Elasticsearch 8.0 Hardening Guide based on Central Log Server SRG V2R1

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1,
Rule Title: The Central Log Server must be configured to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
STIG ID: SRG-APP-000033 **Rule ID:** SV-206447r395499_rule **Vul ID:** V-206447
Severity: CAT I

Documentable: No

Check Content:
Verify the Central Log Server user accounts are configured for granular permissions to separate and control access levels of accounts used to access the application. Users should not have access permissions that are not relevant to their role.

If the Central Log Server is not configured to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts and to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). The recommendation is to integrate Elasticsearch with these services to support centralized account management.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., networks, web servers, and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

This requirement is applicable to access control enforcement applications (e.g., authentication servers) and other applications that perform information and system access control functions.

Legacy Ids: V-81297; SV-96011

CCI: CCI-000213The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.NIST SP 800-53 :: AC-3NIST SP 800-53A :: AC-3.1NIST SP 800-53 Revision 4 :: AC-3

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to protect the data sent from hosts and devices from being altered in a way that may prevent the attribution of an action to an individual (or process acting on behalf of an individual).
STIG ID: SRG-APP-000080 **Rule ID:** SV-206448r395691_rule **Vul ID:** V-206448
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the system is configured with a hash or other method that protects the data against alteration of the log information sent from hosts and devices.

Verify the Central Log Server is configured to log all changes to the machine data.

If the Central Log Server is not configured to protect against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation, this is a finding.

Fix Text:
Steps/Recommendation:

1. In elasticsearch.yml
xpack.security.enabled: true
xpack.security.fips_mode.enabled: true

2. Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

Reference:

a. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without non-repudiation, it is impossible to positively attribute an action to an

individual (or process acting on behalf of an individual).

The records stored by the Central Log Server must be protected against such alteration as removing the identifier. A hash is one way of performing this function. The server must not allow the removal of identifiers or date/time, or it must severely restrict the ability to do so. Additionally, the log administrator access and activity with the user account information.

Legacy Ids: V-81105; SV-95819

CCI: CCI-000166The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.NIST SP 800-53 :: AU-10NIST SP 800-53A :: AU-10.1NIST SP 800-53 Revision 4 :: AU-10

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to aggregate log records from organization-defined devices and hosts within its scope of coverage.
STIG ID: SRG-APP-000086 **Rule ID:** SV-206449r395700_rule **Vul ID:** V-206449
Severity: CAT III

Documentable: No

Check Content:
Examine the documentation that lists the scope of coverage for the specific log server being reviewed.

Verify the system is configured to aggregate log records from organization-defined devices and hosts within its scope of coverage.

If the Central Log Server is not configured to aggregate log records from organization-defined devices and hosts within its scope of coverage, this is a finding.

Fix Text:
Steps/Recommendation:

1. Where possible, recommend using Beats as the primary data collection mechanism. Beats will automatically collect data from host devices and ship that data to Elasticsearch. Review elasticsearch documentation for information about securing beats and connecting to a cluster that has security features enabled.

2. Recommend using Logstash to perform data conversion/enrichment for custom application and device logs not supported by Beats.

The Logstash Elasticsearch output, input, and filter plugins, as well as monitoring and central

management, support authentication and encryption over HTTPS.

References:

a. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
b. Auditbeat: https://www.elastic.co/guide/en/beats/auditbeat/8.0/auditbeat-overview.html
c. Secure Auditbeat:
https://www.elastic.co/guide/en/beats/auditbeat/8.0/securing-auditbeat.html
d. Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/index.html
e. Secure Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
f. Metricbeat: https://www.elastic.co/guide/en/beats/metricbeat/8.0/index.html
g. Secure Metricbeat:
https://www.elastic.co/guide/en/beats/metricbeat/8.0/securing-metricbeat.html
h. Packetbeat: https://www.elastic.co/guide/en/beats/packetbeat/8.0/index.html
i. Secure Packetbeat:
https://www.elastic.co/guide/en/beats/packetbeat/8.0/securing-packetbeat.html
j. Heartbeat: https://www.elastic.co/guide/en/beats/heartbeat/8.0/index.html
k. Secure Heartbeat:
https://www.elastic.co/guide/en/beats/heartbeat/8.0/securing-heartbeat.html
l. Winlogbeat: https://www.elastic.co/guide/en/beats/winlogbeat/8.0/index.html
m. Secure Winlogbeat:
https://www.elastic.co/guide/en/beats/winlogbeat/8.0/securing-winlogbeat.html
n. Logstash: https://www.elastic.co/guide/en/logstash/8.0/index.html
o. Secure your connection to Elasticsearch with logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
p. Install Elastic Agents :
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If the application is not configured to collate records based on the time when the events occurred, the ability to perform forensic analysis and investigations across multiple components is significantly degraded. Centralized log aggregation must also include logs from databases and servers (e.g., Windows) that do not natively send logs using the syslog protocol.

Legacy Ids: V-81107; SV-95821

CCI: CCI-000174The information system compiles audit records from organization-defined information system components into a system-wide (logical or physical) audit trail that is

time-correlated to within organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail.NIST SP 800-53 :: AU-12 (1)NIST SP 800-53A :: AU-12 (1).1 (iii&v)NIST SP 800-53 Revision 4 :: AU-12 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: Time stamps recorded on the log records in the Central Log Server must be configured to synchronize to within one second of the host server or, if NTP is configured directly in the log server, the NTP time source must be the same as the host and devices within its scope of coverage.
STIG ID: SRG-APP-000086 **Rule ID:** SV-206450r395700_rule **Vul ID:** V-206450
Severity: CAT III

Documentable: No

Check Content:
Examine the time stamp that indicates when the Central Log Server received the log records.

Verify the time is synchronized to within one second of the host server.

If an NTP client is configured within the Central Log Server application, verify it is configured to use the same NTP time source as the host and devices within its scope of coverage.

If time stamps recorded on the log records in the Central Log Server are not configured to synchronize to within one second of the host server, or the log server application is not configured to use the same NTP time source as the host and devices within its scope of coverage, this is a finding.

Fix Text:
Steps/Recommendation:

1. Where possible, recommend using Beats as the primary data collection mechanism. Beats will automatically handle date and timezone conversions.

2. Ensure the Elastic Stack indexes are properly configured to use the log timestamp as the index timestamp.

3. When needed, recommend using Logstash to perform data conversion/enrichment for custom application and device logs not supported by Beats.

4. Setup all the host/device to use UTC time zone, use NTP/Chrony to avoid time drift. Also, use Beat/Logstash to have time enabled in all index.
date {
match =>; ...

time zone =>; "%{tz}"; # or whatever you call the field
}

References:

a. For Time in host machine: https://chrony.tuxfamily.org/
b. To add local time zone to Beat:
https://www.elastic.co/guide/en/beats/filebeat/8.0/add-locale.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If the application is not configured to collate records based on the time when the events occurred, the ability to perform forensic analysis and investigations across multiple components is significantly degraded. If the SIEM or other Central Log Server is out of sync with the host and devices for which it stores event logs, this may impact the accuracy of the records stored.

Log records are time correlated if the time stamps in the individual log records can be reliably related to the time stamps in other log records to achieve a time ordering of the records within an organization-defined level of tolerance.

This requirement applies only to applications that compile system-wide log records for multiple systems or system components.

Note: The actual configuration and security requirements for NTP is handled in the host OS or NDM STIGs that are also required as part of a Central Log Server review.

Legacy Ids: V-81109; SV-95823

CCI: CCI-000174The information system compiles audit records from organization-defined information system components into a system-wide (logical or physical) audit trail that is time-correlated to within organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail.NIST SP 800-53 :: AU-12 (1)NIST SP 800-53A :: AU-12 (1).1 (iii&v)NIST SP 800-53 Revision 4 :: AU-12 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: Where multiple log servers are installed in the enclave, each log server must be configured to aggregate log records to a central aggregation server or other consolidated

events repository.
STIG ID: SRG-APP-000086 **Rule ID:** SV-206451r395700_rule **Vul ID:** V-206451
Severity: CAT II

Documentable: No

Check Content:
Examine the network architecture and documentation.

If the log server being reviewed is one of multiple log servers in the enclave or on a network segment, verify that an aggregation server exists and that the log server under review is configured to send records received from the host and devices to the aggregation server or centralized SIEM/events sever.

Where multiple log servers are installed in the enclave, if each log server is not configured to send log records to a central aggregation server or other consolidated events repository, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using Elasticsearch Cross Cluster Search to provide a single view of all logs when multiple Elasticsearch clusters are in use. This approach enables you to minimize how much data is sent across the network. In situations where a copy of the data is required, recommend using Elasticsearch Cross Cluster Replication to ensure multiple clusters have the same copy of the data.

2. Cross Cluster Search index patterns utilize index aliases to target remote indices (e.g., index_alias:index_name):

The following search API request searches the twitter index on a single remote cluster, cluster_one.

```
curl -X GET "localhost:9200/cluster_one:my-index-000001/_search?pretty" -H
'Content-Type: application/json' -d'
{
  "query": {
    "match": {
      "user.id": "kimchy"
    }
  },
  "_source": ["user.id", "message", "http.response.status_code"]
}
'
```

References:

a. Cross Cluster Search:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-cross-cluster-search.html
b. Cross Cluster Replication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-ccr.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Log servers (e.g., syslog servers) are often used on network segments to consolidate from the devices and hosts on that network segment. However, this does not achieve compliance with the DoD requirement for a centralized enclave log server.

To comply with this requirement, create a central log server that aggregates multiple log servers or use another method to ensure log analysis and management is centrally managed and available to enterprise forensics and analysis tools. This server is often called a log aggregator, SIEM, or events server.

Legacy Ids: V-81111; SV-95825

CCI: CCI-000174The information system compiles audit records from organization-defined information system components into a system-wide (logical or physical) audit trail that is time-correlated to within organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail.NIST SP 800-53 :: AU-12 (1)NIST SP 800-53A :: AU-12 (1).1 (iii&v)NIST SP 800-53 Revision 4 :: AU-12 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server log records must be configured to use the syslog protocol or another industry standard format (e.g., Windows event protocol) that can be used by typical analysis tools.
STIG ID: SRG-APP-000088 **Rule ID:** SV-206452r395703_rule **Vul ID:** V-206452
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify log records are configured to use the syslog protocol or another industry standard

format (e.g., Windows event protocol) that can be used by a typical analysis tools.

If the Central Log Server log records are not configured to use the syslog protocol, or another industry standard format (e.g., Windows event protocol) that can be used by typical analysis tools, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using Filebeat with the syslog input to collect syslog data.

2. Recommend using Logstash when Filebeat isn't possible/available.

grok_pattern
 Value type is string
 Default value is "<%{POSINT:priority}>%{SYSLOGLINE}"

Default value depends on whether ecs_compatibility is enabled:
 ECS Compatibility disabled: "<%{POSINT:priority}>%{SYSLOGLINE}"
 ECS Compatibility enabled: "<%{POSINT:[log][syslog][priority]:int}>%{SYSLOGLINE}"

The default value should read and properly parse syslog lines which are fully compliant with RFC3164.

You can override this value to parse non-standard lines with a valid grok pattern which will parse the received lines. If the line is unable to be parsed, the _grokparsefailure_sysloginput tag will be added.

The grok pattern must provide a timestamp field. If the timestamp field is omitted, or is unable to be parsed as RFC3164 style or ISO8601, a _dateparsefailure tag will be added.

syslog_field
   Value type is string
   Default value is "message"

Codecs process the data before the rest of the data is parsed. Some codecs, like CEF, put the syslog data into another field after pre-processing the data. Use this option in conjunction with the grok_pattern configuration to allow the syslog input plugin to fully parse the syslog data in this case.

```
input {
  syslog {
    port => 12345
    codec => cef
    syslog_field => "syslog"
    grok_pattern => "<%{POSINT:priority}>%{SYSLOGTIMESTAMP:timestamp}
```

CUSTOM GROK HERE"
  }
}

3. Organization has to make sure the log lines conform to RFC3164 standards to use logstash syslog plugin.

References:

a. Filebeat syslog input:
https://www.elastic.co/guide/en/beats/filebeat/8.0/filebeat-input-syslog.html
b. Logstash syslog input plugin:
https://www.elastic.co/guide/en/logstash/8.0/plugins-inputs-syslog.html
c. Example for configuring Logstash:
https://www.elastic.co/guide/en/logstash/8.0/config-examples.html
d. Logstash Input Plugins: https://www.elastic.co/guide/en/logstash/8.0/input-plugins.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without a standardized format for log records, the ability to perform forensic analysis may be more difficult. Standardization facilitates production of event information that can be more readily analyzed and correlated.

Log information that is normalized to common standards promotes interoperability and exchange of such information between dissimilar devices and information systems.

If logging mechanisms within applications that send records to the centralized audit system do not conform to standardized formats, the audit system may convert the records into a standardized format when compiling system-wide audit trails. Thus, although the application and other system components should send the information in a standardized format, ultimately the audit aggregation server is responsible for ensuring the records are compiled to meet this requirement.

Legacy Ids: V-81113; SV-95827

CCI: CCI-001353The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.NIST SP 800-53 :: AU-12 (2)NIST SP 800-53A :: AU-12 (2).1NIST SP 800-53 Revision 4 :: AU-12 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to retain the DoD-defined attributes of the log records sent by the devices and hosts.
STIG ID: SRG-APP-000089 **Rule ID:** SV-206453r395706_rule **Vul ID:** V-206453
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server retains the DoD-defined attributes of the log records sent by the devices and hosts.

If the Central Log Server is not configured to retain the DoD-defined attributes of the log records sent by the devices and hosts, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using Beats to collect system and device logs where possible.

2. Recommend using Logstash to collect system and device logs when Beats does not provide out of the box support for a specified format.

3. Logstash and or Beats should be configured to collect application logs with all the required attributes.

4. All applications logs/events should include the required DoD attributes.

5. Recommend using Elasticsearch index templates where possible.
In Elasticsearch, mapping is the description of how documents and the fields they contain are stored and indexed. In the mapping, define, for example, the following:
- The structure of the document (fields and data type of those fields)
- How to transform values before indexing
- What fields use for full-text searching

6. Update the index mapping definitions as needed to include time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

```
curl -X PUT http://localhost:9200/person \
-H 'Content-Type: application/json' \
-d '{
      "mappings": {
```

```
      "dynamic": "strict",
      "properties": {
        "name": {"type": "text"},
        "source address": {"type": "text"},
       "ip_address": {"type": "text"},
        "extra_data": {"type": "object", "dynamic": true}
      }
    }
}'
```

References:

a. AU-12 of NIST 800-53 (https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&number=AU-12), supported by supplemental guidance from AU-3 (https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&number=AU-3)
b. Mapping: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/mapping.html
c. Index Template: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/index-templates.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Log records can be generated from various components within the application (e.g., process, module). Certain specific application functionalities may be audited as well. The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating log records.

DoD has defined a list of information or attributes that must be included in the log record, including date, time, source, destination, module, severity level (category of information), etc. Other log record content that may be necessary to satisfy the requirement of this policy includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Legacy Ids: V-81115; SV-95829

CCI: CCI-000169The information system provides audit record generation capability for the auditable events defined in AU-2 a at organization-defined information system

components.NIST SP 800-53 :: AU-12 aNIST SP 800-53A :: AU-12.1 (ii)NIST SP 800-53 Revision 4 :: AU-12 a

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to allow only the Information System Security Manager (ISSM) (or individuals or roles appointed by the ISSM) to select which auditable events are to be retained.
STIG ID: SRG-APP-000090 **Rule ID:** SV-206454r395709_rule **Vul ID:** V-206454
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the system is configured to allow only the ISSM (or individuals or roles appointed by the ISSM) to select which auditable events are to be retained.

If the Central Log Server is not configured to allow only the ISSM (or individuals or roles appointed by the ISSM) to select which auditable events are to be retained, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm.

2. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

3. Configure the Central Log Server to allow only the ISSM (or individuals or roles appointed by the ISSM) to select which auditable events are to be retained.

4. Verify: GET /_security/privilege can be used to get all the privileges

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
i. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
j. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
k. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without restricting which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events. Misconfigured audits may degrade the system's performance by overwhelming the audit log. Misconfigured audits may also make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating log records.

Legacy Ids: V-81117; SV-95831

CCI: CCI-000171The information system allows organization-defined personnel or roles to select which auditable events are to be audited by specific components of the information system.NIST SP 800-53 :: AU-12 bNIST SP 800-53A :: AU-12.1 (iii)NIST SP 800-53 Revision 4 :: AU-12 b

Rule Title: The Central Log Server must be configured to perform analysis of log records across multiple devices and hosts in the enclave that can be reviewed by authorized individuals.
STIG ID: SRG-APP-000111 **Rule ID:** SV-206455r395808_rule **Vul ID:** V-206455
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the system is configured to perform analysis of log records across multiple devices and hosts in the enclave that can be reviewed by authorized individuals.

If the Central Log Server is not configured to perform analysis of log records across multiple devices and hosts in the enclave that can be reviewed by authorized individuals, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using Beats to collect system and device logs where possible.

2. Recommend using Logstash to collect system and device logs when Beats does not provide out of the box support for a specified format.

3. Recommend using an external Identity Management system for authentication of users.

4. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

5. If users are authenticated with the native or file realms, role assignment can be managed using the user management APIs or the users command-line tool (elasticsearch-users), respectively.

Role-mappings can be defined via an API or managed through files. These two sources of role-mapping are combined inside the Elasticsearch security features, so it is possible for a single user to have some Roles mapped through the API and other Roles mapped through files.

Role-mappings must be created for other types of realms that define which Roles should be assigned to each user based on their username, groups, or other metadata.

References:

a. Elasticsearch authentication:

https://www.elastic.co/blog/a-deep-dive-into-elasticsearch-authentication-realms
b. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
c. Role-based access control (RBAC) in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
d. Mapping users and groups to roles:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/mapping-roles.html#mapping-roles
e. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
f. Auditbeat: https://www.elastic.co/guide/en/beats/auditbeat/8.0/auditbeat-overview.html
g. Secure Auditbeat:
https://www.elastic.co/guide/en/beats/auditbeat/8.0/securing-auditbeat.html
h. Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/index.html
i. Secure Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
j. Metricbeat: https://www.elastic.co/guide/en/beats/metricbeat/8.0/index.html
k. Secure Metricbeat:
https://www.elastic.co/guide/en/beats/metricbeat/8.0/securing-metricbeat.html
l. Packetbeat: https://www.elastic.co/guide/en/beats/packetbeat/8.0/index.html
m. Secure Packetbeat:
https://www.elastic.co/guide/en/beats/packetbeat/8.0/securing-packetbeat.html
n. Heartbeat: https://www.elastic.co/guide/en/beats/heartbeat/8.0/index.html
o. Secure Heartbeat:
https://www.elastic.co/guide/en/beats/heartbeat/8.0/securing-heartbeat.html
p. Winlogbeat: https://www.elastic.co/guide/en/beats/winlogbeat/8.0/index.html
q. Secure Winlogbeat:
https://www.elastic.co/guide/en/beats/winlogbeat/8.0/securing-winlogbeat.html
r. Logstash: https://www.elastic.co/guide/en/logstash/8.0/index.html
s. Secure your connection to Elasticsearch with logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Successful incident response and auditing relies on timely, accurate system information and analysis to allow the organization to identify and respond to potential incidents in a proficient manner. If the application does not provide the ability to centrally review the application logs, forensic analysis is negatively impacted.

Segregation of logging data to multiple disparate computer systems is counterproductive and makes log analysis and event notification difficult to implement and manage, particularly when the system or application has multiple logging components written to different locations

or systems.

Automated mechanisms for centralized reviews and analyses include, for example, Security Information and Event Management (SIEM) products.

Legacy Ids: V-81119; SV-95833

CCI: CCI-000154The information system provides the capability to centrally review and analyze audit records from multiple components within the system.NIST SP 800-53 :: AU-6 (4)NIST SP 800-53A :: AU-6 (4).1NIST SP 800-53 Revision 4 :: AU-6 (4)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to perform on-demand filtering of the log records for events of interest based on organization-defined criteria.
STIG ID: SRG-APP-000115 **Rule ID:** SV-206456r395814_rule **Vul ID:** V-206456
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the system is configured to perform on-demand filtering of the log records for events of interest based on organization-defined criteria.

If the Central Log Server is not configured to perform on-demand filtering of the log records for events of interest based on organization-defined criteria, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch provides search APIs to search and filter on any data required from the stored logs.

2. Recommend using the Kibana UI and Beats dashboards.

References:

a. Search APIs:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/search-search.html
b. Kibana Query: https://www.elastic.co/guide/en/kibana/8.0/kuery-query.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The ability to specify the event criteria that are of interest provides the persons reviewing the logs with the ability to quickly isolate and identify these events without having to review entries that are of little or no consequence to the investigation. Without this capability, forensic investigations are impeded.

Events of interest can be identified by the content of specific log record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required; for example, locations selectable by general networking location (e.g., by network or subnetwork) or by specific information system component. This requires applications to be configured to customize log record reports based on organization-defined criteria.

