ARCHON OS V3.0.0.2

COMMON CRITERIA USER GUIDANCE

Version 1.2

July 2024

DOCUMENT PREPARED BY:

Intertek Acumen Security, LLC

2400 Research Blvd, Suite 395

Rockville, MD 20850

www.acumensecurity.net

CACI.

44590 Guilford Dr

Ashburn, VA 20147

www.caci.com

CACI Support

https://attilasec.zendesk.com/hc/en-us/requests/new

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 PURPOSE

This document describes the operational guidance and preparative procedures for CACI's Archon OS v3.0.0.2. This document defines the necessary steps to configure Archon OS, which is referred to also as the TOE, into the Common Criteria Evaluated Configuration and provides guidance for the ongoing secure usage of the TOE.

1.2 PRODUCT OVERVIEW

Archon OS is an operating system (OS) based on Red Hat Enterprise Linux (RHEL) v8.10 that supports multiple users, user permissions, access controls, and cryptographic functionality.

Archon OS is an ostree-based packaging of Red Hat Enterprise Linux (RHEL), tailored for deployment on End User Devices (EUDs) specifically designed for Commercial Solutions for Classified (CSfC) solutions. The Archon OS ostree incorporates unmodified versions of the RHEL RPMs. Archon OS is curated to incorporate solely the essential OS options and applications pertinent to EUD functionality, with non-applicable components deliberately excluded.

This guide provides instructions to configure and operate CACI Archon OS v3.0.0.2 in the Common Criteria evaluated configuration running on one of the following hardware platforms:

TABLE 1: ARCHON OS V3.0.0.2 HARDWARE PLATFORMS (EUDS)

Vendor	Model	CPU	CPU Microarchitecture	CPU Family
Dell Inc.	Latitude 5400	Intel® Core™ i5-8365U	Skylake	Whiskey Lake
	Latitude 5410	Intel® Core™ i7-10810U	Skylake	Comet Lake
	Latitude 5430	Intel® Core™ i7-1255U	Golden Cove	Alder Lake
	Precision 3260	Intel® Core™ i7-12700	Golden Cove	Alder Lake
	Precision 3570	Intel® Core™ i7-1255U	Golden Cove	Alder Lake
	Latitude 5440	Intel® Core™ i5-1335U	Raptor Cove	Raptor Lake
	Latitude 5540	Intel® Core™ i5-1335U	Raptor Cove	Raptor Lake
	Precision 3580	Intel® Core™ i5-1350P	Raptor Cove	Raptor Lake

2 Installation Guidelines and Preparative Procedures

2.1 Assumptions

The following assumptions are made with regards to the setup, installation, and ongoing operation of this product:

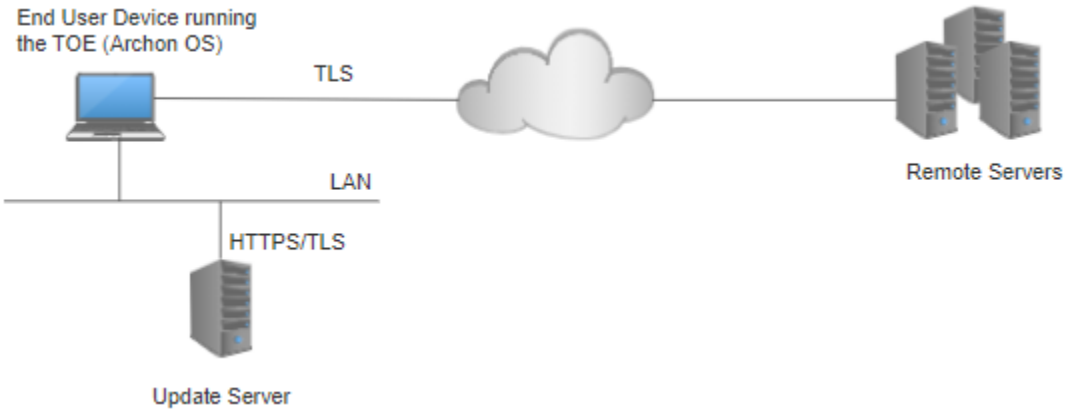
- The Archon OS v3.0.0.2 hardware platform is physically protected and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be enough to protect the device and the data it contains.
- The Security Administrator(s) for the device are trusted and act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have enough strength and entropy and to lack malicious intent when administering the device. The device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.
- The device firmware and software are updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- The administrator's credentials (private key) used to access the device are protected by the platform on which they reside.
- The administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords etc.) when the equipment is discarded or removed from its operational environment.

2.2 Operational Environment

The TOE is a software TOE and has been evaluated on the following host platforms identified in Table 1: Archon OS v3.0.0.2 Hardware Platforms (EUDs)

The diagram below depicts a representative TOE deployment in the operational environment.

FIGURE 1: REPRESENTATIVE TOE DEPLOYMENT



The following items are required for the operational environment.

TABLE 2: HARDWARE AND SOFTWARE ENVIRONMENTAL COMPONENTS

Components	Mandatory/ Optional	Description
End User Device (EUD)	Mandatory	The hardware running the TOE (software). The evaluated systems are identified in Table 2 above.
Update Server	Mandatory	Provides the ability to check for updates to the TOE as well as providing signed updates. The TOE communicates with the Update Server using HTTPS over TLS.
Remote Servers	Mandatory	Servers that support multiple applications and provide multiple services for the EUD users.

2.3 OBTAINING SUPPORT

In the event of software failure, customers may report security issues related to Archon OS via the secure support portal at https://attilasec.zendesk.com/hc/en-us/requests/new [attilasec.zendesk.com].

2.4 SECURITY ISSUES AND MITIGATIONS

CACI provides a security update release for Archon OS at least once every 3 months. Resolution of vulnerabilities is expected within 180 days of public disclosure. For significant vulnerabilities, additional releases may be generated for quicker resolution. Archon OS vulnerabilities may be identified via internal testing, monitoring of CVE reports for Archon OS and third-party components, notification of vulnerabilities from third-party suppliers, or from customer reports. The CACI support team notifies customers of Archon OS vulnerabilities and informs them about resolutions.

Because Archon OS is typically used on systems without internet access, it is expected that customers will download releases to their enterprise infrastructure and make it available to systems from one of their internal web servers. Customers are notified when releases are available and are provided with a URL for download.

For vulnerabilities involving CACI-developed components, the CACI engineering team creates a Github ticket for each vulnerability to track the analysis and resolution of the issue. Issues are prioritized and worked to resolution, then incorporated into a product release.

For vulnerabilities involving third-party components, CACI engineering works with the third-party supplier to ensure the vulnerability is known to them. The latest component fixes are continuously integrated into the Archon OS build cycle. This is particularly used with RHEL fixes, enabling Red Hat's efforts to be quickly integrated into Archon OS.

2.5 DISCLAIMERS

OpenSSL was the only tested cryptographic engine. Other cryptographic engines were not evaluated nor tested, so they should not be used.

The evaluation was limited to verify secure communications using TLS. Other protocols such as TELNET are not secure and should not be used.

The OpenSSL library also provides cryptographic algorithms for the trusted update and secure boot security functions.

2.6 PRODUCT FUNCTIONALITY NOT INCLUDED IN THE SCOPE OF THE EVALUATION

The following security functionality is included in Archon OS v3.0.0.2 but was not evaluated:

- SELinux provided access controls.
- OS Virtualization Infrastructure
- Containerization infrastructure

3 INSTALLATION

3.1 OVERVIEW

This section defines the necessary steps to install and configure Archon OS into the Common Criteria Evaluated Configuration.

3.2 CONFIGURING ARCHON OS INTO THE CC EVALUATED CONFIGURATION

Archon OS supports SCAP (Secure Content Automation Protocol) which is a standard created by NIST to allow content migration between certified security vendors. Additionally, Archon OS includes the FIPS:OSPP (Operating System Protection Profile) system-wide sub-policy which contains further restrictions for cryptographic algorithms required by the Common Criteria (CC) certification.

SCAP support and configuration combined with OSPP support and configuration means that by default, Archon OS v3.0.0.2 is configured with a subset of CC evaluated configuration parameters. Specifically, there are no TLS parameters that need to be configured (with the exception of certificates) and the TOE is automatically configured in FIPS mode (refer to Section 4.1).

Specifically, the following is configured:

- the selected key generation schemes and key sizes,
- the key establishment schemes,
- the encryption/decryption modes and key sizes,
- the supported TLS client cipher suites,
- the supported groups extension, and
- 2048-bit RSA is used for secure boot signatures only.

The TOE is automatically configured in FIPS mode which ensures the system generates all keys (RNG functionality) using FIPS approved algorithms. No other configuration is required to configure RNG functionality.

Once the TOE has been updated to the evaluated version, the TOE must be configured to be in the evaluated configuration. The following is a list of parameters that are required to be set in order to configure Archon OS into the CC evaluated configuration.

1. Configure software restriction policies (fapolicyd) (Section 3.6).
2. Configure TLS Mutual Authentication (load x.509 client certificates) (Section 4.4).
3. Configure update server communication (Section 4.2).
4. Disable SSH client and server (Section 4.6).
5. Configure local audit storage settings (Section 5.1.1).
6. Start auditing (Section 5.1.2).
7. Configure parameters to mitigate CVEs (Section 5.3).
8. Configure password policy (Section 6.1.3).
9. Configure failed authentication timeout (Section 6.1.5).
10. Configure session timeout (Section 6.1.6).
11. Configure inactivity timeout (Section 6.1.7).
12. Configure warning banner (Section 6.1.8).

3.3 TOE's Version Tag

Archon OS uses a 4-field version number:

```
Major.MinorTenths.MinorHundredths,MinorThousandths
```

- `Major` versions are what you expect for any product.
- `Minor Tenths` are meant for minor OS changes that add new capabilities, such as upgrading the component RPMs from RHEL 8.8 to RHEL 8.10.
- `Minor Hundredths` are meant for bug fixes to correct functionality and also introduce new capabilities or adding drivers to support new hardware platforms.
- `Minor Thousandths` are meant for bug fixes to correct functionality and do not introduce new capabilities.

The RPM Epoch is an optional part of an RPM version and is denoted by "n:" at the beginning of the RPM version number. The Epoch is the most significant component of a package's complete version identifier with regards to RPM's version comparison algorithm. When absent from the version number, the Epoch is assumed to be "0:" for comparison purposes. It is often used to facilitate packages from upstream developers that change their versioning scheme (which could otherwise break RPM versioning comparisons).

3.4 System Updates

3.4.1 Secure Acceptance of the TOE

The TOE and its hardware platform (one of the systems listed in Table 1) are ordered by the customer from CACI. CACI uses reputable shipping firms that provide shipment tracking functionality to deliver the hardware, loaded with a previous version of the TOE to the customer.

The shipment includes a pointer to CACI's Update Server. You are to use this secure support portal (https://) to download the latest version of the TOE (in tarball format) to a system on your site and eventually onto the Update Server.

Delivery of the guidance documents is via Archon OS's NIAP Product Compliant List (PCL) web site listing (VID11429).

3.4.2 Installation Prerequisites

1. Ensure your Archon OS hardware is a system identified in Table 1.
2. Ensure Archon OS is installed on your system.
3. Ensure your operational environment is configured as described in Section 2.2.
4. Ensure you checked for TOE updates and have downloaded the latest version of the TOE (in tarball format) and that version is on your Update Server.

Your Archon OS system will be delivered with an older version of Archon OS. The following steps must be taken to ensure that your system is the correct version of the evaluated system (Archon OS v3.0.0.2).

3.4.3 Preliminary Setup

Unpack provided tarball on your Update Server. We recommend that any previously loaded update files be removed from the update server first to avoid confusion.

- `tar xf v3.0.0.2.tar -C /output/path/`

3.4.4 Upgrade Process

Step 1: For ease of reference, set an environmental variable to a URL pointing to the webserver where you unpacked the tarball. The URL needs to point to the `/repo` path in the unpacked tree. Specifying `https` in this URL ensures that the traffic involving this URL will be protected by TLS.

- `export REPO_URL=https://file_server_address:port/directory`

For example, if the tarball was unpacked at the web server root the URL might look like this:

- `export REPO_URL=https://192.168.0.219:8787/repo`

Step 2: This step may be performed separately from actually performing the update. For example, an administrator may configure the remote on the TOE when the repo is installed on the update server, and the actual TOE update could be performed when it is convenient to do so. Note that the last parameter in the "`ostree remote add`" command specifies the ostree branch associated with the repo update (in this case, `gpos/v03.00.00.02/gpos`). The middle portion of the branch indicates the corresponding Archon OS release version (`v03.00.00.02`).

