



## Audit Store Guide 9.1.0.5

Created on: Nov 19, 2024

# Notice

## Copyright

Copyright © 2004-2024 Protegrity Corporation. All rights reserved.

Protegrity products are protected by and subject to patent protections;

Patent: <https://www.protegrity.com/patents>.

The Protegrity logo is the trademark of Protegrity Corporation.

### NOTICE TO ALL PERSONS RECEIVING THIS DOCUMENT

Some of the product names mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective owners.

Windows, Azure, MS-SQL Server, Internet Explorer and Internet Explorer logo, Active Directory, and Hyper-V are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SCO and SCO UnixWare are registered trademarks of The SCO Group.

Sun, Oracle, Java, and Solaris are the registered trademarks of Oracle Corporation and/or its affiliates in the United States and other countries.

Teradata and the Teradata logo are the trademarks or registered trademarks of Teradata Corporation or its affiliates in the United States and other countries.

Hadoop or Apache Hadoop, Hadoop elephant logo, Hive, and Pig are trademarks of Apache Software Foundation.

Cloudera and the Cloudera logo are trademarks of Cloudera and its suppliers or licensors.

Hortonworks and the Hortonworks logo are the trademarks of Hortonworks, Inc. in the United States and other countries.

Greenplum Database is the registered trademark of VMware Corporation in the U.S. and other countries.

Pivotal HD is the registered trademark of Pivotal, Inc. in the U.S. and other countries.

PostgreSQL or Postgres is the copyright of The PostgreSQL Global Development Group and The Regents of the University of California.

AIX, DB2, IBM and the IBM logo, and z/OS are registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

---

Utimaco Safeware AG is a member of the Sophos Group.

Xen, XenServer, and Xen Source are trademarks or registered trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

VMware, the VMware “boxes” logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

Amazon Web Services (AWS) and AWS Marks are the registered trademarks of Amazon.com, Inc. in the United States and other countries.

HP is a registered trademark of the Hewlett-Packard Company.

HPE Ezmeral Data Fabric is the trademark of Hewlett Packard Enterprise in the United States and other countries.

Dell is a registered trademark of Dell Inc.

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

POSIX is a registered trademark of the Institute of Electrical and Electronics Engineers, Inc.

Mozilla and Firefox are registered trademarks of Mozilla foundation.

Chrome and Google Cloud Platform (GCP) are registered trademarks of Google Inc.

Swagger Specification and all public tools under the swagger-api GitHub account are trademarks of Apache Software Foundation and licensed under the Apache 2.0 License.

## Table of Contents

<b>Copyright.....</b>	<b>2</b>
<b>Chapter 1 Introduction to This Guide.....</b>	<b>6</b>
1.1 Sections contained in this Guide.....	6
1.2 Accessing the Protegrity documentation suite.....	6
<b>Chapter 2 Introduction to the Audit Store.....</b>	<b>7</b>
2.1 Logging Architecture.....	7
<b>Chapter 3 Setting Up the Audit Store.....</b>	<b>9</b>
3.1 Installing the Audit Store.....	9
3.2 Verifying Services.....	9
3.3 Rotating Audit Store Certificates.....	10
3.3.1 Rotating Certificates on a Single Node Audit Store Cluster.....	10
3.3.2 Rotating Certificates on a Multi-Node Audit Store Cluster.....	16
<b>Chapter 4 Understanding the Audit Store Status.....</b>	<b>27</b>
4.1 Viewing Cluster Status.....	27
4.2 Viewing the Node Status.....	28
4.3 Viewing the Index Status.....	29
4.4 Working with Roles.....	30
<b>Chapter 5 Clustering Using the Audit Store.....</b>	<b>33</b>
5.1 Adding an ESA to the Audit Store Cluster.....	34
5.1.1 Initializing the Audit Store Cluster on the ESA.....	34
5.1.2 Adding an ESA to the Audit Store Cluster.....	35
5.1.3 Refreshing the Audit Store Cluster Settings .....	37
5.2 Removing an ESA from the Audit Store Cluster.....	38
<b>Chapter 6 Viewing the Audit Store Data.....</b>	<b>40</b>
<b>Chapter 7 Troubleshooting.....</b>	<b>41</b>
7.1 Known Issues for the Audit Store.....	41
<b>Appendix 8 Audit Store CLI Options.....</b>	<b>44</b>
8.1 Rotating Audit Store Certificates.....	44
8.2 Applying Audit Store Security Configuration.....	45
8.3 Setting the Total Memory for the Audit Store Repository.....	46
<b>Appendix 9 Configuring Security for the Log Forwarder.....</b>	<b>48</b>
9.1 Enabling Basic Authentication.....	48
9.1.1 Configuring the Audit Store.....	48
9.1.2 Configuring the Protector.....	52
9.2 Enabling Certificate-Based Authentication.....	53
9.2.1 Configuring the Audit Store.....	53
9.2.2 Configuring the Protector.....	54
<b>Appendix 10 Updating Audit Store Custom Certificates.....</b>	<b>57</b>

---

10.1 Updating Custom Certificates on a Single-Node Audit Store Cluster.....	57
10.2 Updating Custom Certificates on a Multi-Node Audit Store Cluster.....	57
 <b>Appendix 11 Removing the Audit Store from the ESA.....</b>	 <b>66</b>



# Chapter 1

## Introduction to This Guide

### *1.1 Sections contained in this Guide*

### *1.2 Accessing the Protegrity documentation suite*

---

This document provides information about the Audit Store. It contains information for installing, configuring, and using the Audit Store.

## 1.1 Sections contained in this Guide

The guide is broadly divided into the following sections

- Section [Introduction to This Guide](#) defines the purpose and scope for this guide. In addition, it explains how information is organized in this guide.
- Section [Introduction to the Audit Store](#) describes an overview and the architecture of the Audit Store.
- Section [Setting Up the Audit Store](#) lists the steps for installing and configuring the Audit Store. It also describes the steps for rotating Audit Store certificates.
- Section [Understanding the Audit Store Status](#) describes the screens for viewing the status of the nodes in the Audit Store cluster.
- Section [Clustering Using the Audit Store](#) lists the steps for adding and removing a node from the Audit Store cluster.
- Section [Viewing the Audit Store Data](#) provides information for viewing the data stored in the Audit Store.
- Section [Troubleshooting](#) lists the steps for troubleshooting the Audit Store.
- Section [Audit Store CLI Options](#) describes the CLI options available for working with the Audit Store.
- Section [Configuring Security for the Log Forwarder](#) lists the configuration steps for enabling Basic Authentication or Certificate-based Authentication for the Log Forwarder.
- Section [Updating Audit Store Custom Certificates](#) describes the steps for updating custom certificates on a single-node cluster and a multi-node cluster.
- Section [Removing the Audit Store from the ESA](#) describes the steps for removing the Audit Store when you do not require it, such as, when you are using an external SIEM.
- Section [Updating the Domain Name](#) describes the steps for updating the Domain Name for the Audit Store cluster.

## 1.2 Accessing the Protegrity documentation suite

This section describes the methods to access the *Protegrity Documentation Suite* using the [My.Protegrity](#) portal.

# Chapter 2

## Introduction to the Audit Store

### 2.1 Logging Architecture

The Audit Store is a repository for all audit data and logs. The Audit Store is built to support multiple nodes making it scalable. Thus, you can add nodes to the Audit Store cluster as per your requirements. It uses certificates for inter-node communication, making it secure.

## 2.1 Logging Architecture

Logging follows a fixed routine. The system generates logs, which are collected and then forwarded to the Audit Store. The Audit Store holds the logs and these log records are used in various areas, such as, Forensics, alerts, reports, dashboards, and so on. This section explains the logging architecture.

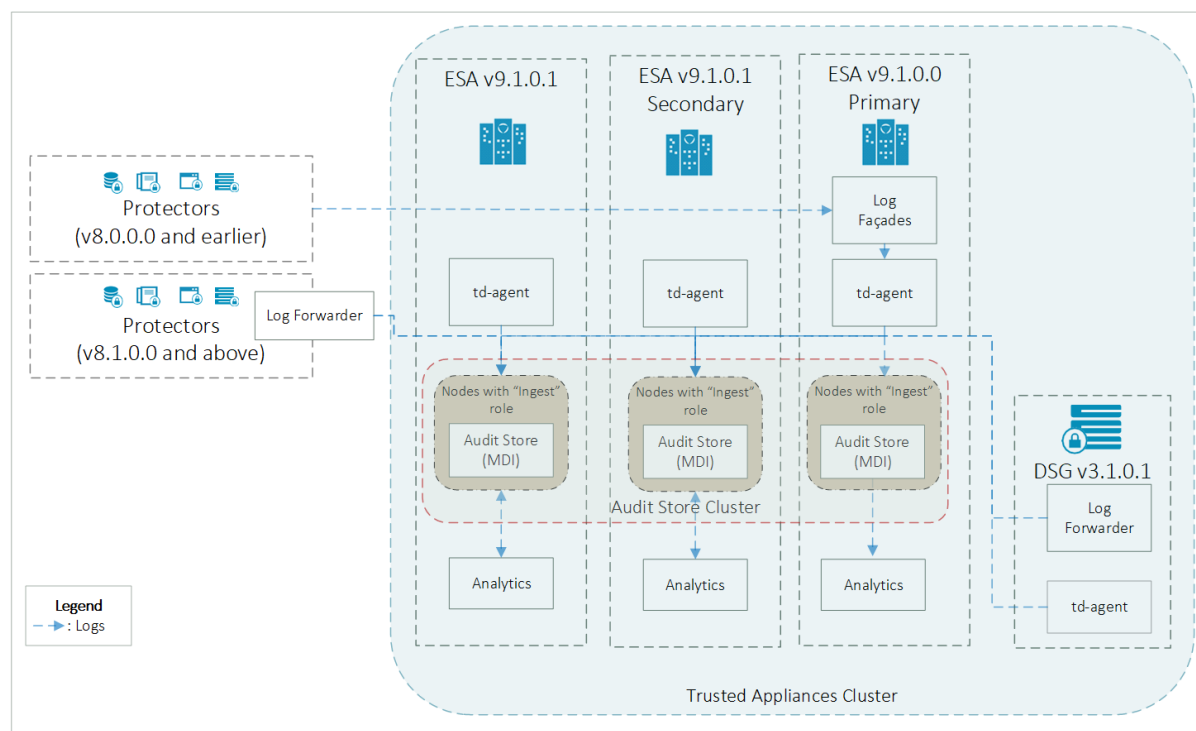


Figure 2-1: Architecture: Overview

- **ESA:**

The ESA has the *td-agent* service installed for receiving and sending logs to the Audit Store. Additionally, the ESA has Protegrity Analytics and the Audit Store installed on it. The ESA receives the logs and stores it in the Audit Store. From this store, the logs are analyzed by Analytics and used in various areas, such as, Forensics, Alerts, Reports, Dashboards, and so

on. Alerts are displayed for events as per the policies configured. Additionally, logs are collected from the log files generated by the P11 Gateway, Hubcontroller, and Membersource services and sent to the Audit Store. By default, all Audit Store nodes have all node roles, that is. Master-eligible, Data, and Ingest. The Audit Store node on the primary ESA can be set to have only Master-eligible node role, which allows it to function as the Master node that manages the Audit Store cluster, when it gets elected as a master.

For more information about roles, refer to the section *Working with Roles* in the [Audit Store Guide 9.1.0.5](#).

**Note:** A minimum of 3 ESAs are required for creating a dependable Audit Store cluster to protect it from system crashes. The architecture diagram shows 3 ESAs. Your architecture might also contain PSUs v9.1.0.0. If you are using the PSUs, then ensure that you keep them updated with all the available patches and fixes.

- **Protectors:**

For v8.1.0.0 and later Protectors, the new logging system is configured to send logs to the Audit Store on the ESA using the Log Forwarder.

For Protectors, the Log Forwarder component is configured in the *pepserver.cfg* file.

For more information about the Log Forwarder-related logging configuration for protectors, refer to the section *Appendix: PEP Server Configuration File* in the [Protegrity Installation Guide 9.1.0.5](#).

For v8.0.0.0 Protectors and earlier, the new logging system is integrated in the Log Facade on the ESA. Using the Log Facade, the logs are received and processed by the *td-agent* service on the ESA 9.1.0.5. Processing involves checking the integrity of the logs and adding audit-related information. The logs are then stored in the Audit Store.

- **DSG 3.1.0.1:**

The DSG has the *td-agent* service installed. The *td-agent* forwards the appliance logs to the Audit Store on the ESA. The *Log Forwarder* service forwards the data security operations-related logs, namely protect, unprotect, and reprotect and the PEP server logs to the Audit Store on the ESA.

For more information about configuring *td-agent* to forward logs, refer to the section [Forwarding System Logs to the Audit Store](#).

For more information about configuring *Log Forwarder* to forward logs, refer to the section *Appendix A: PEP Server Configuration File* in the [Protegrity Installation Guide 9.1.0.5](#).



# Chapter 3

## Setting Up the Audit Store

### [3.1 Installing the Audit Store](#)

### [3.2 Verifying Services](#)

### [3.3 Rotating Audit Store Certificates](#)

An overview about installing the Audit Store is provided in this section. The Audit Store cluster is a collection of nodes that process and store data. The Audit Store is installed on the ESA nodes. The logs generated by the Appliance and Protector machines are stored in this Audit Store. The logs are useful for obtaining information about the nodes and the cluster on the whole. The logs can also be monitored for any data loss, system compromise, or any other issues with the nodes in the Audit Store cluster.

An Audit Store cluster must have a minimum of 3 nodes with the Master-eligible role due to following scenarios:

- 1 master-eligible node: If the only node is present with the Master-eligible role, then it is elected the Master, by default, because it is the only node with the required Master-eligible role. In this case, if the node becomes unavailable due to some failure, then the cluster becomes unstable as there is no additional node with the Master-eligible role.
- 2 master-eligible nodes: A cluster where only 2 nodes have the Master-eligible role will both have the Master-eligible role at the minimum to be up and running for the cluster to remain functional. If any one of those nodes becomes unavailable due to some failure, then the minimum condition for the nodes with the Master-eligible role is not met and cluster becomes unstable.
- 3 master-eligible nodes and above: In this case, if any one node goes down, then the cluster can still remain functional because this cluster requires two nodes with the Master-eligible role to be running at the minimum, as per the minimum Master-eligible role formula.

## 3.1 Installing the Audit Store

The Audit Store consists of Audit Store services for storing logs and for querying to provide information from the Audit Store. The Audit Store is installed by default when you install the ESA 9.1.0.5. The Audit Store is installed on multiple ESA nodes to form the Audit Store Cluster. A minimum of 3 ESAs are required for creating a highly-available multi-node Audit Store cluster.

**Caution:** For more information about creating the Audit Store Cluster, refer to the section *Configuring the Audit Store Cluster* in the *Protegrity Installation Guide 9.1.0.5*.

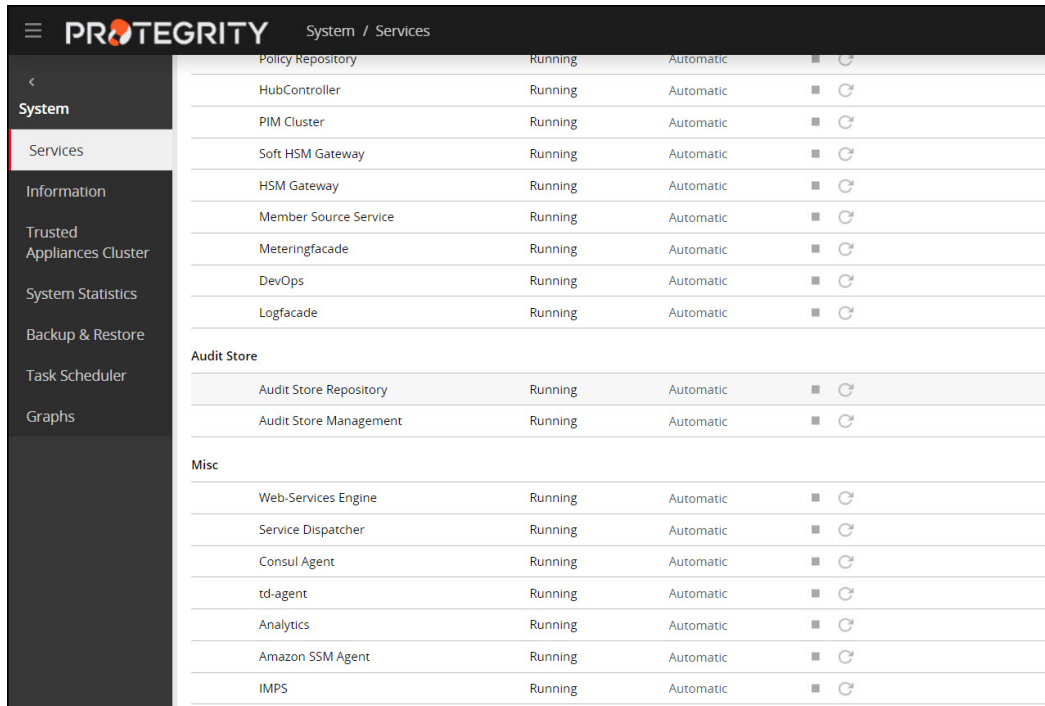
## 3.2 Verifying Services

After you have completed the installation, navigate to the services section on the ESA and verify that the required services are present.

Complete the following steps to check the services.

1. On the ESA Web UI, navigate to **System > Services**.
2. Verify that the following services are installed:
  - **Audit Store**

- **Audit Store Repository:** This service holds the logs and data in the Audit Store.
- **Audit Store Management:** This service manages the nodes in the Audit Store cluster.



PROTEGRITY System / Services			
Policy Repository	Running	Automatic	■ ↻
HubController	Running	Automatic	■ ↻
PIM Cluster	Running	Automatic	■ ↻
Soft HSM Gateway	Running	Automatic	■ ↻
HSM Gateway	Running	Automatic	■ ↻
Member Source Service	Running	Automatic	■ ↻
Meteringfacade	Running	Automatic	■ ↻
DevOps	Running	Automatic	■ ↻
Logfacade	Running	Automatic	■ ↻
<b>Audit Store</b>			
Audit Store Repository	Running	Automatic	■ ↻
Audit Store Management	Running	Automatic	■ ↻
<b>Misc</b>			
Web-Services Engine	Running	Automatic	■ ↻
Service Dispatcher	Running	Automatic	■ ↻
Consul Agent	Running	Automatic	■ ↻
td-agent	Running	Automatic	■ ↻
Analytics	Running	Automatic	■ ↻
Amazon SSM Agent	Running	Automatic	■ ↻
IMPS	Running	Automatic	■ ↻

Figure 3-1: Audit Store Services

### 3. Verify the certificates installed.

For more information about certificates, refer to the section *Audit Store Certificates* in the *Protegrity Certificate Management Guide 9.1.0.5*.

