disabled unless required. (V-71985)

STIG Description

Severity: Medium

Automatically mounting file systems permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Deployer/Auditor notes

Implementation Status: Implemented

The `autofs` service is stopped and disabled if it is found on the system. Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_disable_autofs: no
```

The operating system must remove all software components after updated versions have been installed. (V-71987)

STIG Description

Severity: Low

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that dependent packages are removed automatically when a package is removed, this can cause problems with certain packages, especially kernels. Deployers must opt in to meet the requirements of this STIG control.

Deployers should set the following variable to enable automatic dependent package removal:

```
security_package_clean_on_remove: yes
```

The operating system must enable SELinux. (V-71989)

STIG Description

Severity: High

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role enable the appropriate Linux Security Module (LSM) for the operating system.

For Ubuntu, openSUSE and SUSE Linux Enterprise 12 systems, AppArmor is installed and enabled. This change takes effect immediately.

For CentOS or Red Hat Enterprise Linux systems, SELinux is enabled (in enforcing mode) and its user tools are automatically installed. If SELinux is not in enforcing mode already, a reboot is required to enable SELinux and relabel the filesystem.

> **Warning:** Relabeling a filesystem takes time and the server must be offline for the relabeling to complete. Filesystems with large amounts of files and filesystems on slow disks will cause the relabeling process to take more time.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_enable_linux_security_module: no
```

The operating system must enable the SELinux targeted policy. (V-71991)

STIG Description

Severity: High

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Deployer/Auditor notes

Implementation Status: Implemented

The SELinux targeted policy is enabled on CentOS 7 and Red Hat systems. AppArmor only has one set of policies, so this change has no effect on Ubuntu, openSUSE Leap and SUSE systems running AppArmor.

For more information on this change and how to opt out, refer to *The operating system must enable SELinux. (V-71989)*.

The x86 Ctrl-Alt-Delete key sequence must be disabled. (V-71993)

STIG Description

Severity: High

A locally logged-on user who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In the GNOME graphical environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role disable the control-alt-delete key sequence by masking its systemd service unit.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_disable_ctrl_alt_delete: no
```

The operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files. (V-71995)

STIG Description

Severity: Medium

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Deployer/Auditor notes

Implementation Status: Opt-In - Ubuntu And Suse Only

The STIG requires that the umask for all authenticated users is `077`. This ensures that all new files and directories created by a user are accessible only by that user.

Although this change has a significant security benefit, it can cause problems for users who are not expecting the change. The security role will not adjust the umask by default.

Deployers can opt-in for the change by setting the default umask with an Ansible variable:

```
security_shadow_utils_umask: 077
```

Note: Ubuntu, openSUSE Leap and SUSE Linux Enterpsise 12 use `pam_umask` and it uses the default umask provided by the `UMASK` line in `/etc/login.defs`. The default setting on Ubuntu, openSUSE

Leap and SUSE Linux Enterprise 12 systems is `022`. This allows the users group and other users on the system to read and execute files, but they cannot write to them.

CentOS and Red Hat Enterprise Linux do not use `pam_umask` and instead set a default umask of `0002` for regular users and `0022` for root. This gives the regular users group full access to newly created files, but other users cannot write to those files.

The tasks for this STIG requirement are not currently applied to CentOS and Red Hat Enterprise Linux systems. See Launchpad Bug #1656003 for more details.

The operating system must be a vendor supported release. (V-71997)

STIG Description

Severity: High

An operating system release is considered supported if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The STIG requires that the current release of the operating system is still supported and is actively receiving security updates. Deployers are urged to stay current with the latest releases from Ubuntu, SUSE, CentOS and Red Hat.

The following links provide more details on end of life (EOL) dates for the distributions supported by this role:

- Ubuntu releases
- CentOS EOL dates
- Red Hat Enterprise Linux Life Cycle
- openSUSE EOL dates
- SUSE Linux Enterprise

Vendor packaged system security patches and updates must be installed and up to date. (V-71999)

STIG Description

Severity: Medium

Timely patching is critical for maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. However, failure to keep operating system and application software

patched is a common mistake made by IT professionals. New patches are released daily, and it is often difficult for even experienced System Administrators to keep abreast of all the new patches. When new weaknesses in an operating system exist, patches are usually made available by the vendor to resolve the problems. If the most recent security patches and updates are not installed, unauthorized users may take advantage of weaknesses in the unpatched software. The lack of prompt attention to patching could result in a system compromise.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that security patches and updates are applied when they are made available, this might be disruptive to some systems. Therefore, the tasks in the security role will not configure automatic updates by default.

Deployers can opt in for automatic package updates by setting the following Ansible variable:

```
security_rhel7_automatic_package_updates: yes
```

When enabled, the tasks install and configure `yum-cron` on CentOS and Red Hat Enterprise Linux. On Ubuntu systems, the `unattended-upgrades` package is installed and configured. On openSUSE Leap and SUSE Linux Enterprise systems, a daily cronjob is installed.

The system must not have unnecessary accounts. (V-72001)

STIG Description

Severity: Medium

Accounts providing no operational purpose provide additional opportunities for system compromise. Unnecessary accounts include user accounts for individuals not requiring access to the system and application accounts for applications not installed on the system.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers are strongly urged to review the list of user accounts on each server regularly. Evaluation of user accounts must be done on a case-by-case basis and the tasks in the security role are unable to determine which user accounts are valid. Deployers must complete this work manually.

All Group Identifiers (GIDs) referenced in the /etc/passwd file must be defined in the /etc/group file. (V-72003)

STIG Description

Severity: Low

If a user is assigned the GID of a group not existing on the system, and a group with the GID is subsequently created, the user may have unintended rights to any files associated with the group.

Deployer/Auditor notes

Implementation Status: Implemented

If any users are found with invalid GIDs, those users are printed in the Ansible output. Deployers should review the list and ensure all users are assigned to a valid group that is defined in `/etc/group`.

The root account must be the only account having unrestricted access to the system. (V-72005)

STIG Description

Severity: High

If an account other than root also has a User Identifier (UID) of 0, it has root authority, giving that account unrestricted access to the entire operating system. Multiple accounts with a UID of 0 afford an opportunity for potential intruders to guess a password for a privileged account.

Deployer/Auditor notes

Implementation Status: Implemented

If an account with UID 0 other than `root` exists on the system, the playbook will fail with an error message that includes the other accounts which have a UID of 0.

Deployers are strongly urged to keep only one account with UID 0, `root`, and to use `sudo` any situations where root access is required.

All files and directories must have a valid owner. (V-72007)

STIG Description

Severity: Medium

Unowned files and directories may be unintentionally inherited if a user is assigned the same User Identifier UID as the UID of the un-owned files.

Deployer/Auditor notes

Implementation Status: Opt-In

Searching an entire filesystem with `find` reduces system performance and might impact certain applications negatively. Therefore, the search for files and directories with an invalid owner is **disabled by default**.

Deployers can opt in for this search by setting the following Ansible variable:

```
security_search_for_invalid_owner: yes
```

Any files or directories without a valid user owner are displayed in the Ansible output.

All files and directories must have a valid group owner. (V-72009)

STIG Description

Severity: Medium

Files without a valid group owner may be unintentionally inherited if a group is assigned the same Group Identifier (GID) as the GID of the files without a valid group owner.

Deployer/Auditor notes

Implementation Status: Opt-In

Searching an entire filesystem with `find` reduces system performance and might impact certain applications negatively. Therefore, the search for files and directories with an invalid group owner is **disabled by default**.

Deployers can opt in for this search by setting the following Ansible variable:

```
security_search_for_invalid_group_owner: yes
```

Any files or directories without a valid group owner are displayed in the Ansible output.

All local interactive users must have a home directory assigned in the /etc/passwd file. (V-72011)

STIG Description

Severity: Medium

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Deployer/Auditor notes

Implementation Status: Implemented

The usernames of all users without home directories assigned are provided in the Ansible console output. Deployers should use this list of usernames to audit each system to ensure every user has a valid home directory.

All local interactive user accounts, upon creation, must be assigned a home directory. (V-72013)

STIG Description

Severity: Medium

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Deployer/Auditor notes

Implementation Status: Implemented

The `CREATE_HOME` variable is set to `yes` by the tasks in the security role. This ensures that home directories are created each time a new user account is created.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_shadow_utils_create_home: no
```

Note: On CentOS 7, Red Hat Enterprise Linux 7 systems, openSUSE Leap and SUSE Linux Enterprise 12, home directories are always created with new users by default. Home directories are not created by default on Ubuntu systems.

All local interactive user home directories defined in the /etc/passwd file must exist. (V-72015)

STIG Description

Severity: Medium

If a local interactive user has a home directory defined that does not exist, the user may be given access to the / directory as the current working directory upon logon. This could create a Denial of Service because the user would not be able to access their logon configuration files, and it may give them visibility to system files they normally would not be able to access.

Deployer/Auditor notes

Implementation Status: Implemented

Each interactive user on the system is checked to verify that their assigned home directory exists on the filesystem. If a home directory is missing, the name of the user and their assigned home directory is printed in the Ansible console output.

All local interactive user home directories must have mode 0750 or less permissive. (V-72017)

STIG Description

Severity: Medium

Excessive permissions on local interactive user home directories may allow unauthorized access to user files by other users.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that all home directories have the proper owner, group owner, and permissions, these changes might be disruptive in some environments. These tasks are not executed by default.

Deployers can opt in for the following changes to each home directory:

- Permissions are set to `0750` at a maximum. If permissions are already more restrictive than `0750`, the permissions are left unchanged.
- User ownership is set to the `UID` of the user.
- Group ownership is set to the `GID` of the user.