- `sudo ostree remote add gpos $REPO_URL gpos/v03.00.00.02/gpos`

Step 3: The previous command will create a file named `repo_name.conf` in the `/etc/ostree/remotes.d` directory. Add the following lines to the `repo_name.conf` file to customize the X.509 certificate information for your system.

```
tls-client-cert-path=[client certificate filepath]
tls-client-key-path=[client key filepath]
tls-ca-path=[CA certificate filepath]
```

Step 4: Check if an update is available. This step verifies that a remote ostree build for an update is configured on the TOE.

a. First determine the current OS version.

- `cat /etc/os-release`

```
NAME="ArchonOS"
VERSION="v03.00.00.01 (13697)"
ID="archon"
ID_LIKE="rhel"
VERSION_ID="v03.00.00.01-13697"
PLATFORM_ID="platform:el8"
PRETTY_NAME="ArchonOS v03.00.00.01-13697"
```

The output states that the current OS version is v03.00.00.01.

b. Next determine the OS version for any remote repos configured on the TOE. Depending on local policy and procedures, multiple remote repos may be configured.

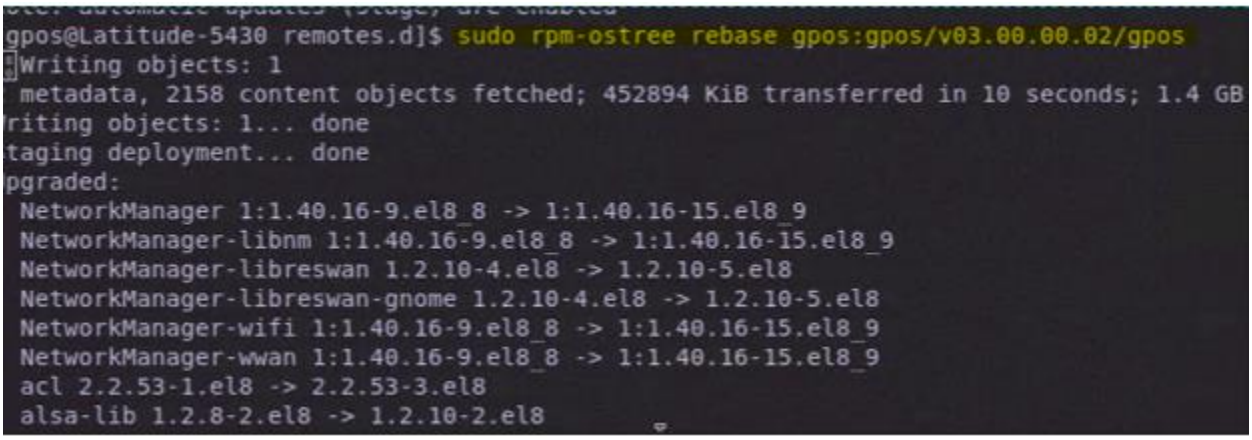
➢ `grep -r –include="*.conf" "branches" /etc/ostree/remotes.d`

```
gpos.conf:branches=gpos/v03.00.00.02/gpos;
```

This output shows that an update is available since v03.00.00.02 is an update to v03.00.00.01.

Step 5: Perform an update. The public key chain for updates is present on the system in `/usr/share/ostree/trusted.gpg.d`. Verify that a list of updated RPMs is displayed (the output shown below is representational; the actual output depends on the update being applied).

➢ `sudo rpm-ostree rebase gpos:gpos/v03.00.00.02/gpos`



The signature is checked during TOE update. Above shows an example of a successful update. There is no indication that the signature verification was successful. If the signature fails verification, the system will display an error message, halts, and the upgrade will not proceed.

Step 6: Reboot the system so that the upgrade takes effect.

➢ `sudo systemctl reboot`

3.4.5 Verify the Current Version of the TOE

To verify the version of the running TOE, view the file `/etc/os-release`. The version of the TOE will be displayed in the format described in Section 3.3. Refer to Section 3.4.4 above, item a, for an example output display.

3.4.6 Checking for Available TOE Updates

You can check if an update is available. Determine the OS version for any remote repos configured for the TOE. Depending on local policy and procedures, multiple remote repos may be configured.

➢ `grep -r –include="*.conf" "branches" /etc/ostree/remotes.d`

```
gpos.conf:branches=gpos/v03.00.00.02/gpos;
```

This output shows that an update version v03.00.00.02 is available.

3.4.7 Update Signature Verification

When an administrator performs an update by invoking the `rpm-ostree rebase` command (Step 3.4.4, Step 5 above), the signature is verified. If the signature fails verification, the system will display an error message, halts, and the upgrade does not proceed. If the signature verification is successful, a message will not be displayed.

3.5 Secure Boot

Secure Boot is a UEFI firmware security feature developed by the UEFI Consortium that ensures only immutable and signed software are loaded during the boot time. Secure Boot leverages digital signatures to validate the authenticity, source, and integrity of the code that is loaded. These validation steps are taken to prevent malicious code from being loaded and to prevent attacks, such as the installation of certain types of rootkits.

Secure Boot is split into several pieces and stages. The first important concept is the Allow DB (DB) and Disallow DB (DBX) databases. The Allow DB (DB) database stores the hashes and keys for trusted loaders and EFI applications that are allowed to be loaded by the machine's firmware. The Disallow DB (DBX) database stores revoked, compromised, and non-trusted hashes and keys. Any attempt to load signed code using the Disallow DB keys or in the case where the hash matches a Disallow DB entry will lead to boot failure.

RSA-2048 is only supported for secure boot; the certs related to secure boot are preloaded by Dell. No configuration by the administrator is necessary.

The second portion of the boot software is signed by a central Certificate Authority using a 4096-bit SHA-512 signature. The public certificate is stored in the hardware, allowing third-party EFI applications signed by this certificate to load successfully.

The TOE's hardware needs to be configured to use UEFI boot, with Secure Boot signature checking enabled. This needs to be performed prior to the installation of the archon operating system.

1. Boot the hardware into a system setup (BIOS) configuration software, by pressing F2 during early boot.
2. Navigate to System BIOS
3. Under Boot Settings, set Boot Mode to UEFI
   - Under System Security, set Secure Boot to Enabled
   - Set Secure Boot Policy to Standard
   - Set Secure Boot Mode to Deployed
4. Then press the Esc key several times and, when asked, save the modified settings and reboot.
5. Secure Boot will be enable for future boots.

3.5.1 Archon OS Boot

CACI Archon OS v3.0.0.2 has two modes of operation:

1. Normal: Once installation has been completed Archon OS is in a secure mode of operation.

2. Error: Archon OS (with the support of the underlying hardware) verifies the integrity of the bootloader and kernel prior to execution. If a bootloader or kernel integrity error is detected, Archon OS enters an error mode and does not boot. This indicates that an unknown integrity error has occurred. To safely boot Archon OS, a specialist must correct the error and determine if any other modifications (accidental or malicious) have been made to the system. Contact your CACI support team (refer to Section 2.3).

3.6 Software Restriction Policies (fapolicyd)

`Fapolicyd` is a daemon that determines whether or not access to files or execution of programs is allowed based on the software's reputation. By default, all applications that are packaged by rpm are automatically trusted and therefore, the following steps must be followed to enable `fapolicyd` policy checks.

`fapolicyd.rules` is a file which contains the rules that `fapolicyd` uses to make decisions about access rights. The rules follow a simple format of:

```
decision perm subject : object
```

The rules are configured in `/etc/fapolicyd/fapolicyd.rules`. They are evaluated from top to bottom with the first rule to match being used for the access control decision. The following section describes the allowed rule keywords. The colon is mandatory to separate subject and object since they share keywords.

`decision`

Either `allow`, `deny`, `allow_audit`, `deny_audit`, `allow_syslog`, `deny_syslog`, `allow_log`, or `deny_log`. If the rule triggers, this is the access decision that `fapolicyd` will tell the kernel. Any rule with a `deny` in the keyword will deny access and any with an `allow` in the keyword will allow access.

`perm`

`perm` describes what kind of permission is being asked for. The permission is either `open`, `execute`, or `any`. If none are given, then `open` is assumed.

`subject`

The `subject` is the process that is performing actions on system resources. The fields in the rule that describe the subject are written in a `name=value` format. There can be one or more subject fields. Each field is and'ed with others to decide if a rule triggers. The name values can be any of the following:

`all`

This matches against any subject. When used, this must be the only subject in the rule.

`auid`

This is the login uid that the audit system assigns users when they log in to the system. Daemons have a value of -1. The given value may be numeric or the account name.

`uid`

This is the user id that the program is running under. The given value may be numeric or the account name.

`gid`

This is the group id that the program is running under. The given value may be numeric or the group name.

`sessionid`

This is the numeric session id that the audit system assigns to users when they log in. Daemons have a value of -1.

`pid`

This is the numeric process id that a program has.

`ppid`

This is the numeric process id of the program's parent. Note that programs that are orphaned or started directly from systemd have a ppid value of 1. Kernel threads have a ppid value of 2.

`trust`

This is a boolean describing whether it is required for the subject to be in the trust database or not. A value of 1 means its required while 0 means its not. Trust checking is extended by the integrity setting in `fapolicyd.conf`. When trust is used on the subject, it could be a daemon. If that daemon gets updated on disk, the trustdb will be updated to the new SHA256 hash. If the integrity setting is not none, the running daemon is not likely to be trusted unless it gets restarted. The default rules are not written in a way that this would happen. But this needs to be highlighted as it may not be obvious when writing a new rule.

`comm`

This is the shortened command name. When an interpreter starts a program, it usually renames the program to the script rather than the interpreter.

`exe`

This is the full path to the executable. Globbing is not supported. You may also use the special keyword untrusted to match on the subject not being listed in the rpm database.

`dir`

If you wish to match a directory, then use this by giving the full path to the directory. Its recommended to end with the / to ensure it matches a directory. There are 3 keywords that `dir` supports: `execdirs, systemdirs, untrusted`.

`execdirs`	The `execdirs` option will match against the following list of directories: `/usr/,/bin/, /sbin/, /lib/, /lib64/, /usr/libexec/.`
`systemdirs`	The `systemdirs` option will match against the same list as `execdirs` but also includes /etc/.

`untrusted` The `untrusted` option will look up the current executable's full path in the rpm database to see if the executable is known to the system. The rule will trigger if the file in question is not in the trust database. This option is deprecated in favor of using obj_trust with execute permission when writing rules.

`ftype`

This option takes the mime type of a file as an argument. If you wish to check the mime type of a file while writing rules, run the following command:

- `fapolicyd-cli --ftype /path-to-file`

`device`

This option will match against the device that the executable resides on. To use it, start with /dev/ and add the target device name.

`pattern`

There are various ways that an attacker may try to execute code that may reveal itself in the pattern of file accesses made during program startup. This rule can take one of several options depending on which access patterns is wished to be blocked. `Fapolicyd` is able to detect these different access patterns and provide the access decision as soon as it identifies the pattern. The pattern type can be any of:

`normal` This matches against any ELF program that is dynamically linked.

`ld_so` This matches against access patterns that indicate that the program is being started directly by the runtime linker.

`ld_preload` This matches against access patterns that indicate that the program is being started with either LD_PRELOAD or LD_AUDIT present in the environment. Note that even without this rule, you have protection against LD_PRELOAD of unknown binaries when the rules are written such that trust is used to determine if a library should be opened. In that case, the preloaded library would be denied but the application will still execute. This rule makes it so that even trusted libraries can be denied and the application will not execute.

`static` This matches against ELF files that are statically linked.

`object`

The object is the file that the subject is interacting with. The fields in the rule that describe the object are written in a name=value format. There can be one or more object fields. Each field is and'ed with others to decide if a rule triggers. The name values can be any of the following:

`all`

This matches against any object. When used, this must be the only object in the rule.

`path`

This is the full path to the file that will be accessed. Globbing is not supported. You may also use the special keyword **untrusted** to match on the object not being listed in the rpm database.

`dir`

If you wish to match on access to any file in a directory, then use this by giving the full path to the directory. Its recommended to end with the / to ensure it matches a directory. There are 3 keywords that `dir` supports: `execdirs, systemdirs, untrusted`. See the `dir` option under `Subject` for an explanation of these keywords.

`device`

This option will match against the device that the file being accessed resides on. To use it, start with /dev/ and add the target device name.

`ftype`

This option matches against the mime type of the file being accessed. See `ftype` under `Subject` for more information on determining the mime type.

`trust`

This is a boolean describing whether it is required for the object to be in the trust database or not. A value of 1 means its required while 0 means its not.