Summary reports provide oversight for security devices, helping to identify when a device is not detecting or blocking to the extent one would expect. A simple top 10 list of what was detected and blocked, with a count by severity, can help prioritize security responses. Operational reports detailing the source hosts for any given malware can then direct remediation responses.

Legacy Ids: V-81121; SV-95835

CCI: CCI-000158The information system provides the capability to process audit records for events of interest based on organization-defined audit fields within audit records.NIST SP 800-53 :: AU-7 (1)NIST SP 800-53A :: AU-7 (1).1NIST SP 800-53 Revision 4 :: AU-7 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to use internal system clocks to generate time stamps for log records.
STIG ID: SRG-APP-000116 **Rule ID:** SV-206457r395817_rule **Vul ID:** V-206457
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server uses internal system clocks to generate time stamps for log records.

If the Central Log Server is not configured to use internal system clocks to generate time stamps for log records, this is a finding.

Fix Text:
Steps/Recommendation:

1. All applications should capture the time of log/event creation.

2. Ingest node processor "@timestamp" should be configured to capture date of record ingestion. This can be configured using processor module in Ingest Node.

3. Recommend setting up NTP or Chrony in all host to avoid time drift in servers.

4. To verify if the ingest pipeline is setup to capture the time, use the following:
GET "localhost:9200/_ingest/pipeline/my-pipeline-id?pretty"

References:

a. Processors: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/processors.html
b. Ingest node: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html
c. Date Processor:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/date-processor.html
d. Get pipeline API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/get-pipeline-api.html
e. Pipeline for Beats:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ingest.html#pipelines-for-beats
f. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
g. Install Elastic Agents :
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without an internal clock used as the reference for the time stored on each event to provide a trusted common reference for the time, forensic analysis would be impeded. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events.

If the internal clock is not used, the system may not be able to provide time stamps for log messages. Additionally, externally generated time stamps may not be accurate. Applications

can use the capability of an operating system or purpose-built module for this purpose.

Legacy Ids: V-81123; SV-95837

CCI: CCI-000159The information system uses internal system clocks to generate time stamps for audit records.NIST SP 800-53 :: AU-8NIST SP 800-53A :: AU-8.1NIST SP 800-53 Revision 4 :: AU-8 a

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to back up the log records repository at least every seven days onto a different system or system component other than the system or component being audited.
STIG ID: SRG-APP-000125 **Rule ID:** SV-206458r395838_rule **Vul ID:** V-206458
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server log records repository is backed up at least every seven days onto a different system or system component other than the system or component being audited.

If the Central Log Server is not configured to back up the log records repository at least every seven days onto a different system or system component other than the system or component being audited, this is a finding.

Fix Text:
Steps/Recommendation:

1. Setup appropriate life cycle for the indices and create snapshots.

2. Elasticsearch can be configured to provide redundancy by storing the Elasticsearch data into a different system or system component other than the system or component being audited.

References:
a. Data Resiliency: https://www.elastic.co/guide/en/logstash/8.0/resiliency.html
b. Manage the index lifecycle:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/index-lifecycle-management.html
c. Configure snapshot lifecycle policies:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/snapshots-take-snapshot.html#automate-snapshots-slm

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protection of log data includes ensuring log data is not accidentally lost or deleted. Backing up log records to a different system or onto separate media than the system being audited on an organizationally defined frequency helps to ensure that in the event of a catastrophic system failure, the log records will be retained.

This helps to ensure that a compromise of the information system being audited does not also result in a compromise of the log records.

This requirement only applies to applications that have a native backup capability for log records. Operating system backup requirements cover applications that do not provide native backup functions.

Legacy Ids: V-81125; SV-95839

CCI: CCI-001348The information system backs up audit records on an organization-defined frequency onto a different system or system component than the system or component being audited.NIST SP 800-53 :: AU-9 (2)NIST SP 800-53A :: AU-9 (2).1 (iii)NIST SP 800-53 Revision 4 :: AU-9 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server system backups must be retained for a minimum of 5 years for SAMLI and a minimum of 7 days for non-SAMI on media capable of guaranteeing file integrity for the minimum applicable information retention period.
STIG ID: SRG-APP-000125 **Rule ID:** SV-206459r767007_rule **Vul ID:** V-206459
Severity: CAT III

Documentable: No

Check Content:
Review the SSP, backup media documentation, and system backup configuration.

Verify the Central Log Server system is backed up to media capable of guaranteeing file integrity for a minimum of five years.
If the Central Log Server does not retain backups for a minimum of five years for SAMI and a minimum of seven days for non-SAMI, this is a finding.

If the Central Log Server system backups are not stored on appropriate media capable of guaranteeing file integrity for a minimum of five years for systems retaining SAMI, this is a finding.

Fix Text:
Steps/Recommendation:

1. This is an organizational requirement; Elastic Stack supports all standard media used for backups.

References:
a. Elastic Stack: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/index.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If backups are not properly processed, protected, and stored on appropriate media, recovery from a system failure or implementation of a contingency plan would not include the data necessary to fully recover in the time required to ensure continued mission support.

Legacy Ids: V-81127; SV-95841

CCI: CCI-000167The organization retains audit records for an organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.NIST SP 800-53 :: AU-11NIST SP 800-53A :: AU-11.1 (iii)NIST SP 800-53 Revision 4 :: AU-11CCI-001348The information system backs up audit records on an organization-defined frequency onto a different system or system component than the system or component being audited.NIST SP 800-53 :: AU-9 (2)NIST SP 800-53A :: AU-9 (2).1 (iii)NIST SP 800-53 Revision 4 :: AU-9 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).
STIG ID: SRG-APP-000148 **Rule ID:** SV-206460r395859_rule **Vul ID:** V-206460
Severity: CAT I

Documentable: No

Check Content:
Examine the configuration.

Verify that individual user accounts are defined within the application. Each account must have a separate identifier. If an authentication server may be used for login, ensure the application audit logs containing management and configuration actions, identify the individual performing each action.

If the Central Log Server is not configured to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users), this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, SAML/OIDC and PKI) to manage accounts and to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). The recommendation is to integrate Elasticsearch with these services to support centralized account management.

Note: Group accounts are not permitted for logon to the Central Log Server.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and any processes acting on behalf of users) must be uniquely identified and authenticated for all accesses.

Legacy Ids: V-81281; SV-95995

CCI: CCI-000764The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).NIST SP 800-53 :: IA-2NIST SP 800-53A :: IA-2.1NIST SP 800-53 Revision 4 :: IA-2

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must use multifactor authentication for network access to privileged user accounts.
STIG ID: SRG-APP-000149 **Rule ID:** SV-206461r397438_rule **Vul ID:** V-206461
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to require DoD PKI or another multifactor authentication method for logon via the network for all privileged accounts. If the account of last resort is used for logon via the network (not recommended), then verify it is configured to require multifactor authentication method.

If the Central Log Server is not configured to use multifactor authentication for network access to privileged user accounts, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which provides multi-factor authentication.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased.

Multifactor authentication requires using two or more factors to achieve authentication.

Factors include:
(i) something a user knows (e.g., password/PIN);
(ii) something a user has (e.g., cryptographic identification device, token); or
(iii) something a user is (e.g., biometric).

A privileged account is defined as an information system account with authorizations of a privileged user.

Network access is defined as access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, or the Internet).

Legacy Ids: V-81307; SV-96021

CCI: CCI-000765The information system implements multifactor authentication for network access to privileged accounts.NIST SP 800-53 :: IA-2 (1)NIST SP 800-53A :: IA-2 (1).1NIST SP 800-53 Revision 4 :: IA-2 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must use multifactor authentication for network access to non-privileged user accounts.
STIG ID: SRG-APP-000150 **Rule ID:** SV-206462r397441_rule **Vul ID:** V-206462
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to require DoD PKI or another multifactor authentication method for logon via the network for all non-privileged accounts.

If the Central Log Server is not configured to use multifactor authentication for network access to non-privileged user accounts, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which provides multi-factor authentication.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To assure accountability and prevent unauthenticated access, non-privileged users must utilize multifactor authentication to prevent potential misuse and compromise of the system.

Multifactor authentication uses two or more factors to achieve authentication.

Factors include:
(i) Something you know (e.g., password/PIN);
(ii) Something you have (e.g., cryptographic identification device, token); or
(iii) Something you are (e.g., biometric).

A non-privileged account is any information system account with authorizations of a non-privileged user.

Network access is any access to an application by a user (or process acting on behalf of a user) where said access is obtained through a network connection.

Applications integrating with the DoD Active Directory and utilize the DoD CAC are examples of compliant multifactor authentication solutions.

Legacy Ids: V-81309; SV-96023

CCI: CCI-000766The information system implements multifactor authentication for network access to non-privileged accounts.NIST SP 800-53 :: IA-2 (2)NIST SP 800-53A :: IA-2 (2).1NIST SP 800-53 Revision 4 :: IA-2 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must use multifactor authentication for local access using privileged user accounts.
STIG ID: SRG-APP-000151 **Rule ID:** SV-206463r397444_rule **Vul ID:** V-206463

Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to require DoD PKI or another multifactor authentication method for local logon.

If the Central Log Server is not configured to use multifactor authentication for local access using privileged accounts, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which provides multi-factor authentication.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To assure accountability and prevent unauthenticated access, privileged users must utilize multifactor authentication to prevent potential misuse and compromise of the system.

Multifactor authentication is defined as: using two or more factors to achieve authentication.

Factors include:
(i) Something a user knows (e.g., password/PIN);
(ii) Something a user has (e.g., cryptographic identification device, token); or
(iii) Something a user is (e.g., biometric).

A privileged account is defined as an information system account with authorizations of a privileged user.

Local access is defined as access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

Applications integrating with the DoD Active Directory and utilize the DoD CAC are examples of compliant multifactor authentication solutions.

Legacy Ids: V-81313; SV-96027

CCI: CCI-000767The information system implements multifactor authentication for local access to privileged accounts.NIST SP 800-53 :: IA-2 (3)NIST SP 800-53A :: IA-2 (3).1NIST SP 800-53 Revision 4 :: IA-2 (3)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to use multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.
STIG ID: SRG-APP-000154 **Rule ID:** SV-206464r397453_rule **Vul ID:** V-206464
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to use DoD PKI or another form of multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

If the Central Log Server is not configured to use multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend organizations integrate Elastic Stack authentication with enterprise identify management provider which provides multi-factor authentication.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards, such as the U.S. Government Personal Identity Verification card and the DoD common access card.

A privileged account is any information system account with authorizations of a privileged user.

Network access is any access to an application by a user (or process acting on behalf of a user) where said access is obtained through a network connection.

Legacy Ids: V-81315; SV-96029

CCI: CCI-001936The information system implements multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.NIST SP 800-53 Revision 4 :: IA-2 (6)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must use FIPS-validated SHA-1 or higher hash function to provide replay-resistant authentication mechanisms for network access to privileged accounts.
STIG ID: SRG-APP-000156 **Rule ID:** SV-206465r397459_rule **Vul ID:** V-206465
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to use FIPS-validated SHA-1 or higher hash function to provide replay-resistant authentication mechanisms for network access to privileged accounts.

If the Central Log Server does not use FIPS-validated SHA-1 or higher hash function to provide replay-resistant authentication mechanisms for network access to privileged accounts, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):

xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

4. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

5. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: A replay attack may enable an unauthorized user to gain access to the application. Authentication sessions between the authenticator and the application validating the user credentials must not be vulnerable to a replay attack.

Anti-replay is a cryptographically based mechanism; thus, it must use FIPS-approved algorithms. An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Note that the anti-replay service is implicit when data contains monotonically increasing sequence numbers and data integrity is assured. Use of DoD PKI is inherently compliant with this requirement for user and device access. Use of Transport Layer Security (TLS), including application protocols, such as HTTPS and DNSSEC, that use TLS/SSL as the underlying security protocol is also complaint.

Configure the information system to use the hash message authentication code (HMAC) algorithm for authentication services to Kerberos, SSH, web management tool, and any other access method.

Legacy Ids: V-81317; SV-96031

CCI: CCI-001941The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.NIST SP 800-53 Revision 4 :: IA-2 (8)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must disable accounts (individuals, groups, roles, and devices) after 35 days of inactivity.
STIG ID: SRG-APP-000163 **Rule ID:** SV-206466r397498_rule **Vul ID:** V-206466
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to disable accounts (individuals, groups, roles, and devices) after 35 days of inactivity.

If the Central Log Server does not disable accounts (individuals, groups, roles, and devices) after 35 days of inactivity, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend to use external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm. The password policy can be configured to to disable accounts (individuals, groups, roles, and devices) after 35 days of inactivity.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Inactive identifiers pose a risk to systems and applications. Attackers that are able to exploit an inactive identifier can potentially obtain and maintain undetected access to the application. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Applications need to track periods of inactivity and disable application identifiers after 35 days of inactivity.

Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user account is the name of an information system account associated with an individual.

To avoid having to build complex user management capabilities directly into their application, wise developers leverage the underlying OS or other user account management infrastructure (AD, LDAP) that is already in place within the organization and meets organizational user account management requirements.

Legacy Ids:

CCI: CCI-000795The organization manages information system identifiers by disabling the identifier after an organization defined time period of inactivity.NIST SP 800-53 :: IA-4 eNIST SP 800-53A :: IA-4.1 (iii)NIST SP 800-53 Revision 4 :: IA-4 e

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to enforce a minimum 15-character password length.
STIG ID: SRG-APP-000164 **Rule ID:** SV-206467r397501_rule **Vul ID:** V-206467
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to enforce a minimum 15-character password length.

If the Central Log Server is not configured to enforce a minimum 15-character password length, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend to use external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm. The password policy can be configured to enforce a minimum 15-character password length.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic

documentation.

Discussion: The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Legacy Ids: V-81321; SV-96035

CCI: CCI-000205The information system enforces minimum password length.NIST SP 800-53 :: IA-5 (1) (a)NIST SP 800-53A :: IA-5 (1).1 (i)NIST SP 800-53 Revision 4 :: IA-5 (1) (a)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to prohibit password reuse for a minimum of five generations.
STIG ID: SRG-APP-000165 **Rule ID:** SV-206468r397504_rule **Vul ID:** V-206468
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to prohibit password reuse for a minimum of five generations.

If the Central Log Server is not configured to prohibit password reuse for a minimum of five generations, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend to use external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm. The password policy can be

configured to prohibit password reuse for a minimum of five generations. Recommend setting the password history to 24 passwords to align with the DoD STIGs.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

To meet password policy requirements, passwords need to be changed at specific policy-based intervals.

If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed as per policy requirements.

Legacy Ids: V-81335; SV-96049

CCI: CCI-000200The information system prohibits password reuse for the organization defined number of generations.NIST SP 800-53 :: IA-5 (1) (e)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (e)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to enforce password complexity by requiring that at least one upper-case character be used.
STIG ID: SRG-APP-000166 **Rule ID:** SV-206469r397507_rule **Vul ID:** V-206469
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to enforce password complexity by requiring that at least one upper-case character be used.

If the Central Log Server is not configured to enforce password complexity by requiring that at least one upper-case character be used, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend to use external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm. The password complexity policy can be enabled to require passwords to contain at least three of the four types of characters (numbers, upper- and lower-case letters, and special characters) and prevents the inclusion of usernames or parts of usernames.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password is, the greater the number of possible combinations that need to be tested before the password is compromised.

Legacy Ids: V-81337; SV-96051

CCI: CCI-000192The information system enforces password complexity by the minimum number of upper case characters used.NIST SP 800-53 :: IA-5 (1) (a)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (a)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to enforce password complexity by requiring that at least one lower-case character be used.
STIG ID: SRG-APP-000167 **Rule ID:** SV-206470r397510_rule **Vul ID:** V-206470
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to enforce password complexity by requiring that at least one lower-case character be used.

If the Central Log Server is not configured to enforce password complexity by requiring that

at least one lower-case character be used, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend to use external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm. The password complexity policy can be enabled to require passwords to contain at least three of the four types of characters (numbers, upper- and lower-case letters, and special characters) and prevents the inclusion of usernames or parts of usernames.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Legacy Ids: V-81339; SV-96053

CCI: CCI-000193The information system enforces password complexity by the minimum number of lower case characters used.NIST SP 800-53 :: IA-5 (1) (a)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (a)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to enforce password complexity by requiring that at least one numeric character be used.
STIG ID: SRG-APP-000168 **Rule ID:** SV-206471r397513_rule **Vul ID:** V-206471
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to enforce password complexity by requiring that at least one numeric character be used.

If the Central Log Server is not configured to enforce password complexity by requiring that at least one numeric character be used, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend to use external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm. The password complexity policy can be enabled to require passwords to contain at least three of the four types of characters (numbers, upper- and lower-case letters, and special characters) and prevents the inclusion of usernames or parts of usernames.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Legacy Ids: V-81345; SV-96059

CCI: CCI-000194The information system enforces password complexity by the minimum number of numeric characters used.NIST SP 800-53 :: IA-5 (1) (a)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (a)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to enforce password complexity by requiring that at least one special character be used.
STIG ID: SRG-APP-000169 **Rule ID:** SV-206472r397516_rule **Vul ID:** V-206472
Severity: CAT III

Documentable: No

Check Content:

Examine the configuration.

Verify the Central Log Server is configured to enforce password complexity by requiring that at least one special character be used.

If the Central Log Server is not configured to enforce password complexity by requiring that at least one special character be used, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend to use external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm. The password complexity policy can be enabled to require passwords to contain at least three of the four types of characters (numbers, upper- and lower-case letters, and special characters) and prevents the inclusion of usernames or parts of usernames.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Use of a complex password helps to increase the time and resources required to

compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor in determining how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Special characters are those characters that are not alphanumeric. Examples include: ~ ! @ # $ % ^ *.

Legacy Ids: V-81349; SV-96063

CCI: CCI-001619The information system enforces password complexity by the minimum number of special characters used.NIST SP 800-53 :: IA-5 (1) (a)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (a)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to require the change of at least 8 of the total number of characters when passwords are changed.
STIG ID: SRG-APP-000170 **Rule ID:** SV-206473r397519_rule **Vul ID:** V-206473
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to enforce password complexity by requiring the change of at least 8 of the total number of characters when passwords are changed.

If the Central Log Server is not configured to require the change of at least 8 of the total number of characters when passwords are changed, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend to use external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm. The password complexity policy can be enabled to require passwords to contain at least three of the four types of characters (numbers, upper- and lower-case letters, and special characters) and prevents the inclusion of usernames or parts of usernames.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If the application allows the user to consecutively reuse extensive portions of passwords, this increases the chances of password compromise by increasing the window of opportunity for attempts at guessing and brute-force attacks.

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. In other words, characters may be the same within the two passwords; however, the positions of the like characters must be different.

Legacy Ids: V-81353; SV-96067

CCI: CCI-000195The information system

CCI: for password-based authentication

CCI: when new passwords are created

CCI: enforces that at least an organization-defined number of characters are changed.NIST

SP 800-53 :: IA-5 (1) (b)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (b)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: For accounts using password authentication, the Central Log Server must be configured to store only cryptographic representations of passwords.
STIG ID: SRG-APP-000171 **Rule ID:** SV-206474r397522_rule **Vul ID:** V-206474
Severity: CAT I

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to store only cryptographic representations of passwords.

If the Central Log Server is not configured to store only cryptographic representations of passwords, this is a finding.

Fix Text:
Step/Recommendation:

1. By default, the passwords are hashed with a salted sha-256 algorithm. A different hashing algorithm can be used by changing the xpack.security.authc.password_hashing.algorithm setting in the elasticsearch.yml.

Reference:

a. User cache and password hash algorithms:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html#hashing-settings

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Passwords need to be protected at all times, and encryption is the standard

method for protecting passwords. If passwords are not encrypted, they can be plainly read and easily compromised. Use of passwords for authentication is intended only for limited situations and should not be used as a replacement for two-factor CAC-enabled authentication.

Examples of situations where a user ID and password might be used include:

- When the user does not use a CAC and is not a current DoD employee, member of the military, or DoD contractor.

- When a user has been officially designated as temporarily unable to present a CAC for some reason (lost, damaged, not yet issued, broken card reader) (i.e., Temporary Exception User) and to satisfy urgent organizational needs must be temporarily permitted to use user ID/password authentication until the problem with CAC use has been remedied.

- When the application is publicly available and or hosting publicly releasable data requiring some degree of need-to-know protection.

If the password is already encrypted and not a plaintext password, this meets this requirement. Implementation of this requirement requires configuration of a FIPS-approved cipher block algorithm and block cipher modes for encryption. This method uses a one-way hashing encryption algorithm with a salt value to validate a user's password without having to store the actual password. Performance and time required to access are factors that must be considered, and the one-way hash is the most feasible means of securing the password and providing an acceptable measure of password security.

Verifying the user knows a password is performed using a password verifier. In its simplest form, a password verifier is a computational function that is capable of creating a hash of a password and determining if the value provided by the user matches the hash. A more secure version of verifying a user knowing a password is to store the result of an iterating hash function and a large random salt value as follows:

H0 = H(pwd, H(salt))
Hn = H(Hn-1,H(salt))

In the above, "n" is a cryptographically-strong random [*3] number. "Hn" is stored along with the salt. When the application wishes to verify that the user knows a password, it simply repeats the process and compares "Hn" with the stored "Hn". A salt is essentially a fixed-length cryptographically strong random value.