## 3.3 Rotating Audit Store Certificates

The steps provided in this section must be completed to rotate the certificates on the nodes in the Audit Store cluster. Complete the steps for one of the two scenarios, for a single-node Audit Store cluster where nodes have still to be added to the Audit Store cluster or a multi-node Audit Store cluster where the nodes are already added to the Audit Store cluster.

**Note:** These steps are only applicable for the system-generated Protegrity certificate and keys. For rotating custom certificates, refer to [Updating Audit Store Custom Certificates](#).

For more information about certificates, refer to the section *Audit Store Certificates* in the *Protegrity Certificate Management Guide 9.1.0.5*.

**Important:** If the ESA keys are rotated, then the Audit Store certificates must be rotated.

### 3.3.1 Rotating Certificates on a Single Node Audit Store Cluster

Complete the steps provided in this section to rotate the certificates when there is a single node in the Audit Store cluster.

**Note:** These steps are only applicable for the system-generated Protegrity certificate and keys. For rotating custom certificates, refer to [Updating Audit Store Custom Certificates](#).

1. Login to the ESA Web UI.
2. Navigate to **System** > **Services** > **Misc**.
3. Stop the **td-agent** service.

**Note:** Skip this step if *Analytics* is not initialized.

System	All	OS	Policy Management	Audit Store	Misc
Services					
Information					
Trusted Appliances Cluster					
System Statistics					
Backup & Restore					
Task Scheduler					
Graphs					
	Services	Status	Mode	Actions	
	Misc				
	LDAP Server	Running	Automatic	■	↻
	Web-Services Engine	Running	Automatic	■	↻
	Service Dispatcher	Running	Automatic	■	↻
	td-agent	Running	Automatic	■	↻
	Analytics	Running	Automatic	■	↻

Figure 3-2: Stopping td-agent

4. On the ESA Web UI, navigate to **System** > **Services** > **Misc**.
5. Stop the **Analytics** service.

System

Services

Information

Trusted Appliances Cluster

System Statistics

Backup & Restore

Task Scheduler

Graphs

AllOSPolicy ManagementAudit StoreMisc

ServicesStatusModeActions

Misc

LDAP ServerRunningAutomatic■↺

Web-Services EngineRunningAutomatic■↺

Service DispatcherRunningAutomatic■↺

⚠td-agentStoppedAutomatic▶

AnalyticsRunningAutomatic■↺

Figure 3-3: Stopping Analytics

6. Navigate to **System** > **Services** > **Audit Store**.
7. Stop the **Audit Store Management** service.

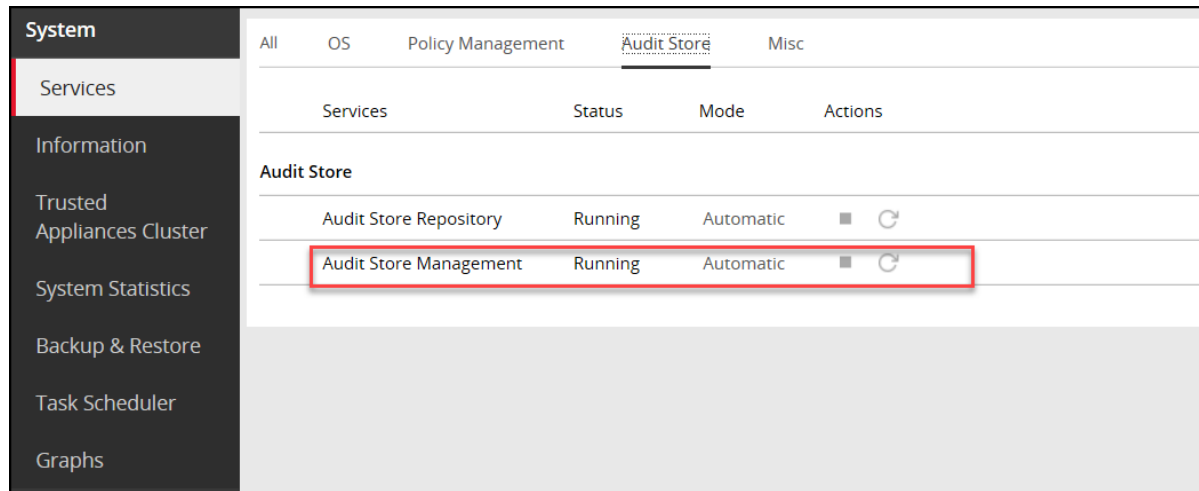


Figure 3-4: Stopping Audit Store Management

8. Navigate to **System > Services > Audit Store**.
9. Stop the **Audit Store Repository** service.

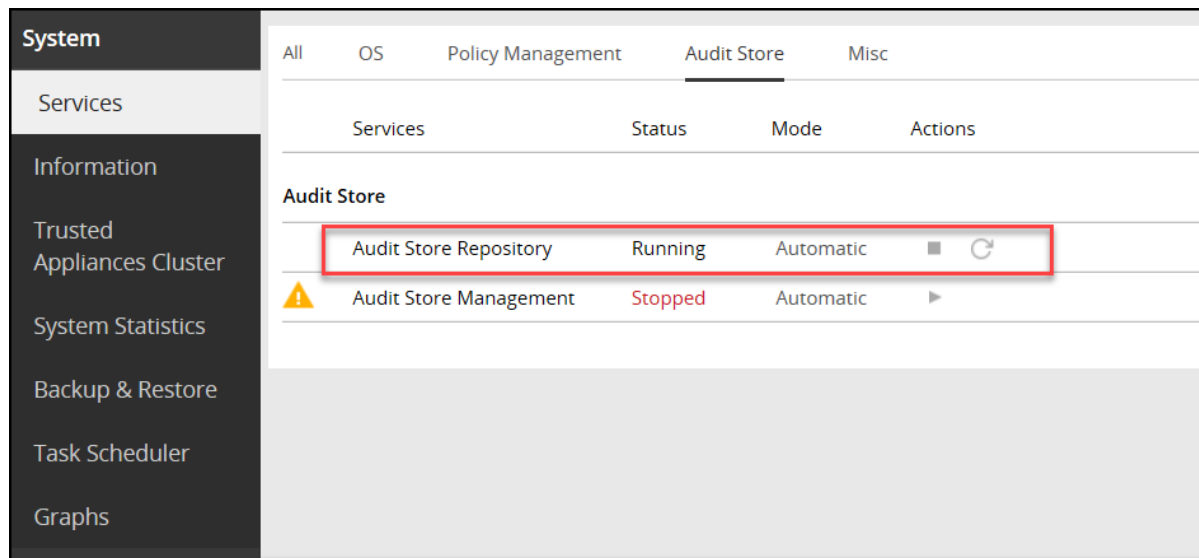


Figure 3-5: Stopping Audit Store Repository

10. Run the Rotate Audit Store Certificates tool on the system.
  - a. From the CLI, navigate to **Tools > Rotate Audit Store Certificates**.

```

Tools:

    Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
-- Analytics Tools --
    Migrate Analytics Configuration
    Migrate Analytics Audits
    Clear Analytics Migration Configuration
-- Cloud Utility AWS Tools --
    CloudWatch Integration
-- Audit Store Tools --
    Rotate Audit Store Certificates
    Apply Audit Store Security Configs
    Set Audit Store Repository Total Memory

```

Figure 3-6: Rotating Certificates

- b. Enter the root password and select **OK**.

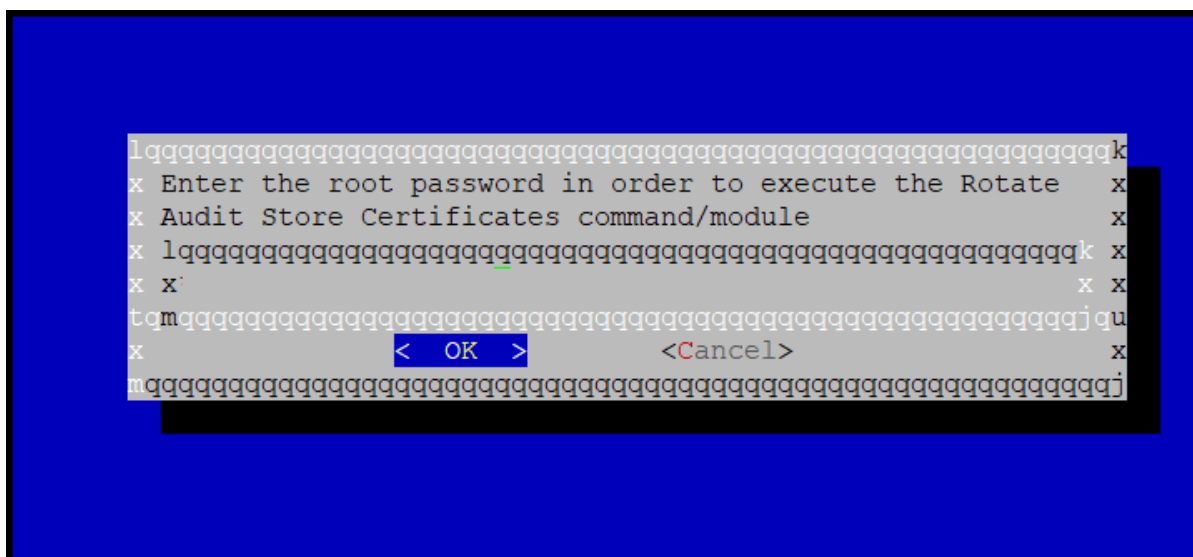


Figure 3-7: Root Password

- c. Enter the *admin* username and password and select **OK**.

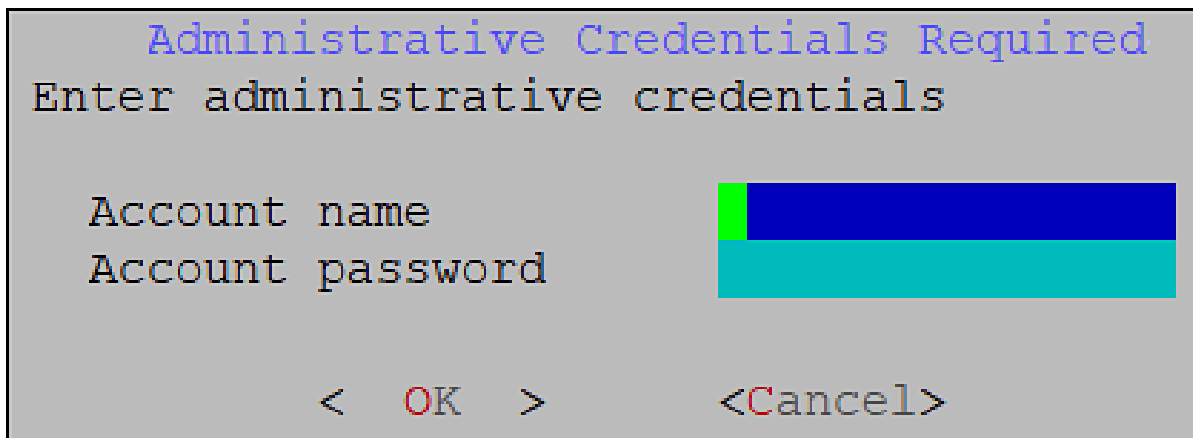


Figure 3-8: Admin Details

- d. Enter the **Target Audit Store Address** as *localhost* or the IP of the local system and select **OK** to rotate the certificates.

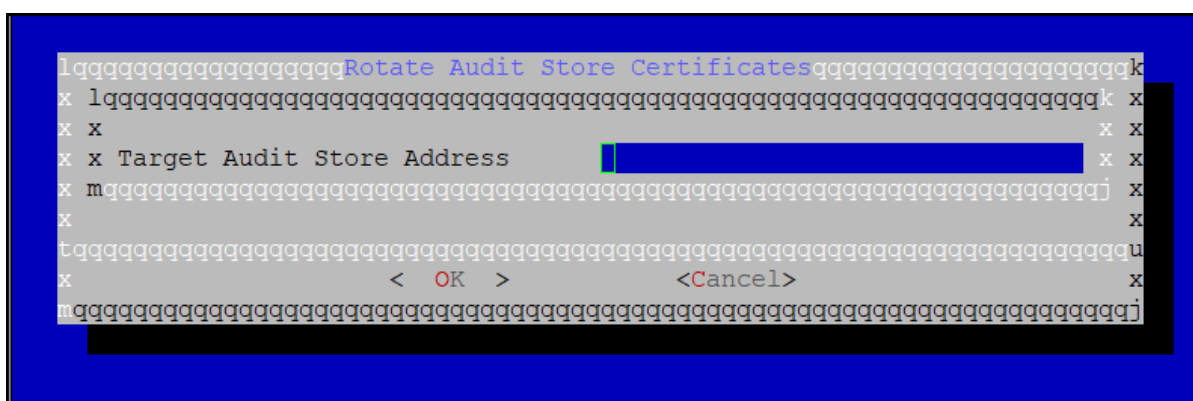


Figure 3-9: Target Audit Store Address

- e. After the rotation is complete select **OK**.

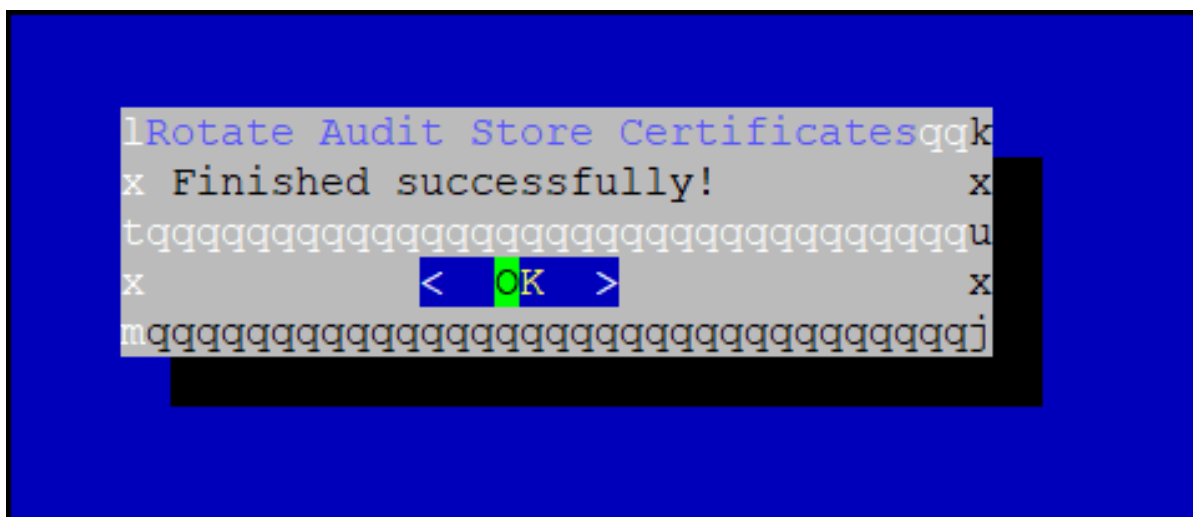


Figure 3-10: Rotation Complete

The CLI screen appears.

```

Tools:

  Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
-- Analytics Tools --
  Migrate Analytics Configuration
  Migrate Analytics Audits
  Clear Analytics Migration Configuration
-- Cloud Utility AWS Tools --
  CloudWatch Integration
-- Audit Store Tools --
  Rotate Audit Store Certificates
  Apply Audit Store Security Configs
  Set Audit Store Repository Total Memory

```

Figure 3-11: Certificates Rotated

11. Navigate to **System > Services > Audit Store**.
12. Start the **Audit Store Repository** service.
13. Navigate to **System > Services > Audit Store**.
14. Start the **Audit Store Management** service.
15. Navigate to **Audit Store Management** and confirm that the cluster is functional and the cluster status is green or yellow. The cluster with status as green is shown in the following figure.

Join, View, or Leave Cluster ⓘ Join Cluster Leave Cluster

Cluster Name: insight ● Cluster Status

Number of Nodes	Number of Data Nodes	Active Primary Shards	Active Shards	Relocating Shards
1	1	17	17	0
Initializing Shards	Unassigned Shards	OS Version	Current Master	Indices Count
0	16	1.3.0		14
Total Docs	Number of Master Nodes	Number of Ingest Nodes		
190,430	1	1		

**Nodes** **Indices**

Details


Node IP	Roles			Action	Name	Up Time	Disk Total (Bytes)	Disk Used (Bytes)	Disk Avail (Bytes)	RAM
	Master	Data	Ingest							
	✓	✓	✓	<a href="#">Edit Roles</a>		8.7h	39,502,524,416	7,033,511,936	32,469,012,480	16,6

Figure 3-12: Audit Store Clustering Started

16. Navigate to **System > Services > Misc**.
17. Start the **Analytics** service.
18. Navigate to **System > Services > Misc**.
19. Start the **td-agent** service.

**Note:** Skip this step if *Analytics* is not initialized.

The following figure shows all the services started.

<b>System</b> Services Information Trusted Appliances Cluster System Statistics Backup & Restore Task Scheduler Graphs	Logfacade	Running	Automatic	■	↺
	Logfacade Legacy	Running	Automatic	■	↺
	<b>Audit Store</b>				
	Audit Store Repository	Running	Automatic	■	↺
	Audit Store Management	Running	Automatic	▼	■ ↺
	<b>Misc</b>				
	LDAP Server	Running	Automatic	■	↺
	Web-Services Engine	Running	Automatic	■	↺
	Service Dispatcher	Running	Automatic	■	↺
	td-agent	Running	Automatic	▼	■ ↺
	Analytics	Running	Automatic	■	↺

Figure 3-13: Services Started

### 3.3.2 Rotating Certificates on a Multi-Node Audit Store Cluster

On a multi-node Audit Store cluster, the certificate rotation must be performed on every node in the cluster. First, rotate the certificates on a Lead node, which is the Primary ESA, and then use the IP address of this Lead node while rotating the certificates on the remaining nodes in the cluster. The services mentioned in this section must be stopped on all the nodes, preferably at the same time with minimum delay during certificate rotation. After certificate rotation, the services that were stopped must be started again on the nodes in the reverse order.