`sha256hash`

This option matches against the sha256 hash of the file being accessed. The hash in the rules should be all lowercase letters and do NOT start with 0x. Lowercase is the default output of sha256sum.

Note: the rules that ship with the daemon are set up to only audit denied access requests. It is possible to audit successful access by changing any rule in `/etc/fapolicyd/fapolicyd.rules` from `deny_audit` to `allow_audit`. Restarting the daemon makes the rule take effect. It is not configured to audit successful access by default because it will result in a large quantity of audit events making it hard to find policy violations.

4 Network Configuration

The TOE provides TLS Client functionality, communicating with an Upload Server and remote servers that provide services to the user. The TOE's operational environment requires an Upload Server and to enable users to initiate TLS sessions both programmatically and by using the CLI. The following sections describe the required configuration for network communication.

4.1 Cryptographic Library Configuration

The TOE includes the OpenSSL v1.1.1k cryptographic library that provides all cryptographic algorithms. The following describes the cryptographic support provided.

The TOE acts as a TLS Client communicating with an Update Server and remote servers. Archon OS supports the following cipher suites:

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

The TOE supports mutual authentication and session renegotiation.

CACI Archon OS also presents the following curve in the Supported Groups Extension without any configuration: secp384r1.

RSA key sizes of 2048 (for secure boot only), 3072, and 4096 are supported, utilizing SHA-256, SHA-384, and SHA-512 hashing algorithms. Additionally, ECDSA curve P-384 is supported, paired with SHA-384.

Archon OS verifies that the presented identifier matches the reference identifier according to RFC 6125 as follows. The TOE establishes the reference identifier by parsing the DNS Name or IP address for the configured TLS server. The reference identifier is matched against the SAN, if present. If the SAN is not present, the referenced identifier is matched against the CN for DNS. For IP addresses, the TOE matches the identifier against the SAN only. The TOE supports wildcards in the DNS name of the server certificate. The TOE does not support URI reference identifiers, SRV reference identifiers, or certificate pinning.

4.2 Configuring Update Server Communication

The CC evaluated configuration requires the operational environment support an Update Server. The TOE communicates with the Update Server using HTTPS over TLS. The following configuration is required to configure communication with the update server.

1. Open the file `/etc/appache2/sites-available/repo.conf` and define the following values:

```
SSLCACertificateFile [CA Cert filename]
SSLCertificateFile [Cert filename]
SSLCertificateKeyFile [none | Key filename]
SSLVerifyClient [none | require]
SSLVerifyDepth n
```

Where:

`CA Cert filename` Points to the Root CA used to validate the presented server certificate.

`Cert filename` The cert to use, if one is requested by the server. The default is not to use a certificate

`Key filename` The private key to use. If not specified then the certificate file will be used.

`Require` An argument given as a parameter to `SSLVerifyClient` that if specified, requires the server to support mutual authentication. If set to `none`, mutual authentication is not required.

`n` The certificate chain length.

2. Save and close the file.

4.3 User Initiated TLS Sessions

Archon OS supports user initiated TLS sessions. TLS session can be invoked by an application program and by the CLI.

4.3.1 Command Line (CLI)

- `openssl s_client -connect [host]:[port] -x509_strict -verify_return_error -CAfile [ca certificate] -cert [client_cert] -key [keyfile] -verify_hostname [hostname] -verify_ip [IP address]-tls1_2`

The options are described as follows:

`-connect [host]:[port]`
Specifies the FQDN or IP address and port of the remote system.

`-x509_strict`
Checks that all certificates, including issuing CAs, are compliant to x509 standards.

`-verify_return_error`
Terminates the connection if an error is found.

`-CAfile [ca certificate]`
Points to the Root CA used to validate the presented server certificate.

`-cert [filename]`

The cert to use, if one is requested by the server. The default is not to use a certificate.

`-key [keyfile]`

The private key to use. If not specified then the certificate file will be used.

`-verify_hostname [hostname]`
Configures the hostname that the TOE will convert into a DNS-ID and CN reference identifier. The left-most component in the presented certificate may be a wildcard (i.e. “*”).

`-verify_ip [IP address]`
Configures the IP address that the TOE will convert into an IP address SAN reference identifier.

`-tls1_2`
Force to use TLSv1.2 only.

4.3.2 Application Program

Application programmers use the same OpenSSL function call with the same parameters as defined above.

Application developers can use the included `gcc` compiler and linker to create applications that run on Archon OS. When invoking `gcc`, developers should follow best practices for secure development:

Include the following compiler flags to enable stack smashing protections:

```
-fstack-protector-strong --param=ssp-buffer-size=4
```

Include the following compiler and linker flags to enable more ASLR:

```
-fpie -Wl,-pie
```

4.4 TLS Mutual Authentication

Archon OS supports optional mutual authentication (MA) communicating with servers. An X.509 device certificate for the TOE must be configured in order to support MA. The TOE will send its client certificate and engage in MA when it sees the certificate request message is sent by the server.

Perform the following steps to create a certificate chain to send to a server who requires mutual authentication.

1. Create a private key
   a. RSA key generation.
      - `openssl genrsa -out client.key.pem 3072`
        ```
        Generating RSA private key, 4096 bit long modulus
        . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . ++
          . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . ++
        e is 65537 (0x10001)
        ```
   b. EC key generation.
      - `openssl ecparam -name prime384v1 -genkey -noout -out client.key.pem`
2. Generate a Certificate Signing Request (CSR) for the client certificate.
   - `openssl req -new -key client.key.pem -out client.csr`

   Sample output from terminal

   ```
   You are about to be asked to enter information that will be
   incorporated into your certificate request.
   What you are about to enter is what is called a Distinguished Name
   or DN.
   ```

```
There are quite a few fields but you can leave some blank.
For some fields there will be a default value,
If you enter '.', the fields will be left blank.
----
Country Name (2 letter code) [IN]:
State or Province Name (full name) [Some-State]:Maryland
Locality Name (eg, city) [BANGALORE]:
Organization Name (eg, company) [Acumen Security]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:ca-server
Email Address []:admin@acumensecurity.com

Please enter the following 'extra' attributes
To be sent with your certificate request.

A challenge password []:
An optional company name []:
```

3. Add certificate extensions

   - `cat client_ext.cnf`

```
basicConstraints = CA:FALSE
nsCertType = cient
nsComment = "Client Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyed,issuer
keyUsage = critical, nonrepudiation,digitalSignature,keyEncipherment
extendedKeyUsage = clientAuth
```

4. Submit to CA your CSR and receive your certificate chain.

4.5 Storing Certificates

To acknowledge applications on your system with a new source of trust, add the corresponding certificate to the system-wide store, and use the `update-ca-trust` command. To add a certificate in the simple PEM or DER file formats to the list of CAs trusted on the system, copy the certificate file to the `/usr/share/pki/ca-trust-source/anchors/` or `/etc/pki/ca-trust/source/anchors/` directory and use the `update-ca-trust` command to update the system-wide trust store configuration.

4.6 Disable SSH

SSH server and client packages are installed by default in Archon OS v3.x.x.x due to dependencies from other packages. SSH functionality is excluded from the Archon OS CC evaluation. Therefore, the following commands should be executed by administrators during initial installation in order to disable the SSH server and client functionality. Once executed, the effect persists across reboots.

- `sudo systemctl disable --now sshd`
- `sudo rm /usr/bin/ssh`

5 System Configuration

5.1 Configuring Audit

5.1.1 Local Audit Storage Settings

The administrator configures the local audit storage by editing `/etc/audit/auditd.conf`. The amount of local audit storage is determined by a combination of the `num_logs` and `max_log_file` settings:

`num_logs = <0-999>`

Indicates the number of log files to rotate. When set to 0 or 1, a single log file is saved

`max_log_file = <number>`

This keyword specifies the maximum file size in megabytes. When this limit is reached, it will trigger a configurable action. The value given must be numeric.

`max_log_file_action = <value>`

This parameter tells the system what action to take when the system has detected that the max file size limit has been reached. Valid values are `ignore`, `syslog`, `suspend`, `rotate`, and `keep_logs`. If set to

- `ignore` - the audit daemon does nothing.
- `syslog` means that it will issue a warning to syslog.
- `suspend` will cause the audit daemon to stop writing records to the disk. The daemon will still be alive.
- `rotate` will cause the audit daemon to rotate the logs. It should be noted that logs with higher numbers are older than logs with lower numbers. This is the same convention used by the `logrotate` utility.
- `keep_logs` option is similar to rotate except it does not use the `num_logs` setting. This prevents audit logs from being overwritten.

The amount of local storage used for audit logs is `num_logs` multiplied by `max_log_file` unless `keep_logs` is specified. All free space on the partition storing logs may be used when `keep_logs` is specified.

5.1.2 Starting and Controlling auditd

`auditd` is the userspace component to Archon OS. It's responsible for writing audit records to the disk. Viewing the logs is done with the `ausearch` or `aureport` utilities. Configuring the audit rules is done with the `auditctl` utility. During startup, the rules in `/etc/audit/audit.rules` are read by `auditctl`. The audit daemon itself has some configuration options that the admin may wish to customize. They are found in the `auditd.conf` file.

1. Configure `auditd` to start at boot time:

```
# systemctl enable auditd
```

The audit logs are sent to the external syslog server via TLS in real-time.

The above command is required to configure the system in the evaluated configuration.

The following commands are also available.

To temporarily disable `auditd` enter the following command.

- `auditctl -e 0`

To re-enable auditd.

- `auditctl -e 1`

To stop `auditd`.

- `auditd stop`

To restart `auditd`.

- `auditd restart`

To display the running status of `auditd`.

- `auditd status`

5.2 Non-Volatile Drives and Keys

All instances of keys in non-volatile storage might not be deleted if the physical drive has replaced a sector containing a key with a spare sector. To minimize this risk, the physical drive should be end-of-life before a significant amount of damage to the drive's health can occur.

5.3 Address CVEs

The following parameters must be set in order to prevent known CVEs.

5.3.1 Disable Kernel Same-page Merging (KSM) (CVE-2024-0564)

- `sudo systemctl disable ksm`
- `sudo systemctl disable ksmtuned`

5.3.2 CVE-2019-19039

Setting the kernel parameter to restrict non privileged users with the command:

- `sudo sysctl -w kernel.dmesg_restrict=1`

And to make persistent between system reboots.

- `echo 'kernel.dmesg_restrict=1' | sudo tee -a /etc/sysctl.conf`

5.3.3 Disabled Unprivileged User Access to Extended Berkely Packet Filter (multiple CVEs)

The default Red Hat Enterprise Linux kernel prevents unprivileged users from being able to use eBPF (Extended Berkely Packet Filter) by the `kernel.unprivileged_bpf_disabled sysctl` command.

For the Archon OS to confirm the current state, inspect the `sysctl` with the command:

- `cat /proc/sys/kernel/unprivileged_bpf_disabled`

The setting of 1 would mean that unprivileged users cannot use eBPF, mitigating the flaw.

- `sudo sysctl kernel.unprivileged_bpf_disabled=1`

5.3.4 Ensure inline_data is Disabled (CVE-2021-40490)

For the Red Hat Enterprise Linux 8 to confirm the current state, inspect the `sysctl` with the command:

- `cat /proc/sys/kernel/inline_data`

The setting of 0 would mean that `inline_data` is disabled, mitigating the flaw.

- `sudo sysctl kernel.inline_data=0`

5.3.5 Blacklist LDAP (CVE-2023-2953)

Append the following line to `/etc/modprobe.d/blacklist.conf` (create that file if it doesn't exist):

```
Install openldap /bin/true
```

Note, the "blacklist" command does not prevent modules from being loaded manually or to satisfy preconditions of other modules. Using the "install modulename /bin/true" always results in the module not being loaded no matter what method is attempted for loading.

5.3.6 PKCS12 (CVE-2024-0727)

Administrators and Users should refrain from using any PKCS12 files from untrusted sources. Using a maliciously formatted PKCS12 file may result in OpenSSL crashing. No PKCS12 files should be required for normal operations.

6 ADMINISTRATION

6.1 USER/ADMINISTRATOR ACCOUNTS

The TOE only supports local logins using username and password at the local console. It does not support remote administration.

6.1.1 CREATING/DELETING USER ACCOUNTS

The administrator can create user accounts using the `useradd [options] <username>` command. The user account will be locked and password-less.

Once a user account has been created, the administrator can make this account an administrator by adding it to the wheel group by running `usermod -aG wheel <username>`.