Another method is using a keyed-hash message authentication code (HMAC). HMAC calculates a message authentication code via a cryptographic hash function used in conjunction with an encryption key. The key must be protected as with any private key.

Legacy Ids: V-81283; SV-95997

CCI: CCI-000196The information system

CCI: for password-based authentication

CCI: stores only encrypted representations of passwords.NIST SP 800-53 :: IA-5 (1) (c)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (c)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: For accounts using password authentication, the Central Log Server must use FIPS-validated SHA-1 or later protocol to protect the integrity of the password authentication process.
STIG ID: SRG-APP-000172 **Rule ID:** SV-206475r397525_rule **Vul ID:** V-206475
Severity: CAT I

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to use FIPS-validated SHA-1 or later protocol to protect the integrity of the password authentication process.

If the Central Log Server is not configured to use FIPS-validated SHA-1 or later protocol to protect the integrity of the password authentication process, this is a finding.

Fix Text:
Steps/Recommendation:

1. By default, the passwords are hashed with a salted sha-256 algorithm. A different hashing algorithm can be used by changing the xpack.security.authc.password_hashing.algorithm setting in the elasticsearch.yml.

2. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

3. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

4. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see

The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

5. Recommend to use external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm.

6. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. User cache and password hash algorithms:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html#hashing-settings
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
d. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
e. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html

m. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
n. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
o. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
p. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
q. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
r. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
s. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
t. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

The information system must specify the hash algorithm used for authenticating passwords. Implementation of this requirement requires configuration of FIPS-approved cipher block algorithm and block cipher modes for encryption.

This requirement applies to all accounts, including authentication server; Authorization, Authentication, and Accounting (AAA); and local accounts such as the root account and the account of last resort.

This requirement only applies to components where this is specific to the function of the device (e.g., TLS VPN or ALG). This does not apply to authentication for the purpose of configuring the device itself (management).

Legacy Ids: V-81285; SV-95999

CCI: CCI-000197The information system

CCI: for password-based authentication

CCI: transmits only encrypted representations of passwords.NIST SP 800-53 :: IA-5 (1) (c)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (c)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to enforce 24 hours/1 day as the minimum password lifetime.
STIG ID: SRG-APP-000173 **Rule ID:** SV-206476r397588_rule **Vul ID:** V-206476
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to enforce 24 hours/1 day as the minimum password lifetime.

If the Central Log Server is not configured to enforce 24 hours/1 day as the minimum password lifetime, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend to use external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm. The password policy can be configured to enforce 24 hours/1 day as the minimum password lifetime.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html

f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Enforcing a minimum password lifetime helps prevent repeated password changes to defeat the password reuse or history enforcement requirement.

Restricting this setting limits the user's ability to change their password. Passwords need to be changed at specific policy based intervals; however, if the application allows the user to immediately and continually change their password, then the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Legacy Ids: V-81355; SV-96069

CCI: CCI-000198The information system enforces minimum password lifetime restrictions.NIST SP 800-53 :: IA-5 (1) (d)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (d)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to enforce a 60-day maximum password lifetime restriction.
STIG ID: SRG-APP-000174 **Rule ID:** SV-206477r397591_rule **Vul ID:** V-206477
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to enforce a 60-day maximum password lifetime

restriction.

If the Central Log Server is not configured to enforce a 60-day maximum password lifetime restriction, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm. The password policy can be configured to enforce a 60-day maximum password lifetime restriction.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed at specific intervals.

One method of minimizing this risk is to use complex passwords and periodically change them. If the application does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the system and/or application passwords could be

compromised.

This requirement does not include emergency administration accounts that are meant for access to the application in case of failure. These accounts are not required to have maximum password lifetime restrictions.

Legacy Ids: V-81359; SV-96073

CCI: CCI-000199The information system enforces maximum password lifetime restrictions.NIST SP 800-53 :: IA-5 (1) (d)NIST SP 800-53A :: IA-5 (1).1 (v)NIST SP 800-53 Revision 4 :: IA-5 (1) (d)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server, when utilizing PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.
STIG ID: SRG-APP-000175 **Rule ID:** SV-206478r397594_rule **Vul ID:** V-206478
Severity: CAT I

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

If the Central Log Server is not configured to validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts.

2. Recommend integrating Elasticsearch with these services to support centralized account management.

3. Recommend using an organizationally maintained certificate authority that has been properly configured which must validate certificates by constructing a certification path

(which includes status information) to an accepted trust anchor.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without path validation, an informed trust decision by the relying party cannot be made when presented with any certificate not already explicitly trusted.

A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC.

When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor; it can be, for example, a Certification Authority (CA). A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

This requirement verifies that a certification path to an accepted trust anchor is used to for certificate validation and that the path includes status information. Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Status information for certification paths includes certificate revocation lists or online certificate status protocol responses. Validation of the certificate status information is out of scope for this requirement.

Legacy Ids: V-81287; SV-96001

CCI: CCI-000185The information system

CCI: for PKI-based authentication validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.NIST SP 800-53 :: IA-5 (2)NIST SP 800-53A :: IA-5 (2).1NIST SP 800-53 Revision 4 :: IA-5 (2) (a)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server, when using PKI-based authentication, must enforce authorized access to the corresponding private key.
STIG ID: SRG-APP-000176 **Rule ID:** SV-206479r397597_rule **Vul ID:** V-206479
Severity: CAT I

Documentable: No

Check Content:
If not using PKI-based authentication this is N/A.

Examine the configuration.

Verify the Central Log Server is configured to enforce authorized access to the corresponding private key when using PKI-based authentication.

If the Central Log Server is not configured to enforce authorized access to the corresponding private key when using PKI-based authentication, this is a finding.

Fix Text:
Steps/Recommendation:

1. Password protection, internode communication secured with Transport Layer Security (TLS), and encrypted connections between Elasticsearch and Kibana are enabled out of the box starting with Elasticsearch 8.0.

2. Encrypt the private key with the elasticsearch-certutil leveraging the --password parameter.

3. Use a certificate issued from an approved DoD PKI Certificate Authority (CA) for both Elasticsearch and Kibana.

4. Disable SSL/TLS versions with non-NSA and non-FIPS approved encryption (i.e. anything less than TLS v1.2):

xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

5. Configure Java to use the Bouncy Castle FIPS 140-2 approved cryptographic provider, see The Legion of the Bouncy Castle - FIPS FAQ and Resources Page.

6. Recommend to use external Identity Provider (IdP) for authentication through Active Directory, LDAPS, SAML or OpenID Connection realm.

7. Once the external IdP is configured, use the Role Mapping API in Elasticsearch to map the group membership in the external system to Roles in Elasticsearch.

Note: Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
b. Secure the Elastic Stack:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/secure-cluster.html#secure-cluster
c. Elasticsearch-certutil:
https://www.elastic.co/guide/en/elasticsearch/reference/current/certutil.html#certutil-parameters
d. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
e. The Legion of the Bouncy Castle - FIPS FAQ and Resources Page:
https://www.bouncycastle.org/fips_faq.html
f. User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
k. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html

l. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
m. Anonymous access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html
n. User authorization:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/authorization.html
o. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
p. Create or update role mappings API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api-put-role-mapping.html
q. Setup Roles and privileges using the APIs (or Kibana UI):
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-api.html
r. To Setup RBAC using Kibana:
https://www.elastic.co/guide/en/kibana/8.0/development-security.html#development-rbac
s. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
t. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If the private key is discovered, an attacker can use the key to authenticate as an authorized user and gain access to the network infrastructure.

The cornerstone of the PKI is the private key used to encrypt or digitally sign information.

If the private key is stolen, this will lead to the compromise of the authentication and non-repudiation gained through PKI because the attacker can use the private key to digitally sign documents and pretend to be the authorized user.

Both the holders of a digital certificate and the issuing authority must protect the computers, storage devices, or whatever they use to keep the private keys.

Legacy Ids: V-81289; SV-96003

CCI: CCI-000186The information system

CCI: for PKI-based authentication enforces authorized access to the corresponding private

key.NIST SP 800-53 :: IA-5 (2)NIST SP 800-53A :: IA-5 (2).1NIST SP 800-53 Revision 4 :: IA-5 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must map the authenticated identity to the individual user or group account for PKI-based authentication.
STIG ID: SRG-APP-000177 **Rule ID:** SV-206480r397600_rule **Vul ID:** V-206480
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to map the authenticated identity to the individual user or group account for PKI-based authentication.

If the Central Log Server is not configured to map the authenticated identity to the individual user or group account for PKI-based authentication, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm.

2. Configure Elasticsearch to use Public Key Infrastructure (PKI) certificates to authenticate users. In this scenario, clients connecting directly to Elasticsearch must present X.509 certificates. For more information, see https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html.

References:

a. FIPS-140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
b. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
d. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
e. PKI User Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
f. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
g. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.

Legacy Ids: V-81363; SV-96077

CCI: CCI-000187The information system

CCI: for PKI-based authentication

CCI: maps the authenticated identity to the account of the individual or group.NIST SP 800-53 :: IA-5 (2)NIST SP 800-53A :: IA-5 (2).1NIST SP 800-53 Revision 4 :: IA-5 (2) (c)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must obfuscate authentication information during the authentication process so that the authentication is not visible.
STIG ID: SRG-APP-000178 **Rule ID:** SV-206481r397603_rule **Vul ID:** V-206481
Severity: CAT I

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to obfuscate authentication information during the authentication process so that the authentication is not visible.

If the Central Log Server is not configured to obfuscate authentication information during the authentication process so that the authentication is not visible, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch provides access via API. Credentials are not visible when using the API and TLS.
2. The Kibana web interface displays asterisks when a user types in a password to obfuscate authentication information during the authentication process so that the authentication is not visible.
3. An additional recommendation is to use tools to interact with the API that do not echo back the password the user writes.

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: To prevent the compromise of authentication information such as passwords during the authentication process, the feedback from the information system must not provide any information that would allow an unauthorized user to compromise the authentication mechanism.

Obfuscation of user-provided information when typed into the system is a method used in addressing this risk.

For example, displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

Legacy Ids: V-81291; SV-96005

CCI: CCI-000206The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.NIST SP 800-53 :: IA-6NIST SP 800-53A :: IA-6.1NIST SP 800-53 Revision 4 :: IA-6

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must use FIPS-validated SHA-1 or higher hash function

to protect the integrity of keyed-hash message authentication code (HMAC), Key Derivation Functions (KDFs), Random Bit Generation, hash-only applications, and digital signature verification (legacy use only).
STIG ID: SRG-APP-000179 **Rule ID:** SV-206482r397606_rule **Vul ID:** V-206482
Severity: CAT I

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to use FIPS-validated SHA-1 or higher hash function to protect the integrity of keyed-hash message authentication code (HMAC), Key Derivation Functions (KDFs), Random Bit Generation, hash-only applications, and digital signature verification (legacy use only).

If the Central Log Server is not configured to use FIPS-validated SHA-1 or higher hash function to protect the integrity of keyed-hash message authentication code (HMAC), Key Derivation Functions (KDFs), Random Bit Generation, hash-only applications, and digital signature verification (legacy use only), this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch uses hashing algorithms compliant with this control out of the box, so no additional configuration is needed.

Reference:

a. Security settings in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

To protect the integrity of the authenticator and authentication mechanism used for the cryptographic module used by the Central Log Server must be configured to use one of the

following hash functions for hashing the password or other authenticator in accordance with SP 800-131Ar1: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256, SHA3-384, and SHA3-512.

Applications also include HMAC, KDFs, Random Bit Generation, and hash-only applications (e.g., hashing passwords and using SHA-1 or higher to compute a checksum). For digital signature verification, SP800-131Ar1 allows SHA-1 for legacy use where needed.

Legacy Ids: V-81295; SV-96009

CCI: CCI-000803The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws

CCI: Executive Orders

CCI: directives

CCI: policies

CCI: regulations

CCI: standards

CCI: and guidance for such authentication.NIST SP 800-53 :: IA-7NIST SP 800-53A :: IA-7.1NIST SP 800-53 Revision 4 :: IA-7

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to perform audit reduction that supports on-demand reporting requirements.
STIG ID: SRG-APP-000181 **Rule ID:** SV-206483r397612_rule **Vul ID:** V-206483
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the system is configured to perform audit reduction that supports on-demand reporting requirements.

If the Central Log Server is not configured to perform audit reduction that supports on-demand reporting requirements, this is a finding.

Fix Text:
Steps/Recommendation:

1. Utilize the Elasticsearch APIs to perform on-demand reporting.

2. Recommend usage of Kibana UI and Beats dashboards for a more robust user experience.

References:

a. Search:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/search-search.html
b. Index and search analysis:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/analysis-index-search-time.html
c. Kibana Query: https://www.elastic.co/guide/en/kibana/8.0/kuery-query.html
d. Kibana Dashboards 8.0: https://www.elastic.co/guide/en/kibana/8.0/dashboard.html
r. Kibana Reporting 8.0:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The ability to generate on-demand reports, including after the audit data has been subjected to audit reduction, greatly facilitates the organization's ability to generate incident reports as needed to better handle larger-scale or more complex security incidents.

Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. The report generation capability provided by the application must support on-demand (i.e., customizable, ad hoc, and as-needed) reports.

This requirement is specific to applications with audit reduction capabilities; however, applications need to support on-demand audit review and analysis.

Legacy Ids: V-81129; SV-95843

CCI: CCI-001876The information system provides an audit reduction capability that supports on-demand reporting requirements.NIST SP 800-53 Revision 4 :: AU-7 a

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security

Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: For devices and hosts within its scope of coverage, the Central Log Server must be configured to notify the System Administrator (SA) and Information System Security Officer (ISSO) when account modification events are received.
STIG ID: SRG-APP-000292 **Rule ID:** SV-206484r399514_rule **Vul ID:** V-206484
Severity: CAT III

Documentable: No

Check Content:
Note: This is not applicable (NA) if notifications are performed by another device.

Examine the configuration.

Verify the Central Log Server is configured to notify the SA and ISSO when account modification events are received for all devices and hosts within its scope of coverage.

If the Central Log Server is not configured to notify the SA and ISSO when account modification events are received for all devices and hosts within its scope of coverage, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend configuring Alerts to provide near real-time notification of matching event criteria.

2. Recommend using SIEM Detection Engine and Machine Learning jobs in combination with Alerts to provide robust coverage of desired event criteria.

References:

a. Alerting on cluster and index events:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
b. Kibana Dashboards 8.0: https://www.elastic.co/guide/en/kibana/8.0/dashboard.html
c. Kibana Reporting 8.0:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
d. Kibana Machine Learning 8.0:https://www.elastic.co/guide/en/kibana/8.0/xpack-ml.html
e. Kibana Detections 7.8:
https://www.elastic.co/guide/en/siem/guide/7.8/detection-engine-overview.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and

guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: When application accounts are modified, user accessibility is affected. Accounts are used for identifying individual users or for identifying the application processes themselves. Sending notification of account modification events to the SA and ISSO is one method for mitigating this risk. Such a function greatly reduces the risk that application accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

Notification may be configured to be sent by the device, SNMP server, or the Central Log Server. The best practice is for these notifications to be sent by a robust events management server.

Legacy Ids: V-81131; SV-95845

CCI: CCI-001684The information system notifies organization-defined personnel or roles for account modification actions.NIST SP 800-53 :: AC-2 (4)NIST SP 800-53A :: AC-2 (4).1 (i&ii)NIST SP 800-53 Revision 4 :: AC-2 (4)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: For devices and hosts within its scope of coverage, the Central Log Server must notify the System Administrator (SA) and Information System Security Officer (ISSO) when events indicating account disabling actions are received.
STIG ID: SRG-APP-000293 **Rule ID:** SV-206485r399517_rule **Vul ID:** V-206485
Severity: CAT III

Documentable: No

Check Content:
Note: This is not applicable (NA) if notifications are performed by another device.

Examine the configuration.

Verify the Central Log Server is configured to notify the SA and ISSO when events indicating account disabling actions are received for all devices and hosts within its scope of coverage.

If the Central Log Server does not notify the SA and ISSO when events indicating account disabling actions are received, this is a finding.

Fix Text:

Steps/Recommendation:

1. Recommend configuring Alerts to provide near real-time notification of matching event criteria.

2. Recommend using SIEM Detection Engine and Machine Learning jobs in combination with Alerts to provide robust coverage of desired event criteria.

References:

a. Alerting on cluster and index events:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
b. Kibana Dashboards 8.0: https://www.elastic.co/guide/en/kibana/8.0/dashboard.html
c. Kibana Reporting 8.0:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
d. Kibana Machine Learning 8.0:https://www.elastic.co/guide/en/kibana/8.0/xpack-ml.html
e. Kibana Detections 7.8:
https://www.elastic.co/guide/en/siem/guide/7.8/detection-engine-overview.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion:

a. The Elastic Stack can be configured to notify the System Administrator (SA) and Information System Security Officer (ISSO) when events indicating account disabling actions are received by using a combination of Rules (Detection Engine), Machine Learning and Alerting.
b. This configuration is typically performed via the Kibana user interface.
c. A Watch is constructed from four simple building blocks:
- Schedule: A schedule for running a query and checking the condition.
- Query: The query to run as input to the condition, which can detect account modifications for user or application. Watches support the full Elasticsearch query language, including aggregations.
- Condition: A condition that determines whether or not to execute the actions. You can use simple conditions (always true), also scripting for more sophisticated scenarios for account modifications.
- Actions: Setup notification the System Administrator (SA) and Information System Security Officer (ISSO) when events indicating account disabling actions are received.

Discussion: When application accounts are disabled, user accessibility is affected. Accounts

are used for identifying individual users or for identifying the application processes themselves. Sending notification of account disabling events to the SA and ISSO is one method for mitigating this risk. Such a function greatly reduces the risk that application accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

Notification may be configured to be sent by the device, SNMP server, or Central Log Server. The best practice is for these notifications to be sent by a robust events management server.

Legacy Ids: V-81133; SV-95847

CCI: CCI-001685The information system notifies organization-defined personnel or roles for account disabling actions.NIST SP 800-53 :: AC-2 (4)NIST SP 800-53A :: AC-2 (4).1 (i&ii)NIST SP 800-53 Revision 4 :: AC-2 (4)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: For devices and hosts within its scope of coverage, the Central Log Server must notify the System Administrator (SA) and Information System Security Officer (ISSO) when events indicating account removal actions are received.
STIG ID: SRG-APP-000294 **Rule ID:** SV-206486r399520_rule **Vul ID:** V-206486
Severity: CAT III

Documentable: No

Check Content:
Note: This is not applicable (NA) if notifications are performed by another device.

Examine the configuration.

Verify the Central Log Server is configured to notify the SA and ISSO when events indicating account removal actions are received for all devices and hosts within its scope of coverage.

If the Central Log Server does not notify the SA and ISSO when events indicating account removal actions are received, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend configuring Alerts to provide near real-time notification of matching event criteria.

2. Recommend using SIEM Detection Engine and Machine Learning jobs in combination

with Alerts to provide robust coverage of desired event criteria.

References:

a. Alerting on cluster and index events:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
b. Kibana Dashboards 8.0: https://www.elastic.co/guide/en/kibana/8.0/dashboard.html
c. Kibana Reporting 8.0:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
d. Kibana Machine Learning 8.0:https://www.elastic.co/guide/en/kibana/8.0/xpack-ml.html
e. Kibana Detections 7.8:
https://www.elastic.co/guide/en/siem/guide/7.8/detection-engine-overview.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: When application accounts are removed, user accessibility is affected. Accounts are used for identifying users or for identifying the application processes themselves. Sending notification of account removal events to the SA and ISSO is one method for mitigating this risk. Such a function greatly reduces the risk that application accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

Notification may be configured to be sent by the device, SNMP server, or Central Log Server. The best practice is for these notifications to be sent by a robust events management server.

Legacy Ids: V-81135; SV-95849

CCI: CCI-001686The information system notifies organization-defined personnel or roles for account removal actions.NIST SP 800-53 :: AC-2 (4)NIST SP 800-53A :: AC-2 (4).1 (i&ii)NIST SP 800-53 Revision 4 :: AC-2 (4)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured for centralized management of the events repository for the purposes of configuration, analysis, and reporting.
STIG ID: SRG-APP-000356 **Rule ID:** SV-206490r401227_rule **Vul ID:** V-206490
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify that centralized management of the events repository is enabled and configured for all hosts and devices within the scope of coverage.

If the Central Log Server is not enabled to allow centralized management of the events repository for the purposes of configuration, analysis, and reporting, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend usage of Kibana UI for a more robust user experience.

References:

a. Kibana Dashboards: https://www.elastic.co/guide/en/kibana/8.0/dashboard.html
b. Kibana Reporting:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html

Elastic Stack 8.0
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If the application is not configured to centrally manage the content captured in the log records, identification, troubleshooting, and correlation of suspicious behavior would be difficult and could lead to a delayed or incomplete analysis of an ongoing attack.

The content captured in log records must be managed from a central location (necessitating automation). Centralized management of log records and logs provides for efficiency in maintenance and management of records, as well as the backup and archiving of those records. Application components requiring centralized audit log management must be configured to support centralized management.