Deployers can opt in for these changes by setting the following Ansible variable:

```
security_set_home_directory_permissions_and_owners: yes
```

All local interactive user home directories must be owned by their respective users. (V-72019)

STIG Description

Severity: Medium

If a local interactive user does not own their home directory, unauthorized users could access or modify the users files, and the users may not be able to access their own files.

Deployer/Auditor notes

Implementation Status: Opt-In

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *All local interactive user home directories must have mode 0750 or less permissive. (V-72017)*

All local interactive user home directories must be group-owned by the home directory owners primary group. (V-72021)

STIG Description

Severity: Medium

If the Group Identifier (GID) of a local interactive users home directory is not the same as the primary GID of the user, this would allow unauthorized access to the users files, and users that share the same group may not be able to access files that they legitimately should.

Deployer/Auditor notes

Implementation Status: Opt-In

This control is implemented by the tasks for another control. Refer to the documentation for more details on the change and how to opt out:

- *All local interactive user home directories must have mode 0750 or less permissive. (V-72017)*

All files and directories contained in local interactive user home directories must be owned by the owner of the home directory. (V-72023)

STIG Description

Severity: Medium

If local interactive users do not own the files in their directories, unauthorized users may be able to access them. Additionally, if files are not owned by the user, this could be an indication of system compromise.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG has requirements for ownership and permissions of files and directories in each users home directory, broad changes to these settings might cause disruptions to users on a system. Therefore, these changes are left to deployers to examine and adjust manually.

All files and directories contained in local interactive user home directories must be group-owned by a group of which the home directory owner is a member. (V-72025)

STIG Description

Severity: Medium

If a local interactive users files are group-owned by a group of which the user is not a member, unintended users may be able to access them.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG has requirements for ownership and permissions of files and directories in each users home directory, broad changes to these settings might cause disruptions to users on a system. Therefore, these changes are left to deployers to examine and adjust manually.

All files and directories contained in local interactive user home directories must have mode 0750 or less permissive. (V-72027)

STIG Description

Severity: Medium

If a local interactive user files have excessive permissions, unintended users may be able to access or modify them.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG has requirements for ownership and permissions of files and directories in each users home directory, broad changes to these settings might cause disruptions to users on a system. Therefore, these changes are left to deployers to examine and adjust manually.

All local initialization files for interactive users must be owned by the home directory user or root. (V-72029)

STIG Description

Severity: Medium

Local initialization files are used to configure the users shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all initialization files for interactive users have proper owners, group owners, and permissions, these changes are often disruptive for users. The tasks in the security role do not make any changes to user initialization files.

Deployers should review the content and discretionary access controls applied to each users initialization files in their home directory.

Local initialization files for local interactive users must be group-owned by the users primary group or root. (V-72031)

STIG Description

Severity: Medium

Local initialization files for interactive users are used to configure the users shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all initialization files for interactive users have proper owners, group owners, and permissions, these changes are often disruptive for users. The tasks in the security role do not make any changes to user initialization files.

Deployers should review the content and discretionary access controls applied to each users initialization files in their home directory.

All local initialization files must have mode 0740 or less permissive. (V-72033)

STIG Description

Severity: Medium

Local initialization files are used to configure the users shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all initialization files for interactive users have proper owners, group owners, and permissions, these changes are often disruptive for users. The tasks in the security role do not make any changes to user initialization files.

Deployers should review the content and discretionary access controls applied to each users initialization files in their home directory.

All local interactive user initialization files executable search paths must contain only paths that resolve to the users home directory. (V-72035)

STIG Description

Severity: Medium

The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory (other than the users home directory), executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. If deviations from the default system search path for the local interactive user are required, they must be documented with the Information System Security Officer (ISSO).

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all initialization files must contain executable search paths that resolve to the users home directory, this change be disruptive for most users. The tasks in the security role do not make any changes to user initialization files.

Local initialization files must not execute world-writable programs. (V-72037)

STIG Description

Severity: Medium

If user start-up files execute world-writable programs, especially in unprotected directories, they could be maliciously modified to destroy user files or otherwise compromise the system at the user level. If the system is compromised at the user level, it is easier to elevate privileges to eventually compromise the system at the root and network level.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should manually search their system for world-writable programs and change the permissions on those programs. They are easily found with this command:

```
find / -perm -002 -type f
```

World-writable executables should not be needed under almost all circumstances.

All system device files must be correctly labeled to prevent unauthorized modification. (V-72039)

STIG Description

Severity: Medium

If an unauthorized or modified device is allowed to exist on the system, there is the possibility the system may perform unintended or unauthorized operations.

Deployer/Auditor notes

Implementation Status: Implemented - Red Hat Only

The tasks in the security role examine the SELinux contexts on each device file found on the system. Any devices without appropriate labels are printed in the Ansible output.

Deployers should investigate the unlabeled devices and ensure that the correct labels are applied for the class of device.

Note: This change applies only to CentOS or Red Hat Enterprise Linux systems since they rely on SELinux as their default Linux Security Module (LSM). Ubuntu, openSUSE Leap and SUSE Linux Enterprise systems use AppArmor, which uses policy files rather than labels applied to individual files.

File systems that contain user home directories must be mounted to prevent files with the setuid and setgid bit set from being executed. (V-72041)

STIG Description

Severity: Medium

The nosuid mount option causes the system to not execute setuid and setgid files with owner privileges. This option must be used for mounting any file system not containing approved setuid and setguid files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should examine any filesystem mounts that contain home directories to ensure that the `nosetuid` option is set.

File systems that are used with removable media must be mounted to prevent files with the setuid and setgid bit set from being executed. (V-72043)

STIG Description

Severity: Medium

The nosuid mount option causes the system to not execute setuid and setgid files with owner privileges. This option must be used for mounting any file system not containing approved setuid and setguid files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should examine any filesystem mounts of removable media to ensure that the `nosetuid` option is set.

File systems that are being imported via Network File System (NFS) must be mounted to prevent files with the setuid and setgid bit set from being executed. (V-72045)

STIG Description

Severity: Medium

The nosuid mount option causes the system to not execute setuid and setgid files with owner privileges. This option must be used for mounting any file system not containing approved setuid and setguid files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should examine any filesystem mounts of NFS imports to ensure that the `nosetuid` option is set.

All world-writable directories must be group-owned by root, sys, bin, or an application group. (V-72047)

STIG Description

Severity: Medium

If a world-writable directory has the sticky bit set and is not group-owned by a privileged Group Identifier (GID), unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

Deployer/Auditor notes

Implementation Status: Opt-In

The tasks in the security role examine the world-writable directories on the system and report any directories that are not group-owned by the `root` user. Those directories appear in the Ansible output.

Deployers should review the list of directories and group owners to ensure that they are appropriate for the directory. Unauthorized group ownership could allow certain users to modify files from other users.

Searching the entire filesystem for world-writable directories will consume a significant amount of disk I/O and could impact the performance of a production system. It can also delay the playbooks completion. Therefore, the search is disabled by default.

Deployers can enable the search by setting the following Ansible variable:

```
security_find_world_writable_dirs: yes
```

The umask must be set to 077 for all local interactive user accounts. (V-72049)

STIG Description

Severity: Medium

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 700 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be 0. This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that all local interactive user accounts have a umask of `077`, this change can be disruptive for users and the applications they run. This change cannot be applied in an automated way.

Deployers should review user initialization files regularly to ensure that the umask is not specified. This allows the system-wide setting of `077` to be applied to all user sessions.

Cron logging must be implemented. (V-72051)

STIG Description

Severity: Medium

Cron logging can be used to trace the successful or unsuccessful execution of cron jobs. It can also be used to spot intrusions into the use of the cron facility by unauthorized and malicious users.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Ubuntu, CentOS, Red Hat Enterprise Linux, openSUSE Leap and SUSE Linux Enterprise already capture the logs from cron.

Ubuntu systems collect cron job logs into the main syslog file (`/var/log/syslog`) rather than separate them into their own log file. CentOS and Red Hat Enterprise Linux systems collect cron logs in `/var/log/cron`. openSUSE Leap and SUSE Linux Enterprise collect cron job in `/var/log/messages`.

Deployers should not need to adjust these configurations unless a specific environment requires it. The tasks in the security role do not make changes to the `rsyslog` configuration.

If the cron.allow file exists it must be owned by root. (V-72053)

STIG Description

Severity: Medium

If the owner of the cron.allow file is not set to root, the possibility exists for an unauthorized user to view or to edit sensitive information.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role check for the existence of `/etc/cron.allow` and set both the user and group ownership to `root`. This is the default on Ubuntu, CentOS, Red Hat Enterprise Linux systems, openSUSE Leap and SUSE Linux Enterprise 12 already.

If the cron.allow file exists it must be group-owned by root. (V-72055)

STIG Description

Severity: Medium

If the group owner of the cron.allow file is not set to root, sensitive information could be viewed or edited by unauthorized users.

Deployer/Auditor notes

Implementation Status: Implemented

The group ownership for `/etc/cron.allow` is already set by the task for the following STIG control:

If the cron.allow file exists it must be owned by root. (V-72053)

Kernel core dumps must be disabled unless needed. (V-72057)

STIG Description

Severity: Medium

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in denial of service by exhausting the available space on the target file system partition.

Deployer/Auditor notes

Implementation Status: Implemented

The `kdump` service is disabled if it exists on the system. Deployers can opt out of this change by setting the following Ansible variable:

```
security_disable_kdump: no
```

A separate file system must be used for user home directories (such as /home or an equivalent). (V-72059)

STIG Description

Severity: Low

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

Deployers should consider using filesystem mounts for home directories during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/home` as a separate filesystem, a warning is printed in the Ansible output.

The system must use a separate file system for /var. (V-72061)

STIG Description

Severity: Low

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

Deployers should consider using filesystem mounts for `/var` during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/var` as a separate filesystem, a warning is printed in the Ansible output.