**Note:** These steps are only applicable for the Protegrity-generated certificate and keys. For rotating custom certificates, refer to [Updating Audit Store Custom Certificates](#).

1. Login to the ESA Web UI.
2. Stop the required services.
  - a. Navigate to **System > Services > Misc**.
  - b. Stop the **td-agent** service.

**Note:** This step must be performed on all the other nodes followed by the Lead node. Skip this step if *Analytics* is not initialized.



System

Services

Information

Trusted Appliances Cluster

System Statistics

Backup & Restore

Task Scheduler

Graphs

AllOSPolicy ManagementAudit StoreMisc

Services

Status

Mode

Actions

Misc

LDAP Server

Running

Automatic

Web-Services Engine

Running

Automatic

Service Dispatcher

Running

Automatic

td-agent

Running

Automatic

Analytics

Running

Automatic

Figure 3-14: Stopping td-agent

- c. On the ESA Web UI, navigate to **System > Services > Misc**.
- d. Stop the **Analytics** service.

**Note:** This step must be performed on all the other nodes followed by the Lead node.

System	All	OS	Policy Management	Audit Store	Misc
Services					
Information					
Trusted Appliances Cluster					
System Statistics					
Backup & Restore					
Task Scheduler					
Graphs					
	Misc				
	Services	Status	Mode	Actions	
	Misc				
	LDAP Server	Running	Automatic	■	↻
	Web-Services Engine	Running	Automatic	■	↻
	Service Dispatcher	Running	Automatic	■	↻
	⚠ td-agent	Stopped	Automatic	▶	
	Analytics	Running	Automatic	■	↻

Figure 3-15: Stopping Analytics

- e. Navigate to **System > Services > Audit Store**.
- f. Stop the **Audit Store Management** service.

**Note:** This step must be performed on all the other nodes followed by the Lead node.

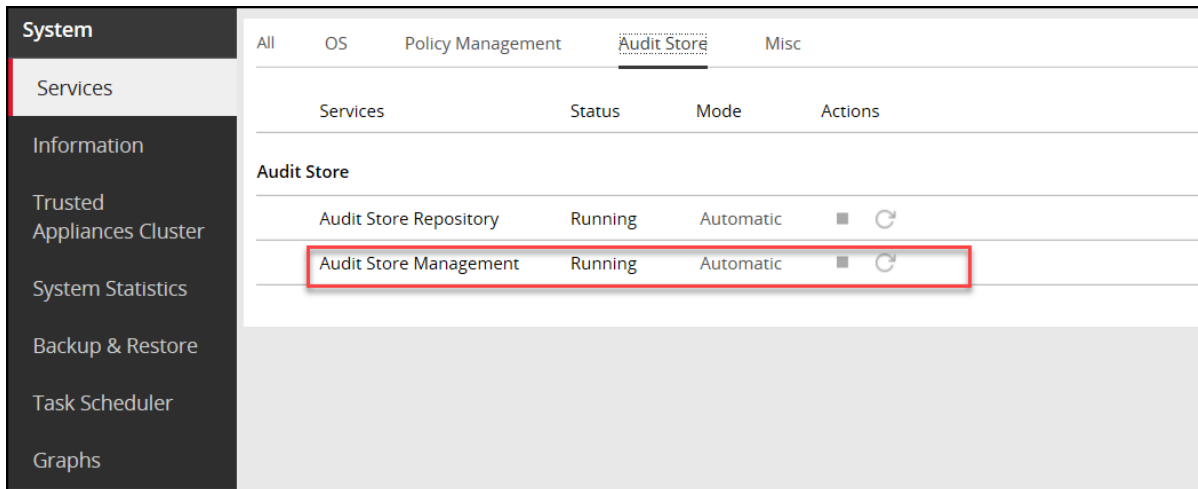


Figure 3-16: Stopping Audit Store Management

- g. Navigate to **System > Services > Audit Store**.
- h. Stop the **Audit Store Repository** service.

**Attention:** This is a very important step and must be performed on all the other nodes followed by the Lead node without any delay. A delay in stopping the service on the nodes will result in that node receiving logs. This will lead to inconsistency in the logs across nodes and logs might be lost.

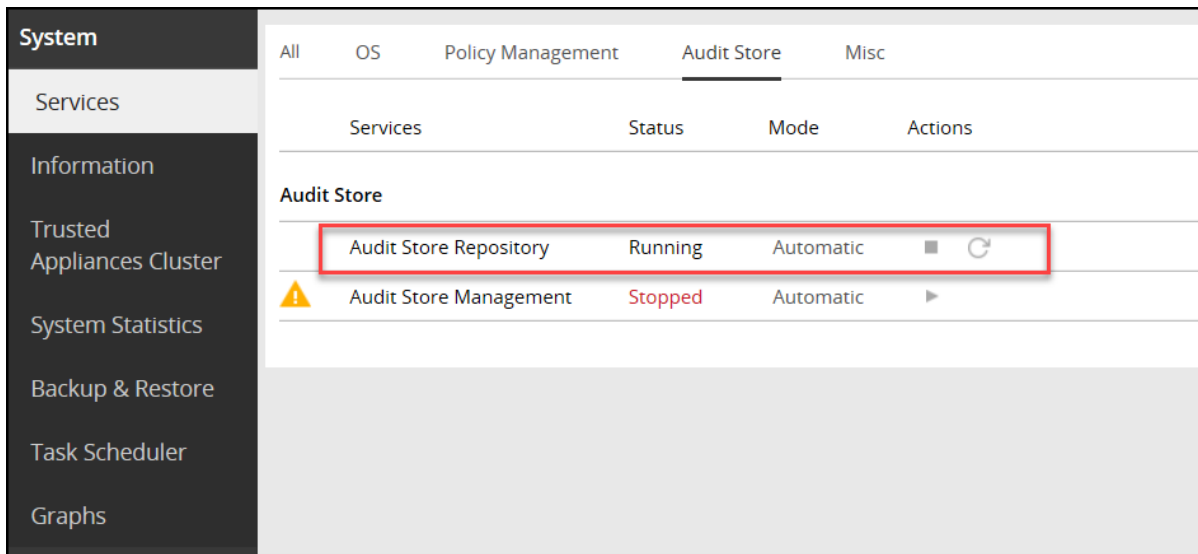


Figure 3-17: Stopping Audit Store Repository

- 3. Run the **Rotate Audit Store Certificates** tool on the Lead node.
  - a. From the ESA CLI Manager of the Lead node, that is the primary ESA, navigate to **Tools > Rotate Audit Store Certificates**.

```

Tools:

    Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
-- Analytics Tools --
    Migrate Analytics Configuration
    Migrate Analytics Audits
    Clear Analytics Migration Configuration
-- Cloud Utility AWS Tools --
    CloudWatch Integration
-- Audit Store Tools --
    Rotate Audit Store Certificates
    Apply Audit Store Security Configs
    Set Audit Store Repository Total Memory

```

Figure 3-18: Rotating Keys

- b. Enter the root password and select **OK**.

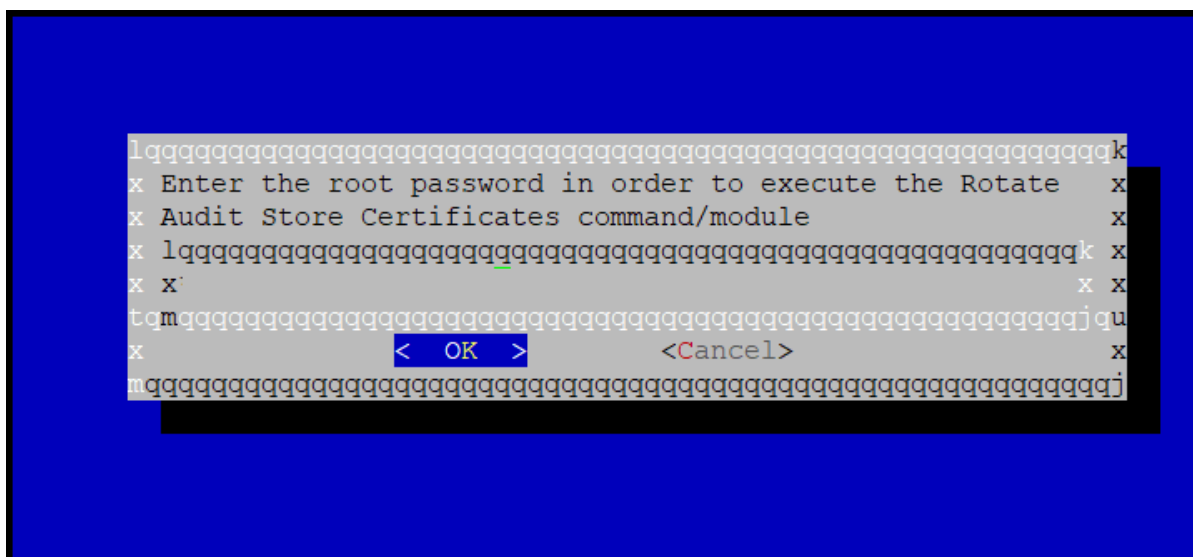


Figure 3-19: Root Password

- c. Enter the *admin* username and password and select **OK**.

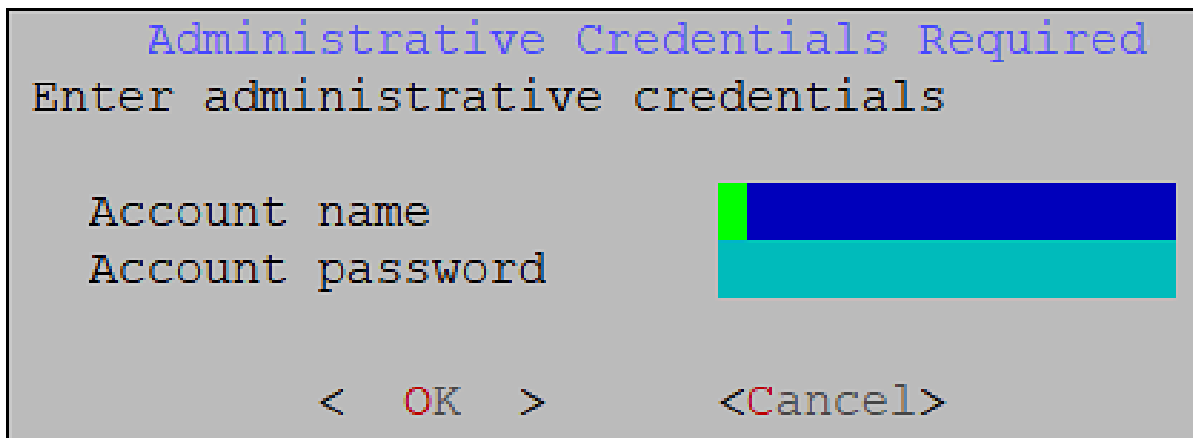


Figure 3-20: Admin Details

- d. Enter the **Target Audit Store Address** as *localhost* or the IP of the local machine and select **OK**.

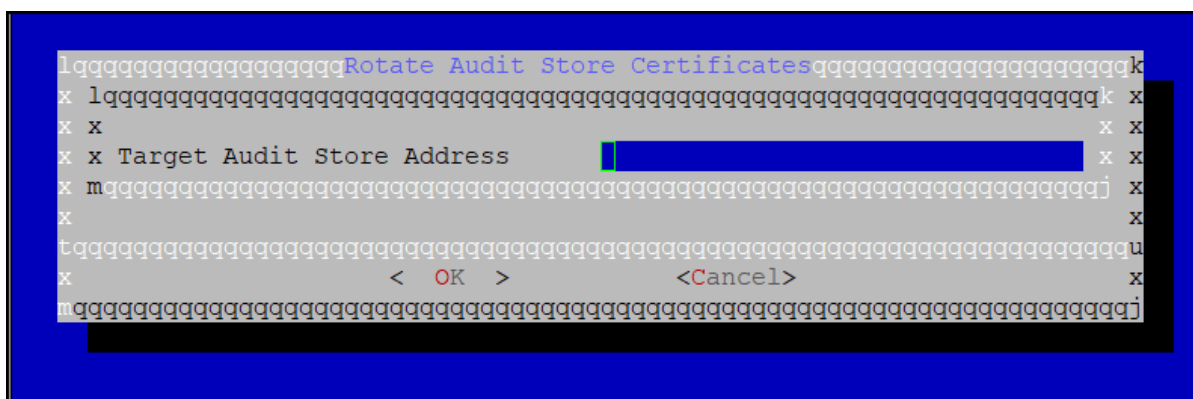


Figure 3-21: Target Audit Store Address

- e. After the rotation is completed without errors, the following screen appears. Select **OK** to go to the CLI menu screen.

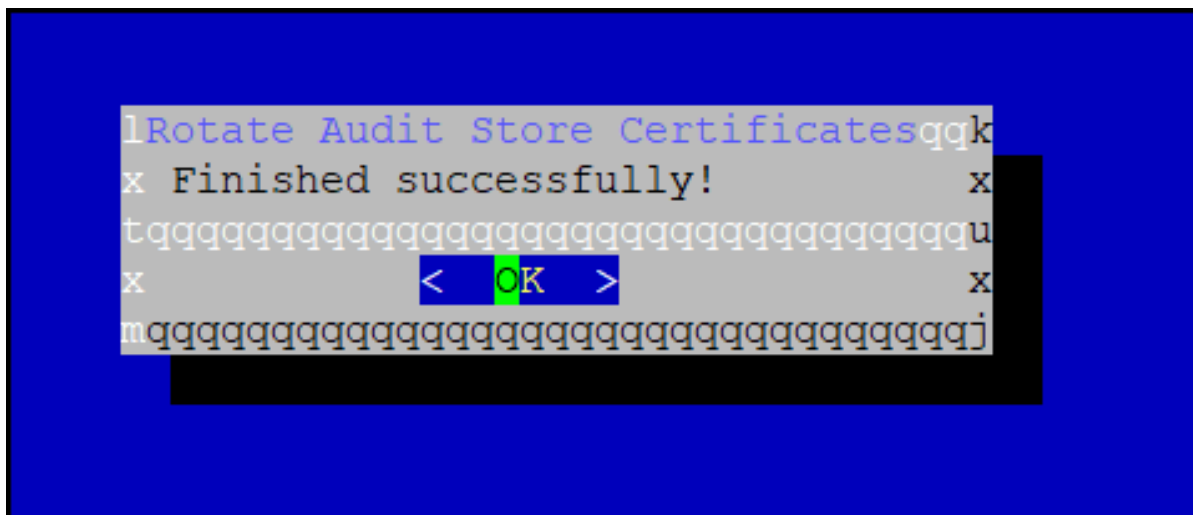


Figure 3-22: Rotation Complete

The CLI screen appears.

```
Tools:

    Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
-- Analytics Tools --
    Migrate Analytics Configuration
    Migrate Analytics Audits
    Clear Analytics Migration Configuration
-- Cloud Utility AWS Tools --
    CloudWatch Integration
-- Audit Store Tools --
    Rotate Audit Store Certificates
    Apply Audit Store Security Configs
    Set Audit Store Repository Total Memory
```

Figure 3-23: Keys Rotated

4. Run the Rotate Audit Store Certificates tool on all the remaining nodes in the Audit Store cluster one node at a time.
  - a. From the ESA CLI Manager of a node in the cluster, navigate to **Tools > Rotate Audit Store Certificates**.

```
Tools:

    Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
-- Analytics Tools --
    Migrate Analytics Configuration
    Migrate Analytics Audits
    Clear Analytics Migration Configuration
-- Cloud Utility AWS Tools --
    CloudWatch Integration
-- Audit Store Tools --
    Rotate Audit Store Certificates
    Apply Audit Store Security Configs
    Set Audit Store Repository Total Memory
```

Figure 3-24: Rotating Keys

- b. Enter the root password and select **OK**.

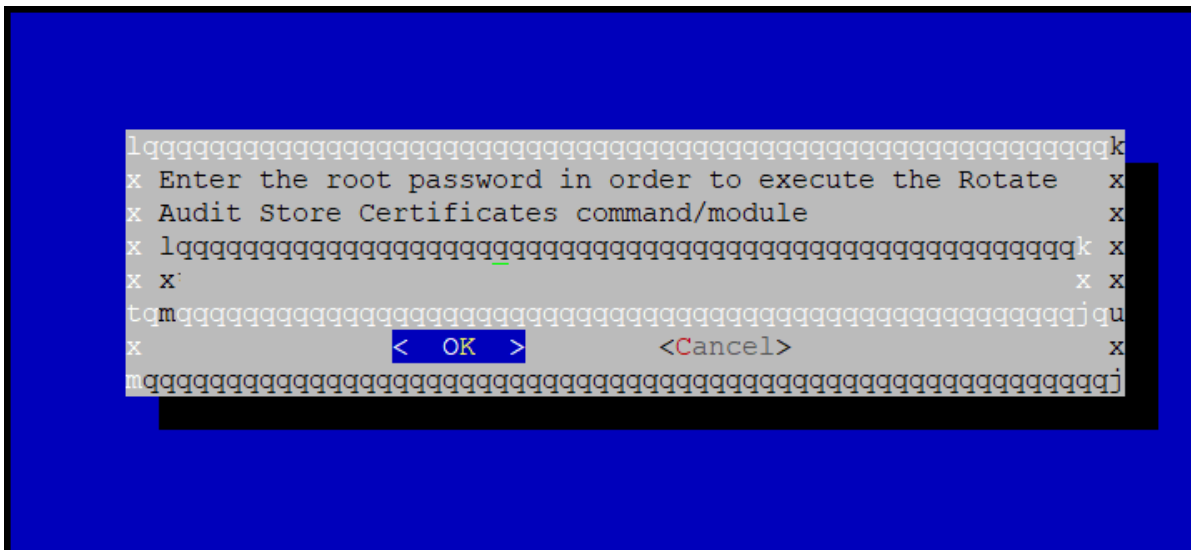


Figure 3-25: Root Password

- c. Enter the *admin* username and password and select **OK**.