Legacy Ids: V-81143; SV-95857

CCI: CCI-001844The information system provides centralized management and configuration of the content to be captured in audit records generated by organization-defined information system components.NIST SP 800-53 Revision 4 :: AU-3 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to off-load log records onto a different system or media than the system being audited.
STIG ID: SRG-APP-000358 **Rule ID:** SV-206491r399880_rule **Vul ID:** V-206491
Severity: CAT II

Documentable: No

Check Content:
Note: This is not applicable (NA) if an external application or operating system manages this function.

Examine the configuration.

Verify the system is configured to off-load log records onto a different system or media than the system being audited.

If the Central Log Server is not configured to off-load log records onto a different system or media than the system being audited, this is a finding.

Fix Text:
Steps/Recommendation:

1. This is an organizational requirement.

2. Configure the Elasticsearch nodes to backup or replicate/off-load log records onto a different system or media than the system being audited.

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity. Although this may be part of the operating system function, for the enterprise events management system, this is most often a function managed through the application since it is

a critical function and requires the use of a large amount of external storage.

Legacy Ids: V-81145; SV-95859

CCI: CCI-001851The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.NIST SP 800-53 Revision 4 :: AU-4 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to send an immediate alert to the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when allocated log record storage volume reaches 75 percent of the repository maximum log record storage capacity.
STIG ID: SRG-APP-000359 **Rule ID:** SV-206492r399883_rule **Vul ID:** V-206492
Severity: CAT III

Documentable: No

Check Content:
Note: This is not applicable (NA) if an external application or operating system manages this function.

Examine the configuration.

Verify the system is configured to send an immediate warning to the SA and ISSO (at a minimum) when allocated log record storage volume reaches 75 percent of the repository's maximum log record storage capacity.

If the Central Log Server is not configured to send an immediate alert to the SA and ISSO (at a minimum) when allocated log record storage volume reaches 75 percent of repository maximum log record storage capacity, this is a finding.

Fix Text:
Steps/Recommendation:

1. The Elastic Stack API can be used to setup Alerts. However, it is recommended to use the Kibana UI for a better user experience.

2. Recommend using Machine Learning to identify anomalies in your environment to reduce the manual steps required to create individual Alerts.

3. Metricbeat is the recommended method for collecting and shipping monitoring data to a

monitoring cluster.

4. If you have previously configured internal collection, you should migrate to using Metricbeat collection. Use either Metricbeat collection or internal collection; do not use both.

5. After you collect monitoring data for one or more products in the Elastic Stack, you can configure Kibana to retrieve that information and display it in on the Stack Monitoring page.

6. At a minimum, you must have monitoring data for the Elasticsearch production cluster. Once that data exists, Kibana can display monitoring data for other products in the cluster.

7. Identify where to retrieve monitoring data from the cluster that contains the monitoring data is referred to as the monitoring cluster. If the monitoring data is stored on a dedicated monitoring cluster, it is accessible even when the cluster you're monitoring is not. If you have at least a gold license, you can send data from multiple clusters to the same monitoring cluster and view them all through the same instance of Kibana.

By default, data is retrieved from the cluster specified in the elasticsearch.hosts value in the kibana.yml file. If you want to retrieve it from a different cluster, set xpack.monitoring.elasticsearch.hosts.

8. If the Elastic security features are enabled on the monitoring cluster, you must provide a user ID and password so Kibana can retrieve the data.
   a. Create a user that has the monitoring_user built-in role on the monitoring cluster.
   b. Add the xpack.monitoring.elasticsearch.username and xpack.monitoring.elasticsearch.password settings in the kibana.yml file. If these settings are omitted, Kibana uses the elasticsearch.username and elasticsearch.password setting values.

9. Configure Kibana to encrypt communications between the Kibana server and the monitoring cluster.

10. If the Elastic security features are enabled on the Kibana server, only users that have the authority to access Kibana indices and to read the monitoring indices can use the monitoring dashboards.
   a. These users must exist on the monitoring cluster. If you are accessing a remote monitoring cluster, you must use credentials that are valid on both the Kibana server and the monitoring cluster.
   b. Create users that have the monitoring_user and kibana_admin built-in roles.

11. Open Kibana in your web browser.
By default, if you are running Kibana locally, go to http://localhost:5601/.
If the Elastic security features are enabled, log in.

12. In the side navigation, click Stack Monitoring.
If data collection is disabled, you are prompted to turn on data collection. If Elasticsearch security features are enabled, you must have manage cluster privileges to turn on data

collection.

NOTE: If you are using a separate monitoring cluster, you do not need to turn on data collection. The dashboards appear when there is data in the monitoring cluster.

You'll see cluster alerts that require your attention and a summary of the available monitoring metrics for Elasticsearch, Logstash, Kibana, and Beats. To view additional information, click the Overview, Nodes, Indices, or Instances links.

Elasticsearch offers cat indices API for querying the size of indices in a cluster.
Use the cat indices API to get the following information for each index in a cluster:
- Shard count
- Document count
- Deleted document count
- Primary store size
- Total store size of all shards, including shard replicas

These metrics are retrieved directly from Lucene, which Elasticsearch uses internally to power indexing and search. As a result, all document counts include hidden nested documents.

To get an accurate count of Elasticsearch documents, use the cat count or count APIs.

References:

a. Configuring monitoring in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/configuring-monitoring.html
b. Viewing monitoring data in Kibana:
https://www.elastic.co/guide/en/kibana/8.0/monitoring-data.html
c. Alerting on cluster and index events:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
d. cat indices API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/cat-indices.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If security personnel are not notified immediately upon storage volume utilization reaching 75 percent, they are unable to plan for storage capacity expansion.

Although this may be part of the operating system function, for the enterprise events

management system, this is most often a function managed through the application since it is a critical function and requires the use of a large amount of external storage.

Legacy Ids: V-81147; SV-95861

CCI: CCI-001855The information system provides a warning to organization-defined personnel

CCI: roles

CCI: and/or locations within organization-defined time period when allocated audit record storage volume reaches organization-defined percentage of repository maximum audit record storage capacity.NIST SP 800-53 Revision 4 :: AU-5 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: For the host and devices within its scope of coverage, the Central Log Server must be configured to send a real-time alert to the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) of all audit failure events, such as loss of communications with hosts and devices, or if log records are no longer being received.
STIG ID: SRG-APP-000360 **Rule ID:** SV-206493r399886_rule **Vul ID:** V-206493
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the system is configured to send an alert to the SA and ISSO, within seconds or less, when communication is lost with any host or device within the scope of coverage that may indicate an audit failure.

Verify the system is configured to send an alert if hosts and devices stop sending log records to the Central Log Server.

If the Central Log Server is not configured to send a real-time alert to the SA and ISSO (at a minimum) of all audit failure events, this is a finding.

Fix Text:
Step/Recommendation:

1.The Elastic Stack can be configured to notify appropriate personnel using a combination of

Rules (Detection Engine), Machine Learning and Alerting. This configuration is typically performed via the Kibana user interface. Elasticsearch's combination of Rules (Detection Engine), Machine Learning and Alerting can be configured to send an immediate alert to the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) of all audit failure events, such as loss of communications with hosts and devices, or if log records are no longer being received.

References:

a. Alerting on cluster and index events:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
b. Kibana Dashboards 8.0: https://www.elastic.co/guide/en/kibana/8.0/dashboard.html
c. Kibana Reporting 8.0:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
d. Kibana Machine Learning 8.0:https://www.elastic.co/guide/en/kibana/8.0/xpack-ml.html
e. Kibana Detections 7.8:
https://www.elastic.co/guide/en/siem/guide/7.8/detection-engine-overview.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without a real-time alert, security personnel may be unaware of an impending failure of the audit function and application operation may be adversely affected.

Alerts provide organizations with urgent messages. Real-time alerts provide these messages immediately (i.e., the time from event detection to alert occurs in seconds or less). User-configurable controls on the Central Log Server help avoid generating excessive numbers of alert messages. Define realistic alerting limits and thresholds to avoid creating excessive numbers of alerts for noncritical events.

This requirement must be mapped to the severity levels used by the system to denote a failure, active attack, attack involving multiple systems, and other critical notifications, at a minimum. However, note that the IDS/IDPS and other monitoring systems may already be configured for direct notification of many types of critical security alerts.

Legacy Ids: V-81149; SV-95863

CCI: CCI-001858The information system provides a real-time alert in organization-defined real-time period to organization-defined personnel

CCI: roles

CCI: and/or locations when organization-defined audit failure events requiring real-time alerts occur.NIST SP 800-53 Revision 4 :: AU-5 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to send an immediate alert to the System Administrator (SA) or Information System Security Officer (ISSO) if communication with the host and devices within its scope of coverage is lost.
STIG ID: SRG-APP-000361 **Rule ID:** SV-206494r399889_rule **Vul ID:** V-206494
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the system is configured to send an immediate alert to the SA or ISSO if communication with the host and devices within its scope of coverage is lost.

If the Central Log Server is not configured to send an immediate alert to the SA or ISSO if communication with the host and devices within its scope of coverage is lost, this is a finding.

Fix Text:
Step/Recommendation:

1. The Elastic Stack can be configured to notify appropriate personnel using a combination of Machine Learning and Watcher. This configuration is typically performed via the Kibana user interface. Elasticsearch's combination of Machine Learning and Watcher can be configured to send an immediate alert to the System Administrator (SA) and Information System Security Officer (ISSO) if communication with the host and devices within its scope of coverage is lost.

References:

a. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
b. Kibana Dashboards: https://www.elastic.co/guide/en/kibana/8.0/dashboard.html
c. Kibana Reporting:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
d. Kibana Machine Learning: https://www.elastic.co/guide/en/kibana/8.0/xpack-ml.html

Elastic Stack 8.0
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If the system were to continue processing after audit failure, actions could be taken on the system that could not be tracked and recorded for later forensic analysis. To perform this function, some type of heartbeat configuration with all of the devices and hosts must be configured.

Because of the importance of ensuring mission/business continuity, organizations may determine that the nature of the audit failure is not so severe that it warrants a complete shutdown of the application supporting the core organizational missions/business operations. In those instances, partial application shutdowns or operating in a degraded mode may be viable alternatives.

This requirement applies to each audit data storage repository (i.e., distinct information system component where log records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Legacy Ids: V-81151; SV-95865

CCI: CCI-001861The information system invokes an organization-defined system mode

CCI: in the event of organization-defined audit failures

CCI: unless an alternate audit capability exists.NIST SP 800-53 Revision 4 :: AU-5 (4)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to perform on-demand sorting of log records for events of interest based on the content of organization-defined audit fields within log records.
STIG ID: SRG-APP-000362 **Rule ID:** SV-206495r399892_rule **Vul ID:** V-206495
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the system is configured to perform on-demand sorting of log records for events of interest based on the content of organization-defined audit fields within log records.

If the Central Log Server is not configured to perform on-demand sorting of log records for events of interest based on the content of organization-defined audit fields within log records, this is a finding.

Fix Text:
Steps/Recommendation:

1. The Elastic Stack provides numerous out of the box dashboards via the Kibana user interface to perform on-demand sorting of log records for events of interest based on the content of organization-defined audit fields within log records. Additionally, organizations can create custom dashboards and visualizations.

2. Elasticsearch also offers cat indices API for querying the size of indices in a cluster.
cat indices API

3. Returns high-level information about indices in a cluster.

Request
GET /_cat/indices/<target>
GET /_cat/indices

Description
Use the cat indices API to get the following information for each index in a cluster:
- Shard count
- Document count
- Deleted document count
- Primary store size
- Total store size of all shards, including shard replicas

4. These metrics are retrieved directly from Lucene, which Elasticsearch uses internally to power indexing and search. As a result, all document counts include hidden nested documents.

5. To get an accurate count of Elasticsearch documents, use the cat count or count APIs.

References:

a. Kibana Dashboards: https://www.elastic.co/guide/en/kibana/8.0/dashboard.html
b. Reporting from Kibana:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
c. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
d. Cat Indices API:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/cat-indices.html

e. Fielddata Mapping Parameters:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/text.html#fielddata-mapping-param

Elastic Stack 8.0
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The ability to sort the log records to better view events of interest provides the persons reviewing the logs with the ability to quickly isolate and identify these events without having to review entries that are of little or no consequence to the investigation. Without this capability, forensic investigations are impeded.

This requires applications to be configured to sort log record reports based on organization-defined criteria.

Legacy Ids: V-81153; SV-95867

CCI: CCI-001886The information system provides the capability to sort audit records for events of interest based on the content of organization-defined audit fields within audit records.NIST SP 800-53 Revision 4 :: AU-7 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to perform on-demand searches of log records for events of interest based on the content of organization-defined audit fields within log records.
STIG ID: SRG-APP-000363 **Rule ID:** SV-206496r399895_rule **Vul ID:** V-206496
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server performs on-demand searches of log records for events of interest based on the content of organization-defined audit fields within log records.

If the Central Log Server is not configured to perform on-demand searches of log records for events of interest based on the content of organization-defined audit fields within log records,

this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend using Kibana for log search. The Elastic Stack Kibana user interface can be used to perform to perform on-demand searches of log records for events of interest based on the content of organization-defined audit fields within log records. Additionally, organizations can create custom dashboards and visualizations.

References:

a. Kibana Dashboards: https://www.elastic.co/guide/en/kibana/8.0/dashboard.html
b. Reporting from Kibana:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
c. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html

Elastic Stack 8.0
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The ability to search the log records to better view events of interest provides the persons reviewing the logs with the ability to quickly isolate and identify these events without having to review entries that are of little or no consequence to the investigation. Without this capability, forensic investigations are impeded.

This requires applications to provide the capability to search log record reports based on organization-defined criteria.

Legacy Ids: V-81155; SV-95869

CCI: CCI-001887The information system provides the capability to search audit records for events of interest based on the content of organization-defined audit fields within audit records.NIST SP 800-53 Revision 4 :: AU-7 (2)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to perform audit reduction that supports on-demand audit review and analysis.
STIG ID: SRG-APP-000364 **Rule ID:** SV-206497r399898_rule **Vul ID:** V-206497
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the system performs audit reduction that supports on-demand audit review and analysis.

If the Central Log Server is not configured to perform audit reduction that supports on-demand audit review and analysis, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend using Kibana for log search. The Elastic Stack Kibana user interface supports on-demand audit review and analysis by performing search in the Elasticsearch. Additionally, organizations can create custom dashboards and visualizations.

References:

a. Kibana Dashboards: https://www.elastic.co/guide/en/kibana/8.0/dashboard.html
b. Reporting from Kibana:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
c. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
d. Fielddata Mapping Parameters:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/text.html#fielddata-mapping-param
e. Search: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/search-search.html
f. Index and search analysis:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/analysis-index-search-time.html

Elastic Stack 8.0
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The ability to perform on-demand audit review and analysis, including after the audit data has been subjected to audit reduction, greatly facilitates the organization's ability to generate incident reports as needed to better handle larger-scale or more complex security incidents.

Audit reduction is a technique used to reduce the volume of log records to facilitate a manual

review. Audit reduction does not alter original log records. The report generation capability provided by the application must support on-demand (i.e., customizable, ad hoc, and as-needed) reports.

This requirement is specific to applications with audit reduction capabilities; however, applications need to support on-demand audit review and analysis.

Legacy Ids: V-81157; SV-95871

CCI: CCI-001875The information system provides an audit reduction capability that supports on-demand audit review and analysis.NIST SP 800-53 Revision 4 :: AU-7 a

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to perform audit reduction that supports after-the-fact investigations of security incidents.
STIG ID: SRG-APP-000365 **Rule ID:** SV-206498r399901_rule **Vul ID:** V-206498
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server performs audit reduction that supports after-the-fact investigations of security incidents.

If the Central Log Server is not configured to perform audit reduction that supports after-the-fact investigations of security incidents, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend using Kibana for log search. The Elastic Stack Kibana user interface supports on-demand audit review and analysis by performing search in the Elasticsearch. Additionally, organizations can create custom dashboards and visualizations.

References:

a. Reporting from Kibana:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
b. Fielddata Mapping Parameters:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/text.html#fielddata-mapping-para

m
c. Search: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/search-search.html
d. Index and search analysis:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/analysis-index-search-time.html

Elastic Stack 8.0
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If the audit reduction capability does not support after-the-fact investigations, it is difficult to establish, correlate, and investigate the events leading up to an outage or attack or identify those responses for one. This capability is also required to comply with applicable Federal laws and DoD policies.

Audit reduction capability must support after-the-fact investigations of security incidents either natively or through the use of third-party tools.

This requirement is specific to applications with audit reduction capabilities.

Legacy Ids: V-81159; SV-95873

CCI: CCI-001877The information system provides an audit reduction capability that supports after-the-fact investigations of security incidents.NIST SP 800-53 Revision 4 :: AU-7 a

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to generate on-demand audit review and analysis reports.
STIG ID: SRG-APP-000366 **Rule ID:** SV-206499r399904_rule **Vul ID:** V-206499
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server generates on-demand audit review and analysis reports.

If the Central Log Server is not configured to generate on-demand audit review and analysis reports, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend using the Kibana UI to configure and interact with the Watcher functionality of the Elastic Stack.

References:

a. Reporting from Kibana:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
b. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html

Elastic Stack 8.0
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The report generation capability must support on-demand review and analysis to facilitate the organization's ability to generate incident reports as needed to better handle larger-scale or more complex security incidents.

Report generation must be capable of generating on-demand (i.e., customizable, ad hoc, and as-needed) reports. On-demand reporting allows personnel to report issues more rapidly to more effectively meet reporting requirements. Collecting log data and aggregating it to present the data in a single, consolidated report achieves this objective.

Audit reduction and report generation capabilities do not always reside on the same information system or within the same organizational entities conducting auditing activities. The audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in log records. The report generation capability provided by the information system can generate customizable reports. Time ordering of log records can be a significant issue if the granularity of the timestamp in the record is insufficient.

This requirement is specific to applications with report generation capabilities; however, applications need to support on-demand audit review and analysis.

Legacy Ids: V-81161; SV-95875

CCI: CCI-001878The information system provides a report generation capability that supports on-demand audit review and analysis.NIST SP 800-53 Revision 4 :: AU-7 a

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to generate reports that support on-demand reporting requirements.
STIG ID: SRG-APP-000367 **Rule ID:** SV-206500r399907_rule **Vul ID:** V-206500
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server generates reports that support on-demand reporting requirements.

If the Central Log Server is not configured to generate reports that support on-demand reporting requirements, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend using the Kibana UI to configure and interact with the Watcher functionality of the Elastic Stack.

References:

a. Reporting from Kibana:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
b. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html

Elastic Stack 8.0
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The report generation capability must support on-demand reporting to facilitate the organization's ability to generate incident reports as needed to better handle larger-scale or more complex security incidents

The report generation capability provided by the application must be capable of generating on-demand (i.e., customizable, ad hoc, and as-needed) reports. On-demand reporting allows personnel to report issues more rapidly to more effectively meet reporting requirements.

Collecting log data and aggregating it to present the data in a single, consolidated report achieves this objective.

This requirement is specific to applications with report generation capabilities; however, applications need to support on-demand reporting requirements.

Legacy Ids: V-81163; SV-95877

CCI: CCI-001879The information system provides a report generation capability that supports on-demand reporting requirements.NIST SP 800-53 Revision 4 :: AU-7 a

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to generate reports that support after-the-fact investigations of security incidents.
STIG ID: SRG-APP-000368 **Rule ID:** SV-206501r399910_rule **Vul ID:** V-206501
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server generates reports that support after-the-fact investigations of security incidents.

If the Central Log Server is not configured to generate reports that support after-the-fact investigations of security incidents, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend using the Kibana UI to configure and interact with the Watcher functionality of the Elastic Stack.

References:

a. Kibana Reporting 8.0:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
b. Watcher: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html

Elastic Stack 8.0
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation

links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If the report generation capability does not support after-the-fact investigations, it is difficult to establish, correlate, and investigate the events leading up to an outage or attack or identify those responses for one. This capability is also required to comply with applicable Federal laws and DoD policies.

The report generation capability must support after-the-fact investigations of security incidents either natively or through the use of third-party tools.

This requirement is specific to applications with report generation capabilities; however, applications need to support on-demand reporting requirements.

Legacy Ids: V-81165; SV-95879

CCI: CCI-001880The information system provides a report generation capability that supports after-the-fact investigations of security incidents.NIST SP 800-53 Revision 4 :: AU-7 a

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to perform audit reduction that does not alter original content or time ordering of log records.
STIG ID: SRG-APP-000369 **Rule ID:** SV-206502r399913_rule **Vul ID:** V-206502
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server performs audit reduction that does not alter original content or time ordering of log records.

If the Central Log Server is not configured to perform audit reduction that does not alter original content or time ordering of log records, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend using the Kibana UI to perform audit reduction analysis. This analysis will not alter the original data or order of the records.