The most basic tasks to manage user accounts and groups, and the appropriate command-line tools, include:

Displaying user and group IDs:

```
id
```

Creating a new user account:

```
useradd [options] user_name
```

Assigning a new password to a user account belonging to *username*:

```
passwd user_name
```

Adding a user to a group:

```
usermod -a -G group_name user_name
```

Deleting a user:

```
userdel -a -G group_name user_name
```

Once an account is created and added to the wheel group, it can be used to administer the TOE from the local console.

6.1.2 MANAGING GROUPS

6.1.2.1 ADD A GROUP

To add a group in Linux, use the `groupadd` command:

When a group is created, a unique group ID gets assigned to that group. You can verify that the group appears (and see its group ID) by looking in the `/etc/group` file.

If you want to create a group with a specific group ID (GID), use the --gid or -g option:

- `groupadd <group name>`

Usage: `groupadd [options] GROUP`

Options:

`-f, --force` Exit successfully if the group already exists, and cancel -g if

	the GID already used.
`-g, --gid GID`	Use GID for the new group.
`-h, --help`	Display this help message and exit.
`-K, --key KEY=VALUE`	Override /etc/login.defs defaults.
`-o, --non-unique`	Allow to create groups with duplicate (non-unique) GID.
`-p, --password PASSWORD`	Use this encrypted password for the new group.
`-r, --system`	Create a system account.
`-R, --root CHROOT_DIR`	Directory to chroot into.
`-P, --prefix PREFIX_DIR`	Directory prefix.

6.1.2.2 Delete a Group

When a group is no longer needed, you delete it by using the `groupdel` command:

- `groupdel <groupname>`

Usage: `groupdel [options] GROUP`

Options:

`-h, --help`	Display this help message and exit.
`-R, --root CHROOT_DIR`	Directory to chroot into.
`-P, --prefix PREFIX_DIR`	Prefix directory where are located the /etc/* files.
`-f, --force`	Delete group even if it is the primary group of a user.

6.1.2.3 Modify a Group

The `groupmems` command allows a user to administer their own group membership list without the requirement of superuser privileges. The `groupmems` utility is for systems that configure its users to be in their own name sake primary group (i.e., guest / guest).

Only the superuser, as administrator, can use `groupmems` to alter the memberships of other groups.

Usage: `groupmems [options] [action]`
`groupmems -a <username> -g <groupname>`

Options:

`-g, --group groupname`	Change groupname instead of the user's group (root only).
`-R, --root CHROOT_DIR`	Directory to chroot into.

Actions:

`-a, --add username`	Add username to the members of the group.
`-d, --delete username`	Remove username from the members of the group.
`-h, --help`	Display this help message and exit.
`-p, --purge`	Purge all members from the group.
`-l, --list`	List the members of the group.

6.1.2.4 Group Credential Change

Usage: `gpasswd [option] GROUP`

`gpasswd <groupname>`

Options:

`-a, --add USER`	Add USER to GROUP.
`-d, --delete USER`	Remove USER from GROUP.
`-h, --help`	Display this help message and exit.
`-Q, --root CHROOT_DIR`	Directory to chroot into.
`-r, --delete-password`	Remove the GROUP's password.
`-R, --restrict`	Restrict access to GROUP to its members.
`-M, --members USER,...`	Set the list of members of GROUP.
`-A, --administrators ADMIN,...`	Set the list of administrators for GROUP.

Except for the -A and -M_options, the options cannot be combined.

6.1.3 CONFIGURE PASSWORD POLICY

The administrator can change the password quality by changing the contents of `pwquality.conf` file. This file provides a way to configure the default password quality requirements for the system passwords. This file is read by the `libpwquality` library and utilities that use this library for checking and generating passwords. The password policy is enforced by the `pam_pwquality` PAM module. The possible options in the file are:

`minlen`

Minimum acceptable size for the new password (plus one if credits are not disabled which is the default) Cannot be set to lower value than 6.

Default = `9`

`dcredit`

The maximum credit for having digits in the new password. If less than 0 it is the minimum number of digits in the new password.

Default = `1`

`ucredit`

The maximum credit for having uppercase characters in the new password. If less than 0 it is the minimum number of uppercase characters in the new password.

Default = `1`

`lcredit`

The maximum credit for having lowercase characters in the new password. If less than 0 it is the minimum number of lowercase characters in the new password.

Default = `1`

`ocredit=1`

The maximum credit for having other characters in the new password. If less than 0 it is the minimum number of other characters in the new password.

Default = `1`

Commenting/removing `enforce_for_root` from `/etc/security/pwquality.conf` will allow root user to bypass password policies set on the TOE.

6.1.4 Change Passwords

A user can change their password using the `passwd` command. The user will be prompted to enter their current password as well as their new password.

6.1.5 Failed Authentication Timeout

The administrator can configure the timeout between failed authentication attempts by editing the `/etc/security/faillock.conf` file. `faillock.conf` provides a way to configure the default settings for locking the user after multiple failed authentication attempts. This file is read by the `pam_faillock` module and is the preferred method over configuring `pam_faillock` directly.

`deny=n`

Deny access if the number of consecutive authentication failures for this user during the recent interval exceeds n.

Default = `3`.

The evaluated configuration requires this parameter to be between 1 and 65,535 (all accounts will be locked).

`fail_interval=n`

The length of the interval during which the consecutive authentication failures must happen for the user account lock out is n seconds.

Default = `900` (15 minutes).

The evaluated configuration requires this parameter to be greater than 0 (all accounts will be locked).

`unlock_time=n`

The access will be re-enabled after `n` seconds after the lock out. The value `0` has the same meaning as value never - the access will not be re-enabled without resetting the `faillock` entries by the `faillock` command.

Default = `600` (10 minutes).

The evaluated configuration requires this parameter to be greater than 0 (all accounts will be locked for a period of time).

`even_deny_root`

The `root` account can become locked as well as regular accounts.

It is recommended that you do NOT enable this parameter in order to always allow access to your system.

`root_unlock_time=n`

This option implies `even_deny_root` option. Allow access after `n` seconds to root account after the account is locked. In case the option is not specified the value is the same as of the `unlock_time option`.

It is recommended that you do NOT enable this parameter in order to always allow access to your system.

`no_log_info`

Don't log informative messages via syslog(3).

The evaluated configuration requires this parameter to NOT be included in the file (all failed login attempts will be logged).

6.1.6 Enable/Disable Session Timeout

6.1.6.1 Enable Session Timeout

1. Create a database for machine-wide setting in `/etc/dconf/db/local.d/00-autologout`.

```
[org/gnome/settings-daemon/plugins/power]
# Set the timeout to 900 seconds when on mains power
sleep-inactive-ac-timeout=900
# Set the timeout to 900 seconds when on mains power
sleep-inactive-ac-types=logout
```

2. Save and close the file.
3. Make the file executable using command:
   - `chmod +x /etc/dconf/db/local.d/00-autologout`
4. Logout or reboot your system for the changes to take effect. The inactive user will automatically be logged out after 900 seconds of idle time.

The normal user can't change this setting.

6.1.6.2 Disable Session Timeout

To disable session timeout, follow steps 1 through 3 above but configure `sleep-inactive-ac-timeout` to `0`. The inactive user will never be automatically logged out.

The normal user can't change this setting.

6.1.7 Inactivity Timeout

Refer to the section above, Enable/Disable Session Timeout.

6.1.8 Warning Banner

The evaluated configuration requires Archon OS to display an advisory notice and consent warning message regarding use of the TOE before any logon attempt. The changes can only be performed by a system administrator and affects all users.

To change the banner message displayed on the login screen:

1. create a gdm (GNOME Display Manager) database for machine-wide settings in `/etc/dconf/db/gdm.d/01-banner-message` and add the following contents:

```
[org/gnome/login-screen]
banner-message-enable=true
banner-message-text='Type the banner message here'
```

6.2 File and Object Management

The TOE supports standard UNIX permission bits to provide one form of DAC. There are three sets of three bits that define access for three categories of users: the owning user, users in the owning group, and other users. The three bits in each set indicate the access permissions granted to each user category: one bit for read (`r`), one for write (`w`) and one for execute (`x`) (`rwxrwxrwx`). Note that “write access” to file systems mounted as read only (e. g. CD-ROM) is always rejected (the exceptions are character and block device files which can still be written to as write operations do not modify the information on the storage media). The SAVETXT attribute is used for world-writable temp directories preventing the removal of files by users other than the owner.

Each process has an inheritable “umask” attribute which is used to determine the default access permissions for new objects. It is a bit mask of the user/group/other read/write/execute bits and specifies the access bits to be removed from new objects. For example, setting the umask to “002” ensures that new objects will be writable by the owner and group, but not by others. The umask is defined by the administrator in the /etc/login.defs file or the value is “022” by default if not specified.

Archon OS also provides support for POSIX type ACLs to define a fine-grained access control on a per-file or per-directory basis. An ACL entry contains the following information:

- A tag type that specifies the type of the ACL entry
- A qualifier that specifies an instance of an ACL entry type
- A permission set that specifies the discretionary access rights for processes identified by the tag type and qualifier.

An ACL contains exactly one entry of three different tag types (called the "required ACL entries” forming the "minimum ACL"). The standard UNIX file permission bits as described above are represented by the entries in the minimum ACL.

A default ACL is an additional ACL which may be associated with a directory. This default ACL has no effect on the access to this directory. Instead, the default ACL is used to initialize the ACL for any file that is created in this directory. If the new file created is a directory it inherits the default ACL from its parent directory. When an object is created within a directory and the ACL is not defined with the function creating the object, the new object inherits the default ACL of its parent directory as its initial ACL.

In addition, the following additional access control bits are processed by the kernel:

- SUID bit: When an executable marked with the SUID bit is executed, the effective UID of the process is changed to the UID of the owner of the file. The SUID bit for file system objects other than files is ignored.

- SGID bit: When an executable marked with the SGID bit is executed, the effective GID of the process is changed to the owning GID of the file. The SGID bit for file system objects other than files is ignored.
- SAVETXT: When a directory is marked with the SAVETXT bit, only the owner of a file system object in that directory can remove it. This bit is commonly used for world-writable directories like /tmp. Only processes with the CAP_FOWNER capability are able to remove the file system object if their UID is different from the owning UID of the file system object.

The TOE uses these permissions to protect the following files from unauthorized modification:

a. Kernel, drivers, and kernel modules – files in:
   - `/boot/`
   - `/usr/lib/modules/`
   - `/usr/lib/firmware/`

b. Security audit logs – files in:
   - `/var/log/audit/`
   - `/var/log/`

c. Shared libraries – files in:
   - `/usr/lib64/`
   - `/usr/lib/`

d. System executables – files in:
   - `/usr/sbin/`
   - `/usr/bin/`
   - `/usr/libexec/`

e. System configuration files – files in:
   - `/etc/`
   - `/usr/lib/`

Both shared libraries and configuration files are stored in `/usr/lib/`; however, all files in `/usr/lib/` are protected from unauthorized modification, regardless of type.

6.3 Storage of Sensitive Data

6.3.1 Called By Applications

Archon OS follows standard conventions for storing sensitive data. Applications must store their sensitive data in the `/etc` directory with restrictive access permissions. Access to sensitive data should be restricted to `root` and/or the application storing the sensitive data. Sensitive data is keys and passwords.