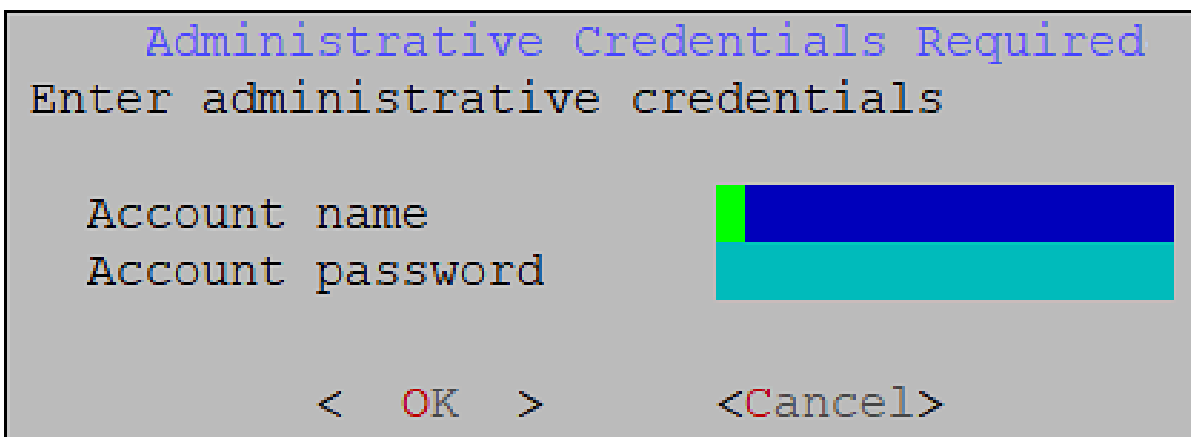


Figure 3-26: Admin Details

- d. Enter the IP address of the Lead node in **Target Audit Store Address** and select **OK**.

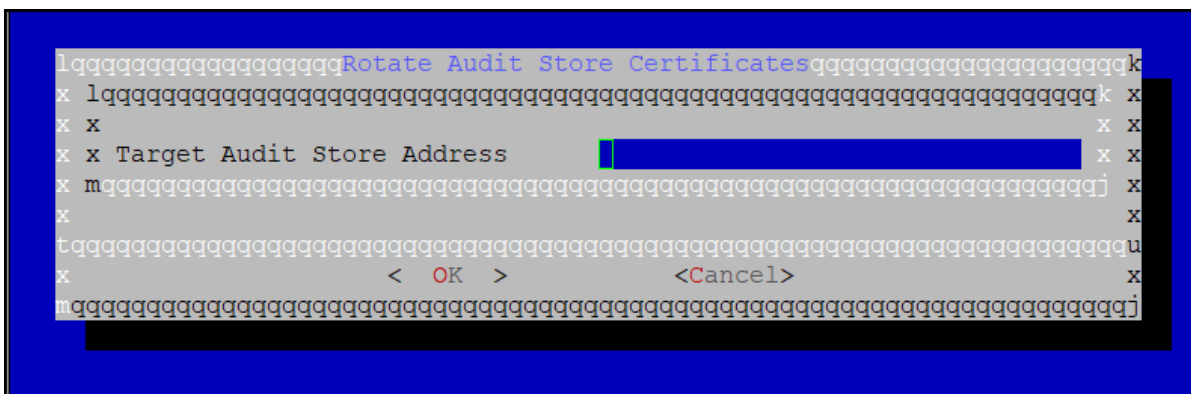


Figure 3-27: Target Audit Store Address

- e. Enter the *admin* username and password for the Lead node and select **OK**.

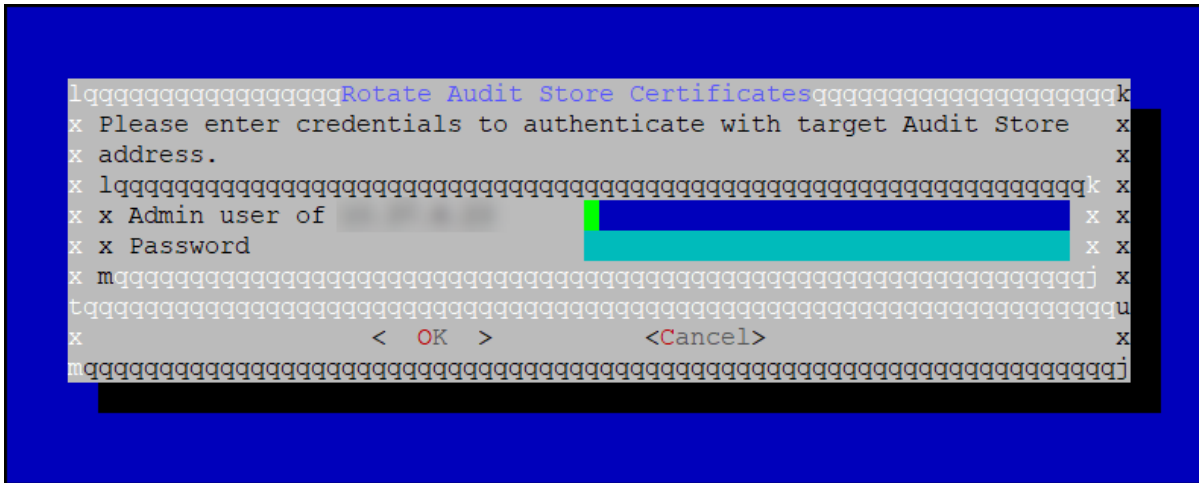


Figure 3-28: Admin Credentials

- f. After the rotation is completed without errors, the following screen appears. Select **OK** to go to the CLI menu screen.

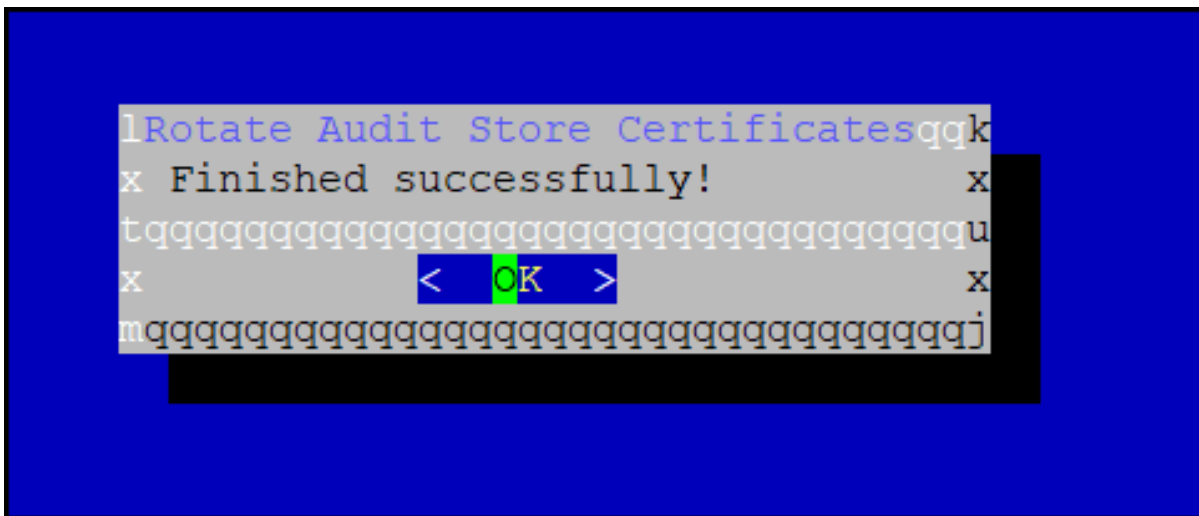


Figure 3-29: Rotation Complete

The CLI screen appears.

```
Tools:

  Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
-- Analytics Tools --
  Migrate Analytics Configuration
  Migrate Analytics Audits
  Clear Analytics Migration Configuration
-- Cloud Utility AWS Tools --
  CloudWatch Integration
-- Audit Store Tools --
  Rotate Audit Store Certificates
  Apply Audit Store Security Configs
  Set Audit Store Repository Total Memory
```

Figure 3-30: Keys Rotated

5. Start the required services.
  - a. Navigate to **System > Services > Audit Store**.
  - b. Start the **Audit Store Repository** service.

**Attention:** This step must be performed on the Lead node followed by all the other nodes without any delay. A delay in starting the services on the nodes will result in that node receiving logs. This will lead to inconsistency in the logs across nodes and logs might be lost.

- c. Navigate to **System > Services > Audit Store**.
  - d. Start the **Audit Store Management** service.

**Note:** This step must be performed on the Lead node followed by all the other nodes.

- e. Navigate to **Audit Store Management** and confirm that the Audit Store cluster is functional and the Audit Store cluster status is green or yellow as shown in the following figure.



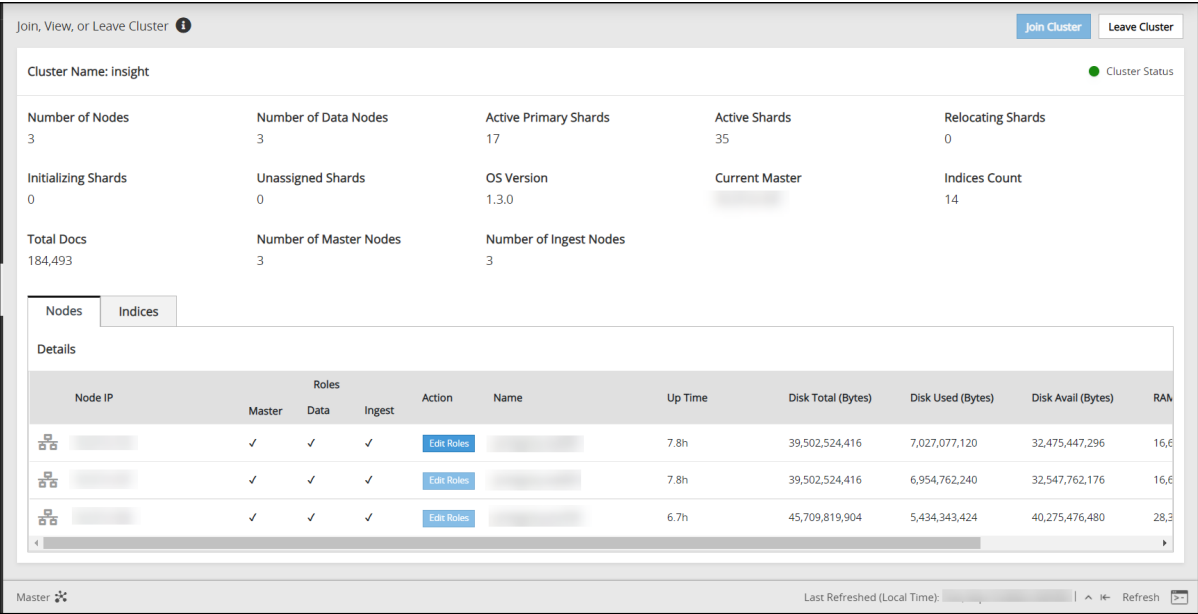


Figure 3-31: Audit Store Clustering Started

- f. Navigate to **System > Services > Misc.**
- g. Start the **Analytics** service.

**Note:** This step must be performed on the Lead node followed by all the other nodes.

- h. Navigate to **System > Services > Misc.**
- i. Start the **td-agent** service.

The following figure shows all services that are started.

**Note:** This step must be performed on the Lead node followed by all the other nodes.  
Skip this step if *Analytics* is not initialized.

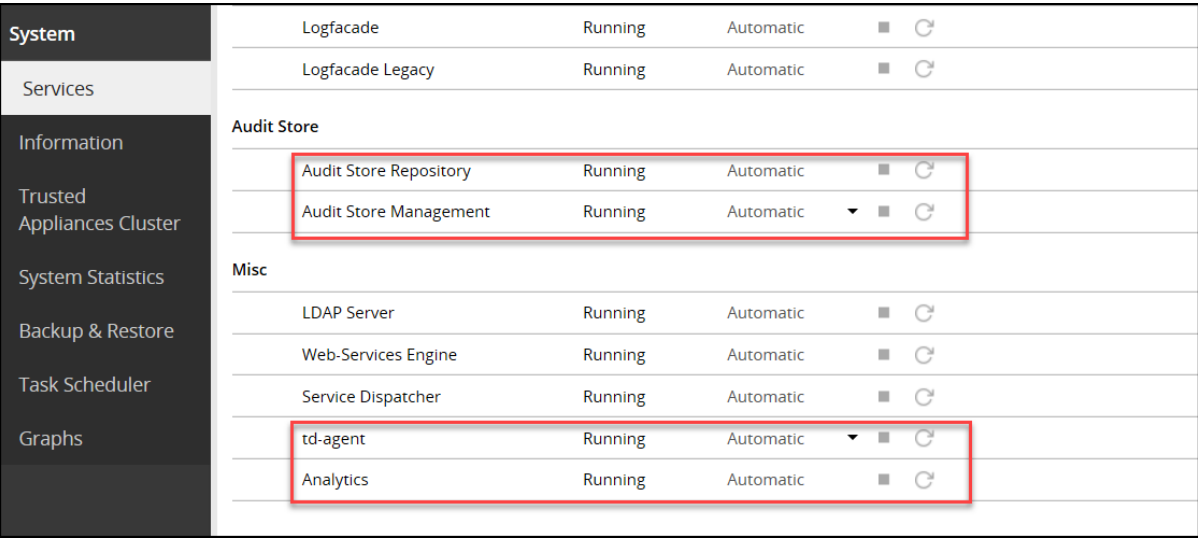


Figure 3-32: Services Started

- 6. Verify that the Audit Store cluster is stable.

- a. On the ESA Web UI, navigate to **Audit Store Management**.
- b. Verify that the nodes are still a part of the Audit Store cluster.

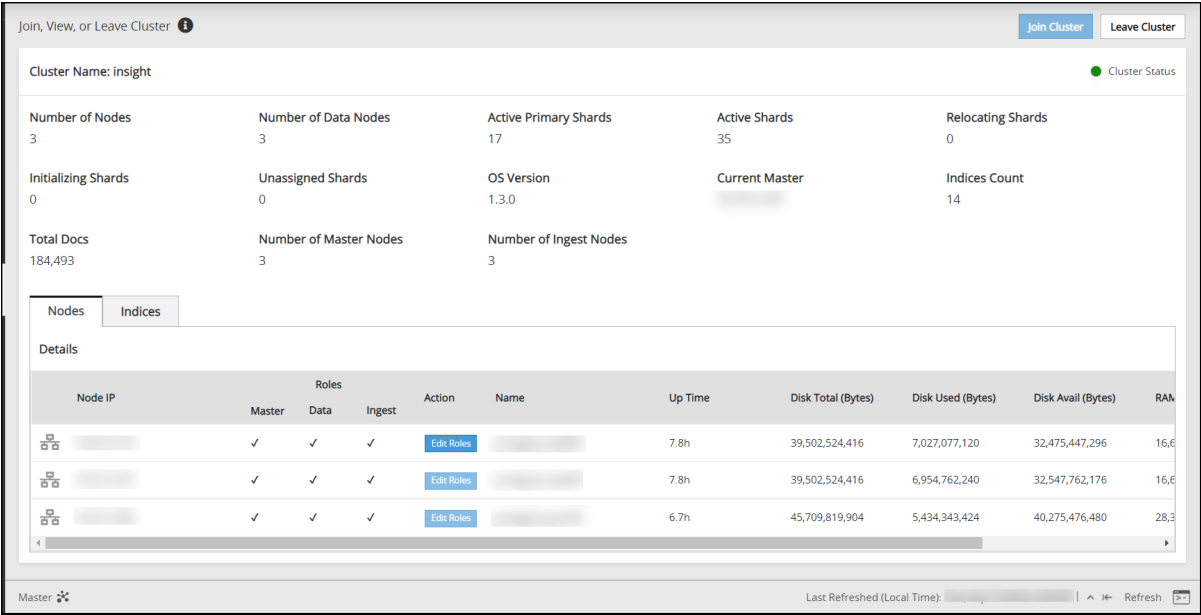


Figure 3-33: Audit Store Nodes

# Chapter 4

## Understanding the Audit Store Status

### 4.1 Viewing Cluster Status

### 4.2 Viewing the Node Status

### 4.3 Viewing the Index Status

### 4.4 Working with Roles

You can configure an Audit Store cluster to enhance the capabilities and quality of the logs. You can achieve this by gathering logs from multiple systems to have a realistic view of the transactions that take place in the ecosystem. You can view the information on the Audit Store clustering screens to understand the status of the nodes and Audit Store cluster. You can identify and fix issues with the Audit Store cluster, if any.

## 4.1 Viewing Cluster Status

The **Cluster Overview** screen shows information about the Audit Store cluster. You can use this information to understand the health of the Audit Store cluster. Here, you can identify and fix Audit Store cluster-related issues, if any.

You can access the **Cluster Overview** screen by navigating to **Audit Store > Cluster > Cluster Overview**. The **Cluster Overview** screen is shown in the following figure.

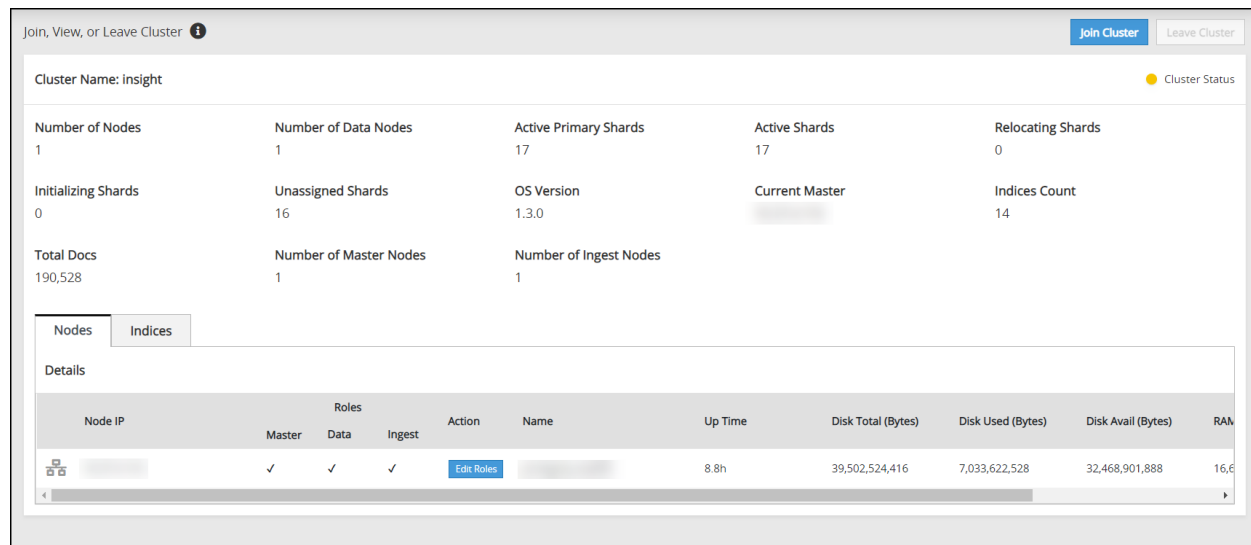


Figure 4-1: Cluster Overview Screen

The following information is shown on the **Cluster Overview** screen:

- **Join Cluster:** Click to add a node to the Audit Store cluster.