References:

a. Kibana Reporting 8.0:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
b. Fielddata Mapping Parameter:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/text.html#fielddata-mapping-param
c. Search: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/search-search.html
d. Index and search analysis:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/analysis-index-search-time.html

Elastic Stack 8.0
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If the audit reduction capability alters the content or time ordering of log records, the integrity of the log records is compromised, and the records are no longer usable for forensic analysis. Time ordering refers to the chronological organization of records based on time stamps. The degree of time stamp precision can affect this.

Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts.

This requirement is specific to applications with audit reduction capabilities; however, applications need to support on-demand audit review and analysis.

Legacy Ids: V-81167; SV-95881

CCI: CCI-001881The information system provides an audit reduction capability that does not alter original content or time ordering of audit records.NIST SP 800-53 Revision 4 :: AU-7 b

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to generate reports that do not alter original content or time ordering of log records.
STIG ID: SRG-APP-000370 **Rule ID:** SV-206503r399916_rule **Vul ID:** V-206503
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server generates reports that do not alter original content or time ordering of log records.

If the Central Log Server is not configured to generate reports that do not alter original content or time ordering of log records, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using the Kibana UI to generate reports that do not alter original content or time ordering of log records.

2. Recommend configuring Role Based Access Control or Attribute Based Access Control to define which users, if any, are allowed to modify data.

References:

a. Kibana Reporting 8.0:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
b. Fielddata Mapping Parameter:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/text.html#fielddata-mapping-param
c. Search: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/search-search.html
d. Index and search analysis:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/analysis-index-search-time.html

Elastic Stack 8.0
This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If the audit report generation capability alters the original content or time ordering of log records, the integrity of the log records is compromised, and the records are no longer usable for forensic analysis. Time ordering refers to the chronological organization of records based on time stamps. The degree of time stamp precision can affect this.

The report generation capability provided by the application can generate customizable reports.

This requirement is specific to applications with audit reduction capabilities; however, applications need to support on-demand audit review and analysis.

Legacy Ids: V-81169; SV-95883

CCI: CCI-001882The information system provides a report generation capability that does not alter original content or time ordering of audit records.NIST SP 800-53 Revision 4 :: AU-7 b

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: Upon receipt of the log record from hosts and devices, the Central Log Server must be configured to record time stamps of the time of receipt that can be mapped to Coordinated Universal Time (UTC).
STIG ID: SRG-APP-000374 **Rule ID:** SV-206504r399928_rule **Vul ID:** V-206504
Severity: CAT III

Documentable: No

Check Content:
Examine the log records stored on the events server.

Verify the Central Log Server records time stamps of the time the record was received from the host or device.

Verify the time stamp is mapped to UTC.

If the Central Log Server is not configured to record time stamps of the time the record was received or the time stamp is not mapped to UTC, this is a finding.

Fix Text:
Step/Recommendation:

1. Run the following command in the test lab:
You can use the time_zone parameter to convert date values to UTC using a UTC offset. For example:

```
curl -X GET "localhost:9200/_search?pretty" -H 'Content-Type: application/json' -d'
{
  "query": {
    "range": {
      "timestamp": {
```

```
        "time_zone": "+01:00",
        "gte": "2020-01-01T00:00:00",
        "lte": "now"
      }
    }
  }
}
'
```

time_zone: Indicates that date values use a UTC offset of +01:00.

gte: With a UTC offset of +01:00, Elasticsearch converts this date to 2019-12-31T23:00:00 UTC.

The time_zone parameter does not affect the now value.

Range query

Returns documents that contain terms within a provided range.
time_zone

(Optional, string) Coordinated Universal Time (UTC) offset or IANA time zone used to convert date values in the query to UTC.

Valid values are ISO 8601 UTC offsets, such as +01:00 or -08:00, and IANA time zone IDs, such as America/Los_Angeles.

For an example query using the time_zone parameter, see Time zone in range queries.

The time_zone parameter does not affect the date math value of now. now is always the current system time in UTC.

However, the time_zone parameter does convert dates calculated using now and date math rounding. For example, the time_zone parameter will convert a value of now/d.

Reference:

a. Range query:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/query-dsl-range-query.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic

documentation.

Discussion: If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis.

Time stamps generated by the application include date and time. Time is commonly expressed in UTC, a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

Legacy Ids: V-81171; SV-95885

CCI: CCI-001890The information system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).NIST SP 800-53 Revision 4 :: AU-8 b

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to record time stamps for when log records are received by the log server that meet a granularity of one second for a minimum degree of precision.
STIG ID: SRG-APP-000375 **Rule ID:** SV-206505r399931_rule **Vul ID:** V-206505
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server records time stamps for when log records are received by the log server that meet a granularity of one second for a minimum degree of precision.

If the Central Log Server is not configured to record time stamps for when log records are received by the log server that meet a granularity of one second for a minimum degree of precision, this is a finding.

Fix Text:
Steps/Recommendation:

1. In JSON, dates are represented as strings. Elasticsearch uses a set of preconfigured formats to recognize and parse these strings into a long value representing milliseconds-since-the-epoch in UTC.

2. Elastic Stack's UI (Kibana) can also be utilized to search records that meet a granularity of

one second for a minimum degree of precision.

Reference:

a. Mapping date format:
https://www.elastic.co/guide/en/elasticsearch/reference/current/mapping-date-format.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without sufficient granularity of time stamps, it is not possible to adequately determine the chronological order of records.

Time stamps generated by the application include date and time. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks.

Note: The actual configuring and security requirements for NTP is handled in the host OS or NDM STIGs that are also required as part of a Central Log Server review.

Legacy Ids: V-81173; SV-95887

CCI: CCI-001889The information system records time stamps for audit records that meets organization-defined granularity of time measurement.NIST SP 800-53 Revision 4 :: AU-8 b

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to accept the DoD CAC credential to support identity management and personal authentication.
STIG ID: SRG-APP-000391 **Rule ID:** SV-206506r400039_rule **Vul ID:** V-206506
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to accept the DoD CAC credential to support

identity management and personal authentication.

If the Central Log Server cannot be configured to accept the DoD CAC credential to support identity management and personal authentication, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend to use external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm. The password policy can be configured to accept the DoD CAC credential to support identity management and personal authentication.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

DoD has mandated the use of the CAC to support identity management and personal authentication for systems covered under HSPD 12, as well as a primary component of

layered protection for national security systems.

If the application cannot meet this requirement, the risk may be mitigated through use of an authentication server.

Legacy Ids: V-81323; SV-96037

CCI: CCI-001953The information system accepts Personal Identity Verification (PIV) credentials.NIST SP 800-53 Revision 4 :: IA-2 (12)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to electronically verify the DoD CAC credential.
STIG ID: SRG-APP-000392 **Rule ID:** SV-206507r400042_rule **Vul ID:** V-206507
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to accept the DoD CAC credentials to support identity management and personal authentication.

If the Central Log Server cannot be configured to accept the DoD CAC credentials to support identity management and personal authentication, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm. The password policy can be configured to accept the DoD CAC credential to electronically verify the DoD CAC credential.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

DoD has mandated the use of the CAC to support identity management and personal authentication for systems covered under HSPD 12, as well as a primary component of layered protection for national security systems.

Legacy Ids: V-81327; SV-96041

CCI: CCI-001954The information system electronically verifies Personal Identity Verification (PIV) credentials.NIST SP 800-53 Revision 4 :: IA-2 (12)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: For locally created accounts in the application, the Central Log Server must be configured to allow the use of a temporary password for system logons with an immediate change to a permanent password.
STIG ID: SRG-APP-000397 **Rule ID:** SV-206508r400114_rule **Vul ID:** V-206508
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to allow the use of a temporary password for system logons with an immediate change to a permanent password.

If the Central Log Server is not configured to allow the use of a temporary password for system logons with an immediate change to a permanent password, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend using external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm. The password policy can be configured to allow the use of a temporary password for system logons with an immediate change to a permanent password.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without providing this capability, an account may be created without a password. Non-repudiation cannot be guaranteed once an account is created if a user is not forced to

change the temporary password upon initial logon.

Temporary passwords are typically used to allow access to applications when new accounts are created or passwords are changed. It is common practice for administrators to create temporary passwords for user accounts that allow the users to log on, yet force them to change the password once they have successfully authenticated.

The risk can be mitigated by allowing only the account of last resort to be configured locally. This requirement does not apply to that account.

Legacy Ids: V-81331; SV-96045

CCI: CCI-002041The information system allows the use of a temporary password for system logons with an immediate change to a permanent password.NIST SP 800-53 Revision 4 :: IA-5 (1) (f)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to protect the confidentiality and integrity of transmitted information.
STIG ID: SRG-APP-000439 **Rule ID:** SV-206509r400474_rule **Vul ID:** V-206509
Severity: CAT I

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to use transmission protection mechanisms, such as TLS, SSL VPNs, or IPsec along with integrity protections such as FIPS 140-2 validated digital signature and hash function.

If the Central Log Server is not configured to protect the confidentiality and integrity of transmitted information, this is a finding.

Fix Text:
Steps/Recommendation:

1. In elasticsearch.yml
xpack.security.enabled: true
xpack.security.fips_mode.enabled: true

2. Disable SSL/TLS versions with non-NSA approved encryption (i.e. anything less than TLS

v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
 - Azure Classic Discovery Plugin
 - Ingest Attachment Plugin
 - The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
 - The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
b. Security settings in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html#hashing-settings
c. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
d. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without protection of the transmitted information, confidentiality and integrity may be compromised since unprotected communications can be intercepted and either read or altered.

This requirement applies only to those applications that are either distributed or can allow access to data non-locally. Use of this requirement will be limited to situations where the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process. When transmitting data, applications need to leverage transmission protection mechanisms, such as TLS, SSL VPNs, or IPSEC.

Communication paths outside the physical protection of a controlled boundary are exposed to

the possibility of interception and modification. Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Legacy Ids: V-81301; SV-96015

CCI: CCI-002418The information system protects the confidentiality and/or integrity of transmitted information.NIST SP 800-53 Revision 4 :: SC-8

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must implement NIST FIPS-validated cryptography for the following: to provision digital signatures; to generate cryptographic hashes; and/or to protect unclassified information requiring confidentiality and cryptographic protection.
STIG ID: SRG-APP-000514 **Rule ID:** SV-206510r400876_rule **Vul ID:** V-206510
Severity: CAT I

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to implement NIST FIPS-validated cryptography for the following: to provision digital signatures; to generate cryptographic hashes; and/or to protect unclassified information requiring confidentiality and cryptographic protection in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

If the Central Log Server is not configured to implement NIST FIPS-validated cryptography for the following: to provision digital signatures; to generate cryptographic hashes; and/or to protect unclassified information requiring confidentiality and cryptographic protection in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards, this is a finding.

Fix Text:
Steps/Recommendation:

1. In elasticsearch.yml
xpack.security.enabled: true
xpack.security.fips_mode.enabled: true

2. Disable SSL/TLS versions with non-NSA approved encryption (i.e. anything less than TLS v1.2):
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.supported_protocols: TLSv1.3,TLSv1.2

3. Due to the limitations that FIPS 140-2 compliance enforces, a small number of features are not available while running in FIPS 140-2 mode. The list is as follows:
- Azure Classic Discovery Plugin
- Ingest Attachment Plugin
- The elasticsearch-certutil tool. However, elasticsearch-certutil can very well be used in a non FIPS 140-2 configured JVM (pointing ES_JAVA_HOME environment variable to a different java installation) in order to generate the keys and certificates that can be later used in the FIPS 140-2 configured JVM.
- The SQL CLI client cannot run in a FIPS 140-2 configured JVM while using TLS for transport security or PKI for client authentication.

References:

a. FIPS 140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
b. Security settings in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html#hashing-settings
c. NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations:
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
d. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: FIPS 140-2 precludes the use of unvalidated cryptography for the cryptographic protection of sensitive or valuable data within Federal systems. Unvalidated cryptography is viewed by NIST as providing no protection to the information or data. In effect, the data would be considered unprotected plaintext. If the agency specifies that the information or data be cryptographically protected, then FIPS 140-2 is applicable. In essence, if cryptography is required, it must be validated. Cryptographic modules that have been approved for classified use may be used in lieu of modules that have been validated against the FIPS 140-2 standard.

Legacy Ids: V-81303; SV-96017

CCI: CCI-002450The information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws

CCI: Executive Orders

CCI: directives

CCI: policies

CCI: regulations

CCI: and standards.NIST SP 800-53 Revision 4 :: SC-13

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to off-load interconnected systems in real time and off-load standalone systems weekly, at a minimum.
STIG ID: SRG-APP-000515 **Rule ID:** SV-206511r400879_rule **Vul ID:** V-206511
Severity: CAT III

Documentable: No

Check Content:
Note: This is not applicable (NA) if an external application or operating system manages this function.

Examine the configuration.

Verify the system is configured to off-load interconnected systems in real time and off-load standalone systems weekly, at a minimum.

If the Central Log Server is not configured to off-load interconnected systems in real time and off-load standalone systems weekly, at a minimum, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch can be configured to provide redundancy by storing the Elasticsearch data on different media to support off-load interconnected systems in real time and off-load standalone systems weekly, at a minimum. Verify that standalone system logs are received when those systems are re-connected and automatically resumed when connectivity is restored after a loss in connectivity.

2. To guard against data loss and ensure that events flow through the pipeline without interruption, Logstash provides data resiliency features.

Persistent queues (PQ) protect against data loss by storing events in an internal queue on disk.
Dead letter queues (DLQ) provide on-disk storage for events that Logstash is unable to process so that you can evaluate them. You can easily reprocess events in the dead letter queue by using the dead_letter_queue input plugin.

These resiliency features are disabled by default. To turn on these features, you must explicitly enable them in the Logstash settings file.
The logstash.yml file is written in YAML. Its location varies by platform (see Logstash Directory Layout). You can specify settings in hierarchical form or use flat keys. For example, to use hierarchical form to set the pipeline batch size and batch delay, you specify:

```
pipeline:
  batch:
    size: 125
    delay: 50
```

References:

a. Data Resiliency: https://www.elastic.co/guide/en/logstash/current/resiliency.html
b. Persistent queues (PQ):
https://www.elastic.co/guide/en/logstash/current/persistent-queues.html
c. Dead letter queues (DLQ):
https://www.elastic.co/guide/en/logstash/current/dead-letter-queues.html
d. Logstash.yml: https://www.elastic.co/guide/en/logstash/current/logstash-settings-file.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity. Although this may be part of the operating system function, for the enterprise events management system, this is most often a function managed through the application since it is a critical function and requires the use of a large amount of external storage.

Legacy Ids: V-81177; SV-95891

CCI: CCI-001851The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.NIST SP 800-53 Revision 4 :: AU-4 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to retain the identity of the original source host or device where the event occurred as part of the log record.
STIG ID: SRG-APP-000516 **Rule ID:** SV-206512r401224_rule **Vul ID:** V-206512
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to include the identity of the original source host or device where the event occurred as part of each aggregated log record.

If the Central Log Server is not configured to include the identity of the original source host or device where the event occurred as part of the aggregated log record, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using Beats to collect system and device logs where possible. Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

2. Recommend using Logstash to collect system and device logs when Beats does not provide out of the box support for a particular format.

3. Logstash and or Beats should be configured to collect application logs with all the required attributes.

4. All applications logs/events should include the DoD attributes.

5. Recommend using Elasticsearch index templates where possible.

6. In Elasticsearch, mapping is the description of how documents and the fields they contain are stored and indexed. In the mapping, you can define, for example, the following:
- The structure of the document(fields and data type of those fields)
- How to transform values before indexing
- What fields use for full-text searching

7. Update your index mapping definitions as needed to include time stamps, source and

destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

```
curl -X PUT http://localhost:9200/person \
-H 'Content-Type: application/json' \
-d '{
     "mappings": {
       "dynamic": "strict",
       "properties": {
         "name": {"type": "text"},
         "source address": {"type": "text"},
        "ip_address": {"type": "text"},
         "extra_data": {"type": "object", "dynamic": true}
       }
     }
}'
```

References:

a. AU-12 of NIST 800-53 (https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&number=AU-12), supported by supplemental guidance from AU-3 (https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&number=AU-3)
b. Mapping: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/mapping.html
c. Index Template: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/index-templates.html
d. Install Elastic Agents : https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html
e. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: In this case the information producer is the device based on IP address or some other identifier of the device producing the information. The source of the record must be bound to the record using cryptographic means.

Some events servers allow the administrator to retain only portions of the record sent by devices and hosts.

This requirement applies to log aggregation servers with the role of fulfilling the DoD

requirement for a central log repository. The syslog, SIEM, or other event servers must retain this information with each log record to support incident investigations.

Legacy Ids: V-81179; SV-95893

CCI: CCI-000366The organization implements the security configuration settings.NIST SP 800-53 :: CM-6 bNIST SP 800-53A :: CM-6.1 (iv)NIST SP 800-53 Revision 4 :: CM-6 b

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server that aggregates log records from hosts and devices must be configured to use TCP for transmission.
STIG ID: SRG-APP-000516 **Rule ID:** SV-206513r401224_rule **Vul ID:** V-206513
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to use TCP.

If the Central Log Server is not configured to use TCP, this is a finding.

Fix Text:
Step/Recommendation:

1. All communication to Elasticsearch and Kibana is over HTTP, which uses TCP for the transport layer. This can be validated with netstat or a tcpdump.

Reference:

a. Elastic network:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/modules-network.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If the default UDP protocol is used for communication between the hosts and

devices to the Central Log Server, then log records that do not reach the log server are not detected as a data loss. The use of TCP to transport log records to the log servers improves delivery reliability, adds data integrity, and gives the option to encrypt the traffic if the log server communication is not protected using a management network (preferred) or VPN based on mission requirements.

Legacy Ids: V-81181; SV-95895

CCI: CCI-000366The organization implements the security configuration settings.NIST SP 800-53 :: CM-6 bNIST SP 800-53A :: CM-6.1 (iv)NIST SP 800-53 Revision 4 :: CM-6 b

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to notify the System Administrator (SA) and Information System Security Officer (ISSO), at a minimum, when an attack is detected on multiple devices and hosts within its scope of coverage.
STIG ID: SRG-APP-000516 **Rule ID:** SV-206514r401224_rule **Vul ID:** V-206514
Severity: CAT II

Documentable: No

Check Content:
Note: This is not applicable (NA) if the Central Log Server (e.g., syslog, SIEM) does not perform analysis. This is NA if notifications are performed by another device.

Examine the configuration.

Verify the Central Log Server is configured to notify the SA and ISSO, at a minimum, when an attack is detected on multiple devices and hosts within its scope of coverage.

If the Central Log Server is not configured to notify the SA and ISSO, at a minimum, when an attack is detected on multiple devices and hosts within its scope of coverage, this is a finding.

Fix Text:
Steps/Recommendation:

1. The Elastic Stack can be configured to notify appropriate personnel using a combination of Rules (Detection Engine), Machine Learning and Alerting. This configuration is typically performed via the Kibana user interface. Elasticsearch's alerting features (Watcher) should be utilized which provide an API for creating and managing alert notification for when an attack is detected on multiple devices and hosts within its scope of coverage.

2. A Watch is constructed from four simple building blocks:
- Schedule: A schedule for running a query and checking the condition.
- Query: The query to run as input to the condition, which can detect account modifications for user or application. Watches support the full Elasticsearch query language, including aggregations.
- Condition: A condition that determines whether or not to execute the actions. You can use simple conditions (always true), also scripting for more sophisticated scenarios for account modifications.
- Actions: Setup notify the System Administrator (SA) and Information System Security Officer (ISSO) when an attack is detected on multiple devices and hosts within its scope of coverage.

A full history of all watches is maintained in an Elasticsearch index. This history keeps track of each time a watch is triggered and records the results from the query, whether the condition was met, and what actions were taken.

References:

a. Alerting on cluster and index events:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
b. Kibana Reporting:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
c. Kibana Machine Learning: https://www.elastic.co/guide/en/kibana/8.0/xpack-ml.html
d. Kibana Detections:
https://www.elastic.co/guide/en/siem/guide/current/detection-engine-overview.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Notification may be configured to be sent by the device, SNMP server, or Central Log Server. The best practice is for these notifications to be sent by a robust events management server.

This is a function provided by most enterprise-level SIEMs. If the Central Log Server does not provide this function, it must forward the log records to a log server that does.

Legacy Ids: V-81183; SV-95897

CCI: CCI-000366The organization implements the security configuration settings.NIST SP 800-53 :: CM-6 bNIST SP 800-53A :: CM-6.1 (iv)NIST SP 800-53 Revision 4 :: CM-6 b

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to automatically create trouble tickets for organization-defined threats and events of interest as they are detected in real time (within seconds).
STIG ID: SRG-APP-000516 **Rule ID:** SV-206515r401224_rule **Vul ID:** V-206515
Severity: CAT II

Documentable: No

Check Content:
Note: This is not applicable (NA) if the Central Log Server (e.g., syslog) does not perform analysis.

Examine the configuration.

Verify the Central Log Server automatically creates trouble tickets for organization-defined threats and events of interest as they are detected in real time (within seconds).

If the Central Log Server is not configured to automatically create trouble tickets for organization-defined threats and events of interest as they are detected in real time (within seconds), this is a finding.