The system must use a separate file system for the system audit data path. (V-72063)

STIG Description

Severity: Low

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

Deployers should consider using filesystem mounts for `/var/log/audit` during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/var/log/audit` as a separate filesystem, a warning is printed in the Ansible output.

The system must use a separate file system for /tmp (or equivalent). (V-72065)

STIG Description

Severity: Low

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

Deployers should consider using filesystem mounts for `/tmp` during the initial server provisioning process. Adding filesystem mounts after a system is provisioned might lead to downtime.

The tasks in the security role do not take action on filesystem mounts. If the server does not mount `/tmp` as a separate filesystem, a warning is printed in the Ansible output.

The operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. (V-72067)

STIG Description

Severity: High

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000185-GPOS-00079, SRG-OS-000396-GPOS-00176, SRG-OS-000405-GPOS-00184, SRG-OS-000478-GPOS-00223

Deployer/Auditor notes

Implementation Status: Implemented - Red Hat And Suse Only

The tasks in the Ansible role install the `dracut-fips` (RHEL and SLE) and `dracut-fips-aesni` (RHEL) packages and check to see if FIPS is enabled on the system. If it is not enabled, a warning message is printed in the Ansible output.

Enabling FIPS at boot time requires additional manual configuration. Refer to Chapter 7. Federal Standards and Regulations in the Red Hat documentation for more details. Section 7.1.1 contains the steps required for updating the bootloader configuration and regenerating the initramfs.

Note: This change only applies to CentOS, Red Hat Enterprise Linux, openSUSE Leap and SUSE Linux Enterprise. Ubuntu does not use dracut by default and the process for enabling the FIPS functionality at boot time is more complex.

The file integrity tool must be configured to verify Access Control Lists (ACLs). (V-72069)

STIG Description

Severity: Low

ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.

Deployer/Auditor notes

Implementation Status: Implemented

CentOS 7 and Red Hat Enterprise Linux 7 already deploy a very secure AIDE configuration that checks access control lists (ACLs) and extended attributes by default. No configuration changes are applied on these systems.

However, Ubuntu lacks the rules that include ACL and extended attribute checks. The tasks in the security role will add a small configuration block at the end of the AIDE configuration file to meet the requirements of this STIG, as well as V-72071.

openSUSE Leap and SUSE Linux Enterprise 12 also lack a rule to check ACLs and extended attributes. The default configuration file is adjusted to include those as well.

The file integrity tool must be configured to verify extended attributes. (V-72071)

STIG Description

Severity: Low

Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.

Deployer/Auditor notes

Implementation Status: Implemented

CentOS 7 and Red Hat Enterprise Linux 7 already deploy a very secure AIDE configuration that checks access control lists (ACLs) and extended attributes by default. No configuration changes are applied on these systems.

However, Ubuntu lacks the rules that include ACL and extended attribute checks. The tasks in the security role will add a small configuration block at the end of the AIDE configuration file to meet the requirements of this STIG, as well as V-72069.

openSUSE Leap and SUSE Linux Enterprise 12 also lack a rule to check ACLs and extended attributes. The default configuration file is adjusted to include those as well.

The file integrity tool must use FIPS 140-2 approved cryptographic hashes for validating file contents and directories. (V-72073)

STIG Description

Severity: Medium

File integrity tools use cryptographic hashes for verifying file contents and directories have not been altered. These hashes must be FIPS 140-2 approved cryptographic hashes.

Deployer/Auditor notes

Implementation Status: Implemented

The default AIDE configuration in CentOS 7, Red Hat Enterprise Linux 7, openSUSE Leap and SUSE Linux Enterprise 12 already uses SHA512 to validate file contents and directories. No changes are required on these systems.

The tasks in the security role add a rule to end of the AIDE configuration on Ubuntu systems that uses SHA512 for validation.

The system must not allow removable media to be used as the boot loader unless approved. (V-72075)

STIG Description

Severity: Medium

Malicious users with removable boot media can gain access to a system configured to use removable media as the boot loader. If removable media is designed to be used as the boot loader, the requirement must be documented with the Information System Security Officer (ISSO).

Deployer/Auditor notes

Implementation Status: Exception - Initial Provisioning

When a server is initially provisioned, deployers should avoid storing the boot loader on removable media. It is not possible to change this via automated tasks.

The telnet-server package must not be installed. (V-72077)

STIG Description

Severity: High

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the telnet server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `telnet-server`
- Ubuntu: `telnetd`
- openSUSE Leap: `telnet-server`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_telnet_server: no
```

Auditing must be configured to produce records containing information to establish what type of events occurred, where the events occurred, the source of the events, and the outcome of the events.

These audit records must also identify individual identities of group account users. (V-72079)

STIG Description

Severity: High

Without establishing what type of events occurred, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in the operating system audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured operating system.

Satisfies: SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000042-GPOS-00021, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role start the audit daemon immediately and ensure that it starts at boot time.

The operating system must shut down upon audit processing failure, unless availability is an overriding concern. If availability is a concern, the system must alert the designated staff (System Administrator [SA] and Information System Security Officer [ISSO] at a minimum) in the event of an audit processing failure. (V-72081)

STIG Description

Severity: Medium

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Satisfies: SRG-OS-000046-GPOS-00022, SRG-OS-000047-GPOS-00023

Deployer/Auditor notes

Implementation Status: Implemented

The audit daemon takes various actions when there is an auditing failure. There are three options for the `-f` flag for `auditctl`:

- `0`: In the event of an auditing failure, do nothing.
- `1`: In the event of an auditing failure, write messages to the kernel log.
- `2`: In the event of an auditing failure, cause a kernel panic.

Most operating systems set the failure flag to 1 by default, which maximizes system availability while still causing an alert. The tasks in the security role set the flag to 1 by default.

Deployers can adjust the following Ansible variable to customize the failure flag:

```
security_rhel7_audit_failure_flag: 1
```

Warning: Setting the failure flag to 2 is **strongly** discouraged unless the security of the system takes priority over its availability. Any failure in auditing causes a kernel panic and the system requires a hard reboot.

The operating system must off-load audit records onto a different system or media from the system being audited. (V-72083)

STIG Description

Severity: Medium

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Deployer/Auditor notes

Implementation Status: Opt-In

The `audispd` service transmits audit logs to other servers. Deployers should specify the address of another server that can receive audit logs by setting the following Ansible variable:

```
security_audisp_remote_server: '10.0.21.1'
```

The operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited. (V-72085)

STIG Description

Severity: Medium

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Deployer/Auditor notes

Implementation Status: Opt-In

The `audispd` daemon transmits audit logs without encryption by default. The STIG requires that these logs are encrypted while they are transferred across the network. The encryption is controlled by the `enable_krb5` option in `/etc/audisp/audisp-remote.conf`.

Deployers can opt-in for encrypted audit log transmission by setting the following Ansible variable:

```
security_audisp_enable_krb5: yes
```

> **Warning:** Only enable this setting if kerberos is already configured.

The audit system must take appropriate action when the audit storage volume is full. (V-72087)

STIG Description

Severity: Medium

Taking appropriate action in case of a filled audit storage volume will minimize the possibility of losing audit records.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role set the `disk_full_action` and `network_failure_action` to `syslog` in the audispd remote configuration. In the event of a full disk on the remote log server or a network interruption, the local system sends warnings to syslog. This is the safest option since it maximizes the availability of the local system.

Deployers have two other options available:

- `single`: Switch the local server into single-user mode in the event of a logging failure.
- `halt`: Shut off the local server gracefully in the event of a logging failure.

> **Warning:** Choosing `single` or `halt` causes a server to go into a degraded or offline state immediately after a logging failure.

Deployers can adjust these configurations by setting the following Ansible variables (the safe defaults are shown here):

```
security_rhel7_auditd_disk_full_action: syslog
security_rhel7_auditd_network_failure_action: syslog
```

The operating system must immediately notify the System Administrator (SA) and Information System Security Officer ISSO (at a minimum) when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity. (V-72089)

STIG Description

Severity: Medium

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

Deployer/Auditor notes

Implementation Status: Implemented

The `space_left` configuration is set to 25% of the size of the disk mounted on `/`. This calculation is done automatically.

Deployers can set a custom threshold for the `space_left` configuration (in megabytes) by setting the following Ansible variable:

```
# Example: A setting of 1GB (1024MB)
security_rhel7_auditd_space_left: 1024
```

The operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) via email when the threshold for the repository maximum audit record storage capacity is reached. (V-72091)

STIG Description

Severity: Medium

If security personnel are not notified immediately when the threshold for the repository maximum audit record storage capacity is reached, they are unable to expand the audit record storage capacity before records are lost.

Deployer/Auditor notes

Implementation Status: Implemented

The `space_left_action` in the audit daemon configuration is set to `email`. This configuration causes the root user to receive an email when the `space_left` threshold is reached.

Deployers can customize this configuration by setting the following Ansible variable:

```
security_rhel7_auditd_space_left_action: email
```

The operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached. (V-72093)

STIG Description

Severity: Medium

If security personnel are not notified immediately when the threshold for the repository maximum audit record storage capacity is reached, they are unable to expand the audit record storage capacity before records are lost.

Deployer/Auditor notes

Implementation Status: Implemented

The `action_mail_acct` configuration in the audit daemon configuration file is set to `root` to meet the requirements of the STIG. Deployers can customize the recipient of the emails that come from auditd by setting the following Ansible variable:

```
security_rhel7_auditd_action_mail_acct: root
```

All privileged function executions must be audited. (V-72095)

STIG Description

Severity: Medium

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

This STIG is difficult to implement in an automated way because the number of applications on a system with setuid/setgid permissions changes over time. In addition, adding audit rules for some of these automatically could cause a significant increase in logging traffic when these applications are used regularly.

Deployers are urged to do the following instead:

- Minimize the amount of applications with setuid/setgid privileges
- Monitor any new applications that gain setuid/setgid privileges
- Add risky applications with setuid/setgid privileges to auditd for detailed syscall monitoring

---

All uses of the chown command must be audited. (V-72097)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `chown` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_chown: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fchown command must be audited. (V-72099)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fchown` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchown: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the lchown command must be audited. (V-72101)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `lchown` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_lchown: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fchownat command must be audited. (V-72103)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fchownat` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchownat: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the chmod command must be audited. (V-72105)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `chmod` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_chmod: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fchmod command must be audited. (V-72107)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fchmod` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchmod: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fchmodat command must be audited. (V-72109)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fchmodat` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fchmodat: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the setxattr command must be audited. (V-72111)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `setxattr` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_setxattr: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fsetxattr command must be audited. (V-72113)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fsetxattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fsetxattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the lsetxattr command must be audited. (V-72115)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `lsetxattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_lsetxattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the removexattr command must be audited. (V-72117)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `removexattr` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_removexattr: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the fremovexattr command must be audited. (V-72119)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `fremovexattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_fremovexattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the lremovexattr command must be audited. (V-72121)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that all `lremovexattr` syscalls are audited, but this change creates a significant increase in logging on most systems. This increase can cause some systems to run out of disk space for logs.

> **Warning:** This rule is disabled by default to avoid high CPU usage and disk space exhaustion. Deployers should only enable this rule if they have tested it thoroughly in a non-production environment with system health monitoring enabled.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_audit_lremovexattr: yes
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the creat command must be audited. (V-72123)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `creat` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_creat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the open command must be audited. (V-72125)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `open` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_open: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the openat command must be audited. (V-72127)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `openat` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_openat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the open_by_handle_at command must be audited. (V-72129)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `open_by_handle_at` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_open_by_handle_at: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the truncate command must be audited. (V-72131)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `truncate` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_truncate: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the ftruncate command must be audited. (V-72133)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `ftruncate` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_ftruncate: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the semanage command must be audited. (V-72135)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit any time the `semanage` command is used.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_semanage: no
```

All uses of the setsebool command must be audited. (V-72137)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit any time the `setsebool` command is used.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_setsebool: no
```

All uses of the chcon command must be audited. (V-72139)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `chcon` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_chcon: no
```

All uses of the setfiles command must be audited. (V-72141)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `restorecon` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_restorecon: no
```

The operating system must generate audit records for all successful/unsuccessful account access count events. (V-72143)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all successful and unsuccessful account access events. Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_audit_account_access: no
```

The operating system must generate audit records for all unsuccessful account access events. (V-72145)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all successful/unsuccessful account access count events. (V-72143)*

The operating system must generate audit records for all successful account access events. (V-72147)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time an account is accessed.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_account_access: no
```

All uses of the passwd command must be audited. (V-72149)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `passwd` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_passwd_command: no
```

All uses of the unix_chkpwd command must be audited. (V-72151)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `unix_chkpwd` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_unix_chkpwd: no
```

All uses of the gpasswd command must be audited. (V-72153)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `gpasswd` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_gpasswd: no
```

All uses of the chage command must be audited. (V-72155)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `chage` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_chage: no
```

All uses of the userhelper command must be audited. (V-72157)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `userhelper` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_userhelper: no
```

All uses of the su command must be audited. (V-72159)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `su` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_su: no
```

All uses of the sudo command must be audited. (V-72161)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the sudo command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_sudo: no
```

All uses of the sudoers command must be audited. (V-72163)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time a user manages the configuration files for sudo.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_sudo_config_changes: no
```

All uses of the newgrp command must be audited. (V-72165)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `newgrp` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_newgrp: no
```

All uses of the chsh command must be audited. (V-72167)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `chsh` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_chsh: no
```

All uses of the sudoedit command must be audited. (V-72169)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `sudoedit` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_sudoedit: no
```

All uses of the mount command must be audited. (V-72171)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `mount` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_mount: no
```

All uses of the umount command must be audited. (V-72173)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `umount` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_umount: no
```

All uses of the postdrop command must be audited. (V-72175)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `postdrop` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_postdrop: no
```

All uses of the postqueue command must be audited. (V-72177)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `postqueue` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_postqueue: no
```

All uses of the ssh-keysign command must be audited. (V-72179)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged ssh commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `ssh-keysign` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_ssh_keysign: no
```

All uses of the crontab command must be audited. (V-72183)

STIG Description

Severity: Medium

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `crontab` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_crontab: no
```

All uses of the pam_timestamp_check command must be audited. (V-72185)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `pam_timestamp_check` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_pam_timestamp_check: no
```

All uses of the init_module command must be audited. (V-72187)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `init_module` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_init_module: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the delete_module command must be audited. (V-72189)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `delete_module` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_delete_module: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the insmod command must be audited. (V-72191)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `insmod` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_insmod: no
```

All uses of the rmmod command must be audited. (V-72193)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `rmmod` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_rmmod: no
```

All uses of the modprobe command must be audited. (V-72195)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `modprobe` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_modprobe: no
```

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000476-GPOS-00221

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time that an account is modified. This includes changes to the following files:

- `/etc/group`
- `/etc/passwd`
- `/etc/gshadow`
- `/etc/shadow`
- `/etc/security/opasswd`

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_account_actions: no
```

All uses of the rename command must be audited. (V-72199)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `rename` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_rename: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the renameat command must be audited. (V-72201)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `renameat` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_renameat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the rmdir command must be audited. (V-72203)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

Rules are added to audit all `rmdir` syscalls on the system.

Deployers can opt out of this change by setting an Ansible variable:

```
security_rhel7_audit_rmdir: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the unlink command must be audited. (V-72205)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `unlink` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_unlink: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

All uses of the unlinkat command must be audited. (V-72207)

STIG Description

Severity: Medium

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks add a rule to auditd that logs each time the `unlinkat` command is used.

Deployers can opt-out of this change by setting an Ansible variable:

```
security_rhel7_audit_unlinkat: no
```

This rule is compatible with x86, x86_64, and ppc64 architectures.

The system must send rsyslog output to a log aggregation server. (V-72209)

STIG Description

Severity: Medium

Sending rsyslog output to another system ensures that the logs cannot be removed or modified in the event that the system is compromised or has a hardware failure.

Deployer/Auditor notes

Implementation Status: Verification Only

The tasks in the security role check for uncommented lines in the rsyslog configuration that contain `@` or `@@`, which signifies that a remote logging configuration is in place. If these lines are not found, a warning message is printed in the Ansible output.

The rsyslog daemon must not accept log messages from other servers unless the server is being used for log aggregation. (V-72211)

STIG Description

Severity: Medium

Unintentionally running a rsyslog server accepting remote messages puts the system at increased risk. Malicious rsyslog messages sent to the server could exploit vulnerabilities in the server software itself, could introduce misleading information in to the systems logs, or could fill the systems storage leading to a Denial of Service. If the system is intended to be a log aggregation server its use must be documented with the ISSO.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers must take manual steps to add or remove syslog reception configuration lines depending on a servers role:

- If the server is a log aggregation server, deployers must configure the server to receive syslog output from the other servers via TCP connections.
- If the server is not a log aggregation server, deployers must configure the server so that it does not accept syslog output from other servers.

The system must use a virus scan program. (V-72213)

STIG Description

Severity: High

Virus scanning software can be used to protect a system from penetration from computer viruses and to limit their spread through intermediate systems.

The virus scanning software should be configured to perform scans dynamically on accessed files. If this capability is not available, the system must be configured to scan, at a minimum, all altered files on the system on a daily basis.

If the system processes inbound SMTP mail, the virus scanner must be configured to scan all received mail.

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that a virus scanner is installed and running, but the value of a virus scanner within an OpenStack control plane or on a hypervisor is negligible in many cases. In addition, the disk I/O impact of a virus scanner can impact a production environment negatively.

The security role has tasks to deploy ClamAV with automatic updates, but the tasks are disabled by default.

Deployers can enable the ClamAV virus scanner by setting the following Ansible variable:

```
security_enable_virus_scanner: yes
```

Warning: The ClamAV packages are provided in the EPEL repository. Setting the `security_enable_virus_scanner` will also cause the EPEL repository to be installed by the role.

The system must update the virus scan program every seven days or more frequently. (V-72215)

STIG Description

Severity: Medium

Virus scanning software can be used to protect a system from penetration from computer viruses and to limit their spread through intermediate systems.

The virus scanning software should be configured to check for software and virus definition updates with a frequency no longer than seven days. If a manual process is required to update the virus scan software or definitions, it must be documented with the Information System Security Officer (ISSO).

Deployer/Auditor notes

Implementation Status: Implemented

By default, CentOS 7, Red Hat Enterprise Linux 7, openSUSE Leap and SUSE Linux Enterprise 12 check for virus database updates 12 times a day. Ubuntu servers have a default of 24 checks per day.

The tasks in the security role do not adjust these defaults as they are more secure than the STIGs requirement.

The operating system must limit the number of concurrent sessions to 10 for all accounts and/or account types. (V-72217)

STIG Description

Severity: Low

Operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to DoS attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that each account is limited to 10 concurrent connections, this change might be disruptive in some environments. Therefore, this change is not applied by default.

Deployers can opt in for this change by setting a concurrent connection limit with this Ansible variable:

```
security_rhel7_concurrent_session_limit: 10
```

The host must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management Component Local Service Assessment (PPSM CLSA) and vulnerability assessments. (V-72219)

STIG Description

Severity: Medium

In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000297-GPOS-00115

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should review each firewall rule on a regular basis to ensure that each port is open for a valid reason.