**Note:** You can add the node to only one Audit Store cluster. This button is disabled after you add the node to the Audit Store cluster.

- **Leave Cluster:** Click to remove a node from the Audit Store cluster.

**Note:** This button is disabled after you remove the node from an Audit Store cluster.

- **Cluster Name:** Displays the Audit Store cluster name.
- **Cluster Status:** The cluster status displays the index status of the worst shard in the Audit Store cluster. Accordingly, the following status information appears:
  - Red status indicates that the specific shard is not allocated in the Audit Store cluster.
  - Yellow status indicates that the primary shard is allocated but replicas are not allocated.
  - Green status indicates that all shards are allocated.
- **Number of Nodes:** The count of active nodes in the Audit Store cluster.
- **Number of Data Nodes:** The count of nodes that have a data role.
- **Active Primary Shards:** The count of active primary shards in the Audit Store cluster.
- **Active Shards:** The total of active primary and replica shards.
- **Relocating Shards:** The count of shards that are being relocated.
- **Initializing Shards:** The count of shards that are under initialization.
- **Unassigned Shards:** The count of shards that are not allocated.
- **OS Version:** The version number of the OpenSearch used for the Audit Store.
- **Current Master:** The IP address of the current Audit Store node that is elected as master.
- **Indices Count:** The count of indices in the Audit Store cluster.
- **Total Docs:** The document count of all indices in the Audit Store cluster, excluding security index docs.
- **Number of Master Nodes:** The count of nodes that have the master-eligible role.
- **Number of Ingest Nodes:** The count of nodes that have the ingest role.

## 4.2 Viewing the Node Status

The **Nodes** tab on the **Cluster Overview** screen shows the status of the nodes in the Audit Store cluster. This tab displays important information about the node. The **Nodes** tab is shown in the following figure.

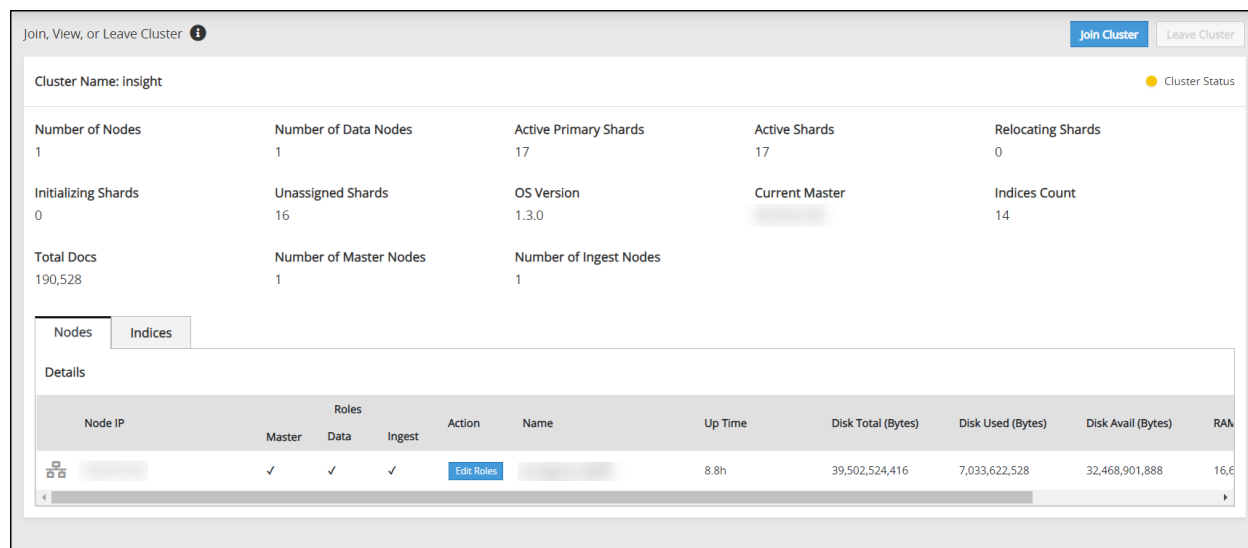


Figure 4-2: Nodes Tab

The following information is shown on the **Nodes** tab:

- **Node IP:** The IP address of the node.
- **Role:** The roles assigned to the node. The following roles are available:
  - **Master:** This is the master-eligible role. The nodes having this role can be elected as the cluster master to control the Audit Store cluster.
  - **Data:** The nodes having the data role hold data and perform data-related operations.
  - **Ingest:** The nodes having the ingest role process the logs received before the logs are stored in the Audit Store.

**Note:** By default, nodes are assigned all the roles.

- **Name:** The name for the node.
- **Up Time:** The uptime for the node.
- **Disk Total (Bytes):** The total disk space in bytes.
- **Disk Used (Bytes):** The disk space used in bytes.
- **Disk Avail (Bytes):** The available disk space in bytes.
- **RAM Max (Bytes):** The total RAM available in bytes.
- **RAM Current (Bytes):** The current RAM used in bytes.

## 4.3 Viewing the Index Status

The **Indices** tab on the **Cluster Overview** screen shows the status of the indexes on the Audit Store cluster. This tab displays important information about the indexes. The **Indices** tab is shown in following figure.

Join, View, or Leave Cluster 

Join ClusterLeave Cluster

Cluster Name: insightCluster Status

Number of Nodes

1

Number of Data Nodes

1

Active Primary Shards

17

Active Shards

17

Relocating Shards

0

Initializing Shards

0

Unassigned Shards

16

OS Version

1.3.0

Current Master

Indices Count

14

Total Docs

190,638

Number of Master Nodes

1

Number of Ingest Nodes

1

Nodes

Indices

Details

Index	Doc Count	Health Status	Pri Store Size (Bytes)	Store Size (Bytes)
.opendistro_security	9	<span></span>	48,847	48,847
pty_insight_audit_v9.1-2022.09.12-000001	146,211	<span></span>	35,705,112	35,705,112
pty_insight_audit_v9.1-2022.09.13-000002	43,795	<span></span>	10,956,763	10,956,763
pty_insight_autosuggestion_v9.1	0	<span></span>	208	208
pty_insight_crons_logs_v9.1	619	<span></span>	290,656	290,656

Figure 4-3: Indices Tab

The following information is shown on the **Indices** tab:

- **Index:** The index name.
- **Doc Count:** The count of indices in the Audit Store cluster.
- **Health Status:** The index health per index. The index level health status is controlled by the worst shard status. Accordingly, the following status information appears:
  - Red status indicates that the specific shard is not allocated in the Audit Store cluster.
  - Yellow status indicates that the primary shard is allocated but replicas are not allocated.
  - Green status indicates that all shards are allocated.
- **Pri Store Size (Bytes):** The primary store size in bytes for all shards, including shard replicas of the index.
- **Store Size (Bytes):** The total store size in bytes for all shards, including shard replicas of the index.

## 4.4 Working with Roles

Roles assigned to the nodes determine the functions performed by the node in the cluster. As the cluster grows, the role of the node can be modified to have nodes with dedicated roles.

A node can have one role or multiple roles. By default, a node is assigned all the roles. The following roles are available for the nodes in the Audit Store cluster:

- **Master-eligible:** This is the master-eligible node. It is eligible to be elected as the master node that controls the Audit Store cluster. A minimum of 3 nodes with the master-eligible role are required in the cluster to make the cluster stable and to make the cluster resilient.
- **Data:** This node holds data and can perform data-related operations. A minimum of 2 nodes with the data role are required in the Audit Store cluster to reduce data loss when a node goes down.

- **Ingest:** This node processes logs received before the log is indexed for further storage and processing. A minimum of 2 nodes with the ingest role are required in the Audit Store cluster.

**Note:** A cluster needs at least one node with each role. Hence, you cannot remove roles of the node in a single-node cluster. Similarly, if the node is the last node in the cluster with a particular role, then you cannot remove the role.

The Audit Store uses the following formula to determine the minimum number of nodes with the Master-eligible role that should be running in the cluster:

```
Minimum number of running nodes with the Master-eligible role in a cluster = (Total number of nodes with the Master-eligible role in a cluster / 2) + 1
```

For example, If the cluster has 5 nodes that have the Master-eligible role, then the minimum number of nodes with the Master-eligible role that needs to be running for the cluster to remain functional is 3.

An Audit Store cluster must have a minimum of 3 nodes with the Master-eligible role due to following scenarios:

- 1 master-eligible node: If the only node is present with the Master-eligible role, then it is elected the Master, by default, because it is the only node with the required Master-eligible role. In this case, if the node becomes unavailable due to some failure, then the cluster becomes unstable as there is no additional node with the Master-eligible role.
- 2 master-eligible nodes: A cluster where only 2 nodes have the Master-eligible role will both have the Master-eligible role at the minimum to be up and running for the cluster to remain functional. If any one of those nodes becomes unavailable due to some failure, then the minimum condition for the nodes with the Master-eligible role is not met and cluster becomes unstable.
- 3 master-eligible nodes and above: In this case, if any one node goes down, then the cluster can still remain functional because this cluster requires two nodes with the Master-eligible role to be running at the minimum, as per the minimum Master-eligible role formula.

For more information about node and roles, refer to <https://opensearch.org/docs/1.3/opensearch/cluster/>.

Based on your requirements, you can modify the roles of a node using the following steps.

1. Login to the Web UI of the system to change the role.
2. Click **Audit Store Management** to open the Audit Store clustering page.

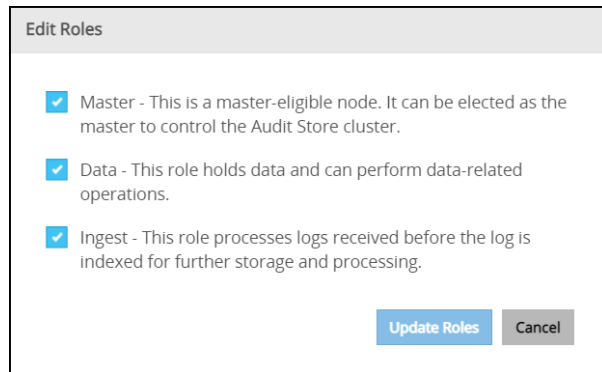
The screenshot displays the 'Join, View, or Leave Cluster' interface for a cluster named 'insight'. It includes buttons for 'Join Cluster' and 'Leave Cluster'. The cluster status is shown as 'Cluster Status' with a green dot. The interface is divided into two tabs: 'Nodes' and 'Indices'. The 'Nodes' tab is active, showing a table of nodes with columns for Node IP, Roles (Master, Data, Ingest), Action (Edit Roles), Name, Up Time, Disk Total (Bytes), Disk Used (Bytes), Disk Avail (Bytes), and RAM. The table lists three nodes, each with a 'Master' role and 'Data' and 'Ingest' roles. The 'Indices' tab is also visible, showing a table of indices.

Cluster Name: insight					Cluster Status
Number of Nodes	Number of Data Nodes	Active Primary Shards	Active Shards	Relocating Shards	
3	3	17	35	0	
Initializing Shards	Unassigned Shards	OS Version	Current Master	Indices Count	
0	0	1.3.0		14	
Total Docs	Number of Master Nodes	Number of Ingest Nodes			
185,017	3	3			

Node IP	Roles			Action	Name	Up Time	Disk Total (Bytes)	Disk Used (Bytes)	Disk Avail (Bytes)	RAM
	Master	Data	Ingest							
[Node IP]	✓	✓	✓	Edit Roles	[Node Name]	7.9h	39,502,524,416	7,027,818,496	32,474,705,920	16,6
[Node IP]	✓	✓	✓	Edit Roles	[Node Name]	7.9h	39,502,524,416	6,955,098,112	32,547,426,304	16,6
[Node IP]	✓	✓	✓	Edit Roles	[Node Name]	6.7h	45,709,819,904	5,434,920,960	40,274,898,944	28,3

Figure 4-4: Audit Store Management Screen

3. Click **Edit Roles**.
4. Select the check box to add a role. Alternatively, clear the check box to remove a role.



**Edit Roles**

- ☒ Master - This is a master-eligible node. It can be elected as the master to control the Audit Store cluster.
- ☒ Data - This role holds data and can perform data-related operations.
- ☒ Ingest - This role processes logs received before the log is indexed for further storage and processing.

**Update Roles** **Cancel**

*Figure 4-5: Edit Roles Screen*

5. Click **Update Roles**.
6. Click **Dismiss** in the message box that appears after the role update.



# Chapter 5

## Clustering Using the Audit Store

- 5.1 Adding an ESA to the Audit Store Cluster
- 5.2 Removing an ESA from the Audit Store Cluster

Add nodes to the Audit Store to increase the number of systems in the cluster. Adding nodes increases the storage capacity and the processing capabilities of the Audit Store cluster.

**Note:** The ESA cluster called TAC is different from the Audit Store cluster. A TAC is used to create a cluster of the ESAs, Audit Store clustering is used to create a cluster of nodes for storing Audit Store data.

The *viewer* role user or a user with the *viewer* role can only view the Audit Store cluster information. You need to log in using the *admin* role to join or leave a cluster.

**Caution:** For more information about creating the Audit Store Cluster, refer to the section *Configuring the Audit Store Cluster* in the *Protegrity Installation Guide 9.1.0.5*.

Cluster management for the Audit Store is managed using the **Audit Store Management** tab from the ESA. From this tab, you can add and remove nodes from the cluster. You can also monitor the various nodes and shard information about the nodes. The **Audit Store Management** tab is shown in the following figure.

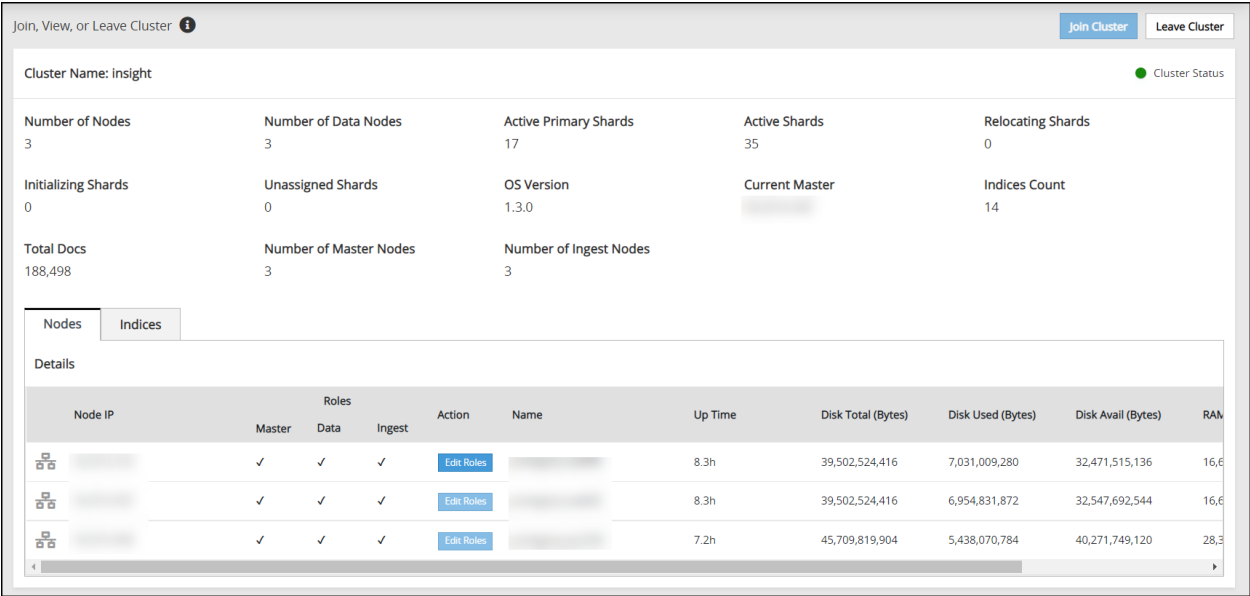


Figure 5-1: Audit Store Management Tab

## 5.1 Adding an ESA to the Audit Store Cluster

Install the ESA and configure it using the steps provided in this section to add an ESA to the Audit Store Cluster.

- For the first ESA, complete the following steps:
  - Initializing the Audit Store on ESA*
  - Refreshing the Audit Store Cluster Settings*
- For the subsequent ESAs, complete the following steps:
  - Adding an ESA to the Audit Store Cluster*
  - Refreshing the Audit Store Cluster Settings*

### 5.1.1 Initializing the Audit Store Cluster on the ESA

Complete the steps provided in this section on the first ESA or the Primary ESA in the TAC. When you select this option, Protegrity Analytics is configured to retrieve data from the local Audit Store. Additionally, the required processes, such as, *td-agent*, is started and Protegrity Analytics is initialized. The Audit Store cluster is initialized on the local machine so that other nodes can join this Audit Store cluster.

Perform the following steps to configure the Audit Store.

- Login to the ESA Web UI.
- Verify that the Audit Store services are running by navigating to **System > Services > Audit Store**.
- Navigate to **Analytics**.

The following screen appears.