Fix Text:
Steps/Recommendation:

1. The Elastic Stack can be configured to generate alerts for trouble tickets through a combination of Rules (Detection Engine), Machine Learning and Alerting. This configuration is typically performed via the Kibana user interface. Elasticsearch service console (Kibana UI) can be used to setup alerts, alerts can be send by email, slack, HipChat, PagerDuty.

2. Recommend using the Kibana UI to perform Alerting and Reporting.

3. Recommend using Machine Learning to automatically find anomalies in the data as it is streaming in.

4. Recommend using the Detection Engine to automatically find events of interest.

References:

a. Alerting on cluster and index events:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
b. Kibana Reporting:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
c. Kibana Machine Learning: https://www.elastic.co/guide/en/kibana/8.0/xpack-ml.html

d. Kibana Detections:
https://www.elastic.co/guide/en/siem/guide/current/detection-engine-overview.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: In most Central Log Server products today, log review (threat detection), can be automated by creating correlation content matching the organizational-defined Events of Interest (e.g., account change actions, privilege command use, and other AU and AC family controls) to automatically notify or automatically create trouble tickets for threats as they are detected in real time. Auditors have repeatedly expressed a strong preference for automated ticketing. They are also more likely to follow up on the threat and action items needed to address the detected issues if the ticketing process is automated.

This is a function provided by most enterprise-level SIEMs. If the Central Log Server does not provide this function, it must forward the log records to a log server that does.

Legacy Ids: V-81185; SV-95899

CCI: CCI-000366The organization implements the security configuration settings.NIST SP 800-53 :: CM-6 bNIST SP 800-53A :: CM-6.1 (iv)NIST SP 800-53 Revision 4 :: CM-6 b

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: For devices and hosts within the scope of coverage, the Central Log Server must be configured to automatically aggregate events that indicate account actions.
STIG ID: SRG-APP-000516 **Rule ID:** SV-206516r401224_rule **Vul ID:** V-206516
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server automatically aggregates events that indicate account actions for each device and host within its scope of coverage.

If the Central Log Server is not configured to automatically aggregate events that indicate

account actions for each device and host within its scope of coverage, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using the Kibana UI to perform Alerting and Reporting.

2. Recommend using Machine Learning to automatically find anomalies in the data as it is streaming in.

3. Recommend using the Detection Engine to automatically find events of interest.

References:

a. Kibana Dashboards: https://www.elastic.co/guide/en/kibana/8.0/dashboard.html
b. Kibana Reporting:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
c. Alerting on cluster and index events:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
d. Kibana Machine Learning: https://www.elastic.co/guide/en/kibana/8.0/xpack-ml.html
e. Kibana Detections:
https://www.elastic.co/guide/en/siem/guide/current/detection-engine-overview.html
f. cat indices API: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/cat-indices.html
g. Mapping -> Mapping parameters -> fielddata:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/text.html#fielddata-mapping-param

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If the Central Log Server is configured to filter or remove account log records transmitted by devices and hosts within its scope of coverage, forensic analysis tools will be less effective at detecting and reporting on important attack vectors. A comprehensive account management process must include capturing log records for the creation of user accounts and notification of administrators and/or application owners. Such a process greatly reduces the risk that accounts will be surreptitiously created and provides logging that can be used for forensic purposes.

This requirement addresses the concern that the Central Log Server may be configured to filter out certain levels of information, which may result in the discarding of DoD-required accounting actions addressed in the AC-2 (4) controls such as creation, modification, deletion, and removal of privileged accounts.

Legacy Ids: V-81187; SV-95901

CCI: CCI-000366The organization implements the security configuration settings.NIST SP 800-53 :: CM-6 bNIST SP 800-53A :: CM-6.1 (iv)NIST SP 800-53 Revision 4 :: CM-6 b

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured with the organization-defined severity or criticality levels of each event that is being sent from individual devices or hosts.
STIG ID: SRG-APP-000516 **Rule ID:** SV-206517r401224_rule **Vul ID:** V-206517
Severity: CAT II

Documentable: No

Check Content:
Obtain the site's SSP to see which criticality levels are used for each system within the scope of the Central Log Server. Examine the configuration of the Central Log Server.

Verify the Central Log Server is configured with the organization-defined severity or criticality levels of each event that is being sent from individual devices or hosts.

If the Central Log Server is not configured with the organization-defined severity or criticality levels of each event that is being sent from individual devices or hosts, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using the Elastic Stack Detection Engine (rules) to define custom severity/criticality levels for events. This is done via the Kibana user interface.

2. Recommend using the Kibana UI to perform Alerting and Reporting.

3. Recommend using Machine Learning to automatically find anomalies in the data as it is streaming in.

4. Recommend using the Detection Engine to automatically find events of interest.

References:

a. Kibana Dashboards: https://www.elastic.co/guide/en/kibana/8.0/dashboard.html
b. Kibana Reporting:
https://www.elastic.co/guide/en/kibana/8.0/reporting-getting-started.html
c. Alerting on cluster and index events:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
d. Kibana Machine Learning: https://www.elastic.co/guide/en/kibana/8.0/xpack-ml.html
e. Kibana Detections:
https://www.elastic.co/guide/en/siem/guide/current/detection-engine-overview.html
f. cat indices API: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/cat-indices.html
g. Mapping -> Mapping parameters -> fielddata:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/text.html#fielddata-mapping-param

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: This supports prioritization functions, which is a major reason why centralized management is a requirement in DoD. This includes different features that help highlight the important events over less critical security events. This may be accomplished by correlating security events with vulnerability data or other asset information. Prioritization algorithms often use severity information provided by the original log source as well. The criticality levels used by the site and the actions that are taken based on the levels established for each system are documented in the SSP. These levels and actions can only be leveraged for alerts, notifications, and reports which correlate asset information if they are configured in the Central Log Server.

Legacy Ids: V-81189; SV-95903

CCI: CCI-000366The organization implements the security configuration settings.NIST SP 800-53 :: CM-6 bNIST SP 800-53A :: CM-6.1 (iv)NIST SP 800-53 Revision 4 :: CM-6 b

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: Analysis, viewing, and indexing functions, services, and applications used as part of the Central Log Server must be configured to comply with DoD-trusted path and access requirements.
STIG ID: SRG-APP-000516 **Rule ID:** SV-206518r401224_rule **Vul ID:** V-206518
Severity: CAT II

Documentable: No

Check Content:

Examine the configuration.

Verify analysis, viewing, and indexing functions, services, and applications used with the Central Log Server are configured to comply with DoD-trusted path and access requirements.

If analysis, viewing, and indexing functions, services, and applications used with the Central Log Server are not configured to comply with DoD-trusted path and access requirements, this is a finding.

Fix Text:
Steps/Recommendation:

1. Enable Authentication and Authorization

2. Enable SSL/TLS encryption

3. Enable IP filtering

4. Disable Anonymous user access to Elasticsearch

References:

a. DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA:
https://csrc.nist.gov/csrc/media/publications/white-paper/1985/12/26/dod-rainbow-series/final/documents/std001.txt
b. FIPS-140-2:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/fips-140-compliance.html
c. Start the Elastic Stack with security:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
d. Setting Up TLS on a Cluster:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-basic-setup.html#encrypt-internode-communication
e. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html
f. Anonymous Access:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/anonymous-access.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Analysis, viewing, and indexing functions, services, and applications, such as

analysis tools and other vendor-provided applications, must be secured. Software used to perform additional functions, which resides on the server, must also be secured or could provide a vector for unauthorized access to the events repository.

Legacy Ids: V-81191; SV-95905

CCI: CCI-000366The organization implements the security configuration settings.NIST SP 800-53 :: CM-6 bNIST SP 800-53A :: CM-6.1 (iv)NIST SP 800-53 Revision 4 :: CM-6 b

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must automatically audit account creation.
STIG ID: SRG-APP-000026 **Rule ID:** SV-221900r420044_rule **Vul ID:** V-221900
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to automatically audit account creation.

If the Central Log Server is not configured to automatically audit account creation, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch can preform audit logging. Enable the audit logging:
   Set xpack.security.audit.enabled to true in elasticsearch.yml.
   Restart Elasticsearch.

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see

https://www.elastic.co/subscriptions.

2. Elasticsearch supports external Identity Providers (IdP) for authentication through Active Directory, LDAP/S, SAML/OIDC or PKI realm to manage accounts and authenticate users. The recommendation is to integrate Elasticsearch with one of these services to support centralized account management.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
f. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
h. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
i. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
j. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
m. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
n. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
o. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and

guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of re-establishing access. One way to accomplish this is for the attacker to simply create a new account. Auditing of account creation is one method for mitigating this risk. A comprehensive account management process will ensure an audit trail documents the creation of application user accounts and, as required, notifies administrators and/or application owners exists. Such a process greatly reduces the risk that accounts will be surreptitiously created and provides logging that can be used for forensic purposes.

To address access requirements, many application developers choose to integrate their applications with enterprise-level authentication/access/auditing mechanisms meeting or exceeding access control policy requirements. Such integration allows the application developer to off-load those access control functions and focus on core application features and functionality.

Legacy Ids: V-100025; SV-109129

CCI: CCI-000018The information system automatically audits account creation actions.NIST SP 800-53 :: AC-2 (4)NIST SP 800-53A :: AC-2 (4).1 (i&ii)NIST SP 800-53 Revision 4 :: AC-2 (4)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must automatically audit account modification.
STIG ID: SRG-APP-000027 **Rule ID:** SV-221901r420047_rule **Vul ID:** V-221901
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to automatically audit account modification.

If the Central Log Server is not configured to automatically audit account modification, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch can preform audit logging. Enable the audit logging:
   Set xpack.security.audit.enabled to true in elasticsearch.yml.
   Restart Elasticsearch.

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. Elasticsearch supports external Identity Providers (IdP) for authentication through Active Directory, LDAP/S, SAML/OIDC or PKI realm to manage accounts and authenticate users. The recommendation is to integrate Elasticsearch with one of these services to support centralized account management.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
f. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
h. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
i. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
j. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
k. Integrating with Other Authentication Systems:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
m. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
n. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
o. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of re-establishing access. One way to accomplish this is for the attacker to simply modify an existing account. Auditing of account creation is one method for mitigating this risk. A comprehensive account management process will ensure an audit trail documents the creation of application user accounts and, as required, notifies administrators and/or application owners exists. Such a process greatly reduces the risk that accounts will be surreptitiously created and provides logging that can be used for forensic purposes.

To address access requirements, many application developers choose to integrate their applications with enterprise-level authentication/access/auditing mechanisms meeting or exceeding access control policy requirements. Such integration allows the application developer to off-load those access control functions and focus on core application features and functionality.

Legacy Ids: V-100027; SV-109131

CCI: CCI-001403The information system automatically audits account modification actions.NIST SP 800-53 :: AC-2 (4)NIST SP 800-53A :: AC-2 (4).1 (i&ii)NIST SP 800-53 Revision 4 :: AC-2 (4)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must automatically audit account disabling actions.
STIG ID: SRG-APP-000028 **Rule ID:** SV-221902r420050_rule **Vul ID:** V-221902
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to automatically audit account disabling.

If the Central Log Server is not configured to automatically audit account disabling, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch can preform audit logging. Enable the audit logging:
   Set xpack.security.audit.enabled to true in elasticsearch.yml.
   Restart Elasticsearch.

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. Elasticsearch supports external Identity Providers (IdP) for authentication through Active Directory, LDAP/S, SAML/OIDC or PKI realm to manage accounts and authenticate users. The recommendation is to integrate Elasticsearch with one of these services to support centralized account management.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authenti

cation.html
e. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
f. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
h. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
i. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
j. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
m. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
n. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
o. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: When application accounts are disabled, user accessibility is affected. Once an attacker establishes access to an application, the attacker often attempts to disable authorized accounts to disrupt services or prevent the implementation of countermeasures. Auditing account disabling actions provides logging that can be used for forensic purposes.

To address access requirements, many application developers choose to integrate their applications with enterprise-level authentication/access/audit mechanisms meeting or exceeding access control policy requirements. Such integration allows the application developer to off-load those access control functions and focus on core application features and functionality.

Legacy Ids: V-100029; SV-109133

CCI: CCI-001404The information system automatically audits account disabling actions.NIST SP 800-53 :: AC-2 (4)NIST SP 800-53A :: AC-2 (4).1 (i&ii)NIST SP 800-53 Revision 4 :: AC-2 (4)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must automatically audit account removal actions.
STIG ID: SRG-APP-000029 **Rule ID:** SV-221903r420053_rule **Vul ID:** V-221903
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to automatically audit account removal.

If the Central Log Server is not configured to automatically audit account removal, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elasticsearch can preform audit logging. Enable the audit logging:
   Set xpack.security.audit.enabled to true in elasticsearch.yml.
   Restart Elasticsearch.

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. Elasticsearch supports external Identity Providers (IdP) for authentication through Active Directory, LDAP/S, SAML/OIDC or PKI realm to manage accounts and authenticate users. The recommendation is to integrate Elasticsearch with one of these services to support

centralized account management.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
f. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
h. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
i. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
j. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
m. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
n. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html
o. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: When application accounts are removed, user accessibility is affected. Once an

attacker establishes access to an application, the attacker often attempts to remove authorized accounts to disrupt services or prevent the implementation of countermeasures. Auditing account removal actions provides logging that can be used for forensic purposes.

To address access requirements, many application developers choose to integrate their applications with enterprise-level authentication/access/audit mechanisms meeting or exceeding access control policy requirements. Such integration allows the application developer to off-load those access control functions and focus on core application features and functionality.

Legacy Ids: V-100031; SV-109135

CCI: CCI-001405The information system automatically audits account removal actions.NIST SP 800-53 :: AC-2 (4)NIST SP 800-53A :: AC-2 (4).1 (i&ii)NIST SP 800-53 Revision 4 :: AC-2 (4)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.
STIG ID: SRG-APP-000065 **Rule ID:** SV-221904r420056_rule **Vul ID:** V-221904
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to lock out the account after 3 consecutive invalid attempts during a 15 minute period.

If the Central Log Server is not configured to lock out the account after 3 consecutive invalid attempts in 15 minutes, this is a finding.

Fix Text:
Step/Recommendation:

1. Recommend to use external Identity Provider (IdP) for authentication through "Active Directory, LDAP/S, SAML or OpenID Connection" realm. The password policy can be configured to lock out the account after 3 consecutive invalid attempts during a 15 minute period.

References:

a. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
b. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
c. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
d. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
e. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
f. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
g. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
h. OpenID Connect Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/oidc-realm.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: By limiting the number of failed login attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the account.

Legacy Ids: V-100033; SV-109137

CCI: CCI-000044The information system enforces the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.NIST SP 800-53 :: AC-7 aNIST SP 800-53A :: AC-7.1 (ii)NIST SP 800-53 Revision 4 :: AC-7 a

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the Central Log Server.
STIG ID: SRG-APP-000068 **Rule ID:** SV-221905r420059_rule **Vul ID:** V-221905
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to display the Mandatory DoD Notice and Consent Banner before granting access to the Central Log Server.

If the Central Log Server is not configured to display the Mandatory DoD Notice and Consent Banner, this is a finding.

Fix Text:
Step/Recommendation:

1. Kibana supports a banner, however it is disabled by default. It needs to be manually configured in order to use the feature.

Configure the xpack.banners settings in the kibana.yml file:

xpack.banners.placement
  Set to top to display a banner above the Elastic header. Defaults to disabled.
xpack.banners.textContent
  The text to display inside the banner, either plain text or Markdown.
xpack.banners.textColor
  The color for the banner text. Defaults to #8A6A0A.
xpack.banners.backgroundColor
  The color of the banner background. Defaults to #FFF9E8.
xpack.banners.disableSpaceBanners
  If true, per-space banner overrides will be disabled. Defaults to false.

Note: Banners are a subscription feature.

Reference:

a. Banner settings in Kibana:
https://www.elastic.co/guide/en/kibana/master/banners-settings-kb.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Display of the DoD-approved use notification before granting access to the application ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with DTM-08-060. Use the following verbiage for applications that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

Legacy Ids: V-100037; SV-109141

CCI: CCI-000048The information system displays an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws

CCI: Executive Orders

CCI: directives

CCI: policies

CCI: regulations

CCI: standards

CCI: and guidance.NIST SP 800-53 :: AC-8 aNIST SP 800-53A :: AC-8.1 (ii)NIST SP 800-53 Revision 4 :: AC-8 a

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must retain the Standard Mandatory DoD Notice and Consent Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access.
STIG ID: SRG-APP-000069 **Rule ID:** SV-221906r420062_rule **Vul ID:** V-221906
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to retain the Mandatory DoD Notice and Consent Banner until users acknowledge the usage conditions.

If the Central Log Server is not configured to retain the Mandatory DoD Notice and Consent Banner until users acknowledge the usage conditions, this is a finding.

Fix Text:
Step/Recommendation:

1. Kibana supports a banner, however it is disabled by default. It needs to be manually configured in order to use the feature.

Configure the xpack.banners settings in the kibana.yml file:

xpack.banners.placement
Set to top to display a banner above the Elastic header. Defaults to disabled.
xpack.banners.textContent

The text to display inside the banner, either plain text or Markdown.
xpack.banners.textColor
The color for the banner text. Defaults to #8A6A0A.
xpack.banners.backgroundColor
The color of the banner background. Defaults to #FFF9E8.
xpack.banners.disableSpaceBanners
If true, per-space banner overrides will be disabled. Defaults to false.

Note: Banners are a subscription feature.

Reference:

a. Banner settings in Kibana:
https://www.elastic.co/guide/en/kibana/master/banners-settings-kb.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: The banner must be acknowledged by the user prior to allowing the user access to the application. This provides assurance that the user has seen the message and accepted the conditions for access. If the consent banner is not acknowledged by the user, DoD will not be in compliance with system use notifications required by law.

To establish acceptance of the application usage policy, a click-through banner at application logon is required. The application must prevent further activity until the user executes a positive action to manifest agreement by clicking on a box indicating "OK".

Legacy Ids: V-100039; SV-109143

CCI: CCI-000050The information system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access.NIST SP 800-53 :: AC-8 bNIST SP 800-53A :: AC-8.1 (iii)NIST SP 800-53 Revision 4 :: AC-8 b

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must initiate session auditing upon startup.
STIG ID: SRG-APP-000092 **Rule ID:** SV-221907r420065_rule **Vul ID:** V-221907
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server initiates session logging upon startup.

If the Central Log Server is not configured to initiate session logging upon startup, this is a finding.

Fix Text:
Steps/Recommendation:

1. By enabling Set xpack.security.audit.enabled to true in elasticsearch.yml. for each cluster node, Elastic starts up auditing when the node is started.

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) which must be configured to initiate session logging upon startup.

References:
a. Auditing Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
f. Active Directory User Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
k. Monitoring Overview:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/monitoring-overview.html
l. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If auditing is enabled late in the startup process, the actions of some start-up processes may not be audited. Some audit systems also maintain state information only available if auditing is enabled before a given process is created.

Legacy Ids: V-100043; SV-109147

CCI: CCI-001464The information system initiates session audits at system start-up.NIST SP 800-53 :: AU-14 (1)NIST SP 800-53A :: AU-14 (1).1NIST SP 800-53 Revision 4 :: AU-14 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must produce audit records containing information to establish what type of events occurred.
STIG ID: SRG-APP-000095 **Rule ID:** SV-221908r420068_rule **Vul ID:** V-221908
Severity: CAT III

Documentable: No

Check Content:

12. Completed (Final)

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to): access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information to establish what type of events occurred.

Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
f. Setting Up User Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
h. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
i. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
j. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
m. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
n. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
o. Auditbeat: https://www.elastic.co/guide/en/beats/auditbeat/8.0/auditbeat-overview.html
p. Secure Auditbeat:
https://www.elastic.co/guide/en/beats/auditbeat/8.0/securing-auditbeat.html
q. Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/index.html
r. Secure Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
s. Metricbeat: https://www.elastic.co/guide/en/beats/metricbeat/8.0/index.html
t. Secure Metricbeat:
https://www.elastic.co/guide/en/beats/metricbeat/8.0/securing-metricbeat.html
q. Packetbeat: https://www.elastic.co/guide/en/beats/packetbeat/8.0/index.html
u. Secure Packetbeat:
https://www.elastic.co/guide/en/beats/packetbeat/8.0/securing-packetbeat.html
v. Heartbeat: https://www.elastic.co/guide/en/beats/heartbeat/8.0/index.html
w. Secure Heartbeat:
https://www.elastic.co/guide/en/beats/heartbeat/8.0/securing-heartbeat.html
x. Winlogbeat: https://www.elastic.co/guide/en/beats/winlogbeat/8.0/index.html
y. Secure Winlogbeat:
https://www.elastic.co/guide/en/beats/winlogbeat/8.0/securing-winlogbeat.html
z. Logstash: https://www.elastic.co/guide/en/logstash/8.0/index.html
aa. Secure your connection to Elasticsearch with logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
ab. Install Elastic Agents :
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html
ac. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and

guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without establishing what type of event occurred, it would be difficult to establish, correlate, and investigate the events relating to an incident, or identify those responsible for one.

Audit record content that may be necessary to satisfy the requirement of this policy includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in the application and audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured application.