6.3.2 Called by CLI

Archon OS also provides the ability to encrypt/decrypt sensitive files using OpenSSL. The command to use is the following:

- ```
  openssl enc [-d] -aes-256-cbc -in <file> -out <file> \
  -pass file:<file_with_password> -pbkdf2
  ```

The -d option is used for decryption instead of encryption.
  ```

7 Audit Event Reference

7.1 Audit Record Description

The local audit logs are found in `/var/log/audit/audit.log`. The `ausearch` utility is intended to be the way to see the events. The Audit event format is as follows:

node=ospp type=<type> msg=audit(<timestamp>: <serial_number>): pid=<pid> uid=<uid> auid=<auid> ses=<session> <message> <source> res=<res>

a) <host> Hostname of the system

b) <type> SERVICE_START, SERVICE_STOP, USER_AUTH, SYSCALL, ADD_USER, DEL_USER, USER_CMD, PROCTITLE, CWD, SYSTEM_BOOT, SYSTEM_SHUTDOWN, PATH, FANOTIFY, or CHAUTHTOK.

c) <timestamp> Epoch time (seconds since January 1, 1970 12:00:00 AM) to the millisecond

d) <serial_number> unique numerical event identifier appended to the timestamp. Repeats across multiple records that are related to the same event

e) <uid> user ID of the process at the time the audit event was generated

f) <auid> user ID of the user authenticated by the system (regardless if the user has changed his real and / or effective user ID afterwards)

g) <pid> Process ID of the subject that caused the event

h) <session> session ID - used to disambiguating actions when a single user has multiple active sessions

i) <message> Information about the intended operation

j) <source> hostname=<host>, addr=<IP_address>, and/or terminal=<terminal> - identifies how the subject is connected to RHEL

k) <res> success or failure - indicates whether the action succeeded or failed **Note:** Events of type 'SYSCALL' do not contain a 'res' field and instead use the 'success=<no/yes>' syntax to represent the status of the event.

7.2 Audit Record Examples

The TOE generates audit logs for the following events (note: some information has been edited, such as IP addresses and DNS names).

1. Audit record for: Start-up and shut-down of the audit functions.

   - Start-up

     ```
     node=Latitude_5410 type=SERVICE_START msg=audit(04/19/2024
     11:21:57.327:175277): pid= 1 uid=root auid-unset ses=unset
     subj=system_u:system_r:init_t:s0 msg='unit=auditd comm =systemd
     exe=/usr/lib/systemd/systemd hostname=? addr=? terminal=?
     res=success
     ```

   - Shutdown

```
node=Latitude_5410 type=SERVICE_STOP msg=audit(04/08/2024
11:21:57.327:175278): pid=1 uid=root auid=unset ses=unset
subj=system_u:system_r:init_t:s0 msg='unit=auditd comm= systemd
exe=/usr/lib/systemd/systemd hostname=? addr=? terminal=?
res=success'
```

2. Audit record for: Authentication events (Success/Failure)

   - Success

     ```
     node=Latitude_5410 type=USER_AUTH msg=audit(03/27/2024
     11:38:49.639:1953966) : pid=375347 uid=gpos auid=gpos ses=4
     subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
     msg='op=PAM:authentication grantors=pam_faillock,pam_unix
     acct=test_1 exe=/usr/bin/su hostname=Latitude_5410 addr=?
     terminal=pts/62 res=success'
     ```

   - Failure

     ```
     node=Latitude_5410 type=USER_AUTH msg=audit(03/27/2024
     11:31:32.857:1953571) : pid=375268 uid=gpos auid=gpos ses=4
     subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
     msg='op=PAM:authentication grantors=? acct=test_1 exe=/usr/bin/su
     hostname=Latitude_5410 addr=? terminal=pts/62 res=failed'
     ```

3. Audit record for: Use of privileged/special rights events (Successful and unsuccessful security, authentication events (Success/Failure))

   - Security Changes

     - Success

       ```
       node=Latitude_5410 type=PROCTITLE msg=audit(03/27/2024
       11:49:49.482:1958609) : proctitle=sudo vi
       /etc/selinux/semanage.conf
       node=Latitude_5410 type=PATH msg=audit(03/27/2024
       11:49:49.482:1958609) : item=1
       name=/etc/selinux/.semanage.conf.swp inode=402760084 dev=fd:00
       mode=file,644 ouid=root ogid=root rdev=00:00
       obj=unconfined_u:object_r:selinux_config_t:s0 nametype=DELETE
       cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
       node=Latitude_5410 type=PATH msg=audit(03/27/2024
       11:49:49.482:1958609) : item=0 name=/etc/selinux/ inode=402722769
       dev=fd:00 mode=dir,755 ouid=root ogid=root rdev=00:00
       obj=system_u:object_r:selinux_config_t:s0 nametype=PARENT
       cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
       node=Latitude_5410 type=CWD msg=audit(03/27/2024
       11:49:49.482:1958609) : cwd=/var/home/gpos
       node=Latitude_5410 type=SYSCALL msg=audit(03/27/2024
       11:49:49.482:1958609) : arch=x86_64 syscall=unlink success=yes
       exit=0 a0=0x55efc1e020b0 a1=0x1 a2=0x17 a3=0x7ffc6213e3a7 items=2
       ppid=375509 pid=375511 auid=gpos uid=root gid=root euid=root
       suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts62
       ses=4 comm=vi exe=/usr/bin/vi
       subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
       key=MAC-policy
       ```

     - Failure

```
node=Latitude_5410 type=PROCTITLE msg=audit(03/27/2024
11:47:38.351:1957912) : proctitle=vi /etc/selinux/semanage.conf
node=Latitude_5410 type=PATH msg=audit(03/27/2024
11:47:38.351:1957912) : item=0 name=/etc/selinux/ inode=402722769
dev=fd:00 mode=dir,755 ouid=root ogid=root rdev=00:00
obj=system_u:object_r:selinux_config_t:s0 nametype=PARENT
cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
node=Latitude_5410 type=CWD msg=audit(03/27/2024
11:47:38.351:1957912) : cwd=/var/home/gpos
node=Latitude_5410 type=SYSCALL msg=audit(03/27/2024
11:47:38.351:1957912) : arch=x86_64 syscall=openat success=no
exit=EACCES(Permission denied) a0=AT_FDCWD a1=0x55c5ca566090
a2=O_RDWR|O_CREAT|O_EXCL|O_NOFOLLOW a3=0x180 items=1 ppid=375221
pid=375464 auid=gpos uid=gpos gid=gpos euid=gpos suid=gpos
fsuid=gpos egid=gpos sgid=gpos fsgid=gpos tty=pts62 ses=4 comm=vi
exe=/usr/bin/vi subj=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023 key=MAC-policy
```

- Audit Changes
  - Success

```
node=Latitude_5410 type=PROCTITLE msg=audit(03/27/2024
11:49:49.482:1958609) : proctitle=sudo vi /etc/audit/auditd.conf
node=Latitude_5410 type=PATH msg=audit(03/27/2024
11:49:49.482:1958609) : item=1
name=/etc/selinux/.semanage.conf.swp inode=402760084 dev=fd:00
mode=file,644 ouid=root ogid=root rdev=00:00
obj=unconfined_u:object_r:selinux_config_t:s0 nametype=DELETE
cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
node=Latitude_5410 type=PATH msg=audit(03/27/2024
11:49:49.482:1958609) : item=0 name=/etc/selinux/ inode=402722769
dev=fd:00 mode=dir,755 ouid=root ogid=root rdev=00:00
obj=system_u:object_r:selinux_config_t:s0 nametype=PARENT
cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
node=Latitude_5410 type=CWD msg=audit(03/27/2024
11:49:49.482:1958609) : cwd=/var/home/gpos
node=Latitude_5410 type=SYSCALL msg=audit(03/27/2024
11:49:49.482:1958609) : arch=x86_64 syscall=unlink success=yes
exit=0 a0=0x55efc1e020b0 a1=0x1 a2=0x17 a3=0x7ffc6213e3a7 items=2
ppid=375509 pid=375511 auid=gpos uid=root gid=root euid=root
suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts62
ses=4 comm=vi exe=/usr/bin/vi
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=MAC-policy
```

  - Failure

```
node=Latitude_5410 type=PROCTITLE msg=audit(04/08/2024
15:47:31.385:225311) : proctitle=vi /ect/audit/auditd.conf
node=Latitude_5410 type=PATH msg=audit(04/08/2024
15:47:31.385:225311) : item=0 name=/var/log/audit/audit.log
nametype=UNKNOWN cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
cap_frootid=0
node=Latitude_5410 type=CWD msg=audit(04/08/2024
15:47:31.385:225311) : cwd=/var/home/gpos
```

```
node=Latitude_5410 type=SYSCALL msg=audit(04/08/2024
15:47:31.385:225311) : arch=x86_64 syscall=openat success=no
exit=EACCES(Permission denied) a0=AT_FDCWD a1=0x7ffd79152a3c
a2=O_RDONLY a3=0x0 items=1 ppid=45828 pid=48340 auid=gpos
uid=gpos gid=gpos euid=gpos suid=gpos fsuid=gpos egid=gpos
sgid=gpos fsgid=gpos tty=pts8 ses=2 comm=cat exe=/usr/bin/cat
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=unsuccessful-access
```

- Configuration Changes
  - Success

```
node=Latitude_5410 type=PROCTITLE msg=audit(03/27/2024
11:49:49.482:1958609) : proctitle=vi /etc/rsyslog.conf
node=Latitude_5410 type=PATH msg=audit(03/27/2024
11:49:49.482:1958609) : item=1
name=/etc/selinux/.semanage.conf.swp inode=402760084 dev=fd:00
mode=file,644 ouid=root ogid=root rdev=00:00
obj=unconfined_u:object_r:selinux_config_t:s0 nametype=DELETE
cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
node=Latitude_5410 type=PATH msg=audit(03/27/2024
11:49:49.482:1958609) : item=0 name=/etc/selinux/ inode=402722769
dev=fd:00 mode=dir,755 ouid=root ogid=root rdev=00:00
obj=system_u:object_r:selinux_config_t:s0 nametype=PARENT
cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
node=Latitude_5410 type=CWD msg=audit(03/27/2024
11:49:49.482:1958609) : cwd=/var/home/gpos
node=Latitude_5410 type=SYSCALL msg=audit(03/27/2024
11:49:49.482:1958609) : arch=x86_64 syscall=unlink success=yes
exit=0 a0=0x55efc1e020b0 a1=0x1 a2=0x17 a3=0x7ffc6213e3a7 items=2
ppid=375509 pid=375511 auid=gpos uid=root gid=root euid=root
suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts62
ses=4 comm=vi exe=/usr/bin/vi
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=successful-create
```

  - Failure

```
node=Latitude_5410 type=PROCTITLE msg=audit(03/27/2024
11:47:38.351:1957912) : proctitle=vi /etc/rsyslog.conf
node=Latitude_5410 type=PATH msg=audit(03/27/2024
11:47:38.351:1957912) : item=0 name=/etc/selinux/ inode=402722769
dev=fd:00 mode=dir,755 ouid=root ogid=root rdev=00:00
obj=system_u:object_r:selinux_config_t:s0 nametype=PARENT
cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
node=Latitude_5410 type=CWD msg=audit(03/27/2024
11:47:38.351:1957912) : cwd=/var/home/gpos
node=Latitude_5410 type=SYSCALL msg=audit(03/27/2024
11:47:38.351:1957912) : arch=x86_64 syscall=openat success=no
exit=EACCES(Permission denied) a0=AT_FDCWD a1=0x55c5ca566090
a2=O_RDWR|O_CREAT|O_EXCL|O_NOFOLLOW a3=0x180 items=1 ppid=375221
pid=375464 auid=gpos uid=gpos gid=gpos euid=gpos suid=gpos
fsuid=gpos egid=gpos sgid=gpos fsgid=gpos tty=pts62 ses=4 comm=vi
exe=/usr/bin/vi subj=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023 key=successful-create
```

4. Audit record for: Privilege or role escalation events (Success/Failure).
   - Success

     ```
     node=Latitude_5410 type=USER_CMD msg=audit(04/08/2024
     13:09:02.456:213861) : pid=46247
     uid=gpos auid=gpos ses=2
     subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 m
     sg='cwd=/var/home/gpos cmd=usermod -L user exe=/usr/bin/sudo
     terminal=pts/8 res=success
     ```

   - Failure

     ```
     node=Latitude_5410 type=USER_CMD msg=audit(04/08/2024
     13:08:40.664:213416) : pid=46213
     uid=gpos auid=gpos ses=2
     subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0. c1023 m
     sg='cwd=/var/home/gpos cmd=usermode -L user exe=/usr/bin/sudo
     terminal=pts/8 res=failed
     ```

5. Audit record for: File and object events (Successful and unsuccessful attempts to create, access, delete, modify, modify permissions).

   - Create

     - Success

       ```
       node=Latitude_5410 type=PROCTITLE msg=audit(03/27/2024
       12:15:11.790:1960645) : proctitle=touch newfile.txt
       node=Latitude_5410 type=PATH msg=audit(03/27/2024
       12:15:11.790:1960645) : item=1 name=newfile.txt inode=2960
       dev=fd:06 mode=file,640 ouid=gpos ogid=gpos rdev=00:00
       obj=unconfined_u:object_r:user_home_t:s0 nametype=CREATE
       cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
       node=Latitude_5410 type=PATH msg=audit(03/27/2024
       12:15:11.790:1960645) : item=0 name=/var/home/gpos inode=131
       dev=fd:06 mode=dir,755 ouid=gpos ogid=gpos rdev=00:00
       obj=unconfined_u:object_r:user_home_dir_t:s0 nametype=PARENT
       cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
       node=Latitude_5410 type=CWD msg=audit(03/27/2024
       12:15:11.790:1960645) : cwd=/var/home/gpos
       node=Latitude_5410 type=SYSCALL msg=audit(03/27/2024
       12:15:11.790:1960645) : arch=x86_64 syscall=openat success=yes
       exit=3 a0=AT_FDCWD a1=0x7ffdf9929a2d
       a2=O_WRONLY|O_CREAT|O_NOCTTY|O_NONBLOCK a3=0x1b6 items=2
       ppid=375221 pid=375872 auid=gpos uid=gpos gid=gpos euid=gpos
       suid=gpos fsuid=gpos egid=gpos sgid=gpos fsgid=gpos tty=pts62
       ses=4 comm=touch exe=/usr/bin/touch
       subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
       key=successful-create
       ```

     - Failure

       ```
       node=Latitude_5410 type=PROCTITLE msg=audit(03/27/2024
       12:21:07.645:1960995) : proctitle=touch /root/newfile.txt
       node=Latitude_5410 type=PATH msg=audit(03/27/2024
       12:21:07.645:1960995) : item=0 name=/root/newfile.txt
       nametype=UNKNOWN cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
       cap_frootid=0
       ```