A FIPS 140-2 approved cryptographic algorithm must be used for SSH communications. (V-72221)

STIG Description

Severity: Medium

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

Operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general purpose computing system.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173

Deployer/Auditor notes

Implementation Status: Implemented

The `Ciphers` configuration is set to `aes128-ctr,aes192-ctr,aes256-ctr` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can change the list of ciphers by setting the following Ansible variable:

```
security_sshd_cipher_list: 'cipher1,cipher2,cipher3'
```

All network connections associated with a communication session must be terminated at the end of the session or after 10 minutes of inactivity from the user at a command prompt, except to fulfill documented and validated mission requirements. (V-72223)

STIG Description

Severity: Medium

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role set a 600 second (10 minute) timeout for network connections associated with a communication session. Deployers can change the timeout value by setting the following Ansible variable:

```
# Example: shorten the timeout to 5 minutes (300 seconds)
security_rhel7_session_timeout: 300
```

The Standard Mandatory DoD Notice and Consent Banner must be displayed immediately prior to, or as part of, remote access logon prompts. (V-72225)

STIG Description

Severity: Medium

Display of a standardized and approved use notification before granting access to the publicly accessible operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is␣
↪provided for USG-authorized use only.
```

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

```
-The USG routinely intercepts and monitors communications on this IS for␣
↪purposes including, but not limited to, penetration testing, COMSEC␣
↪monitoring, network operations and defense, personnel misconduct (PM), law␣
↪enforcement (LE), and counterintelligence (CI) investigations.
```

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interestsnot for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007 , SRG-OS-000228-GPOS-00088

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role deploy a standard notice and consent banner into `/etc/motd` on each server. Ubuntu, CentOS, Red Hat Enterprise Linux, openSUSE Leap and SUSE Linux Enterprise display this banner after each successful login via ssh or the console.

Deployers can choose a different destination for the banner by setting the following Ansible variable:

```
security_sshd_banner_file: /etc/motd
```

The message is customized with the following Ansible variable:

```
security_login_banner_text: |
  ------------------------------------------------------------------------
↪--
  * WARNING                                                              ␣
↪ *
  * You are accessing a secured system and your actions will be logged along ␣
↪ *
  * with identifying information. Disconnect immediately if you are not an   ␣
↪ *
  * authorized user of this system.                                       ␣
↪ *
  ------------------------------------------------------------------------
↪--
```

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) authentication communications. (V-72227)

STIG Description

Severity: Medium

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers are strongly urged to utilize `sssd` for systems that authenticate against LDAP or Active Directory (AD) servers.

The ldap connector for `sssd` connects only to LDAP servers over encrypted connections. Review the man page for sssd-ldap for more details on this requirement.

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications. (V-72229)

STIG Description

Severity: Medium

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers are strongly urged to utilize `sssd` for systems that authenticate against LDAP or Active Directory (AD) servers.

To meet this control, deployers must ensure that `ldap_tls_cacert` or `ldap_tls_cacertdir` are set in the `/etc/sssd/sssd.conf` file. The `ldap_tls_cacert` directive specifies a single certificate while `ldap_tls_cacertdir` specifies a directory where `sssd` can find CA certificates.

> **Warning:** Use caution when adjusting these settings. If the correct CA certificates are not already deployed to the servers that perform LDAP authentication, their attempts to authenticate users might fail.
>
> Consult with administrators of the LDAP system and test all changes on a non-production system first.

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications. (V-72231)

STIG Description

Severity: Medium

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers are strongly urged to utilize `sssd` for systems that authenticate against LDAP or Active Directory (AD) servers.

To meet this control, deployers must ensure that `ldap_tls_cacert` or `ldap_tls_cacertdir` are set in the `/etc/sssd/sssd.conf` file. The `ldap_tls_cacert` directive specifies a single certificate while `ldap_tls_cacertdir` specifies a directory where `sssd` can find CA certificates.

> **Warning:** Use caution when adjusting these settings. If the correct CA certificates are not already deployed to the servers that perform LDAP authentication, their attempts to authenticate users might fail.
>
> Consult with administrators of the LDAP system and test all changes on a non-production system first.

All networked systems must have SSH installed. (V-72233)

STIG Description

Severity: Medium

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that every system has an ssh client and server installed. The role installs the following packages:

- CentOS: `openssh-clients`, `openssh-server`
- Ubuntu: `openssh-client`, `openssh-server`
- openSUSE Leap: `openssh`

All networked systems must use SSH for confidentiality and integrity of transmitted and received information as well as information during preparation for transmission. (V-72235)

STIG Description

Severity: Medium

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers,

printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000423-GPOS-00188, SRG-OS-000423-GPOS-00189, SRG-OS-000423-GPOS-00190

Deployer/Auditor notes

Implementation Status: Implemented

The STIG has a requirement that the `sshd` daemon is running and enabled at boot time. The tasks in the security role ensure that these requirements are met.

Some deployers may not have `sshd` enabled on highly specialized systems and those deployers should opt out of this change by setting the following Ansible variable:

```
security_enable_sshd: no
```

Note: Setting `security_enable_sshd` to `no` causes the tasks to ignore the state of the service entirely. A setting of `no` does not stop or alter the `sshd` service.

All network connections associated with SSH traffic must terminate at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements. (V-72237)

STIG Description

Severity: Medium

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Deployer/Auditor notes

Implementation Status: Implemented

The `ClientAliveInterval` configuration is set to `600` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can adjust the length of the interval by changing the following Ansible variable:

```
security_sshd_client_alive_interval: 600
```

Note: The STIG requires that `ClientAliveInterval` is set to 600 and `ClientAliveCountMax` is set to zero, which sets a 10 minute session timeout. If no data is transferred in a 10 minute period, the session is disconnected.

The `ClientAliveInterval` specifies how long the ssh daemon waits before it sends a message to the client to see if it is still alive. The `ClientAliveCountMax` specifies how many of these messages are sent without receiving a response.

Deployers should refer to *All network connections associated with SSH traffic must terminate after a period of inactivity. (V-72241)* to customize the `ClientAliveCountMax` setting.

The SSH daemon must not allow authentication using RSA rhosts authentication. (V-72239)

STIG Description

Severity: Medium

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Deployer/Auditor notes

Implementation Status: Implemented

This STIG is already applied by the changes for *The SSH daemon must not allow authentication using known hosts authentication. (V-72249)*.

All network connections associated with SSH traffic must terminate after a period of inactivity. (V-72241)

STIG Description

Severity: Medium

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Deployer/Auditor notes

Implementation Status: Implemented

The `ClientAliveCountMax` configuration is set to `0` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can adjust the maximum amount of client alive intervals by changing the following Ansible variable.

```
security_sshd_client_alive_count_max: 0
```

Note: The STIG requires that `ClientAliveInterval` is set to 600 and `ClientAliveCountMax` is set to zero, which sets a 10 minute session timeout. If no data is transferred in a 10 minute period, the session is disconnected.

The `ClientAliveInterval` specifies how long the ssh daemon waits before it sends a message to the client to see if it is still alive. The `ClientAliveCountMax` specifies how many of these messages are sent without receiving a response.

Deployers should refer to *All network connections associated with SSH traffic must terminate at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements. (V-72237)* to customize the `ClientAliveInterval` setting.

The SSH daemon must not allow authentication using rhosts authentication. (V-72243)

STIG Description

Severity: Medium

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Deployer/Auditor notes

Implementation Status: Implemented

The `IgnoreRhosts` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_rhosts_auth: no
```

The system must display the date and time of the last successful account logon upon an SSH logon. (V-72245)

STIG Description

Severity: Medium

Providing users with feedback on when account accesses via SSH last occurred facilitates user recognition and reporting of unauthorized account use.

Deployer/Auditor notes

Implementation Status: Implemented

The `PrintLastLog` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_print_last_log: no
```

The system must not permit direct logons to the root account using remote access via SSH. (V-72247)

STIG Description

Severity: Medium

Even though the communications channel may be encrypted, an additional layer of security is gained by extending the policy of not logging on directly as root. In addition, logging on with a user-specific account provides individual accountability of actions performed on the system.

Deployer/Auditor notes

Implementation Status: Implemented

The `PermitRootLogin` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can select another setting for PermitRootLogin, from the available options `without-password`, `prohibit-password`, `forced-commands-only`, `yes`, or `no` by setting the following variable:

```
security_sshd_permit_root_login: no
```

> **Warning:** Ensure that a regular user account exists with a pathway to root access (preferably via `sudo`) before applying the security role. This configuration change disallows any direct logins with the `root` user.

The SSH daemon must not allow authentication using known hosts authentication. (V-72249)

STIG Description

Severity: Medium

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Deployer/Auditor notes

Implementation Status: Implemented

The `IgnoreUserKnownHosts` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_known_hosts_auth: no
```

The SSH daemon must be configured to only use the SSHv2 protocol. (V-72251)

STIG Description

Severity: High

SSHv1 is an insecure implementation of the SSH protocol and has many well-known vulnerability exploits. Exploits of the SSH daemon could provide immediate root access to the system.