Legacy Ids: V-100045; SV-109149

CCI: CCI-000130The information system generates audit records containing information that establishes what type of event occurred.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must produce audit records containing information to establish when (date and time) the events occurred.
STIG ID: SRG-APP-000096 **Rule ID:** SV-221909r420071_rule **Vul ID:** V-221909
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server produces audit records containing information to establish when the events occurred.

If the Central Log Server is not configured to produce audit records containing information to establish when the events occurred, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to):access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. To satisfy this control, @timestamp has to be captured.

5. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information of when the events occurred.

Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
f. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html

h. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
i. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
j. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
m. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
n. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
o. Auditbeat: https://www.elastic.co/guide/en/beats/auditbeat/8.0/auditbeat-overview.html
p. Secure Auditbeat:
https://www.elastic.co/guide/en/beats/auditbeat/8.0/securing-auditbeat.html
q. Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/index.html
r. Secure Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
s. Metricbeat: https://www.elastic.co/guide/en/beats/metricbeat/8.0/index.html
t. Secure Metricbeat:
https://www.elastic.co/guide/en/beats/metricbeat/8.0/securing-metricbeat.html
q. Packetbeat: https://www.elastic.co/guide/en/beats/packetbeat/8.0/index.html
u. Secure Packetbeat:
https://www.elastic.co/guide/en/beats/packetbeat/8.0/securing-packetbeat.html
v. Heartbeat: https://www.elastic.co/guide/en/beats/heartbeat/8.0/index.html
w. Secure Heartbeat:
https://www.elastic.co/guide/en/beats/heartbeat/8.0/securing-heartbeat.html
x. Winlogbeat: https://www.elastic.co/guide/en/beats/winlogbeat/8.0/index.html
y. Secure Winlogbeat:
https://www.elastic.co/guide/en/beats/winlogbeat/8.0/securing-winlogbeat.html
z. Logstash: https://www.elastic.co/guide/en/logstash/8.0/index.html
aa. Secure your connection to Elasticsearch with logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
ab. Install Elastic Agents :
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html
ac. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without establishing when events occurred, it is impossible to establish, correlate, and investigate the events relating to an incident.

In order to compile an accurate risk assessment, and provide forensic analysis, it is essential for security personnel to know when events occurred (date and time).

Associating event types with detected events in the application and audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured application.

Legacy Ids: V-100047; SV-109151

CCI: CCI-000131The information system generates audit records containing information that establishes when an event occurred.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must produce audit records containing information to establish where the events occurred.
STIG ID: SRG-APP-000097 **Rule ID:** SV-221910r420074_rule **Vul ID:** V-221910
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server produces audit records containing information to establish where the events occurred.

If the Central Log Server is not configured to produce audit records containing information to establish where the events occurred, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername> audit.json file on the host file system (on each node). Refer to the list of the

events that can be generated at
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see
https://www.elastic.co/subscriptions.

2. Log files audited events can be set using the following configuration
xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to):access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. To satisfy this control, node.name, node.id, host.ip, host.name, origin.address, origin.type, has to be captured.

5. For event.type equal to transport, then extra attributes should be captured: action, indices, request.name

6. For event.type equal to ip_filter, transport_profile and rule should be captured.

7. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information to establish where the events occurred.

Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
f. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html

h. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
i. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
j. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
m. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
n. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
o. Auditbeat: https://www.elastic.co/guide/en/beats/auditbeat/8.0/auditbeat-overview.html
p. Secure Auditbeat:
https://www.elastic.co/guide/en/beats/auditbeat/8.0/securing-auditbeat.html
q. Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/index.html
r. Secure Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
s. Metricbeat: https://www.elastic.co/guide/en/beats/metricbeat/8.0/index.html
t. Secure Metricbeat:
https://www.elastic.co/guide/en/beats/metricbeat/8.0/securing-metricbeat.html
q. Packetbeat: https://www.elastic.co/guide/en/beats/packetbeat/8.0/index.html
u. Secure Packetbeat:
https://www.elastic.co/guide/en/beats/packetbeat/8.0/securing-packetbeat.html
v. Heartbeat: https://www.elastic.co/guide/en/beats/heartbeat/8.0/index.html
w. Secure Heartbeat:
https://www.elastic.co/guide/en/beats/heartbeat/8.0/securing-heartbeat.html
x. Winlogbeat: https://www.elastic.co/guide/en/beats/winlogbeat/8.0/index.html
y. Secure Winlogbeat:
https://www.elastic.co/guide/en/beats/winlogbeat/8.0/securing-winlogbeat.html
z. Logstash: https://www.elastic.co/guide/en/logstash/8.0/index.html
aa. Secure your connection to Elasticsearch with logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
ab. Install Elastic Agents :
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html
ac. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without establishing where events occurred, it is impossible to establish, correlate, and investigate the events relating to an incident.

In order to compile an accurate risk assessment, and provide forensic analysis, it is essential for security personnel to know where events occurred, such as application components, modules, session identifiers, filenames, host names, and functionality.

Associating information about where the event occurred within the application provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured application.

Legacy Ids: V-100049; SV-109153

CCI: CCI-000132The information system generates audit records containing information that establishes where the event occurred.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must produce audit records containing information to establish the source of the events.
STIG ID: SRG-APP-000098 **Rule ID:** SV-221911r420077_rule **Vul ID:** V-221911
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server produces audit records containing information to establish the source of the events.

If the Central Log Server is not configured to produce audit records containing information to establish the source of the events, this is a finding.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated

<clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to):access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. To satisfy this control, node.name, node.id, host.ip, host.name, origin.address, origin.type, has to be captured.

5. For event.type equal to transport, then extra attributes should be captured: action, indices, request.name

6. For event.type equal to ip_filter, transport_profile and rule should be captured.

7. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information to establish the source of the events.

Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
f. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. SAML Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
h. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
i. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
j. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
m. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
n. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
o. Auditbeat: https://www.elastic.co/guide/en/beats/auditbeat/8.0/auditbeat-overview.html
p. Secure Auditbeat:
https://www.elastic.co/guide/en/beats/auditbeat/8.0/securing-auditbeat.html
q. Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/index.html
r. Secure Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
s. Metricbeat: https://www.elastic.co/guide/en/beats/metricbeat/8.0/index.html
t. Secure Metricbeat:
https://www.elastic.co/guide/en/beats/metricbeat/8.0/securing-metricbeat.html
q. Packetbeat: https://www.elastic.co/guide/en/beats/packetbeat/8.0/index.html
u. Secure Packetbeat:
https://www.elastic.co/guide/en/beats/packetbeat/8.0/securing-packetbeat.html
v. Heartbeat: https://www.elastic.co/guide/en/beats/heartbeat/8.0/index.html
w. Secure Heartbeat:
https://www.elastic.co/guide/en/beats/heartbeat/8.0/securing-heartbeat.html
x. Winlogbeat: https://www.elastic.co/guide/en/beats/winlogbeat/8.0/index.html
y. Secure Winlogbeat:
https://www.elastic.co/guide/en/beats/winlogbeat/8.0/securing-winlogbeat.html
z. Logstash: https://www.elastic.co/guide/en/logstash/8.0/index.html
aa. Secure your connection to Elasticsearch with logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
ab. Install Elastic Agents :
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html
ac. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic

documentation.

Discussion: Without establishing the source of the event, it is impossible to establish, correlate, and investigate the events leading up to an outage or attack.

In addition to logging where events occur within the application, the application must also produce audit records that identify the application itself as the source of the event.

In the case of centralized logging, the source would be the application name accompanied by the host or client name.

In order to compile an accurate risk assessment, and provide forensic analysis, it is essential for security personnel to know the source of the event, particularly in the case of centralized logging.

Associating information about the source of the event within the application provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured application.

Legacy Ids: V-100051; SV-109155

CCI: CCI-000133The information system generates audit records containing information that establishes the source of the event.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must produce audit records that contain information to establish the outcome of the events.
STIG ID: SRG-APP-000099 **Rule ID:** SV-221912r420080_rule **Vul ID:** V-221912
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server produces audit records containing information to establish the outcome of the events.

If the Central Log Server is not configured to produce audit records containing information to establish the outcome of the events, this is a finding.

Fix Text:

Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername>_audit.json file on the host file system (on each node). Refer to the list of the events that can be generated at https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

2. Log files audited events can be set using the following configuration xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to): access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. event.action captures the type of event that occurred: anonymous_access_denied, authentication_failed, authentication_success, realm_authentication_failed, access_denied, access_granted, connection_denied, connection_granted, tampered_request, run_as_denied, or run_as_granted.

5. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information to establish the outcome of the events.

Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html

e. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
f. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
h. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
i. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
j. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
m. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
n. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
o. Auditbeat: https://www.elastic.co/guide/en/beats/auditbeat/8.0/auditbeat-overview.html
p. Secure Auditbeat:
https://www.elastic.co/guide/en/beats/auditbeat/8.0/securing-auditbeat.html
q. Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/index.html
r. Secure Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
s. Metricbeat: https://www.elastic.co/guide/en/beats/metricbeat/8.0/index.html
t. Secure Metricbeat:
https://www.elastic.co/guide/en/beats/metricbeat/8.0/securing-metricbeat.html
q. Packetbeat: https://www.elastic.co/guide/en/beats/packetbeat/8.0/index.html
u. Secure Packetbeat:
https://www.elastic.co/guide/en/beats/packetbeat/8.0/securing-packetbeat.html
v. Heartbeat: https://www.elastic.co/guide/en/beats/heartbeat/8.0/index.html
w. Secure Heartbeat:
https://www.elastic.co/guide/en/beats/heartbeat/8.0/securing-heartbeat.html
x. Winlogbeat: https://www.elastic.co/guide/en/beats/winlogbeat/8.0/index.html
y. Secure Winlogbeat:
https://www.elastic.co/guide/en/beats/winlogbeat/8.0/securing-winlogbeat.html
z. Logstash: https://www.elastic.co/guide/en/logstash/8.0/index.html
aa. Secure your connection to Elasticsearch with logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
ab. Install Elastic Agents :
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html
ac. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without information about the outcome of events, security personnel cannot make an accurate assessment as to whether an attack was successful or if changes were made to the security state of the system.

Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). As such, they also provide a means to measure the impact of an event and help authorized personnel to determine the appropriate response.

Legacy Ids: V-100053; SV-109157

CCI: CCI-000134The information system generates audit records containing information that establishes the outcome of the event.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must generate audit records containing information that establishes the identity of any individual or process associated with the event.
STIG ID: SRG-APP-000100 **Rule ID:** SV-221913r420083_rule **Vul ID:** V-221913
Severity: CAT III

Documentable: No

Check Content:
The Central Log Server must generate audit records containing information that establishes the identity of any individual or process associated with the event.

Fix Text:
Steps/Recommendation:

1. To enable auditing: xpack.security.audit.enabled should be set to true in elasticsearch.yml

Note: Audit logs are disabled by default. You must explicitly enable audit logging. When audit logging is enabled, security events are persisted to a dedicated <clustername> audit.json file on the host file system (on each node). Refer to the list of the

events that can be generated at
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see
https://www.elastic.co/subscriptions.

2. Log files audited events can be set using the following configuration
xpack.security.audit.logfile.events.include

3. Following are the common attributes in the log file (not limited to):
access_denied, access_granted, anonymous_access_denied, authentication_failed, connection_denied, tampered_request, run_as_denied, run_as_granted, security_config_change

4. To satisfy this control, there are a few events that have some more attributes in addition to those that have been previously described:
authentication_success: realm, user.name, user.run_by.name
authentication_failed: user.name
realm_authentication_failed: user.name, realm
run_as_denied and run_as_granted: user.roles, user.name, user.realm, user.run_as.name, user.run_as.realm
access_granted or access_denied: user.roles, user.name, user.realm, user.run_by.name, user.run_by.realm

5. Configure the log ingestion pipeline including Logstash/Beats to produce audit records containing information that establishes the identity of any individual or process associated with the event.

Fleet managed Elastic Agents can be used to deploy and centrally manage beats.

References:

a. Auditing security settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
b. Audit event types:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
c. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
d. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. Elasticsearch Security Settings:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
f. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
g. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
h. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
i. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
j. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
k. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
l. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
m. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html
n. Beats and Security: https://www.elastic.co/guide/en/elasticsearch/reference/8.0/beats.html
o. Auditbeat: https://www.elastic.co/guide/en/beats/auditbeat/8.0/auditbeat-overview.html
p. Secure Auditbeat:
https://www.elastic.co/guide/en/beats/auditbeat/8.0/securing-auditbeat.html
q. Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/index.html
r. Secure Filebeat: https://www.elastic.co/guide/en/beats/filebeat/8.0/securing-filebeat.html
s. Metricbeat: https://www.elastic.co/guide/en/beats/metricbeat/8.0/index.html
t. Secure Metricbeat:
https://www.elastic.co/guide/en/beats/metricbeat/8.0/securing-metricbeat.html
q. Packetbeat: https://www.elastic.co/guide/en/beats/packetbeat/8.0/index.html
u. Secure Packetbeat:
https://www.elastic.co/guide/en/beats/packetbeat/8.0/securing-packetbeat.html
v. Heartbeat: https://www.elastic.co/guide/en/beats/heartbeat/8.0/index.html
w. Secure Heartbeat:
https://www.elastic.co/guide/en/beats/heartbeat/8.0/securing-heartbeat.html
x. Winlogbeat: https://www.elastic.co/guide/en/beats/winlogbeat/8.0/index.html
y. Secure Winlogbeat:
https://www.elastic.co/guide/en/beats/winlogbeat/8.0/securing-winlogbeat.html
z. Logstash: https://www.elastic.co/guide/en/logstash/8.0/index.html
aa. Secure your connection to Elasticsearch with logstash:
https://www.elastic.co/guide/en/logstash/8.0/ls-security.html
ab. Install Elastic Agents :
https://www.elastic.co/guide/en/fleet/current/elastic-agent-installation.html
ac. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without information that establishes the identity of the subjects (i.e., users or processes acting on behalf of users) associated with the events, security personnel cannot determine responsibility for the potentially harmful event.

Event identifiers (if authenticated or otherwise known) include, but are not limited to, user database tables, primary key values, user names, or process identifiers.

Legacy Ids: V-100055; SV-109159

CCI: CCI-001487The information system generates audit records containing information that establishes the identity of any individuals or subjects associated with the event.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must protect audit information from any type of unauthorized read access.
STIG ID: SRG-APP-000118 **Rule ID:** SV-221914r420086_rule **Vul ID:** V-221914
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to protect audit information from any unauthorized read access.

If the Central Log Server is not configured to protect audit information from any unauthorized read access, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Elastic stack must be configured to be secured by using TLS encrypted communication, role based access control (RBAC).

2. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts which needs to be secured by using TLS encrypted communication, role based access control (RBAC).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
k. Configuring security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
l. Start the Elastic Stack with security enabled :
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If audit data were to become compromised, then competent forensic analysis and discovery of the true source of potentially malicious system activity is difficult if not impossible to achieve. In addition, access to audit records provides information an attacker could potentially use to his or her advantage.

To ensure the veracity of audit data, the information system and/or the application must protect audit information from any and all unauthorized access. This includes read, write, and copy access.

This requirement can be achieved through multiple methods which will depend upon system architecture and design. Commonly employed methods for protecting audit information include least privilege permissions as well as restricting the location and number of log file repositories.

Additionally, applications with user interfaces to audit records should not allow for the unfettered manipulation of or access to those records via the application. If the application provides access to the audit data, the application becomes accountable for ensuring audit information is protected from unauthorized access.

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Legacy Ids: V-100057; SV-109161

CCI: CCI-000162The information system protects audit information from unauthorized access.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must protect audit information from unauthorized modification.
STIG ID: SRG-APP-000119 **Rule ID:** SV-221915r420089_rule **Vul ID:** V-221915
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to protect audit information from any unauthorized modification.

If the Central Log Server is not configured to protect audit information from any unauthorized modification, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Elastic stack must be configured to be secured by using TLS encrypted communication, role based access control (RBAC).

2. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts which needs to be secured by using TLS encrypted communication, role based access control (RBAC).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
k. Configuring security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
l. Start the Elastic Stack with security enabled :
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If audit data were to become compromised, then forensic analysis and discovery of the true source of potentially malicious system activity is impossible to achieve.

To ensure the veracity of audit data, the information system and/or the application must protect audit information from unauthorized modification.

This requirement can be achieved through multiple methods, which will depend upon system architecture and design. Some commonly employed methods include ensuring log files receive the proper file system permissions, and limiting log data locations.

Applications providing a user interface to audit data will leverage user permissions and roles identifying the user accessing the data and the corresponding rights that the user enjoys in order to make access decisions regarding the modification of audit data.

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Legacy Ids: V-100059; SV-109163

CCI: CCI-000163The information system protects audit information from unauthorized modification.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must protect audit information from unauthorized deletion.
STIG ID: SRG-APP-000120 **Rule ID:** SV-221916r420092_rule **Vul ID:** V-221916
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to protect audit information from unauthorized deletion.

If the Central Log Server is not configured to protect audit information from unauthorized deletion, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Elastic stack must be configured to be secured by using TLS encrypted communication, role based access control (RBAC).

2. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts which needs to be secured by using TLS encrypted communication, role based access control (RBAC).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
k. Configuring security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
l. Start the Elastic Stack with security enabled :
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If audit data were to become compromised, then forensic analysis and discovery of the true source of potentially malicious system activity is impossible to achieve.

To ensure the veracity of audit data, the information system and/or the application must protect audit information from unauthorized deletion. This requirement can be achieved

through multiple methods, which will depend upon system architecture and design.

Some commonly employed methods include: ensuring log files receive the proper file system permissions utilizing file system protections, restricting access, and backing up log data to ensure log data is retained.

Applications providing a user interface to audit data will leverage user permissions and roles identifying the user accessing the data and the corresponding rights the user enjoys in order make access decisions regarding the deletion of audit data.

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. Audit information may include data from other applications or be included with the audit application itself.

Legacy Ids: V-100061; SV-109165

CCI: CCI-000164The information system protects audit information from unauthorized deletion.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must protect audit tools from unauthorized access.
STIG ID: SRG-APP-000121 **Rule ID:** SV-221917r420095_rule **Vul ID:** V-221917
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to protect audit tools from unauthorized access.

If the Central Log Server is not configured to protect audit tools from unauthorized access, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Elastic stack must be configured to be secured by using TLS encrypted communication, role based access control (RBAC).

2. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts which needs to be secured by using TLS encrypted

communication, role based access control (RBAC).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
k. Configuring security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
l. Start the Elastic Stack with security enabled :
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protecting audit data also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit data.

Applications providing tools to interface with audit data will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user enjoys in order make access decisions regarding the access to audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Legacy Ids: V-100063; SV-109167

CCI: CCI-001493The information system protects audit tools from unauthorized access.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must protect audit tools from unauthorized modification.
STIG ID: SRG-APP-000122 **Rule ID:** SV-221918r420098_rule **Vul ID:** V-221918
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to protect audit tools from unauthorized modification.

If the Central Log Server is not configured to protect audit tools from unauthorized modification, this is a finding.

Fix Text:
Steps/Recommendation:

1. Audit Logs are stored in Elasticsearch and indexed. Elastic stack must be configured to be secured by using TLS encrypted communication, role based access control (RBAC).

2. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts which needs to be secured by using TLS encrypted communication, role based access control (RBAC).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch
Authentication:https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html

c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. Setting Up User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
e. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
f. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
g. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
h. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
i. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
j. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
k. Configuring security in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html
l. Start the Elastic Stack with security enabled :
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-stack-security.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protecting audit data also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit data.

Applications providing tools to interface with audit data will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user enjoys in order make access decisions regarding the modification of audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Legacy Ids: V-100065; SV-109169

CCI: CCI-001494The information system protects audit tools from unauthorized modification.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision

4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must protect audit tools from unauthorized deletion.
STIG ID: SRG-APP-000123 **Rule ID:** SV-221919r420101_rule **Vul ID:** V-221919
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to protect audit tools from unauthorized deletion.

If the Central Log Server is not configured to protect audit tools from unauthorized deletion, this is a finding.

Fix Text:
Steps/Recommendation:

1. Elastic Audit tools uses the default elasticsearch.yml file to configure audit information's. To implement and secure the elastic stack, following has to be implemented:
- Preventing unauthorized access with password protection, role-based access control, and IP filtering.
- Preserving the integrity of your data with SSL/TLS encryption.

2. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts which needs to be secured by using TLS encrypted communication, role based access control (RBAC), and IP filtering.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. Configure TLS:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html
k. Restricting connections with IP filtering:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ip-filtering.html

Elastic Stack 8.0

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Protecting audit data also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit data.

Applications providing tools to interface with audit data will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user enjoys in order make access decisions regarding the deletion of audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Legacy Ids: V-100067; SV-109171

CCI: CCI-001495The information system protects audit tools from unauthorized deletion.NIST SP 800-53 :: AU-9NIST SP 800-53A :: AU-9.1NIST SP 800-53 Revision 4 :: AU-9

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured to disable non-essential capabilities.
STIG ID: SRG-APP-000141 **Rule ID:** SV-221920r420104_rule **Vul ID:** V-221920
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to disable non-essential capabilities.