```
node=Latitude_5410 type=CWD msg=audit(03/27/2024
12:21:07.645:1960995) : cwd=/var/home/gpos
node=Latitude_5410 type=SYSCALL msg=audit(03/27/2024
12:21:07.645:1960995) : arch=x86_64 syscall=openat success=no
exit=EACCES(Permission denied) a0=AT_FDCWD a1=0x7ffe2adcea27
a2=O_WRONLY|O_CREAT|O_NOCTTY|O_NONBLOCK a3=0x1b6 items=1
ppid=375221 pid=375940 auid=gpos uid=gpos gid=gpos euid=gpos
suid=gpos fsuid=gpos egid=gpos sgid=gpos fsgid=gpos tty=pts62
ses=4 comm=touch exe=/usr/bin/touch
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=unsuccessful-create
```

- Access
  - Success

```
node=Latitude_5410 type=PROCTITLE msg=audit(03/27/2024
13:57:49.427:1965749) : proctitle=cat newfile.txt
node=Latitude_5410 type=PATH msg=audit(03/27/2024
13:57:49.427:1965749) : item=0 name=/usr/lib/locale/en_
US.utf8/LC_MONETARY inode=272173259 dev=fd:00 mode=file,644
ouid=root ogid=root rdev=00:00 obj=system_u:o
bject_r:locale_t:s0 nametype=NORMAL cap_fp=none cap_fi=none
cap_fe=0 cap_fver=0 cap_frootid=0
node=Latitude_5410 type=CWD msg=audit(03/27/2024
13:57:49.427:1965749) : cwd=/var/home/gpos
node=Latitude_5410 type=SYSCALL msg=audit(03/27/2024
13:57:49.427:1965749) : arch=x86_64 syscall=openat s
uccess=yes exit=3 a0=AT_FDCWD a1=0x56501663d750
a2=O_RDONLY|O_CLOEXEC a3=0x0 items=1 ppid=375221 pid=377037
auid=gpos uid=gpos gid=gpos euid=gpos suid=gpos fsuid=gpos
egid=gpos sgid=gpos fsgid=gpos tty=pts62 s$s=4 comm=cat
exe=/usr/bin/cat subj=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023 key=successful-access
```

  - Failure

```
node=Latitude_5410 type=PROCTITLE msg=audit(03/27/2024
12:23:55.933:1961262) : proctitle=cat /root/newfile.txt
node=Latitude_5410 type=PATH msg=audit(03/27/2024
12:23:55.933:1961262) : item=0 name=/root/newfile.txt
nametype=UNKNOWN cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
cap_frootid=0
node=Latitude_5410 type=CWD msg=audit(03/27/2024
12:23:55.933:1961262) : cwd=/var/home/gpos
node=Latitude_5410 type=SYSCALL msg=audit(03/27/2024
12:23:55.933:1961262) : arch=x86_64 syscall=openat success=no
exit=EACCES(Permission denied) a0=AT_FDCWD a1=0x7ffeafab3a2b
a2=O_RDONLY a3=0x0 items=1 ppid=375221 pid=375983 auid=gpos
uid=gpos gid=gpos euid=gpos suid=gpos fsuid=gpos egid=gpos
sgid=gpos fsgid=gpos tty=pts62 ses=4 comm=cat exe=/usr/bin/cat
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=unsuccessful-access
```

- Delete
  - Success

```
node=Latitude_5410 type=PROCTITLE msg=audit(03/27/2024
14:05:49.825:1966335) : proctitle=rm newfile.txt
node=Latitude_5410 type=PATH msg=audit(03/27/2024
14:05:49.825:1966335) : item=1 name=newfile.txt inode=2962
dev=fd:06 mode=file,640 ouid=gpos ogid=gpos rdev=00:00
obj=unconfined_u:object_r:user_home_t:s0 nametype=DELETE
cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
node=Latitude_5410 type=PATH msg=audit(03/27/2024
14:05:49.825:1966335) : item=0 name=/var/home/gpos inode=131
dev=fd:06 mode=dir,755 ouid=gpos ogid=gpos rdev=00:00
obj=unconfined_u:object_r:user_home_dir_t:s0 nametype=PARENT
cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
node=Latitude_5410 type=CWD msg=audit(03/27/2024
14:05:49.825:1966335) : cwd=/var/home/gpos
node=Latitude_5410 type=SYSCALL msg=audit(03/27/2024
14:05:49.825:1966335) : arch=x86_64 syscall=unlinkat success=yes
exit=0 a0=AT_FDCWD a1=0x55e1b7b71640 a2=0x0 a3=0x100 items=2
ppid=375221 pid=377352 auid=gpos uid=gpos gid=gpos euid=gpos
suid=gpos fsuid=gpos egid=gpos sgid=gpos fsgid=gpos tty=pts62
ses=4 comm=rm exe=/usr/bin/rm
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=successful-delete
```

- Failure

```
node=Latitude_5410 type=PROCTITLE msg=audit(03/28/2024
07:33:46.437:1997254) : proctitle=rm -f /root/newfile.txt
node=Latitude_5410 type=PATH msg=audit(03/28/2024
07:33:46.437:1997254) : item=0 name=/root/newfile.txt
nametype=UNKNOWN cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
cap_frootid=0
node=Latitude_5410 type=CWD msg=audit(03/28/2024
07:33:46.437:1997254) : cwd=/var/home/gpos
node=Latitude_5410 type=SYSCALL msg=audit(03/28/2024
07:33:46.437:1997254) : arch=x86_64 syscall=unlinkat success=no
exit=EACCES(Permission denied) a0=AT_FDCWD a1=0x55d746d4f640
a2=0x0 a3=0x0 items=1 ppid=375221 pid=387284 auid=gpos uid=gpos
gid=gpos euid=gpos suid=gpos fsuid=gpos egid=gpos sgid=gpos
fsgid=gpos tty=pts62 ses=4 comm=rm exe=/usr/bin/rm
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=unsuccessful-delete
```

- Modification
  - Success

```
node=Latitude_5410 type=PROCTITLE msg=audit(03/28/2024
07:40:03.020:1997710) : proctitle=vi newfile.txt
node=Latitude_5410 type=SYSCALL msg=audit(03/28/2024
07:40:03.020:1997710) : arch=x86_64 syscall=ftruncate success=yes
exit=0 a0=0x3 al=0x0 a2=0x41 a3=0x1a0 items=0 ppid=
375221 pid=387365 auid=gpos uid=gpos gid=gpos euid=gpos suid=gpos
fsuid=gpos egid=gpos sgid=gpos fsgid=gpos tty=pts62 ses=4 comm=vi
exe=/usr/bin/vi subj=unconfined_u:unconfined r:unconfined t:s0-
s0:c0.c1023 key=successfulul-modification
```

  - Failure

```
node=Latitude_5410 type=PROCTITLE msg=audit(04/08/2024
15:47:31.385:225311) : proctitle=cat /var/log/audit/audit.log
node=Latitude_5410 type=PATH msg=audit(04/08/2024
15:47:31.385:225311) : item=0 name=/var/log/audit/audit.log
nametype=UNKNOWN cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
cap_frootid=0
node=Latitude_5410 type=CWD msg=audit(04/08/2024
15:47:31.385:225311) : cwd=/var/home/gpos
node=Latitude_5410 type=SYSCALL msg=audit(04/08/2024
15:47:31.385:225311) : arch=x86_64 syscall=openat success=no
exit=EACCES(Permission denied) a0=AT_FDCWD a1=0x7ffd79152a3c
a2=O_RDONLY a3=0x0 items=1 ppid=45828 pid=48340 auid=gpos
uid=gpos gid=gpos euid=gpos suid=gpos fsuid=gpos egid=gpos
sgid=gpos fsgid=gpos tty=pts8 ses=2 comm=cat exe=/usr/bin/cat
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=unsuccessful-access
```

- Permission Change
  - Success

    ```
    node=Latitude_5410 type=PROCTITLE msg=audit(03/28/2024
    07:50:24.798:1998612) : proctitle=chmod 777 newfile.txt
    node=Latitude_5410 type=PATH msg=audit(03/28/2024
    07:50:24.798:1998612) : item=0 name=newfile.txt inode=2963
    dev=fd:06 mode=file,640 ouid=gpos ogid=gpos rdev=00:00
    obj=unconfined_u:object_r:user_home_t:s0 nametype=NORMAL
    cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
    node=Latitude_5410 type=CWD msg=audit(03/28/2024
    07:50:24.798:1998612) : cwd=/var/home/gpos
    node=Latitude_5410 type=SYSCALL msg=audit(03/28/2024
    07:50:24.798:1998612) : arch=x86_64 syscall=fchmodat
    success=yes exit=0 a0=AT_FDCWD a1=0x556377cc4670 a2=0777
    a3=0xfff items=1 ppid=375221 pid=387535 auid=gpos uid=gpos
    gid=gpos euid=gpos suid=gpos fsuid=gpos egid=gpos sgid=gpos
    fsgid=gpos tty=pts62 ses=4 comm=chmod exe=/usr/bin/chmod
    subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
    key=successful-perm-change
    ```

  - Failure

    ```
    node=Latitude_5410 type=PROCTITLE msg=audit(03/28/2024
    07:56:09.853:1999062) : proctitle=chmod 777 /home/newfile.txt
    node=Latitude_5410 type=PATH msg=audit(03/28/2024
    07:56:09.853:1999062) : item=0 name=/home/newfile.txt
    inode=2960 dev=fd:06 mode=file,111 ouid=root ogid=root
    rdev=00:00 obj=unconfined_u:object_r:home_root_t:s0
    nametype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
    cap_frootid=0
    node=Latitude_5410 type=CWD msg=audit(03/28/2024
    07:56:09.853:1999062) : cwd=/var/home/gpos
    node=Latitude_5410 type=SYSCALL msg=audit(03/28/2024
    07:56:09.853:1999062) : arch=x86_64 syscall=fchmodat
    success=no exit=EPERM(Operation not permitted) a0=AT_FDCWD
    a1=0x5560f21b3670 a2=0777 a3=0xfff items=1 ppid=375221
    pid=387631 auid=gpos uid=gpos gid=gpos euid=gpos suid=gpos
    fsuid=gpos egid=gpos sgid=gpos fsgid=gpos tty=pts62 ses=4
    ```

```
comm=chmod exe=/usr/bin/chmod
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=unsuccessful-perm-change
```

6. Audit record for: User and Group management events (Successful and unsuccessful add, delete, modify, disable, enable, and credential change).

- Add user
  - Success

```
node=Latitude_5410 type=ADD_USER msg=audit(03/28/2024
08:08:58.663:1999785) : pid=387758 uid=root auid=gpos ses=4
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
msg='op=add-user acct=test1 exe=/usr/sbin/useradd
hostname=Latitude_5410 addr=? terminal=pts/62 res=success'
```

  - Failure

```
node=Latitude_5410 type=ADD_USER msg=audit(03/28/2024
08:15:28.286:2002152) : pid=387890 uid=root auid=gpos ses=4
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
msg='op=add-user acct=test_1 exe=/usr/sbin/useradd
hostname=Latitude_5410 addr=? terminal=pts/62 res=failed'
```

- Delete User
  - Success

```
node=Latitude_5410 type=DEL_USER msg=audit(03/28/2024
08:09:27.893:2001252) : pid=387793 uid=root auid=gpos ses=4
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
msg='op=delete-user id=test1 exe=/usr/sbin/userdel
hostname=Latitude_5410 addr=? terminal=pts/62 res=success'
```

  - Failure

```
node=Latitude_5410 type=DEL_USER msg=audit(03/28/2024
08:18:26.234:2002504) : pid=387933 uid=root auid=gpos ses=4
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
msg='op=deleting-user-not-found acct=test exe=/usr/sbin/userdel
hostname=Latitude_5410 addr=? terminal=pts/62 res=failed'
```

- Modify User
  - Success