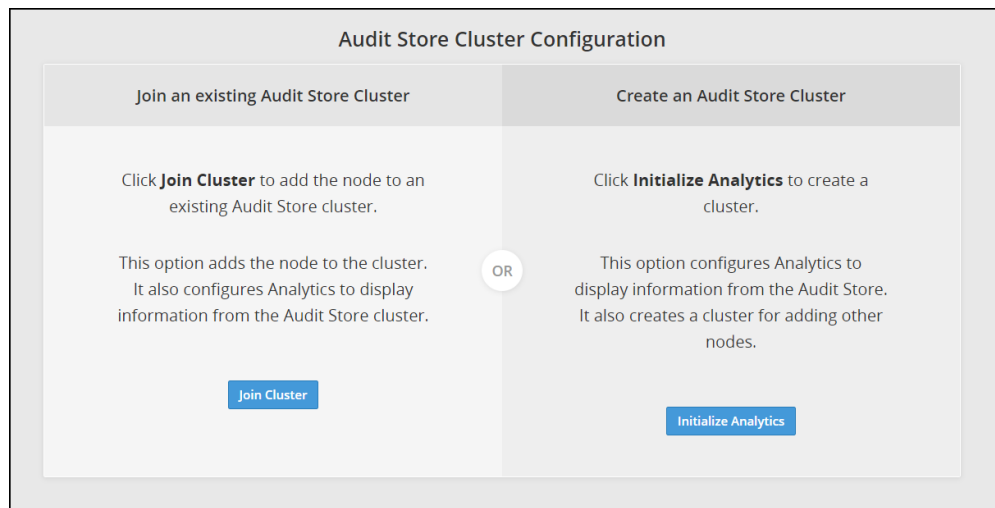


Figure 5-2: Analytics Screen

- Click **Initialize Analytics**.

Protegrity Analytics is initialized, the internal configuration is updated for creating the local Audit Store cluster, the *td-agent* service is started, and logs are read from the Audit Store. Other Audit Store nodes can now join this Audit Store cluster.

Protegrity Analytics is now configured and retrieves data for the reports from the Audit Store. The data is available on the **Analytics > Forensics** tab on the ESA Web UI as shown in the following figure.

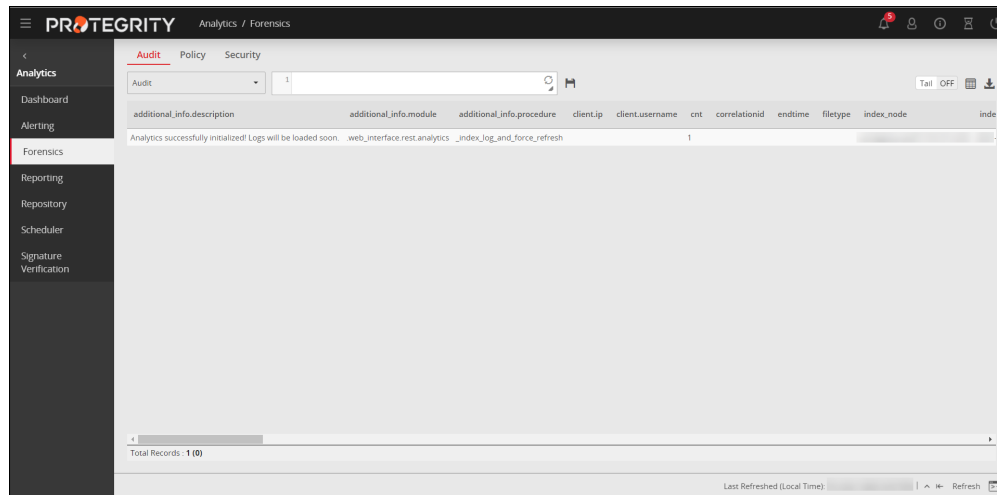


Figure 5-3: Forensics

## 5.1.2 Adding an ESA to the Audit Store Cluster

If multiple ESAs need to be added to the Audit Store cluster, such as multiple ESAs in a TAC, then the steps in this section need to be performed. In this case, the current ESA that you are adding will be a node in the Audit Store cluster. After the configurations are completed, the required processes are started and the logs are read from the Audit Store cluster. Complete the steps in this section to join an existing Audit Store cluster.

### Caution:

The Audit Store cluster information is updated when a node joins the Audit Store cluster. This information is updated across the Audit Store cluster. Hence, nodes must be added to an Audit Store cluster one at a time. Adding multiple nodes to the Audit Store at the same time using the ESA Web UI would make the cluster information inconsistent, make the Audit Store cluster unstable, and would lead to errors.

Ensure that the following prerequisites are met:

- The health status of the Audit Store node that you are connecting to is green or yellow.
- The health status of the Audit Store node that you are adding to the cluster is green or yellow.

**Note:** To check the health status of a node, login to ESA Web UI of the node, click **Audit Store Management**, and view the **Cluster Status** from the upper-right corner of the screen.

Perform the following steps to add a node to the Audit Store cluster.

**Note:** Ensure that the Audit Store cluster is created on the node that you want to join. You need to perform this step only if you need multiple ESAs or are implementing a TAC.

For more information about creating an Audit Store cluster, refer to the section [Initializing the Audit Store Cluster on the ESA](#).

**Important:** Before joining an Audit Store cluster, ensure that the SSH Authentication type is set to **Public key** or **Password + PublicKey**. For more information about setting the authentication, refer to the section [Working with Secure Shell \(SSH\) Keys](#) in the *Protegrity Appliances Overview Guide 9.1.0.5*.

1. Login to the Web UI of the second ESA.
2. Verify that the Audit Store services are running by navigating to **System** > **Services** > **Audit Store**.
3. Navigate to **Analytics**.

The following screen appears.

**Audit Store Cluster Configuration**

**Join an existing Audit Store Cluster**

Click **Join Cluster** to add the node to an existing Audit Store cluster.

This option adds the node to the cluster. It also configures Analytics to display information from the Audit Store cluster.

**Join Cluster**

**OR**

**Create an Audit Store Cluster**

Click **Initialize Analytics** to create a cluster.

This option configures Analytics to display information from the Audit Store. It also creates a cluster for adding other nodes.

**Initialize Analytics**

Figure 5-4: Analytics Screen

4. Click **Join Cluster**.

The following screen appears.

**Join an existing Audit Store Cluster**

**Target node IP/Hostname\***

Node IP/Hostname

**Username\***

Username

**Password\***

Password

☐ Clear cluster data! This operation will clear data from the node. I have backed up the data and want to continue with this operation.

**Join Cluster** **Cancel**

Figure 5-5: Joining an Audit Store Cluster

- Specify the IP address or the hostname of the Audit Store cluster to join.

**Note:** Only use hostname if the hostname is resolved between the nodes.

Ensure that Protegrity Analytics is initialized and the Audit Store cluster is already created on the target node. A node cannot join the cluster if Protegrity Analytics is not initialized on the target node.

For more information about initializing the Audit Store, refer to the section [Initializing the Audit Store Cluster on the ESA](#).

- Specify the admin username and password for the Audit Store cluster.

**Note:** If required, then select the **Clear cluster data** check box to clear the Audit Store data from the current node before joining the Audit Store cluster. The check box will only be enabled if the node has data, that is, if Analytics is installed and initialized on the node. Else, this check box is disabled.

- Click **Join Cluster**.

The internal configuration is updated for the Audit Store cluster, the *td-agent* service is started, and the node is added to the Audit Store cluster.

Protegrity Analytics is now configured and retrieves data for the reports from the Audit Store cluster. The data is available on the **Analytics** tab on the ESA Web UI as shown in the following figure.

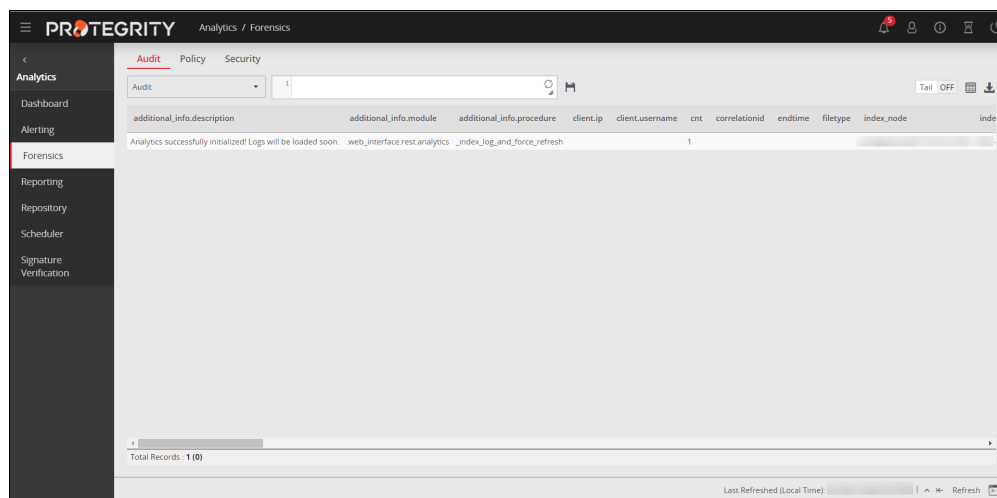


Figure 5-6: Protegrity Analytics

### 5.1.3 Refreshing the Audit Store Cluster Settings

Complete the steps in this section to refresh the Audit Store Cluster settings.

- Login to the ESA Web UI.
- Navigate to **System > Task Scheduler**.
- Click the **Audit Store Management Update Unicast Hosts** task.
- Click **Run now** and then click **OK** in the confirmation box.
- If you are using a TAC, then perform the steps provided here on the other ESAs in the Audit Store Cluster.

## 5.2 Removing an ESA from the Audit Store Cluster

If you have multiple ESAs in the Audit Store Cluster and do not need an ESA node, then you can remove the ESA from the Audit Store cluster. When you remove the ESA from the Audit Store cluster, the *td-agent* service is stopped, then the indexes for the node are removed and the node is detached from the Audit Store cluster. The ports to the node are closed.

► To remove the ESA node:

1. From the ESA Web UI, click **Audit Store Management** to open the Audit Store clustering page. The Cluster Overview screen appears.

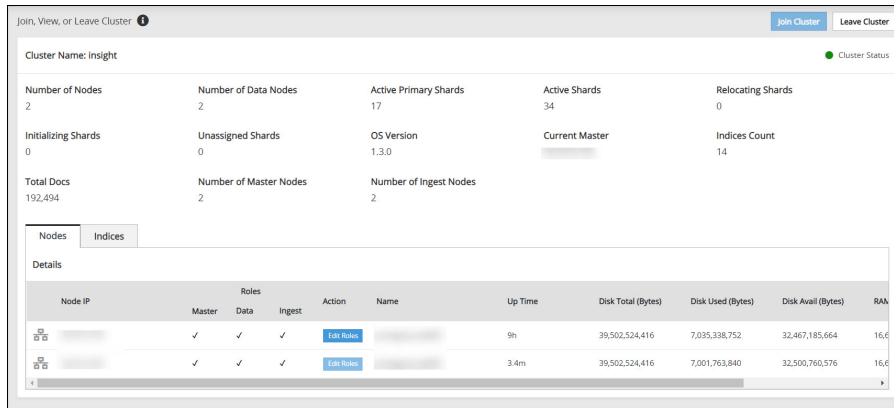


Figure 5-7: Cluster Overview Screen

2. Click **Leave Cluster**.

A confirmation dialog box appears.

**Note:** The Audit Store cluster information is updated when a node leaves the Audit Store cluster, hence, nodes must be removed from the Audit Store cluster one at a time. Removing multiple nodes from the Audit Store cluster at the same time using the ESA Web UI would lead to errors.

3. Click **YES**.

The ESA is removed from the Audit Store cluster. The **Leave Cluster** button is disabled and the **Join Cluster** button is enabled.

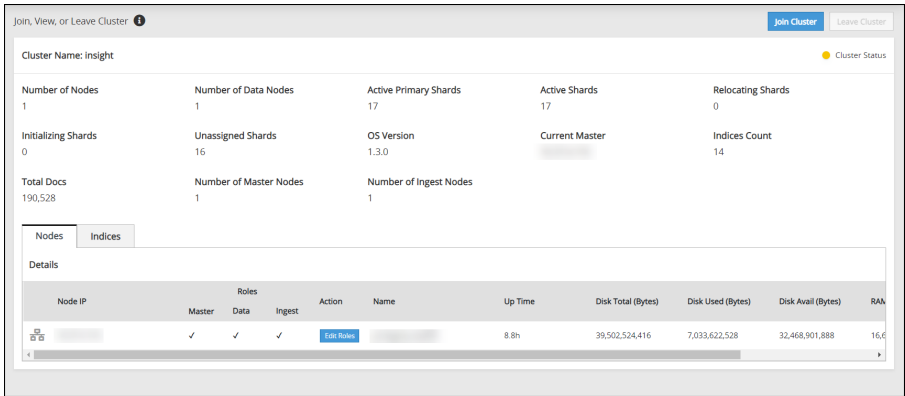


Figure 5-8: Leaving a Cluster

**Note:** The process takes time to complete. Ensure that you stay on the same page and do not navigate to any other page while the process is in progress.

After leaving the Audit Store cluster, the configuration of the node and data is reset. The node will be uninitialized. Before using the node again, Protegrity Analytics needs to be initialized on the node or the node needs to be added to another Audit Store cluster.

# Chapter 6

## Viewing the Audit Store Data

The data in the Audit Store provides valuable information about the working of the systems. The data is valuable as Forensics data for analysis in case of issues. You can view the Audit Store data using tables and graphs from Protegrity Analytics.

For more information about Protegrity Analytics, refer to *Protegrity Analytics Guide 9.1.0.5*.



# Chapter 7

## Troubleshooting

### 7.1 Known Issues for the Audit Store

This section describes the problems that you might face and the solutions or workarounds to resolve those problems.

## 7.1 Known Issues for the Audit Store

A list of known issues with their solution or workaround are provided here. The steps provided to resolve the known issues ensure that your product does not display errors or crash.

- **Known Issue:** After you perform an export and import in the ESA as part of the replication task in the TAC cluster, and Logging certificates (`--import-method 'OS/CoreOsExport/Certificates'`) are a part of the operation, then the Audit Store cluster fails.

**Issue:** When the certificates are exported and imported in the ESA, the ESA-related certificates are replaced on the node where the import happened causing the Audit Store cluster to fail. This is applicable for Protegrity-system certificates.

### Workaround

After the export and import operation involving Protegrity-system certificates is performed, immediately shut down the full Audit Store cluster and rotate the Audit Store certificates to fix the failed Audit Store cluster. For more information about rotating Audit Store certificates, refer to the section [Rotating Audit Store Certificates](#).

- **Known Issue:** The Audit Store node security remains uninitialized and the message *Audit Store Security is not initialized* appears on the Audit Store Management page.

### Resolution:

Run the following steps to resolve the issue.

1. From the ESA Web UI, navigate to **System > Services > Audit Store**.
  2. Ensure that the **Audit Store Repository** service is running.
  3. Open the ESA CLI.
  4. Navigate to **Tools**.
  5. Run **Apply Audit Store Security Configs**.
- **Known Issue:** The Audit Store Repository service stops when the user logs out from the ESA admin console after changing the hostname from the admin console tools menu.

### Issue:

The Audit Store Repository service stops when the user rotates audit store certificate, finalizes an appliance (as in the case of cloud environments), changes the hostname, or starts or stops the audit store repository service, by logging into admin console and then logging out from admin console. The Audit Store Repository service also stops when the user logs out of the admin console after starting or stopping the Audit Store Repository service from the admin console.

**Resolution:**

Manually start the **Audit Store Repository** service from **System > Services** on the ESA Web UI.

- **Known Issue:** Logs sent to the Audit Store do not get saved and errors might be displayed.

**Issue:**

The Audit Store cannot receive and store logs when the disk space available on the ESA is low. In this case, errors or warnings similar to *high disk watermark [90%] exceeded* are displayed in the logs.

**Resolution:**

Perform one of the following steps to resolve the issue:

- Delete old indices that are not required using ILM in Analytics.
- Increase the disk space on all nodes.
- Add new nodes or ESAs to the cluster.
- **Known Issue:** The Audit Store Repository fails to start after updating the domain name.

**Issue:**

After updating the domain name, the Audit Store Repository service fails to start.

**Resolution:**

The Audit Store Repository depends on the domain name. However, the domain name configuration in the Audit Store does not get updated automatically when there is a change in the domain name.

To apply the updated domain name to the Audit Store perform the following steps:

1. Login to the ESA CLI Manager.
2. Navigate to **Administration > OS Console**.
3. Enter the root password and select **OK**.
4. Navigate to the `/opt/protectgrity/auditstore/config` directory using the following command:

```
cd /opt/protectgrity/auditstore/config
```

5. Open the `opensearch.yml` file in a text editor.
6. Replace the existing domain name attribute with your domain name for the following configuration attributes.
  - **network.host**
  - **http.host**

Consider the following example where the domain name of *protectgrity.com* is updated to *example.com*.

Existing configuration:

```
network.host: [ "localhost", "127.0.0.1", "192.168.1.120", "protectgrity-esal23", "protectgrity-esal23.protectgrity.com" ]
```

Updated configuration:

```
network.host: [ "localhost", "127.0.0.1", "192.168.1.120", "protectgrity-esal23", "protectgrity-esal23.example.com" ]
```

7. Save and close the file.
8. Rotate the certificates for the Audit Store.

For more information about rotating certificates, refer to the section *Rotating Audit Store Certificates* in the *Audit Store Guide 9.1.0.5*.

9. Login to the ESA CLI Manager.
10. Navigate to **Administration > OS Console**.
11. Enter the root password and select **OK**.
12. Run the following commands to refresh the network settings.

```
/etc/opt/scripts/on-hostname-set/90_update_asrepository.sh  
/etc/opt/scripts/on-hostname-set/91_update_cluster_user_ssh_keys.sh
```

# Appendix

## A

### Audit Store CLI Options

*8.1 Rotating Audit Store Certificates*

*8.2 Applying Audit Store Security Configuration*

*8.3 Setting the Total Memory for the Audit Store Repository*

---

The Audit Store CLI settings can be accessed by logging in to the ESA CLI and navigating to the **Tools** menu. The following settings are available in the CLI for working with the Audit Store.

- **Rotate Audit Store Certificates**
- **Apply Audit Store Security Configs**
- **Set Audit Store Repository Total Memory**

### 8.1 Rotating Audit Store Certificates

Rotate the Audit Store certificates after the the ESA certificates are rotated. This refreshes the Audit Store-related certificates that is required for the Audit Store nodes to communicate with the other nodes in the Audit Store cluster and the ESA.

```
Tools:

  Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
-- Analytics Tools --
  Migrate Analytics Configuration
  Migrate Analytics Audits
  Clear Analytics Migration Configuration
-- Cloud Utility AWS Tools --
  CloudWatch Integration
-- Audit Store Tools --
  Rotate Audit Store Certificates
  Apply Audit Store Security Configs
  Set Audit Store Repository Total Memory
```

Figure A-1: Rotate Audit Store Certificates

For more information about rotating the Audit Store certificates, refer to the section [Rotating Audit Store Certificates](#).