Satisfies: SRG-OS-000074-GPOS-00042, SRG-OS-000480-GPOS-00227

Deployer/Auditor notes

Implementation Status: Implemented

The `Protocol` configuration is set to `2` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_protocol: 2
```

> **Warning:** There is no reason to enable any other protocol than SSHv2. SSHv1 has multiple vulnerabilities, and it is no longer widely used.

The SSH daemon must be configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms. (V-72253)

STIG Description

Severity: Medium

DoD information systems are required to use FIPS 140-2 approved cryptographic hash functions. The only SSHv2 hash algorithm meeting this requirement is SHA.

Deployer/Auditor notes

Implementation Status: Implemented

The `MACs` configuration is set to `hmac-sha2-256,hmac-sha2-512` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can adjust the allowed Message Authentication Codes (MACs) by setting the following Ansible variable:

```
security_sshd_allowed_macs: 'hmac-sha2-256,hmac-sha2-512'
```

The SSH public host key files must have mode 0644 or less permissive. (V-72255)

STIG Description

Severity: Medium

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Deployer/Auditor notes

Implementation Status: Implemented

The permissions on ssh public host keys is set to `0644`. If the existing permissions are more restrictive than `0644`, the tasks do not make changes to the files.

The SSH private host key files must have mode 0600 or less permissive. (V-72257)

STIG Description

Severity: Medium

If an unauthorized user obtains the private SSH host key file, the host could be impersonated.

Deployer/Auditor notes

Implementation Status: Implemented

The permissions on ssh private host keys is set to `0600`. If the existing permissions are more restrictive than `0600`, the tasks do not make changes to the files.

The SSH daemon must not permit Generic Security Service Application Program Interface (GSSAPI) authentication unless needed. (V-72259)

STIG Description

Severity: Medium

GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through SSH exposes the systems GSSAPI to remote hosts, increasing the attack surface of the system. GSSAPI authentication must be disabled unless needed.

Deployer/Auditor notes

Implementation Status: Implemented

The `GSSAPIAuthentication` setting is set to `no` to meet the requirements of the STIG.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disallow_gssapi: no
```

The SSH daemon must not permit Kerberos authentication unless needed. (V-72261)

STIG Description

Severity: Medium

Kerberos authentication for SSH is often implemented using Generic Security Service Application Program Interface (GSSAPI). If Kerberos is enabled through SSH, the SSH daemon provides a means of access to the systems Kerberos implementation. Vulnerabilities in the systems Kerberos implementation may then be subject to exploitation. To reduce the attack surface of the system, the Kerberos authentication mechanism within SSH must be disabled for systems not using this capability.

Deployer/Auditor notes

Implementation Status: Implemented

The `KerberosAuthentication` configuration is set to `no` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_disable_kerberos_auth: no
```

The SSH daemon must perform strict mode checking of home directory configuration files. (V-72263)

STIG Description

Severity: Medium

If other users have access to modify user-specific SSH configuration files, they may be able to log on to the system as another user.

Deployer/Auditor notes

Implementation Status: Implemented

The `StrictModes` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_enable_strict_modes: no
```

The SSH daemon must use privilege separation. (V-72265)

STIG Description

Severity: Medium

SSH daemon privilege separation causes the SSH process to drop root privileges when not needed, which would decrease the impact of software vulnerabilities in the unprivileged section.

Deployer/Auditor notes

Implementation Status: Implemented

The `UsePrivilegeSeparation` configuration is set to `sandbox` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_enable_privilege_separation: no
```

Note: Although the STIG requires this setting to be `yes`, the `sandbox` setting actually provides more security because it enables privilege separation during the early authentication process.

The SSH daemon must not allow compression or must only allow compression after successful authentication. (V-72267)

STIG Description

Severity: Medium

If compression is allowed in an SSH connection prior to authentication, vulnerabilities in the compression software could result in compromise of the system from an unauthenticated connection, potentially with root privileges.

Deployer/Auditor notes

Implementation Status: Implemented

The `Compression` configuration is set to `delayed` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can choose another option by setting the following Ansible variable:

```
security_sshd_compression: 'no'
```

Note: The following are the available settings for `Compression` in the ssh configuration file:

- `delayed`: Compression is enabled after authentication.
- `no`: Compression is disabled.
- `yes`: Compression is enabled during authentication and during the session (not allowed by the STIG).

The `delayed` option balances security with performance and is an approved option in the STIG.

The operating system must, for networked systems, synchronize clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS). (V-72269)

STIG Description

Severity: Medium

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Satisfies: SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in the security role make the following changes on each host:

- The `chrony` package is installed.
- The service (`chronyd` on Red Hat, CentOS, SLE and openSUSE Leap, `chrony` on Ubuntu) is started and enabled at boot time.
- A configuration file template is deployed that includes `maxpoll 10` on each server line.

Deployers can opt out of these changes by setting the following Ansible variable:

```
security_rhel7_enable_chrony: no
```

Note: Although the STIG mentions the traditional `ntpd` service, this role uses `chrony`, which is a more modern implementation.

The operating system must protect against or limit the effects of Denial of Service (DoS) attacks by validating the operating system is implementing rate-limiting measures on impacted network interfaces. (V-72271)

STIG Description

Severity: Medium

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of the operating system to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Deployer/Auditor notes

Implementation Status: Opt-In

Although the STIG requires that incoming TCP connections are rate limited with `firewalld`, this setting can cause problems with certain applications which handle large amounts of TCP connections. Therefore, the tasks in the security role do not apply the rate limit by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_enable_firewalld_rate_limit: yes
```

The STIG recommends a limit of 25 connection per minute and allowing bursts up to 100 connections. Both of these options are adjustable with the following Ansible variables:

```
security_enable_firewalld_rate_limit_per_minute: 25
security_enable_firewalld_rate_limit_burst: 100
```

Warning: Deployers should test rate limiting in a non-production environment first before applying it to production systems. Ensure that the application running on the system is receiving a large volume of requests so that the rule can be thoroughly tested.

The operating system must enable an application firewall, if available. (V-72273)

STIG Description

Severity: Medium

Firewalls protect computers from network attacks by blocking or limiting access to open network ports. Application firewalls limit which applications are allowed to communicate over the network.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000480-GPOS-00231, SRG-OS-000480-GPOS-00232

Deployer/Auditor notes

Implementation Status: Opt-In

The STIG requires that a firewall is configured on each server. This might be disruptive to some environments since the default firewall policy for `firewalld` is very restrictive. Therefore, the tasks in the security role do not install or enable the `firewalld` daemon by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_enable_firewalld: yes
```

Warning: Deployers must pre-configure `firewalld` or copy over a working XML file in `/etc/firewalld/zones/` from another server. The default firewalld restrictions on Ubuntu, CentOS, Red Hat Enterprise Linux and openSUSE Leap are highly restrictive.

The system must display the date and time of the last successful account logon upon logon. (V-72275)

STIG Description

Severity: Low

Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.

Deployer/Auditor notes

Implementation Status: Verification Only

The PAM configuration is checked for the presence of `pam_lastlogin` and a warning message is printed if the directive is not found. The tasks in the security role do not adjust PAM configurations since these changes might be disruptive in some environments.

Deployers should review their PAM configurations and add `pam_lastlogin` to `/etc/pam.d/postlogin` on CentOS and Red Hat Enterprise Linux or to `/etc/pam.d/login` on Ubuntu, openSUSE Leap and SUSE Linux Enterprise.

There must be no .shosts files on the system. (V-72277)

STIG Description

Severity: High

The .shosts files are used to configure host-based authentication for individual users or the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Deployer/Auditor notes

Implementation Status: Opt-In

The tasks in the security role examine the filesystem for any `.shosts` or `shosts.equiv` files. If they are found, they are deleted.

The search for these files will take a very long time on systems with slow disks or systems with a large amount of files. Therefore, this task is skipped by default.

Deployers can opt in for this change by setting the following Ansible variable:

```
security_rhel7_remove_shosts_files: yes
```

There must be no shosts.equiv files on the system. (V-72279)

STIG Description

Severity: High

The shosts.equiv files are used to configure host-based authentication for the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *There must be no .shosts files on the system. (V-72277)*

For systems using DNS resolution, at least two name servers must be configured. (V-72281)

STIG Description

Severity: Low

To provide availability for name resolution services, multiple redundant name servers are mandated. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.

Deployer/Auditor notes

Implementation Status: Implemented

If a server has fewer than two nameservers configured in `/etc/resolv.conf`, a warning is printed in the Ansible output.

The system must not forward Internet Protocol version 4 (IPv4) source-routed packets. (V-72283)

STIG Description

Severity: Medium

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures.

This requirement applies only to the forwarding of source-routed traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in this role set `net.ipv4.conf.all.accept_source_route` and `net.ipv4.conf.default.accept_source_route` to `0` by default. This prevents the system from forwarding source-routed IPv4 packets on all new and existing interfaces.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_source_routed_packet_forward_ipv4: no
```

For more details on source routed packets, refer to the Red Hat documentation.

The system must not forward Internet Protocol version 4 (IPv4) source-routed packets by default. (V-72285)

STIG Description

Severity: Medium

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The system must not forward Internet Protocol version 4 (IPv4) source-routed packets. (V-72283)*

The system must not respond to Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) echoes sent to a broadcast address. (V-72287)

STIG Description

Severity: Medium

Responding to broadcast (ICMP) echoes facilitates network mapping and provides a vector for amplification attacks.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in this role set `net.ipv4.icmp_echo_ignore_broadcasts` to 1 by default. This prevents the system from responding to IPv4 ICMP echoes sent to the broadcast address.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_echoes_broadcast_address: no
```

The system must prevent Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages from being accepted. (V-72289)

STIG Description

Severity: Medium

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the hosts route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages. (V-73175)*

The system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default. (V-72291)

STIG Description

Severity: Medium

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the systems route table, possibly revealing portions of the network topology.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in this role set `net.ipv4.conf.default.send_redirects` and `net.ipv4.conf.all.send_redirects` to `0` by default. This prevents a system from sending IPv4 ICMP redirect packets on all new and existing interfaces.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_icmp_redirects: no
```

The system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects. (V-72293)

STIG Description

Severity: Medium

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the systems route table, possibly revealing portions of the network topology.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default. (V-72291)*

Network interfaces must not be in promiscuous mode. (V-72295)

STIG Description

Severity: Medium

Network interfaces in promiscuous mode allow for the capture of all network traffic visible to the system. If unauthorized individuals can access these applications, it may allow then to collect information such as logon IDs, passwords, and key exchanges between systems.