```
node=Latitude_5410 type=PROCTITLE msg=audit(04/08/2024
12:53:37.513:211070) : proctitl
e=sudo usermod -l test12 test1
node=Latitude_5410 type=PATH msg=audit(04/08/2024
12:53:37.513:211070) : item=0 name=(
null) inode=134234461 dev=fd:00 mode=file, eee ouid=root
ogid=root rdev=00:00 obj=syste
m_u:object_r: shadow_t:s0 nametype=NORMAL cap_fp=none cap_fi=none
cap_fe=0 cap_fver=0 c
ap_frootid=0
node=Latitude_5410 type=CWD msg=audit(04/08/2024
12:53:37.513:211070) : cwd=/var/home/
gpos
```

```
node=Latitude_5410 type=SYSCALL msg=audit(04/08/2024
12:53:37.513:211070) : arch=x86_6
4 syscall=fchown success=yes exit=0 a0=0x5 al=0x0 a2=0x0 a3=0x1b6
items=1 ppid=45951 p
id=45953 auid=gpos uid=root gid=root euid=root suid=root
fsuid=root egid=root sgid=roo
t fsgid=root tty=pts8 ses=2 comm=usermod exe=/usr/sbin/usermod
subj=unconfined_u:uncon
fined_r:unconfined_t:s0-s0:c0.c1023 key=successful -owner-change
```

- Failure

```
node=Latitude_5410 type=PROCTITLE msg=audit(04/08/2024
13:01:48.781:212801) : proctitl
e=usermod -l test1 test12
node=Latitude_5410 type=PATH msg=audit(04/08/2024
13:01:48.781:212801) : item=0 name=/
etc/shadow inode=134234461 dev=fd:00 mode=file,000 ouid=root
ogid=root rdev=00:00 obj=
system_u:object_r: shadow_t:s0 nametype=NORMAL cap_fp=none
cap_fi=none cap_fe=0 cap_fve
r=0 cap_frootid=0
node=Latitude_5410 type=CWD msg=audit(04/08/2024
13:01:48.781:212801) : cwd=/var/home/
gpos
node=Latitude_5410 type=SYSCALL msg=audit(04/08/2024
13:01:48.781:212801) : arch=x86_6
4 syscall=openat success=no exit=EACCES(Permission denied)
a0=AT_FDCWD a1=0x7f8656cd0e
c6 a2=0_RDONLY|0_CLOEXEC a3=0x0 items=1 ppid=45828 pid=46135
auid=gpos uid=gpos gid=gp
os euid=gpos suid=gpos fsuid=gpos egid=gpos sgid=gpos fsgid=gpos
tty=pts8 ses=2 comm=u
sermod exe=/usr/sbin/usermod
subj=unconfined_u:unconfined_r:unconfined_t:50-s0:c0.c102
3 key=unsuccessful-access
```

- Disable User
  - Success

```
node=Latitude_5410 type=USER_CMD msg=audit(04/08/2024
13:09:02.456:213861) : pid=46247
uid=gpos auid=gpos ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 m
sg='cwd=/var/home/gpos cmd=usermod -L user exe=/usr/bin/sudo
terminal=pts/8 res=success
```

  - Failure

```
node=Latitude_5410 type=USER_CMD msg=audit(04/08/2024
13:08:40.664:213416) : pid=46213
uid=gpos auid=gpos ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0. c1023 m
sg='cwd=/var/home/gpos cmd=usermode -L user exe=/usr/bin/sudo
terminal=pts/8 res=failed
```

- Enable User

- Success

```
node=Latitude_5410 type=USER_CMD msg=audit(04/08/2024
13:15:00.311:216268) : pid=46397
uid=gpos auid=gpos ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0. c1023 m
sg='cwd=/var/home/gpos cmd=usermod -U user exe=/usr/bin/sudo
terminal=pts/8 res=succes
```

- Failure

```
node=Latitude_5410 type=PROCTITLE msg=audit(04/08/2024
13:18:07.934:219878) : proctitl
e=usermod -U gpos
node=Latitude_5410 type=PATH msg=audit(04/08/2024
13:18:07.934:219878) : item=0 name=/
etc/shadow inode=134234456 dev=fd:00 mode=file, 00e ouid=root
ogid=root rdev=00:00 obj=
system_u:object_r: shadow_t: s0 nametype=NORMAL cap_fp=none
cap_fi=none cap_fe=0 cap_fve
r=0 cap_frootid=0
node=Latitude_5410 type=CWD msg=audit(04/08/2024
13:18:07.934:219878) : cwd=/var/home/
user
node=Latitude_5410 type=SYSCALL msg=audit(04/08/2024
13:18:07.934:219878) : arch=x86 6
4 syscall=openat success=no exit=EACCES(Permission denied)
a0=AT_FDCWD al=0x7efddc9d0e
c6 a2=0_RDONLY|0_CLOEXEC a3=0x0 items=1 ppid=46469 pid=46515
auid=gpos uid=user gid=us
er euid=user suid=user fsuid=user egid=user sgid=user fsgid=user
tty=pts8 ses=2 comm=u
sermod exe=/usr/sbin/usermod
subj=unconfined_u:unconfined_r:unconfined_t: s0-s0: c0. c102
3 key=unsuccessful-access
```

- User Credential Change
  - Success

```
node=Latitude_5410 type=USER_CHAUTHTOK msg=audit(04/08/2024
13:37:01.612:220900) : pid
=46710 uid=root auid=gpos ses=2
subj=unconfined_u:unconfined_r:passwd_t:s0-s0:c0. c1023
msg='op=PAM: chauthtok grantors=pam_pwquality, pam_localuser,
pam_pwhistory, pam_unix acc
t=user exe=/usr/bin/passwd hostname=Latitude_5410 addr =?
terminal=pts/8 res=success'
```

  - Failure

```
node=Latitude_5410 type=USER_CHAUTHTOK msg=audit(04/08/2024
13:42:37.100:221593) : pid
=46790 uid=gpos auid=gpos ses=2
subj=unconfined_u:unconfined_r:passwd_t:s0-s0: c0. c1023
msg='op=attempted-to-change-password id=gpos exe=/usr/bin/passwd
hostname=Latitude_54
10 addr =? terminal=pts/8 res=failed'
```

- Add Group

- Success

```
node=Latitude-5410 type=ADD_GROUP msg=audit(07/05/2024
17:53:30.165:500632) : pi
d=32617 uid=root auid=gpos ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-
s0:cO.c1023 msg='op=add-group id=project1 exe=/usr/sbin/groupadd
hostname=Latitude-5410 addr =? terminal=pts/0 res=success'
```

- Failure

```
node=Latitude-5410 type=PROCTITLE msg=audit(07/05/2024
18:25:38.847:522967) : proctitl
e=groupadd project2
node=Latitude-5410 type=PATH msg=audit(07/05/2024
18:25:38.847:522967) : item=1 name=/
etc/.pwd.lock inode=402720871 dev=fd:00 mode=file,6ee ouid=root
ogid=root rdev=ee:ee o
bj=system_u:object_r:passwd_file_t:se nametype=NORMAL cap_fp=none
cap_fi=none cap_fe=0
cap_fver=0 cap_frootid=e
node=Latitude-5410 type=PATH msg=audit(07/05/2024
18:25:38.847:522967) : item=0 name=/
etc/ inode=402719956 dev=fd:00 mode=dir,755 ouid=root ogid=root
rdev=00:00 obj=system
u:object_r:etc_t:s0 nametype=PARENT cap_fp=none cap_fi=none
cap_fe=0 cap_fver=0 cap_fr
ootid=0
node=Latitude-5410 type=CWD msg=audit(07/05/2024
18:25:38.847:522967) : cwd=/var/home/
user
node=Latitude-5410 type=SYSCALL msg=audit(07/05/2024
18:25:38.847:522967) : arch=x86 6
4 syscallmopenat success no exit EACCES(Permission denied)
a0=AT_FDCWD al=0x7fb651a018
f9 a2=0_WRONLY|0_CREAT|0_CLOEXEC a3=0x180 items 2 ppid=33442 pid
33543 auid gpos uid-u
ser gid user euid user suid=user fsuid=user egid=user sgid=user
fsgid=user tty=pts1 se
s=3 comm=groupadd exe=/usr/sbin/groupadd
subj=unconfined_u:unconfined_r:unconfined_t:s
0-s0:c0.c1023 key=unsuccessful-create
```

- Delete Group
  - Success

```
node=Latitude-5410 type=DEL_GROUP msg=audit(07/05/2024
18:03:33.631:509616) : pid=32
929 uid=root auid=gpos ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.cl
023 msg='op=delete-group id=unknown(1001) exe=/usr/sbin/groupdel
hostname=Latitude-5
410 addr =? terminal=pts/1 res=success'
```

  - Failure

```
node=Latitude-5410 type=GRP_MGMT msg=audit(07/08/2024
15:47:38.150:596975) : pid=37853
```

```
uid=root auid=gpos ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:ce. c1023 m
sg='op=delete-group acct=project2 exe=/usr/sbin/groupdel
hostname=Latitude-5410 addr =?
terminal=pts/0 res=failed'
```

- Modify Group
  - Success

```
node=Latitude-5410 type=PROCTITLE msg=audit(07/08/2024
14:25:43.697:590836) : proctitl
e=sudo groupmems -d user -g project1
node=Latitude-5410 type=PATH msg=audit(07/08/2024
14:25:43.697:590836) : item=0 name=/
lib/passwd inode=1695272 dev=fd:00 mode=file, 644 ouid=root
ogid=root rdev=00:00 obj=sy
stem_u:object_r:lib_t:s0 nametype=NORMAL cap_fp=none cap_fi=none
cap_fe=0 cap_fver=0 c
ap_frootid=0
node=Latitude-5410 type=CWD msg=audit(07/08/2024
14:25:43.697:590836) : cwd=/var/home/
gpos
node=Latitude-5410 type=SYSCALL msg=audit(07/08/2024
14:25:43.697:590836) : arch=x86 6
4 syscall=openat success=yes exit=3 a0=AT_FDCWD a1=0x7fb79056771f
a2=0_RDONLY|0_CLOEXE
C a3=0x0 items=1 ppid=37279 pid=37552 auid=gpos uid=gpos gid=root
euid=root suid=root
fsuid=root egid=root sgid=root fsgid=root tty=pts13 ses=6
comm=sudo exe=/usr/bin/sudo
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=successful-access
```

  - Failure

```
node=Latitude-5410 type=PROCTITLE msg=audit (07/05/2024
18:18:53.680:522189) : proctitl
e=groupmod -n project2 project1
node=Latitude-5410 type=PATH msg=audit(07/05/2024
18:18:53.680:522189) : item=1 name=/
etc/.pwd. lock inode=402720871 dev=fd:00 mode=file, 600 ouid=root
ogid=root rdev=00:00 0
bj=system_u:object_r:passwd_file_t:s0 nametype=NORMAL cap_fp=none
cap_fi=none cap_fe=0
cap_fver=0 cap_frootid=0
node=Latitude-5410 type=PATH msg=audit(07/05/2024
18:18:53.680:522189) : item=0 name=/
etc/ inode=402719956 dev=fd:00 mode=dir,755 ouid=root ogid=root
rdev=00:00 obj=system
u:object_r:etc_t:s0 nametype=PARENT cap_fp=none cap_fi=none
cap_fe=0 cap_fver=0 cap_fr
ootid=0
node=Latitude-5410 type=CWD msg=audit(07/05/2024
18:18:53.680:522189) : cwd=/var/home/
user
node=Latitude-5410 type=SYSCALL msg=audit(07/05/2024
```

```
18:18:53.680:522189) : arch=x86 6
4 syscall=openat success=no exit=EACCES(Permission denied)
a0=AT_FDCWD al=0x7faeldf4e8
f9 a2=0_WRONLY|0_CREAT|0_CLOEXEC a3=0x180 items=2 ppid=33442
pid=33492 auid=gpos uid=u
ser gid=user euid=user suid=user fsuid=user egid=user sgid=user
fsgid=user tty=ptsl se
S=3 comm=groupmod exe=/usr/sbin/groupmod
subj=unconfined_u:unconfined_r:unconfined_t:s
0-s0:c0.c1023 key=unsuccessful-create
```

- Group Credential Change
  - Success

```
node=Latitude-5410 type=GRP_CHAUTHTOK msg=audit(07/05/2024
18:51:25.105:523880) : pid=
33591 uid=root auid=gpos ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1
023 msg='op=change-password grp=project1 acct=root
exe=/usr/bin/gpasswd hostname=Latit
ude-5410 addr =? terminal=pts/0 res=success
```

  - Failure