## 8.2 Applying Audit Store Security Configuration

The **Apply Audit Store Security Configs** setting is available for configuring the Audit Store security. This setting must be used after upgrading from an earlier version of the ESA to the ESA 9.1.0.5 when you use custom certificates. Run the following steps after the upgrade is complete and custom certificates are applied for td-agent, Audit Store, and Analytics, if installed.

1. From the ESA Web UI, navigate to **System > Services > Audit Store**.
2. Start the **Audit Store Repository** service.
3. Open the ESA CLI.
4. Navigate to **Tools**.
5. Run **Apply Audit Store Security Configs**.

```
Tools:

  Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
-- Analytics Tools --
  Migrate Analytics Configuration
  Migrate Analytics Audits
  Clear Analytics Migration Configuration
-- Cloud Utility AWS Tools --
  CloudWatch Integration
-- Audit Store Tools --
  Rotate Audit Store Certificates
  Apply Audit Store Security Configs
  Set Audit Store Repository Total Memory
```

Figure A-2: Apply Audit Store Security Configs Setting

## 8.3 Setting the Total Memory for the Audit Store Repository

The **Set Audit Store Repository Total Memory** tool allows setting the total RAM allocated for the Audit Store Repository on the ESA.

The RAM allocated for the Audit Store on the Appliance is set to a optimal default value. If you find that this value is not as per your requirement, then you can use this tool to modify the RAM allocation. However, when certain operations are performed, such as, when the role for the node is modified or a node is removed from the cluster, then the value that you set is overwritten and the RAM allocation reverts to the optimal default value. In this case, you need to perform these steps again for setting the RAM allocation after you modify the role of the node or add a node back to the Audit Store cluster.

1. From the ESA Web UI, navigate to **System > Services > Audit Store**.
2. Start the **Audit Store Repository** service.
3. Open the ESA CLI.
4. Navigate to **Tools**.
5. Run **Set Audit Store Repository Total Memory**.

```
Tools:
    Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
-- Analytics Tools --
    Migrate Analytics Configuration
    Migrate Analytics Audits
    Clear Analytics Migration Configuration
-- Cloud Utility AWS Tools --
    CloudWatch Integration
-- Audit Store Tools --
    Rotate Audit Store Certificates
    Apply Audit Store Security Configs
    Set Audit Store Repository Total Memory
```

Figure A-3: Set Audit Store Repository Total Memory Setting

6. Enter the password for the root user and select **OK**.

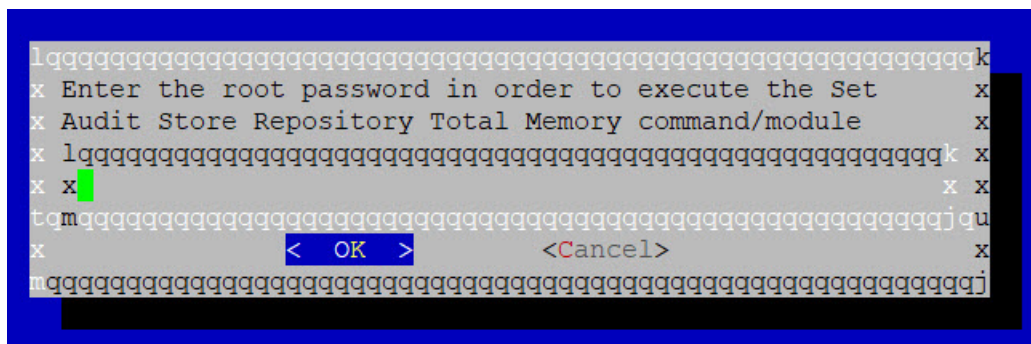
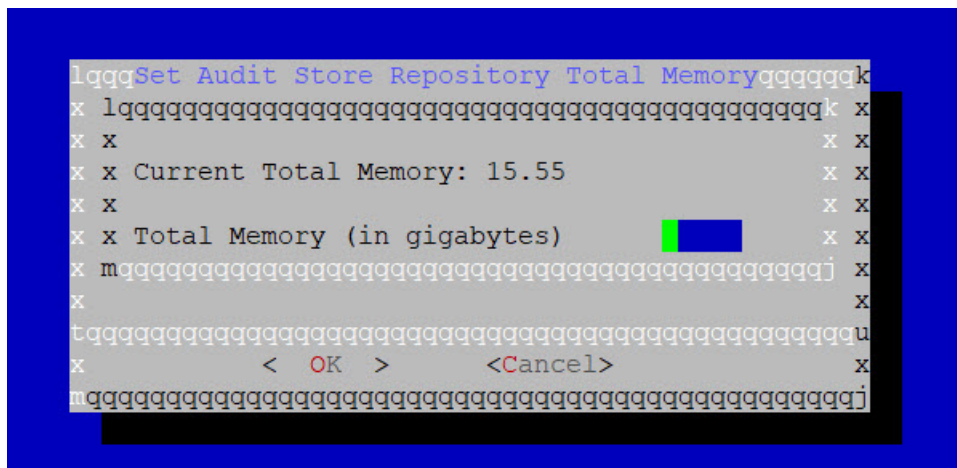


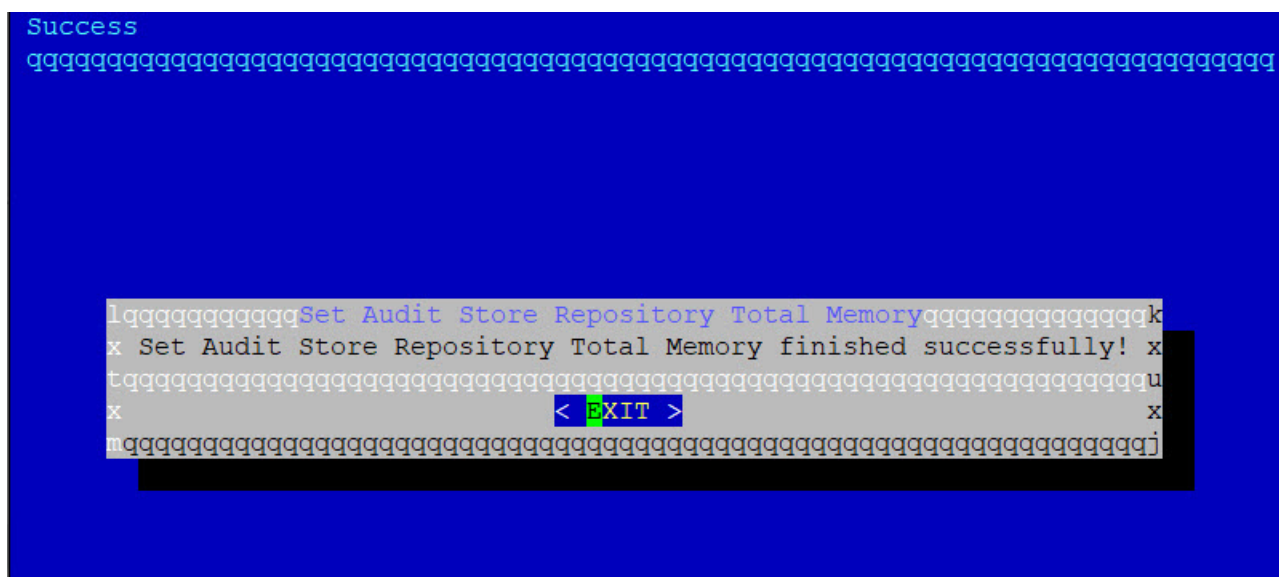
Figure A-4: Root User Password

7. Specify the total memory that must be allocated for the Audit Store Repository and select **OK**.



*Figure A-5: Specifying the Audit Store Repository Size*

8. Select **Exit** to return to the menu.



*Figure A-6: Success Message*

9. Repeat the steps on the remaining nodes, if required.

# Appendix

## B

### Configuring Security for the Log Forwarder

#### *9.1 Enabling Basic Authentication*

#### *9.2 Enabling Certificate-Based Authentication*

The *Log Forwarder* is present on the Protector and sends logs to the Audit Store. This communication needs to take place securely. Hence, the Log Forwarder needs to authenticate with the Audit Store for sending logs that must be stored in the Audit Store. The credentials for the Log Forwarder are added to the Audit Store and the settings are the configurations are then added to the Log Forwarder.

You can use the following authentication methods for configuring the communication between the Log Forwarder and the Audit Store:

- Basic Authentication
- Certificate Authentication

**Note:** For configuring security, you need to back up the existing configuration files and create configuration files as per your requirement. To revert to the existing security configuration, you need to delete the new configuration files that you created and use the back up files for restoring the settings.

### 9.1 Enabling Basic Authentication

HTTP Basic Authentication uses a username and password to authenticate the Log Forwarder with the Audit Store. In this example, you set up the credentials that the Log Forwarder will use to connect to the Audit Store. Next, you add the credentials on the Log Forwarder.

For more information about authentication, refer to <https://opensearch.org/docs/1.3/security/configuration/configuration/#authentication> and <https://opensearch.org/docs/1.3/security/configuration/configuration/#http-basic>.

#### 9.1.1 Configuring the Audit Store

Enable Basic Authentication on the Audit Store by updating the *YAML* files using the steps provided here.

1. Open the CLI Manager on the ESA.
  - a. Login to the CLI Manager on the ESA.



- b. Navigate to **Administration > OS Console**.
  - c. Enter the root password.
2. Navigate to the `/opt/tegrity/auditstore/config/security` directory.

```
cd /opt/tegrity/auditstore/config/security
```

3. Backup the files that must be modified.

```
cp config.yml config.yml_prebasicauth
cp internal_users.yml internal_users.yml_prebasicauth
cp roles_mapping.yml roles_mapping.yml_prebasicauth
```

**Note:** If the backup name already exists, then use a different backup name.

4. Update the `config.yml` file by performing the following steps.
  - a. Open the `config.yml` file.

```
vi config.yml
```

- b. Disable anonymous authentication by setting the `anonymous_auth_enabled` configuration parameter to `false`.  
The extract of the updated `config.yml` file is shown here.

```
.
.<existing configuration>
.
  http:
    anonymous_auth_enabled: false
.
.<existing configuration>
.
```

- c. Add the basic authentication configuration under the `authc:` section.  
The extract of the file is shown here.

```
.
.<existing configuration>
.
  authc:
    basic_internal_auth_domain:
      description: "Authenticate via HTTP Basic against internal users database"
      http_enabled: true
      transport_enabled: true
      order: 1
      http_authenticator:
        type: basic
        challenge: true
      authentication_backend:
        type: intern
.
.<existing configuration>
.
```

Here, you are configuring a basic internal authentication domain, which is enabled for http and transport traffic. The users for authentication are defined in the `internal_users.yml` file.

- d. Save and close the file.
5. Set up the user credentials in the `internal_users.yml` file by performing the following steps. These user credentials are used by the Log Forwarder to authenticate with the Audit Store. The `internal_users.yml` file stores the password in the form of a bcrypt hash, which can be generated using the hash tool.

- a. Run the *hash.sh* tool from the ESA CLI to generate the password hash.

```
docker exec -e "JAVA_HOME=/usr/share/openssl/jdk" auditstore bash /usr/share/openssl/plugins/openssl-security/tools/hash.sh -p <password>
```

For example:

```
docker exec -e "JAVA_HOME=/usr/share/openssl/jdk" auditstore bash /usr/share/openssl/plugins/openssl-security/tools/hash.sh -p fluentbit
```

The password hash will be displayed on the CLI. Copy the password hash because you need to specify it later. For this scenario, *fluentbit* is used as the password and the following sample hash value might be obtained:  
*\$2y\$12\$rmvizuURiE0G6VZRBwqk5O7Jx87A8vs3vaRo0gpWbB9VNoD.wLp.G*

**Note:** Ensure that you use the hash value that you have generated.

- b. Clear the contents of the *internal\_users.yml* file.

```
> internal_users.yml
```

- c. Open the *internal\_users.yml* file.

```
vi internal_users.yml
```

- d. Add the following content to the *internal\_users.yml* file.

```
# This is the internal user database
# The hash value is a bcrypt hash and can be generated with plugin/tools/hash.sh

_meta:
  type: "internalusers"
  config_version: 2

fluentbit:
  reserved: true
  hash: $2y$12$5e6yhwCHWczUQwojhRf7AeGqPeVblHVobQPXhrURNx7cfVKlPVO/y
```

**Note:** The password hash provided here is just an example. Use the password hash that you generated earlier.

- e. Save and close the file.
6. Update the *roles\_mapping.yml* configuration by performing the following steps.
  - a. Open the *roles\_mapping.yml* file.

```
vi roles_mapping.yml
```

- b. Search for the *plug* role.
- c. Delete the following two lines.

```
backendroles:
  - 'opendistro_security_anonymous_backendrole'
```

- d. Add the user you created to the *plug* role. In this scenario, you created the *fluentbit* user.

**Note:** Ensure that you follow the structure of the YAML file.

The *roles\_mapping.yml* file with the role updates appears as shown in the following snippet.

```
.
. <existing configuration>
.
plug:
  reserved: true
```

```

users:
  - 'plug'
  - 'fluentbit'
.
. <existing configuration>
.

```

e. Save and close the file.

7. Update the Audit Store Repository container.

a. Go to the `/opt/protegrity/auditstore/config` directory.

```
cd /opt/protegrity/auditstore/config
```

b. Backup the `volume_mapping.sh` file that must be modified.

```
cp volume_mapping.sh volume_mapping.sh_prebasicauth
```

**Note:** If the backup name already exists, then use a different backup name.

c. Open the `volume_mapping.sh` file.

```
vi volume_mapping.sh
```

d. Add the volume mapping for the `internal_users.yml` config file on a new line at the end of the file.

```
INTERNAL_USERS_VOLUME="--volume ${SECURITY_CONFIG_DIR}/internal_users.yml:${
{OPENSEARCH_HOME}/plugins/opensearch-security/securityconfig/internal_users.yml"
```

e. Save and close the file.

f. Navigate to the `/etc/init.d` directory.

```
cd /etc/init.d
```

g. Open the `asrepository` file.

```
vi asrepository
```

h. Locate the **VOLUME\_OPTS** variable in the file.

i. Backup the **VOLUME\_OPTS** variable by copying the variable and contents on a new line, commenting the original mapping, and update the value to include the variable for the `internal_users.yml` volume mapping.

```

# Original mappings
# VOLUME_OPTS="$OPENSEARCH_YML_VOLUME $LOG4J2_PROPERTIES_VOLUME $UNICAST_HOSTS_VOLUME
$JVM_OPTIONS_VOLUME $CONFIG_YML_VOLUME $ROLES_YM
L_VOLUME $ROLES_MAPPING_YML_VOLUME $DATA_VOLUME $LOGS_VOLUME $HEAP_DUMP_VOLUME
$TMP_VOLUME $CLUSTER_CERT_VOLUME $REST_CERT_VOLUME"

# Added internal_users.yml volume mapping
VOLUME_OPTS="$INTERNAL_USERS_VOLUME $OPENSEARCH_YML_VOLUME $LOG4J2_PROPERTIES_VOLUME
$UNICAST_HOSTS_VOLUME $JVM_OPTIONS_VOLUME $CONFIG_YML_VOLUME $ROLES_YM
L_VOLUME $ROLES_MAPPING_YML_VOLUME $DATA_VOLUME $LOGS_VOLUME $HEAP_DUMP_VOLUME
$TMP_VOLUME $CLUSTER_CERT_VOLUME $REST_CERT_VOLUME"

```

j. Save and close the file.

k. Stop the *Audit Store Repository* service.

```
/etc/init.d/asrepository stop
```

l. Remove the existing *Audit Store Repository* container before creating the container with the new volume mappings.

```
/etc/init.d/asrepository remove
```

- m. Start the *Audit Store Repository* service.

```
/etc/init.d/asrepository start
```

8. Apply the Audit Store security configurations.
  - a. Login to the CLI Manager on the ESA.
  - b. Navigate to **Tools > Apply Audit Store Security Configs**.

## 9.1.2 Configuring the Protector

Configure the Basic Authentication settings on the Protector by updating the configuration files using the steps provided here.

1. Identify the Fluent Bit version of your Protector using the following steps:
  - a. Login and open a CLI on the Protector machine
  - b. Restart the Log Forwarder using the following commands.

```
/opt/protectrity/fluent-bit/bin/logforwarderctrl stop
/opt/protectrity/fluent-bit/bin/logforwarderctrl start
```

- c. View the version number in the output displayed.

```
[root@ip-192-168-0-10 bin]# /opt/protectrity/fluent-bit/bin/logforwarderctrl start
Fluent Bit v1.6.10-1.0.0+4.g2f46.master
```

Table B-1: Configuration Information for Fluent Bit Version

Configuration	v1.6	v1.9 or v2.2
Name of <i>.conf</i> file	<i>out_elastic.conf</i>	<i>out.conf</i>
Name of <i>.cfg</i> file	<i>upstream_es.cfg</i>	<i>upstream.cfg</i>

2. Backup the existing configuration.
  - a. On the Protector node, navigate to the */opt/protectrity/fluent-bit/data/config.d* directory.

```
cd /opt/protectrity/fluent-bit/data/config.d
```

- b. Backup the existing configuration by using the following command.

```
cp out_elastic.conf out_elastic.conf_prebasicauth
```

3. Update the *out\_elastic.conf* configuration file.
  - a. Open the *out\_elastic.conf* file.

```
vi out_elastic.conf
```

- b. Add the username and the password to the *[OUTPUT]* plugin that are named *Name es*.

The updated file extract appears as shown here.

```
.
<existing configuration>
.
[OUTPUT]
  Name es
  .
  <existing config>
  .
  HTTP_User fluentbit
  HTTP_Passwd fluentbit
.
<existing configuration>
.
```

In this example, *fluentbit* is used for the username and password. Ensure that you use the username that you created and the password that you used earlier to create the hash.

For more information about configuring the *es* plugin, refer to <https://docs.fluentbit.io/manual/v1.9-pre/pipeline/outputs/opensearch>.