If the system is being used to perform a network troubleshooting function, the use of these tools must be documented with the Information System Security Officer (ISSO) and restricted to only authorized personnel.

Deployer/Auditor notes

Implementation Status: Verification Only

All interfaces are examined to ensure they are not in promiscuous mode. A warning message is printed in the Ansible output if any promiscuous interfaces are found.

The system must be configured to prevent unrestricted mail relaying. (V-72297)

STIG Description

Severity: Medium

If unrestricted mail relaying is permitted, unauthorized senders could use this host as a mail relay for the purpose of sending spam or other unauthorized activity.

Deployer/Auditor notes

Implementation Status: Implemented

The `smtpd_client_restrictions` configuration in postfix is set to `permit_mynetworks, reject` to meet the STIGs requirements.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_rhel7_restrict_mail_relaying: no
```

A File Transfer Protocol (FTP) server package must not be installed unless needed. (V-72299)

STIG Description

Severity: High

The FTP service provides an unencrypted remote access that does not provide for the confidentiality and integrity of user passwords or the remote session. If a privileged user were to log on using this service, the privileged user password could be compromised. SSH or other encrypted file transfer methods must be used in place of this service.

Deployer/Auditor notes

Implementation Status: Not Implemented

This STIG is not yet implemented.

The Trivial File Transfer Protocol (TFTP) server package must not be installed if not required for operational support. (V-72301)

STIG Description

Severity: High

If TFTP is required for operational support (such as the transmission of router configurations) its use must be documented with the Information System Security Officer (ISSO), restricted to only authorized personnel, and have access control rules established.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the TFTP server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `tftp-server`
- Ubuntu: `tftpd`
- openSUSE Leap: `tftp`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_tftp_server: no
```

Remote X connections for interactive users must be encrypted. (V-72303)

STIG Description

Severity: High

Open X displays allow an attacker to capture keystrokes and execute commands remotely.

Deployer/Auditor notes

Implementation Status: Implemented

The `X11Forwarding` configuration is set to `yes` in `/etc/ssh/sshd_config` and sshd is restarted.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_sshd_enable_x11_forwarding: no
```

If the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon must be configured to operate in secure mode. (V-72305)

STIG Description

Severity: Medium

Restricting TFTP to a specific directory prevents remote users from copying, transferring, or overwriting system files.

Deployer/Auditor notes

Implementation Status: Verification Only

The tasks in the security role examine the TFTP server configuration file (if it exists) to verify that the secure operation flag (`-s`) is listed on the `server_args` line. If it is missing, a warning message is printed in the Ansible output.

An X Windows display manager must not be installed unless approved. (V-72307)

STIG Description

Severity: Medium

Internet services that are not required for system or application processes must not be active to decrease the attack surface of the system. X Windows has a long history of security vulnerabilities and will not be used unless approved and documented.

Deployer/Auditor notes

Implementation Status: Implemented

The role will remove the xorg server package from the system if it is installed. The package name differs between Linux distributions:

- CentOS: `xorg-x11-server-Xorg`
- Ubuntu: `xorg-xserver`
- openSUSE Leap: `xorg-x11-server`

Deployers can opt-out of this change by setting the following Ansible variable:

```
security_rhel7_remove_xorg: no
```

The system must not be performing packet forwarding unless the system is a router. (V-72309)

STIG Description

Severity: Medium

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

Deployer/Auditor notes

Implementation Status: Opt-In

Disabling IP forwarding on a system that routes packets or host virtual machines might cause network interruptions. The tasks in this role do not adjust the `net.ipv4.ip_forward` configuration by default.

Deployers can opt in for this change and disable IP forwarding by setting the following Ansible variable:

```
security_disallow_ip_forwarding: yes
```

> **Warning:** IP forwarding is required in some environments. Always test in a non-production environment before changing this setting on a production system.

The Network File System (NFS) must be configured to use RPCSEC_GSS. (V-72311)

STIG Description

Severity: Medium

When an NFS server is configured to use RPCSEC_SYS, a selected userid and groupid are used to handle requests from the remote user. The userid and groupid could mistakenly or maliciously be set incorrectly. The RPCSEC_GSS method of authentication uses certificates on the server and client systems to more securely authenticate the remote mount request.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers using NFS should examine their mounts to ensure `krb5:krb5i:krb5p` is provided with the `sec` option. Kerberos must be installed and configured before making the change.

SNMP community strings must be changed from the default. (V-72313)

STIG Description

Severity: High

Whether active or not, default Simple Network Management Protocol (SNMP) community strings must be changed to maintain security. If the service is running with the default authenticators, anyone can gather data about the system and the network and use the information to potentially compromise the integrity of the system or network(s). It is highly recommended that SNMP version 3 user authentication and message encryption be used in place of the version 2 community strings.

Deployer/Auditor notes

Implementation Status: Verification Only

The tasks in the security role examine the contents of the `/etc/snmp/snmpd.conf` file (if it exists) and search for the default community strings: `public` and `private`. If either default string is found, a message is printed in the Ansible output.

The system access control program must be configured to grant or deny system access to specific hosts and services. (V-72315)

STIG Description

Severity: Medium

If the systems access control program is not configured with appropriate rules for allowing and denying access to system network resources, services may be accessible to unauthorized hosts.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The `firewalld` service is optionally enabled and configured in the tasks for another STIG control:

- *The operating system must enable an application firewall, if available. (V-72273)*

Deployers should review their `firewalld` ruleset regularly to ensure that each firewall rule is specific as possible. Each rule should allow the smallest number of hosts to access the smallest number of services.

The system must not have unauthorized IP tunnels configured. (V-72317)

STIG Description

Severity: Medium

IP tunneling mechanisms can be used to bypass network filtering. If tunneling is required, it must be documented with the Information System Security Officer (ISSO).

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should review all tunneled connections on a regular basis to ensure each is valid and properly secured. This requires careful verification that cannot be done with automated Ansible tasks.

The system must not forward IPv6 source-routed packets. (V-72319)

STIG Description

Severity: Medium

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv6 forwarding is enabled and the system is functioning as a router.

Deployer/Auditor notes

Implementation Status: Implemented

The tasks in this role set `net.ipv6.conf.all.accept_source_route` to `0` by default. This prevents the system from forwarding source-routed IPv6 packets.

Deployers can opt out of this change by setting the following Ansible variable:

```
security_disallow_source_routed_packet_forward_ipv6: no
```

Refer to IPv6 source routing: history repeats itself for more details on IPv6 source routed packets.

The operating system must have the required packages for multifactor authentication installed. (V-72417)

STIG Description

Severity: Medium

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Implemented

The STIG requires that the following multifactor authentication packages are installed:

- authconfig
- authconfig-gtk
- esc

- pam_pkcs11

These packages are benign if they are not needed on a system, but `authconfig-gtk` may cause some graphical dependencies to be installed which may not be needed on some systems. The security role installs these packages, but it skips the installation of `authconfig-gtk`. Deployers can install the graphical package manually if needed.

The operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules (PAM). (V-72427)

STIG Description

Severity: Medium

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Although the STIG requires that the `sssd.conf` contains both `nss` and `pam` authentication modules, this change can be disruptive in environments that are already using LDAP or Active Directory for authentication. Deployers should make these changes only if their environment is compatible.

The operating system must implement certificate status checking for PKI authentication. (V-72433)

STIG Description

Severity: Medium

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Any adjustment to PKI authentication can cause disruptions for users. Deployers should verify that enabling OCSP validation is compatible with their existing configuration.

The operating system must implement smart card logons for multifactor authentication for access to privileged accounts. (V-72435)

STIG Description

Severity: Medium

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Any adjustment to PKI authentication can cause disruptions for users. Deployers should verify that their environment is compatible with smart cards before requiring them for authentication.

The operating system must set the lock delay setting for all connection types. (V-73155)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. (V-71891)*

The operating system must set the session idle delay setting for all connection types. (V-73157)

STIG Description

Severity: Medium

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a users session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. (V-71891)*

When passwords are changed or new passwords are established, pwquality must be used. (V-73159)

STIG Description

Severity: Medium

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Pwquality enforces complex password construction configuration on the system.

Deployer/Auditor notes

Implementation Status: Opt-In

The security role can require new or changed passwords to follow the pwquality rules, but this change can be disruptive for users without proper communication. Deployers must opt in for this change by setting the following variable:

```
security_enable_pwquality_password_set: yes
```

File systems that are being imported via Network File System (NFS) must be mounted to prevent binary files from being executed. (V-73161)

STIG Description

Severity: Medium

The noexec mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should review their NFS mounts to ensure they are mounted with the `noexec` option. Deployers should skip this change if they execute applications from NFS mounts.

The audit system must take appropriate action when there is an error sending audit records to a remote system. (V-73163)

STIG Description

Severity: Medium

Taking appropriate action when there is an error sending audit records to a remote system will minimize the possibility of losing audit records.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The audit system must take appropriate action when the audit storage volume is full. (V-72087)*

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group. (V-73165)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow. (V-73167)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow. (V-73171)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd. (V-73173)

STIG Description

Severity: Medium

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)*

The system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages. (V-73175)

STIG Description

Severity: Medium

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the hosts route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Deployer/Auditor notes

Implementation Status: Implemented

This control is implemented by the tasks for another control:

- *The system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects. (V-72293)*

Wireless network adapters must be disabled. (V-73177)

STIG Description

Severity: Medium

The use of wireless networking can introduce many different attack vectors into the organizations network. Common attack vectors such as malicious association and ad hoc networks will allow an attacker to spoof a wireless access point (AP), allowing validated systems to connect to the malicious AP and enabling the attacker to monitor and record network traffic. These malicious APs can also serve to create a man-in-the-middle attack or be used to create a denial of service to valid network resources.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Deployers should review the configuration of any wireless networking device connected to the system to ensure it must be enabled. The STIG requires that all wireless network devices are enabled unless required.

The operating system must uniquely identify and must authenticate users using multifactor authentication via a graphical user logon. (V-77819)

STIG Description

Severity: Medium

To assure accountability and prevent unauthenticated access, users must be identified and authenticated to prevent potential misuse and compromise of the system.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

Satisfies: SRG-OS-000375-GPOS-00161,SRG-OS-000375-GPOS-00162

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

The STIG requires that multifactor authentication is used for graphical user logon, but this change requires custom configuration based on the authentication solution that is used.

Deployers should review the available options, such as traditional smartcards, USB devices (such as Yubikeys), or software token systems, and use one of these solutions on each system.

The Datagram Congestion Control Protocol (DCCP) kernel module must be disabled unless required. (V-77821)

STIG Description

Severity: Medium

Disabling DCCP protects the system against exploitation of any flaws in the protocol implementation.

Deployer/Auditor notes

Implementation Status: Implemented

The ansible-hardening role disables the DCCP kernel module by default. Each system must be rebooted to fully apply the change.

Deployers can opt out of the change by setting the following Ansible variable:

```
security_rhel7_disable_dccp: no
```

The operating system must require authentication upon booting into single-user and maintenance modes. (V-77823)

STIG Description

Severity: Medium

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system.

Deployer/Auditor notes

Implementation Status: Exception - Manual Intervention

Modifying sensitive systemd unit files directly or via overrides could cause a system to have issues during the boot process. The role does not make any adjustments to the `rescue.service` because this service is critical during emergencies.

All of the distributions supported by the role already require authentication for single user mode.

The operating system must implement virtual address space randomization. (V-77825)

STIG Description

Severity: Medium

Address space layout randomization (ASLR) makes it more difficult for an attacker to predict the location of attack code he or she has introduced into a processs address space during an attempt at exploitation. Additionally, ASLR also makes it more difficult for an attacker to know the location of existing code in order to repurpose it using return-oriented programming (ROP) techniques.

Deployer/Auditor notes

Implementation Status: Implemented

Most modern systems enable Address Space Layout Randomization (ASLR) by default (with a setting of 2), and the role ensures that the secure default is maintained.

Deployers can opt out of the change by setting the following Ansible variable:

```
security_enable_aslr: no
```

For more details on the ASLR settings, review the sysctl documentation.

3.6 Additional hardening configurations

Although the Security Technical Implementation Guide (STIG) contains a very comprehensive set of security configurations, some ansible-hardening contributors want to add extra security configurations to the role. The *contrib* portion of the ansible-hardening role is designed to implement those configurations as an optional set of tasks.

The *contrib* hardening configurations are disabled by default, but they can be enabled by setting the following Ansible variable:

```
security_contrib_enabled: yes
```

The individual tasks are controlled by Ansible variables in `defaults/main.yml` that begin with `security_contrib_`.

3.6.1 Kernel

C-00001 - Disable IPv6

Some systems do not require IPv6 connectivity and the presence of link local IPv6 addresses can present an additional attack surface for lateral movement. Deployers can set the following variable to disable IPv6 on all network interfaces:

```
security_contrib_disable_ipv6: yes
```

Warning: Deployers should test this change in a test environment before applying it in a production deployment. Applying this change to a production system that relies on IPv6 connectivity will cause unexpected downtime.

3.7 Developer Guide

3.7.1 Building a development environment

The OpenStack gate runs the tox tests found within `tox.ini`. Developers should use these tox tests to verify that their changes will work when the gate jobs run. Some systems may need additional packages for these tests to run properly.

To install all of the prerequisites and run the functional tests, use the `run_tests.sh` script:

```
./run_tests.sh
```

Note: This script will apply the default security hardening configurations to the local host. Avoid running this script on production servers which have not been properly tested with the security role.

3.7.2 Writing documentation

Documentation consists of two parts: metadata and deployer notes. The metadata exists as YAML front-matter for each STIG configuration. The frontmatter is followed by the text of the deployer note itself.

All of the notes are found within `doc/metadata/rhel7`. Here is an example of V-71989:

```
---
id: V-71989
```

(continues on next page)

(continued from previous page)

```
status: implemented
tag: lsm
---

The tasks in the security role enable the appropriate Linux Security Module
(LSM) for the operating system.

For Ubuntu, openSUSE and SUSE Linux Enterprise 12 systems, AppArmor is␣
↪installed and
enabled. This change takes effect immediately.

For CentOS or Red Hat Enterprise Linux systems, SELinux is enabled (in
enforcing mode) and its user tools are automatically installed. If SELinux is
not in enforcing mode already, a reboot is required to enable SELinux and
relabel the filesystem.

.. warning::

    Relabeling a filesystem takes time and the server must be offline for the
    relabeling to complete. Filesystems with large amounts of files and
    filesystems on slow disks will cause the relabeling process to take more
    time.

Deployers can opt out of this change by setting the following Ansible␣
↪variable:

.. code-block:: yaml

    security_rhel7_enable_linux_security_module: no
```

The block after the first three dashes (`---`) is the metadata. The metadata must include:

- `id`: The ID of the STIG configuration item.
- `status`: The implementation status of the STIG configuration, such as `implemented`, `exception`, or `opt-in`.
- `tag`: The Ansible tag associated with the task(s) that make changes based on the STIG requirement, such as `auditd`, `kernel`, or `lsm`.

The next block is the deployer note. The note should be brief, but it must answer a few critical questions:

- What does the change do to a system?
- What is the value of making this change?
- How can a deployer opt out or opt in for a particular change?
- Is there additional documentation available online that may help a deployer decide whether or not this change is valuable to them?

Run `tox -e docs` to rebuild the documentation from the metadata and review your changes.

3.7.3 Release notes

Adding release notes helps deployers and other developers discover the new additions to the role in a concise format. Release notes should be added to incoming patches if they would change something noticeable in the role, such as bug fixes, new functionality, or variable name changes.

To add a release note, use `reno`:

```
reno new i-made-a-new-feature-that-does-something-awesome
```

Once you run the `reno new` command with a release note slug, a new file appears in `releasenotes/notes`. Edit that file and adjust the relevant section to explain the changes found within your patch. Delete any unused sections and submit the release note with your patch.

For more details, refer to the documentation on release notes found in the OpenStack-Ansible developer documentation

CHAPTER

FOUR

RELEASES

Deployers should use the latest stable release for all production deployments.

4.1 Train

- **Status:** Latest stable release
- **STIG Version:** RHEL 7 STIG Version 1, Release 3 *(Published on 2017-10-27)*
- **Supported Operating Systems:**
  - CentOS 7
  - Debian 10 Buster
  - openSUSE Leap 15 and 15.1
  - Red Hat Enterprise Linux 7
  - Ubuntu 18.04 Bionic

4.2 Stein

- **Status:** Latest stable release
- **STIG Version:** RHEL 7 STIG Version 1, Release 3 *(Published on 2017-10-27)*
- **Supported Operating Systems:**
  - CentOS 7
  - Debian 9 Stretch and 10 Buster
  - openSUSE Leap 15 and 15.1
  - Red Hat Enterprise Linux 7
  - Ubuntu 18.04 Bionic

4.3 Rocky

- **Status:** Latest stable release
- **STIG Version:** RHEL 7 STIG Version 1, Release 3 *(Published on 2017-10-27)*
- **Supported Operating Systems:**
  - CentOS 7
  - openSUSE Leap 42.3
  - Red Hat Enterprise Linux 7
  - Ubuntu 16.04 Xenial and 18.04 Bionic

4.4 Queens

- **Status:** Latest stable release
- **STIG Version:** RHEL 7 STIG Version 1, Release 3 *(Published on 2017-10-27)*
- **Supported Operating Systems:**
  - CentOS 7
  - Debian 8 Jessie
  - Fedora 26
  - openSUSE Leap 42.2 and 42.3
  - Red Hat Enterprise Linux 7 *(partial automated test coverage)*
  - SUSE Linux Enterprise 12 (*experimental*)
  - Ubuntu 16.04 Xenial
- **Documentation:**
  - ansible-hardening Queens Release Notes

4.5 Pike

- **Status:** Latest stable release *(released: September 2017)*
- **STIG Version:** RHEL 7 STIG Version 1, Release 1 *(Published on 2017-02-27)*
- **Supported Operating Systems:**
  - CentOS 7
  - Debian 8 Jessie
  - Fedora 26
  - openSUSE Leap 42.2 and 42.3
  - Red Hat Enterprise Linux 7 *(partial automated test coverage)*
  - SUSE Linux Enterprise 12 (*experimental*)

  - Ubuntu 14.04 Trusty *(Deprecated)*
  - Ubuntu 16.04 Xenial
- **Documentation:**
  - ansible-hardening Pike Documentation
  - ansible-hardening Pike Release Notes

4.6 Ocata

- **Status:** Latest stable release *(released February 2017)*
- **Supported Operating Systems:**
  - CentOS 7
  - Red Hat Enterprise Linux 7 *(partial automated test coverage)*
  - Ubuntu 14.04 Trusty *(Deprecated)*
  - Ubuntu 16.04 Xenial
- **Documentation:**
  - ansible-hardening Ocata Documentation
  - ansible-hardening Ocata Release Notes

4.7 Newton

- **Status:** Previous stable release *(released October 2016)*
- **Supported Operating Systems:**
  - Ubuntu 14.04 Trusty
  - Ubuntu 16.04 Xenial
  - CentOS 7
  - Red Hat Enterprise Linux 7 *(partial automated test coverage)*
- **Documentation:**
  - ansible-hardening Newton Documentation
  - ansible-hardening Newton Release Notes