```
node=Latitude-5410 type=GRP_CHAUTHTOK msg=audit(07/05/2024
18:55:34.944:525022) : pid=
33663 uid=user auid=gpos ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1
023 msg='op=change-password grp=project1 acct=user
exe=/usr/bin/gpasswd hostname=Latit
ude-5410 addr =? terminal=pts/1 res=failed'
```

7. Audit record for: Audit and log data access events (Success/Failure)

- Success

```
node=Latitude_5410 type=PROCTITLE msg=audit(04/08/2024
15:47:40.830:225583) : proctitle=sudo cat /var/log/audit/audit.log
node=Latitude_5410 type=PATH msg=audit(04/08/2024
15:47:40.830:225583) : item=0 name=/etc/passwd inode=134234458
dev=fd:00 mode=file,644 ouid=root ogid=root rdev=00:00
obj=system_u:object_r:passwd_file_t:s0 nametype=NORMAL cap_fp=none
cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
node=Latitude_5410 type=CWD msg=audit(04/08/2024
15:47:40.830:225583) : cwd=/var/home/gpos
node=Latitude_5410 type=SYSCALL msg=audit(04/08/2024
15:47:40.830:225583) : arch=x86_64 syscall=openat success=yes exit=5
a0=AT_FDCWD a1=0x7f2b3cafaeae a2=O_RDONLY|O_CLOEXEC a3=0x0 items=1
ppid=45828 pid=48353 auid=gpos uid=root gid=root euid=root suid=root
fsuid=root egid=root sgid=root fsgid=root tty=pts8 ses=2 comm=sudo
exe=/usr/bin/sudo subj=unconfined_u:unconfined_r:un
confined_t:s0-s0:c0.c1023 key=successful-access
```

- Failure

```
node=Latitude_5410 type=PROCTITLE msg=audit(04/08/2024
15:47:31.385:225311) : proctitle=cat /var/log/audit/audit.log
```

```
node=Latitude_5410 type=PATH msg=audit(04/08/2024
15:47:31.385:225311) : item=0 name=/var/log/audit/audit.log
nametype=UNKNOWN cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
cap_frootid=0
node=Latitude_5410 type=CWD msg=audit(04/08/2024
15:47:31.385:225311) : cwd=/var/home/gpos
node=Latitude_5410 type=SYSCALL msg=audit(04/08/2024
15:47:31.385:225311) : arch=x86_64 syscall=openat success=no
exit=EACCES(Permission denied) a0=AT_FDCWD a1=0x7ffd79152a3c
a2=O_RDONLY a3=0x0 items=1 ppid=45828 pid=48340 auid=gpos uid=gpos
gid=gpos euid=gpos suid=gpos fsuid=gpos egid=gpos sgid=gpos
fsgid=gpos tty=pts8 ses=2 comm=cat exe=/usr/bin/cat
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=unsuccessful-access
```

8. Audit record for: Attempted application invocation with arguments (Success/Failure e.g due to software restriction policy).
   - Success

     ```
     node=Latitude_5410 type=PROCTITLE msg=audit(04/08/2024
     16:23:31.328:228690) : proctitle=/usr/bin/ls
     node=Latitude_5410 type=PATH msg=audit(04/08/2024
     16:23:31.328:228690) : name=/usr/lib/locale/en_US.utf8/LC_TIME
     node=Latitude_5410 type=SYSCALL msg=audit(04/08/2024
     16:23:31.328:228690) : arch=x86_64 syscall=init_module success=yes
     exit=0 a0=0x560f1e943590 a1=0x9be0 a2=0x560f1d0d98b6 a3=0x2 items=0
     ppid=45779 pid=48900 auid=gpos uid=gpos gid=root euid=root suid=root
     fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=2
     comm=modprobe exe=/usr/bin/kmod
     subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
     key=successful-access
     ```

   - Failure

     ```
     node=Latitude_5410 type=PROCTITLE msg=audit(04/08/2024
     16:23:31.328:228690) : proctitle=/usr/bin/ls
     node=Latitude_5410 type=PATH msg=audit(04/08/2024
     16:23:31.328:228690) : name=/usr/lib/locale/en_US.utf8/LC_TIME
     node=Latitude_5410 type=SYSCALL msg=audit(04/08/2024
     16:23:31.328:228690) : arch=x86_64 syscall=init_module success=no
     exit=EPERM(Operation not permitted) a0=0x560f1e943590 a1=0x9be0
     a2=0x560f1d0d98b6 a3=0x2 items=0 ppid=45779 pid=48900 auid=gpos
     uid=gpos gid=root euid=root suid=root fsuid=root egid=root sgid=root
     fsgid=root tty=pts0 ses=2 comm=bash exe=/usr/bin/bash
     exe=/usr/bin/kmod subj=unconfined_u:unconfined_r:unconfined_t:s0-
     s0:c0.c1023 key=(null)
     node=Latitude_5410 type=FANOTIFY msg=audit(04/08/2024
     16:23:31.328:228690) resp=deny
     ```

9. Audit record for: System reboot, restart, and shutdown events (Success/Failure).
   - System reboot
     - Success

       ```
       node=Latitude_5410 type=SYSTEM_BOOT msg=audit(04/11/2024
       12:45:30.821:206): pid =1287 uid=root auid=unset ses=unset
       subj=system_u:system_r:init_t:s0 msg=' comm= systemd-update-
       ```

```
utmp_exe=/usr/lib/systemd/systemd-update-utmp hostname=? addr=?
terminal=? res=success'
```

- Failure

```
node=Latitude_5410 type=USER_CMD_msg=audit(05/07/2024
06:21:08.192:47659): pid=13829
node=Latitude_5410 uid=user auid=gpos ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
msg='cwd=/var/home/user cmd=reboot exe=/usr/bin/sudo
terminal=pts/0_res=failed'
```

- System shutdown
  - Success

```
node=Latitude_5410 type=SYSTEM_SHUTDOWN msg=audit(04/11/2024
12:44:56.249:348665 ): pid=87214 uid=root auid=unset ses=unset
subj=system_u:system_r:init_t:s0 msg =' comm=systemd-update-utmp
exe=/usr/lib/systemd/systemd-update-utmp hostname=? addr=?
terminal=? res=success'Unsuccessful system shutdown
```

  - Failure

```
node=Latitude_5410 type=USER_CMD msg=audit(05/07/2024
06:21:31.914:47855): pid=13841 uid=user auid=gpos_ses=2
subj=unconfined_u:unconfined_r: unconfined_t:s0-s0:c0.c1023
msg='cwd=/var/home/user cmd=shutdown exe=/usr/bin/sudo
terminal=pts/0 res=failed'
```

10. Audit record for: Kernel module loading and unloading events (Success/Failure).

- Module Loading
  - Success

```
node=Latitude_5410 type=PROCTITLE msg=audit(04/08/2024
16:23:31.328:228690) : proctitle=modprobe sha1_mb
node=Latitude_5410 type=KERN_MODULE msg=audit(04/08/2024
16:23:31.328:228690) : name=sha1_mb
node=Latitude_5410 type=SYSCALL msg=audit(04/08/2024
16:23:31.328:228690) : arch=x86_64 syscall=init_module success=yes
exit=0 a0=0x560f1e943590 a1=0x9be0 a2=0x560f1d0d98b6 a3=0x2 items=0
ppid=45779 pid=48900 auid=gpos uid=root gid=root euid=root suid=root
fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=2
comm=modprobe exe=/usr/bin/kmod
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=module-load
```

  - Failure

```
node=Latitude_5410 type=PROCTITLE msg=audit(04/22/2024
21:31:01.803:326317) : proctitle=modprobe sha1_mb
node=Latitude_5410 type=SYSCALL msg=audit(04/22/2024
21:31:01.803:326317) : arch=x86_ 64 syscall=init_module success=no
exit=EPERM(Operation not permitted) a0=0x55e5620da5 00 a1=0x9be0
a2=0x55e5601178b6 a3=0x2 items=0 ppid=3001 pid=100328 auid=gpos
uid=gpos gid=gpos euid=gpos suid=gpos fsuid=gpos egid=gpos sgid=gpos
fsgid=gpos tty=pts2 ses= 2 comm=modprobe exe=/usr/bin/kmod
subj=unconfined_u: unconfined_r: unconfined_t:s0-50:c 0.c1023 key-
module-load
```

- Module Unloading
  - Success

```
node=Latitude_5410 type=PROCTITLE msg=audit(04/08/2024
16:23:31.328:228690) : proctitle=modprobe -r sha1_mb
node=Latitude_5410 type=KERN_MODULE msg=audit(04/08/2024
16:23:31.328:228690) : name=sha1_mb
node=Latitude_5410 type=SYSCALL msg=audit(04/08/2024
16:23:31.328:228690) : arch=x86_64 syscall=init_module success=yes
exit=0 a0=0x560f1e943590 a1=0x9be0 a2=0x560f1d0d98b6 a3=0x2 items=0
ppid=45779 pid=48900 auid=gpos uid=root gid=root euid=root suid=root
fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=2
comm=modprobe exe=/usr/bin/kmod
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=module-unload
```

  - Failure

```
node=Latitude_5410 type=PROCTITLE msg=audit(04/22/2024
21:31:01.803:326317) : proctitle=modprobe -r shal_mb
node=Latitude_5410 type=SYSCALL msg=audit(04/22/2024
21:31:01.803:326317) : arch=x86_ 64 syscall=init_module success=no
exit=EPERM(Operation not permitted) a0=0x55e5620da5 00 a1=0x9be0
a2=0x55e5601178b6 a3=0x2 items=0 ppid=3001 pid=100328 auid=gpos
uid=gpos gid=gpos euid=gpos suid=gpos fsuid=gpos egid=gpos sgid=gpos
fsgid=gpos tty=pts2 ses= 2 comm=modprobe exe=/usr/bin/kmod
subj=unconfined_u: unconfined_r: unconfined_t:s0-50:c 0.c1023 key-
module-unload
```

11. Audit record for: Administrator or root-level access events (Success/Failure).

- Success

```
node=Latitude_5410 type=USER_CHAUTHTOK msg=audit(04/08/2024
13:37:01.612:220900) : pid
=46710 uid=root auid=gpos ses=2
subj=unconfined_u:unconfined_r:passwd_t:s0-s0:c0. c1023
msg='op=PAM: chauthtok grantors=pam_pwquality, pam_localuser,
pam_pwhistory, pam_unix acc
t=user exe=/usr/bin/passwd hostname=Latitude_5410 addr =?
terminal=pts/8 res=success'
```

- Failure

```
node=Latitude_5410 type=USER_CHAUTHTOK msg=audit(04/08/2024
13:42:37.100:221593) : pid
=46790 uid=gpos auid=gpos ses=2
subj=unconfined_u:unconfined_r:passwd_t:s0-s0: c0. c1023
msg='op=attempted-to-change-password id=gpos exe=/usr/bin/passwd
hostname=Latitude_54
10 addr =? terminal=pts/8 res=failed'
```

8 Acronyms and Abbreviations

Table 3: Acronyms and Abbreviations

Term	Definition
ACL	Access Control List
BIOS	Basic Input/Output System
CA	Certificate Authority
CC	Common Criteria
CLI	Command Line Interface
CN	Common Name
CRL	Certificate Revocation List
CSfC	Commercial Solutions for Classified
CSR	Certificate Signing Request
CVE	Common Vulnerabilities and Exposures
DAC	Discretionary Access Control
DER	Distinguished Encoding Rules
DIY	Do it Yourself
DNS	Domain Name System
eBPF	Extended Berkely Packet Filter
EUD	End User Device
FIPS	Federal Information Processing Standards
gdm	GNOME Display Manager
GID	Group ID
GNOME	GNU Network Object Module Environment
GNU	GNU's Not Unix
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
KSM	Kernel Same-page Merging
LAN	Local Area Network

Term	Definition
MA	Mutual Authentication
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OS	Operating System
OSPP	Operating System Protection Profile
PCL	Product Compliant List
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography Standards
POSIX	Portable Operating System Interface
RPM	Red Hat Package Manager
RHEL	Red Hat Enterprise Linux
SAN	Subject Alternative Name
SCAP	Secure Content Automation Protocol
SGID	Set Group ID
SRV	Services
SSH	Secure Shell
SSL	Secure Sockets Layer
SUID	Set owner User ID
TLS	Transport Layer Security
TOE	Target of Evaluation
UEFI	Unified Extensible Firmware Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus


CACI