If the Central Log Server is not configured to disable non-essential capabilities, this is a finding.

Fix Text:
Steps/Recommendation:

1. All audit logging requirements can be configured in elasticsearch.yml. The audit requirement should be defined by the line of business in security plan document. The configuration should match all the required audit attributes defined in the security plan document.

2. To enable the required attributes as defined in the document, Refer to latest documentation for full set of supported attributes:
https://www.elastic.co/guide/en/elasticsearch/reference/current/audit-event-types.html

3. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts which needs to be secured to match all the required audit attributes defined in the security plan document.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

Elastic Stack 8.0

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: It is detrimental for applications to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Applications are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, advertising software or browser plug-ins not related to requirements or providing a wide array of functionality not required for every mission, but cannot be disabled.

Legacy Ids: V-100069; SV-109173

CCI: CCI-000381The organization configures the information system to provide only essential capabilities.NIST SP 800-53 :: CM-7NIST SP 800-53A :: CM-7.1 (ii)NIST SP 800-53 Revision 4 :: CM-7 a

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must notify system administrators and ISSO when accounts are created.
STIG ID: SRG-APP-000291 **Rule ID:** SV-221921r420107_rule **Vul ID:** V-221921
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to notify system administrators and the ISSO when accounts are created.

If the Central Log Server is not configured to notify system administrators and ISSO when accounts are created, this is a finding.

Fix Text:
Steps/Recommendation:

1. The Elastic Stack can be configured to notify the System Administrator (SA) and Information System Security Officer (ISSO) when account creation events are received, typically performed via the Kibana user interface.

2. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts and to notify the System Administrator (SA) and Information System Security Officer (ISSO) when account creation events are received.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html
j. X-Pack Alerting:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/xpack-alerting.html

Elastic Stack 8.0

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Once an attacker establishes access to an application, the attacker often attempts to create a persistent method of re-establishing access. One way to accomplish this is for the attacker to simply create a new account. Sending notification of account creation events to the

system administrator and ISSO is one method for mitigating this risk.

To address access requirements, many application developers choose to integrate their applications with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements. Such integration allows the application developer to off-load those access control functions and focus on core application features and functionality.

Legacy Ids: V-100021; SV-109125

CCI: CCI-001683The information system notifies organization-defined personnel or roles for account creation actions.NIST SP 800-53 :: AC-2 (4)NIST SP 800-53A :: AC-2 (4).1 (i&ii)NIST SP 800-53 Revision 4 :: AC-2 (4)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.
STIG ID: SRG-APP-000295 **Rule ID:** SV-221922r420110_rule **Vul ID:** V-221922
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to automatically terminate a user session after organization-defined conditions or trigger events.

If the Central Log Server is not configured to automatically terminate a user session after organization-defined conditions or trigger events, this is a finding.

Fix Text:
Steps/Recommendation:

1. Sessions are tied to user logins, not the queries the user executes. Elasticsearch itself does not provide session control. You can use Kibana as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to support automatically terminating a user session after organization-defined conditions or trigger events requiring session disconnect.

2. Kibana Session timeout and a few other Kibana security-related settings are available at: https://www.elastic.co/guide/en/kibana/8.0/security-settings-kb.html

Examples:
xpack.security.session.idleTimeout
Sets the session duration. By default, sessions stay active until the browser is closed. When this is set to an explicit idle timeout, closing the browser still requires the user to log back in to Kibana.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 70ms, 5s, 3d, 1Y).

xpack.security.session.lifespan
Sets the maximum duration, also known as "absolute timeout". By default, a session can be renewed indefinitely. When this value is set, a session will end once its lifespan is exceeded, even if the user is not idle. NOTE: if idleTimeout is not set, this setting will still cause sessions to expire.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 70ms, 5s, 3d, 1Y).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

Elastic Stack 8.0

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Automatic session termination addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions.

Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.

Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on information system use.

This capability is typically reserved for specific application system functionality where the system owner, data owner, or organization requires additional assurance. Based upon requirements and events specified by the data or application owner, the application developer must incorporate logic into the application that will provide a control mechanism that disconnects users upon the defined event trigger. The methods for incorporating this requirement will be determined and specified on a case by case basis during the application design and development stages.

Legacy Ids: V-100015; SV-109119

CCI: CCI-002361The information system automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect.NIST SP 800-53 Revision 4 :: AC-12

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must provide a logout capability for user initiated communication session.
STIG ID: SRG-APP-000296 **Rule ID:** SV-221923r420113_rule **Vul ID:** V-221923
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server provides a logout capability for user initiated sessions.

If the Central Log Server does not provide a logout capability for user initiated sessions, this is a finding.

Fix Text:
Steps/Recommendation:

1. Sessions are tied to user logins, not the queries the user executes. Elasticsearch itself does not provide session control. You can use Kibana as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to support automatically terminate a user session after organization-defined conditions or trigger events.

2. Kibana Session timeout and a few other Kibana security-related settings are available at:
https://www.elastic.co/guide/en/kibana/8.0/security-settings-kb.html

Examples:
xpack.security.session.idleTimeout
Sets the session duration. By default, sessions stay active until the browser is closed. When this is set to an explicit idle timeout, closing the browser still requires the user to log back in to Kibana.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 70ms, 5s, 3d, 1Y).

xpack.security.session.lifespan
Sets the maximum duration, also known as "absolute timeout". By default, a session can be renewed indefinitely. When this value is set, a session will end once its lifespan is exceeded, even if the user is not idle. NOTE: if idleTimeout is not set, this setting will still cause sessions to expire.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 70ms, 5s, 3d, 1Y).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

Elastic Stack 8.0

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If a user cannot explicitly end an application session, the session may remain open and be exploited by an attacker; this is referred to as a zombie session.

Information resources to which users gain access via authentication include, for example, local workstations, databases, and password-protected websites/web-based services. However, for some types of interactive sessions including, for example, file transfer protocol (FTP) sessions, information systems typically send logout messages as final messages prior to terminating sessions.

Legacy Ids: V-100017; SV-109121

CCI: CCI-002363The information system provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to organization-defined information resources.NIST SP 800-53 Revision 4 :: AC-12 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must display an explicit logout message to users indicating the reliable termination of authenticated communications sessions.
STIG ID: SRG-APP-000297 **Rule ID:** SV-221924r420116_rule **Vul ID:** V-221924
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to display an explicit logout message to users indicating the reliable termination of authenticated sessions.

If the Central Log Server is not configured to display an explicit logout message to users, it is

a finding.

Fix Text:
Steps/Recommendation:

1. Sessions are tied to user logins, not the queries the user executes. Elasticsearch itself does not provide session control.

2. Kibana supports a banner, however it is disabled by default. It needs to be manually configured in order to use the feature.

Configure the xpack.banners settings in the kibana.yml file:

xpack.banners.placement
  Set to top to display a banner above the Elastic header. Defaults to disabled.
xpack.banners.textContent
  The text to display inside the banner, either plain text or Markdown.
xpack.banners.textColor
  The color for the banner text. Defaults to #8A6A0A.
xpack.banners.backgroundColor
  The color of the banner background. Defaults to #FFF9E8.
xpack.banners.disableSpaceBanners
  If true, per-space banner overrides will be disabled. Defaults to false.

Note: Banners are a subscription feature.

3. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to display an explicit logout message to users indicating the reliable termination of authenticated sessions.

References:

a. Banner settings in Kibana:
https://www.elastic.co/guide/en/kibana/master/banners-settings-kb.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html

g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If a user cannot explicitly end an application session, the session may remain open and be exploited by an attacker; this is referred to as a zombie session. Users need to be aware of whether or not the session has been terminated.

Information resources to which users gain access via authentication include, for example, local workstations, databases, and password-protected websites/web-based services. Logout messages for web page access, for example, can be displayed after authenticated sessions have been terminated. However, for some types of interactive sessions including, for example, file transfer protocol (FTP) sessions, information systems typically send logout messages as final messages prior to terminating sessions.

Legacy Ids: V-100019; SV-109123

CCI: CCI-002364The information system displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.NIST SP 800-53 Revision 4 :: AC-12 (1)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must automatically lock the account until the locked account is released by an administrator when three unsuccessful login attempts in 15 minutes are exceeded.
STIG ID: SRG-APP-000345 **Rule ID:** SV-221925r420119_rule **Vul ID:** V-221925
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server is configured to lock out the account until released by an administrator when 3 consecutive invalid attempts during a 15 minute period is exceeded.

If the Central Log Server is not configured to lock out the account until released by an administrator when 3 consecutive invalid attempts in 15 minutes is exceeded, this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts and perform this configuration The recommendation is to integrate Elasticsearch with these services to automatically lock the account until the locked account is released by an administrator when three unsuccessful login attempts in 15 minutes are exceeded.

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: By limiting the number of failed login attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are

imposed by locking the account.

Legacy Ids: V-100035; SV-109139

CCI: CCI-002238The information system automatically locks the account or node for either an organization-defined time period until the locked account or node is released by an administrator or delays the next login prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.NIST SP 800-53 Revision 4 :: AC-7 b

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must require users to reauthenticate when organization-defined circumstances or situations require reauthentication.
STIG ID: SRG-APP-000389 **Rule ID:** SV-221926r420122_rule **Vul ID:** V-221926
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server requires users to reauthenticate when situations require reauthentication.

If the Central Log Server is not configured to reauthenticate when necessary, this is a finding.

Fix Text:
Steps/Recommendation:

1. Sessions are tied to user logins, not the queries the user executes. Elasticsearch itself does not provide session control. You can use Kibana as the front end, and Kibana manages its sessions. Alternatively, Elasticsearch supports integration with centralized authentication services (LDAP/S, Active Directory, and PKI) to manage accounts and to uniquely identify and authenticate organizational users. The recommendation is to integrate Elasticsearch with these services to require users to reauthenticate when situations require reauthentication.

2. Kibana Session timeout and a few other Kibana security-related settings are available at: https://www.elastic.co/guide/en/kibana/8.0/security-settings-kb.html

Examples:
xpack.security.session.idleTimeout
Sets the session duration. By default, sessions stay active until the browser is closed. When this is set to an explicit idle timeout, closing the browser still requires the user to log back in

to Kibana.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 70ms, 5s, 3d, 1Y).

xpack.security.session.lifespan
Sets the maximum duration, also known as "absolute timeout". By default, a session can be renewed indefinitely. When this value is set, a session will end once its lifespan is exceeded, even if the user is not idle. NOTE: if idleTimeout is not set, this setting will still cause sessions to expire.

The format is a string of <count>[ms|s|m|h|d|w|M|Y] (e.g. 70ms, 5s, 3d, 1Y).

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. SAML Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-kibana.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without reauthentication, users may access resources or perform tasks for which they do not have authorization.

When applications provide the capability to change security roles or escalate the functional capability of the application, it is critical the user reauthenticate.

In addition to the reauthentication requirements associated with session locks, organizations may require reauthentication of individuals and/or devices in other situations, including (but not limited to) the following circumstances.

(i) When authenticators change;
(ii) When roles change;
(iii) When security categories of information systems change;
(iv) When the execution of privileged functions occurs;
(v) After a fixed period of time; or
(vi) Periodically.

Within the DoD, the minimum circumstances requiring reauthentication are privilege escalation and role changes.

Legacy Ids: V-100071; SV-109175

CCI: CCI-002038The organization requires users to reauthenticate when organization-defined circumstances or situations requiring reauthentication.NIST SP 800-53 Revision 4 :: IA-11

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must only allow the use of DoD PKI established certificate authorities for verification of the establishment of protected sessions.
STIG ID: SRG-APP-000427 **Rule ID:** SV-221927r420125_rule **Vul ID:** V-221927
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to only allow the use of DoD PKI certificate authorities.

If the Central Log Server is not configured to only allow DoD PKI certificate authorities, this is a finding.

Fix Text:
Step/Recommendation:

1. The certificate used should be DoD approved certificate authority.

Enabling TLS/SSL across the entire Elastic cluster for transport communication is required for satisfying this control. Recommended approach is to use Public key Infrastructure (PKI - client certificate) for all username/password including that is used for Kibana/or other applications interacting with Elasticsearch.

References:

a. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
b. Elasticsearch Security: Configure TLS/SSL & PKI Authentication :
https://www.elastic.co/blog/elasticsearch-security-configure-tls-ssl-pki-authentication
c. Configure TLS:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/configuring-tls.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Untrusted Certificate Authorities (CA) can issue certificates, but they may be issued by organizations or individuals that seek to compromise DoD systems or by organizations with insufficient security controls. If the CA used for verifying the certificate is not a DoD-approved CA, trust of this CA has not been established.

The DoD will only accept PKI certificates obtained from a DoD-approved internal or external certificate authority. Reliance on CAs for the establishment of secure sessions includes, for example, the use of TLS certificates.

This requirement focuses on communications protection for the application session rather than for the network packet.

This requirement applies to applications that utilize communications sessions. This includes, but is not limited to, web-based applications and Service-Oriented Architectures (SOA).

Legacy Ids: V-100075; SV-109179

CCI: CCI-002470The information system only allows the use of organization-defined certificate authorities for verification of the establishment of protected sessions.NIST SP 800-53 Revision 4 :: SC-23 (5)

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security

Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must generate audit records when successful/unsuccessful logon attempts occur.
STIG ID: SRG-APP-000503 **Rule ID:** SV-221928r420128_rule **Vul ID:** V-221928
Severity: CAT II

Documentable: No

Check Content:
Examine the configuration.

Verify that the Central Log Server generates audit records when successful/unsuccessful logon attempts occur.

If the Central Log Server is not configured to generate audit records when successful/unsuccessful logon attempts occur, this is a finding.

Fix Text:
Steps/Recommendation:

1. The security-related events such as authentication failures and refused connection to monitor a cluster can be logged by enabling audit logging.

2. To Enable audit Logging: Set xpack.security.audit.enabled to true in elasticsearch.yml.

For the hosted Elasticsearch Service (SaaS offering), Elastic Cloud audit logging needs to be explicitly enabled. For more information, see https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Audit logs are only available on certain subscription levels. For more information, see https://www.elastic.co/subscriptions.

3. To satisfy this control following events must be logged (not limited to): authentication_success, authentication_failed, realm_authentication_failed, access_denied, access_granted, run_as_denied, run_as_granted, tampered_request

References:

a. Kibana Authentication:
https://www.elastic.co/guide/en/kibana/8.0/kibana-authentication.html
b. Elasticsearch Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/setting-up-authentication.html
c. Elasticsearch Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html
d. SAML Authentication:

https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-realm.html
e. Active Directory User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/active-directory-realm.html
f. PKI User Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/pki-realm.html
g. Lightweight Directory Access Protocol (LDAP) Authentication:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/ldap-realm.html
h. Integrating with Other Authentication Systems:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/custom-realms.html
i. SAML single-sign-on (SSO) into Kibana, using Elasticsearch as a backend service:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/saml-guide-stack.html#saml-configure-kibana
j. Auditing Security Settings:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/auditing-settings.html
k. Audit Event Type:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/audit-event-types.html
l. Enable Elastic Cloud logging and monitoring:
https://www.elastic.co/guide/en/cloud/current/ec-enable-logging-and-monitoring.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident, or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Legacy Ids: V-100041; SV-109145

CCI: CCI-000172The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.NIST SP 800-53 :: AU-12 cNIST SP 800-53A :: AU-12.1 (iv)NIST SP 800-53 Revision 4 :: AU-12 c

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must use FIPS-validated SHA-2 or higher hash function for digital signature generation and verification (non-legacy use).

STIG ID: SRG-APP-000610 **Rule ID:** SV-221929r531240_rule **Vul ID:** V-221929
Severity: CAT I

Documentable: No

Check Content:
Examine the configuration.

Verify the Central Log Server is configured to use FIPS-validated SHA-1 or higher hash function to protect the integrity of keyed-hash message authentication code (HMAC), Key Derivation Functions (KDFs), Random Bit Generation, hash-only applications, and digital signature verification (legacy use only).

If the Central Log Server is not configured to use FIPS-validated SHA-1 or higher hash function to protect the integrity of keyed-hash message authentication code (HMAC), Key Derivation Functions (KDFs), Random Bit Generation, hash-only applications, and digital signature verification (legacy use only), this is a finding.

Fix Text:
Step/Recommendation:

1. Elasticsearch uses hashing algorithms compliant with this control out of the box, so no additional configuration is needed.

Reference:

a. Security settings in Elasticsearch:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/security-settings.html

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

To protect the integrity of the authenticator and authentication mechanism used for the cryptographic module used by the network device, the application, operating system, or protocol must be configured to use one of the following hash functions for hashing the password or other authenticator in accordance with SP 800-131Ar1: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256, SHA3-384, and

SHA3-512.

For digital signature verification, SP800-131Ar1 allows SHA-1 for legacy use where needed.

Legacy Ids: V-100073; SV-109177

CCI: CCI-000803The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.NIST SP 800-53 :: IA-7NIST SP 800-53A :: IA-7.1NIST SP 800-53 Revision 4 :: IA-7

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The System Administrator (SA) and Information System Security Manager (ISSM) must configure the retention of the log records based on criticality level, event type, and/or retention period, at a minimum.
STIG ID: SRG-APP-000095 **Rule ID:** SV-241819r695402_rule **Vul ID:** V-241819
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the SA and ISSM have been assigned the privileges needed to allow these roles to change the level and type of log records that are retained in the centralized repository based on any selectable event criteria.

Verify the retention configuration for each host and device is in compliance with the documented organization criteria, including the identified criticality level, event type, and/or retention period.

If the Central Log Server is not configured to allow the SA and ISSM to change the retention of the log records, this is a finding.

If the retention is not in compliance with the organization's documentation, this is a finding.

Fix Text:
Steps/Recommendation:

1. Recommend using Elasticsearch's Index Lifecycle Management (ILM) feature to enforce a defined retention policy.

2. Recommend using Elasticsearch's Snapshot Lifecycle Management (SLM) feature to enforce a defined retention policy.

References:

a. Get started: Automate rollover with ILM:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/getting-started-index-lifecycle-management.html
b. Automate Snapshots with SLM:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/snapshots-take-snapshot.html#automate-snapshots-slm

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If authorized individuals do not have the ability to modify auditing parameters in response to a changing threat environment, the organization may not be able to respond effectively and important forensic information may be lost.

The organization must define and document log retention requirements for each device and host and then configure the Central Log Sever to comply with the required retention period.

This requirement enables organizations to extend or limit auditing as necessary to meet organizational requirements. Auditing that is limited to conserve information system resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of events to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which audit actions are changed; for example, in near real time, within minutes, or within hours.

Legacy Ids: V-81137; SV-95851

CCI: CCI-001914The information system provides the capability for organization-defined individuals or roles to change the auditing to be performed on organization-defined information system components based on organization-defined selectable event criteria within organization-defined time thresholds.NIST SP 800-53 Revision 4 :: AU-12 (3)CCI-000130The information system generates audit records containing information that establishes what type of event occurred.NIST SP 800-53 :: AU-3NIST SP 800-53A :: AU-3.1NIST SP 800-53 Revision 4 :: AU-3

STIG: Elasticsearch 8.0 Hardening Guide based on Central Log Server Security Requirement Guide :: Version 2, Release 1 Benchmark Date: 24 June 2021 :: Version 1
Rule Title: The Central Log Server must be configured so changes made to the level and type of log records stored in the centralized repository must take effect immediately without the need to reboot or restart the application.
STIG ID: SRG-APP-000516 **Rule ID:** SV-241820r695405_rule **Vul ID:** V-241820
Severity: CAT III

Documentable: No

Check Content:
Examine the configuration.

Verify the system is configured so changes made to the level and type of log records stored in the centralized repository take effect immediately without the need to reboot or restart the application.

If the Central Log Server is not configured so changes made to the level and type of log records stored in the centralized repository must take effect immediately without the need to reboot or restart the application, this is a finding.

Fix Text:

1. Elasticsearch's Index modules (index.refresh_interval) features can also be utilized, so changes made to the level and type of log records stored in the centralized repository must take effect immediately without the need to reboot or restart the application.

Reference:

a. Index modules:
https://www.elastic.co/guide/en/elasticsearch/reference/8.0/index-modules.html#dynamic-index-settings

Elastic Stack 8.0:

This STIG was tested and evaluated using Elastic Stack 8.0. All controls and documentation links are accurate for version 8.0. However, many of the controls, recommendations, and guidance will work for newer versions of the Elastic Stack. Always verify the version of the Stack you are using and ensure you are using the matching version of the Elastic documentation.

Discussion: If authorized individuals do not have the ability to modify auditing parameters in response to a changing threat environment, the organization may not be able to respond effectively and important forensic information may be lost.

This requirement enables organizations to extend or limit auditing as necessary to meet

organizational requirements. Auditing that is limited to conserve information system resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of events to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which audit actions are changed; for example, in near real time, within minutes, or within hours.

Legacy Ids: V-81139; SV-95853

CCI: CCI-000366 The organization implements the security configuration settings. NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b CCI-001914 The information system provides the capability for organization-defined individuals or roles to change the auditing to be performed on organization-defined information system components based on organization-defined selectable event criteria within organization-defined time thresholds. NIST SP 800-53 Revision 4 :: AU-12 (3)