- c. Save and close the file.
4. Restart the Log Forwarder on the Protector using the following commands.

```
/opt/protectrity/fluent-bit/bin/logforwarderctrl stop
/opt/protectrity/fluent-bit/bin/logforwarderctrl start
```

5. Complete the configurations provided in this section on the remaining Protector machines.

## 9.2 Enabling Certificate-Based Authentication

You can configure the Protector to connect to and authenticate with the Audit Store cluster using certificates. In certificate-based authentication, the certificates from the Audit Store cluster are stored on the Protector machine. These certificates are used by the Protector to connect to the Audit Store cluster.

For more information about authentication, refer to <https://opensearch.org/docs/1.3/security/configuration/configuration/#authentication>.

### 9.2.1 Configuring the Audit Store

Enable Certificate-based Authentication on the Audit Store by updating the *YAML* files using the steps provided here.

1. Open the CLI Manager on the ESA.
  - a. Login to the CLI Manager on the ESA.
  - b. Navigate to **Administration** > **OS Console**.
  - c. Enter the root password.
2. Navigate to the */opt/protectrity/auditstore/config/security* directory.

```
cd /opt/protectrity/auditstore/config/security
```

3. Backup the files that must be modified.

```
cp config.yml config.yml_precertauth
cp roles_mapping.yml roles_mapping.yml_precertauth
```

**Note:** If the backup name already exists, then use a different backup name.

4. Update the *config.yml* file by performing the following steps.
  - a. Open the *config.yml* file.

```
vi config.yml
```

- b. Disable anonymous authentication by setting the *anonymous\_auth\_enabled* configuration parameter to *false*.  
The extract of the updated *config.yml* file is shown here.

```
.<existing configuration>
.
  http:
    anonymous_auth_enabled: false
```

```
.
.<existing configuration>
.
```

c. Save and close the file.

5. Update the *roles\_mapping.yml* configuration by performing the following steps.

a. Open the *roles\_mapping.yml* file.

```
vi roles_mapping.yml
```

b. Search for the *plug* role.

c. Delete the following two lines.

```
backendroles:
  - 'opendistro_security_anonymous_backendrole'
```

d. Save and close the file.

6. Update the Audit Store Repository container.

a. Stop the *Audit Store Repository* service.

```
/etc/init.d/asrepository stop
```

b. Remove the existing *Audit Store Repository* container before creating the container with the new volume mappings.

```
/etc/init.d/asrepository remove
```

c. Start the *Audit Store Repository* service.

```
/etc/init.d/asrepository start
```

7. Apply the Audit Store security configurations.

a. Login to the CLI Manager on the ESA.

b. Navigate to **Tools > Apply Audit Store Security Confgs**.

## 9.2.2 Configuring the Protector

Configure the Certificate Authentication-related settings on the Protector by updating the configuration files using the steps provided here.

**Caution:** For configuring the Certificate-based Authentication at the protector level, you must use your own custom certificates only. For more information about creating your own certificates, refer to the section *Using Custom Certificates in the Audit Store* in the *Protegrity Certificate Management Guide 9.1.0.5*.

1. Open the command prompt on the Protector machine.

2. Identify the Fluent Bit version of your Protector using the following steps:

a. Restart the Log Forwarder using the following commands.

```
/opt/protegrity/fluent-bit/bin/logforwarderctrl stop
/opt/protegrity/fluent-bit/bin/logforwarderctrl start
```

b. View the version number in the output displayed.

```
[root@ip-192-168-0-10 bin]# /opt/protegrity/fluent-bit/bin/logforwarderctrl start
Fluent Bit v1.6.10-1.0.0+4.g2f46.master
```

Table B-2: Configuration Information for Fluent Bit Version

Configuration	v1.6	v1.9 or v2.2
Name of <i>.conf</i> file	<i>out_elastic.conf</i>	<i>out.conf</i>
Name of <i>.cfg</i> file	<i>upstream_es.cfg</i>	<i>upstream.cfg</i>

## 3. Prepare a directory with the custom certificates.

- a. Navigate to the
- fluent-bit*
- directory using the following command.

```
cd /opt/protegrity/fluent-bit
```

- b. Create a
- certs*
- directory to store the certificates using the following command:

```
mkdir certs
```

- c. Download the following certificates from the
- /etc/ksa/certificates/plug*
- directory of the ESA to the
- /opt/protegrity/fluent-bit/certs*
- directory on the Protector machine:

- *CA.pem*
- *client.key*
- *client.pem*

4. Update the *upstream\_es.cfg* configuration file.

- a. On the Protector, navigate to the
- /opt/protegrity/fluent-bit/data/config.d*
- directory using the following command:

```
cd /opt/protegrity/fluent-bit/data/config.d
```

- b. Create a backup of the
- upstream\_es.cfg*
- file, for example, name the file as
- upstream\_es.cfg\_precertauth*
- using the following command.

```
cp upstream_es.cfg upstream_es.cfg_precertauth
```

- c. Open the
- upstream\_es.cfg*
- file in a text editor.

- d. Set the following properties in all the
- NODE*
- tags of the
- upstream\_es.cfg*
- file:

- Set the *Host* and the *Port* for the Audit Store. In this example, the target IP is *192.168.1.100* and the port is *9200*.
- Set *tls* to *on*.
- Set *tls.verify* to *on*.
- Specify the path to the *tls.ca\_file* certificate. In this example, the certificate location is */opt/protegrity/fluent-bit/certs/CA.pem*.
- Specify the path to the *tls.key\_file* certificate. In this example, the certificate location is */opt/protegrity/fluent-bit/certs/client.key*.
- Specify the path to the *tls.crt\_file* certificate. In this example, the certificate location is */opt/protegrity/fluent-bit/certs/client.pem*.
- Specify the host name of the ESA machine for the *tls.vhost*. In this example, the host name is *protegrity-esa123*.

An extract of the updated sample file is shown here.

```
.
. <existing configuration>
.
[NODE]
  Name      node-1
  Host      192.168.1.100
  Port      9200
  tls on
  tls.verify on
  # file path of CA.pem
  tls.ca_file /opt/protegrity/fluent-bit/certs/CA.pem
  # file path of client.key
  tls.key_file /opt/protegrity/fluent-bit/certs/client.key
  # file path of client.pem
  tls.crt_file /opt/protegrity/fluent-bit/certs/client.pem
```

```
# host name of ESA
tls.vhost protegrity-esa123
.
. <existing configuration>
.
```

e. Save and close the file.

5. Restart the Log Forwarder on the Protector using the following commands.

```
/opt/protegrity/fluent-bit/bin/logforwarderctrl stop
/opt/protegrity/fluent-bit/bin/logforwarderctrl start
```

6. Complete the configurations provided in this section on the remaining Protector machines.



# Appendix

# C

## Updating Audit Store Custom Certificates

### *10.1 Updating Custom Certificates on a Single-Node Audit Store Cluster*

### *10.2 Updating Custom Certificates on a Multi-Node Audit Store Cluster*

You might need to update certificates in certain cases, such as, when the certificates expire or become invalid. If the ESA Management and Web Services certificates are rotated, then the Audit Store certificates must be rotated. The steps provided in this section must be completed to rotate custom certificates on the nodes in the Audit Store cluster. Complete the steps for one of the two scenarios, for a single-node Audit Store cluster where nodes have still to be added to the Audit Store cluster or a multi-node Audit Store cluster where the nodes are already added to the Audit Store cluster.

**Note:** These steps are only applicable for custom certificates and keys.

For more information about certificates, refer to the section *Audit Store Certificates* in the *Protegrity Certificate Management Guide 9.1.0.5*.

## 10.1 Updating Custom Certificates on a Single-Node Audit Store Cluster

Rotate custom certificates on the Audit Store cluster that has a single node in the cluster using the steps provided in the section *Certificate Management in ESA* in the *Protegrity Certificate Management Guide 9.1.0.5*.

**Note:** These steps are only applicable for custom certificate and keys.

Ensure that you disable any default or custom CAs that are not required

## 10.2 Updating Custom Certificates on a Multi-Node Audit Store Cluster

On a multi-node Audit Store cluster, the certificate rotation must be performed on every node in the cluster. First, rotate the certificates on a Lead node, which is the Primary ESA, and then use the IP of this Lead node while rotating the certificates on the remaining nodes in the cluster. The services mentioned in this section must be stopped on all the nodes, preferably at the

same time with minimum delay during certificate rotation. After updating the certificates, the services that were stopped must be started again on the nodes in the reverse order.

**Note:** These steps are only applicable for custom certificate and keys. For rotating custom certificates, refer to [Updating Audit Store Custom Certificates](#).

- 1. Login to the ESA Web UI.
- 2. Navigate to **System > Services > Misc**.
- 3. Stop the **td-agent** service.

**Note:** This step must be performed on all the other nodes followed by the Lead node.

<div>System</div> <div>Services</div> <div>Information</div> <div>Trusted Appliances Cluster</div> <div>System Statistics</div> <div>Backup &amp; Restore</div> <div>Task Scheduler</div> <div>Graphs</div>	All	OS	Policy Management	Audit Store	Misc
	Services		Status	Mode	Actions
	Misc				
	LDAP Server		Running	Automatic	<div><div></div><div></div></div>
	Web-Services Engine		Running	Automatic	<div><div></div><div></div></div>
	Service Dispatcher		Running	Automatic	<div><div></div><div></div></div>
	td-agent		Running	Automatic	<div><div></div><div></div></div>
	Analytics		Running	Automatic	<div><div></div><div></div></div>

Figure C-1: Stopping td-agent

- 4. On the ESA Web UI, navigate to **System > Services > Misc**.
- 5. Stop the **Analytics** service.

**Note:** This step must be performed on all the other nodes followed by the Lead node.  
The other nodes might not have Analytics installed. In this case, skip this step on those nodes.

System

Services

Information

Trusted Appliances Cluster

System Statistics

Backup & Restore

Task Scheduler

Graphs

AllOSPolicy ManagementAudit StoreMisc

Services

Status

Mode

Actions

Misc

LDAP ServerRunningAutomatic

Web-Services EngineRunningAutomatic

Service DispatcherRunningAutomatic

td-agentStoppedAutomatic

AnalyticsRunningAutomatic

Figure C-2: Stopping Analytics

6. Navigate to **System > Services > Audit Store**.
7. Stop the **Audit Store Management** service.

**Note:** This step must be performed on all the other nodes followed by the Lead node.

System

Services

Information

Trusted Appliances Cluster

System Statistics

Backup & Restore

Task Scheduler

Graphs

AllOSPolicy ManagementAudit StoreMisc

ServicesStatusModeActions

Audit Store

Audit Store RepositoryRunningAutomatic■↺

Audit Store ManagementRunningAutomatic■↺

Figure C-3: Stopping Audit Store Management

8. Navigate to **System > Services > Audit Store**.
9. Stop the **Audit Store Repository** service.

**Attention:** This is a very important step and must be performed on all the other nodes followed by the Lead node without any delay. A delay in stopping the service on the nodes will result in that node receiving logs. This will lead to inconsistency in the logs across nodes and logs might be lost.

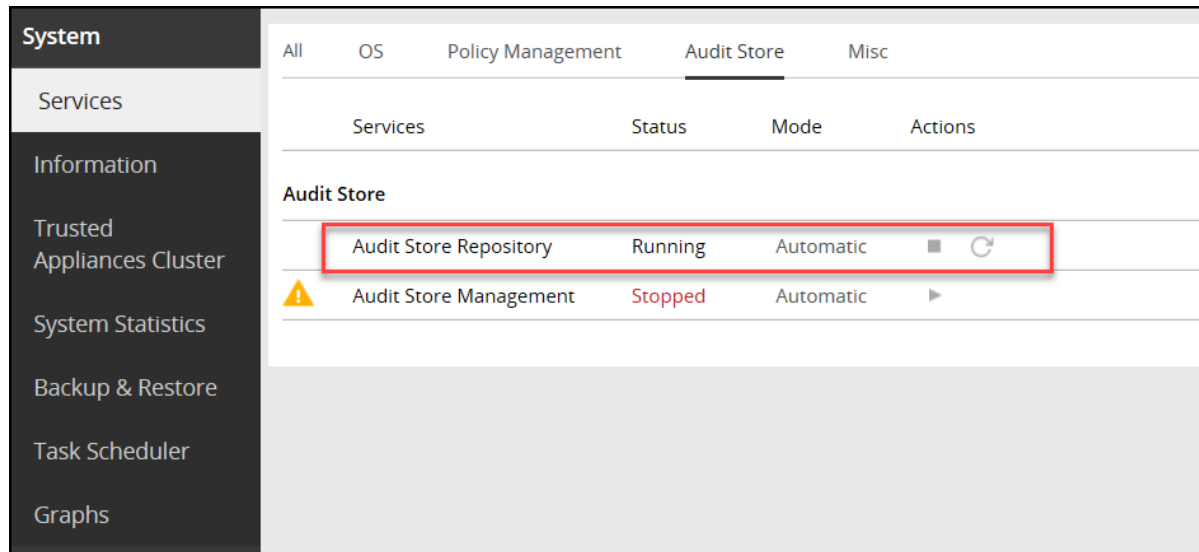


Figure C-4: Stopping Audit Store Repository

10. Apply the custom certificates on the Lead ESA node.

For more information about certificates, refer to the section *Certificate Management in ESA* in the *Protegrity Certificate Management Guide 9.1.0.5*.

11. Complete any one of the following steps on the remaining nodes in the Audit Store cluster.

- Apply the custom certificates on the remaining nodes in the Audit Store cluster.

For more information about certificates, refer to the section *Certificate Management in ESA* in the *Protegrity Certificate Management Guide 9.1.0.5*.

**Note:** Ensure that you disable any default or custom CAs that are not required

- Run the Rotate Audit Store Certificates tool on all the remaining nodes in the Audit Store cluster one node at a time.
  - a. Login to the ESA CLI Manager of a node in the Audit Store cluster.
  - b. Navigate to **Tools > Rotate Audit Store Certificates**.

```
Tools:
    Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
-- Analytics Tools --
    Migrate Analytics Configuration
    Migrate Analytics Audits
    Clear Analytics Migration Configuration
-- Cloud Utility AWS Tools --
    CloudWatch Integration
-- Audit Store Tools --
    Rotate Audit Store Certificates
    Apply Audit Store Security Configs
    Set Audit Store Repository Total Memory
```

Figure C-5: Rotating Keys

- c. Enter the root password and select **OK**.

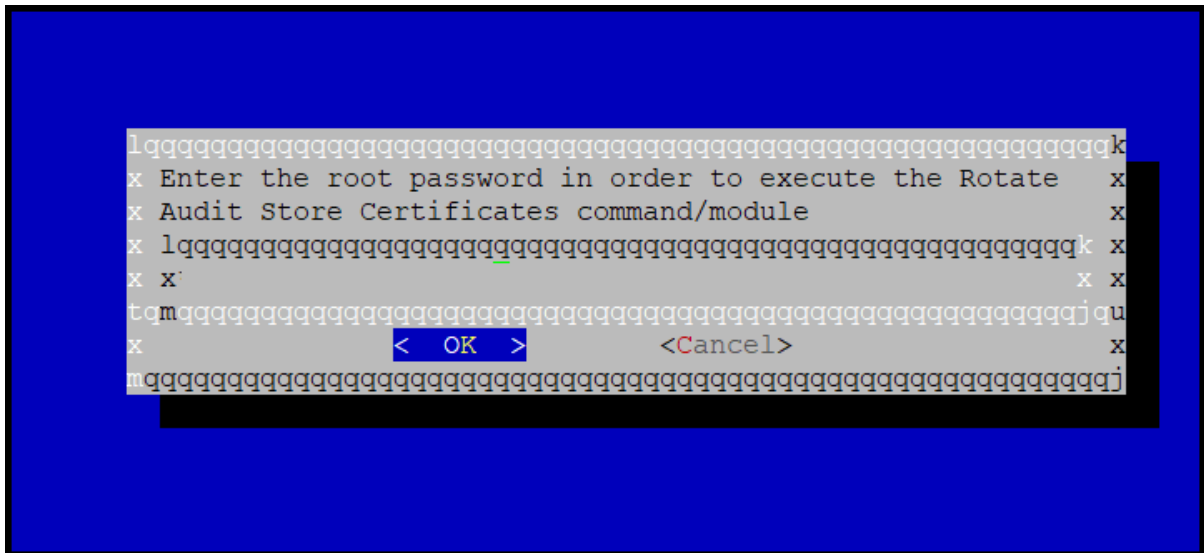


Figure C-6: Root Password

- d. Enter the *admin* username and password and select **OK**.

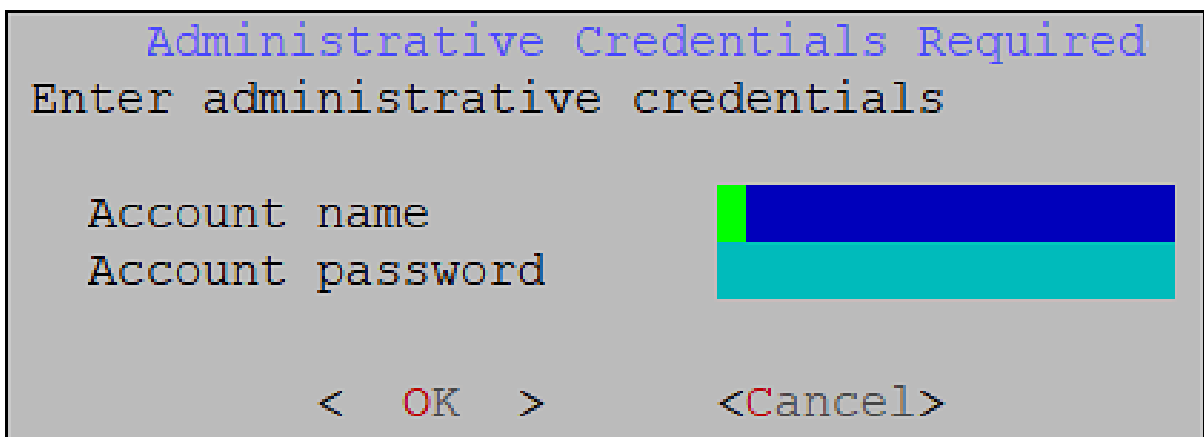


Figure C-7: Admin Details

- e. Enter the IP address of the Lead node in **Target Audit Store Address** and select **OK**.

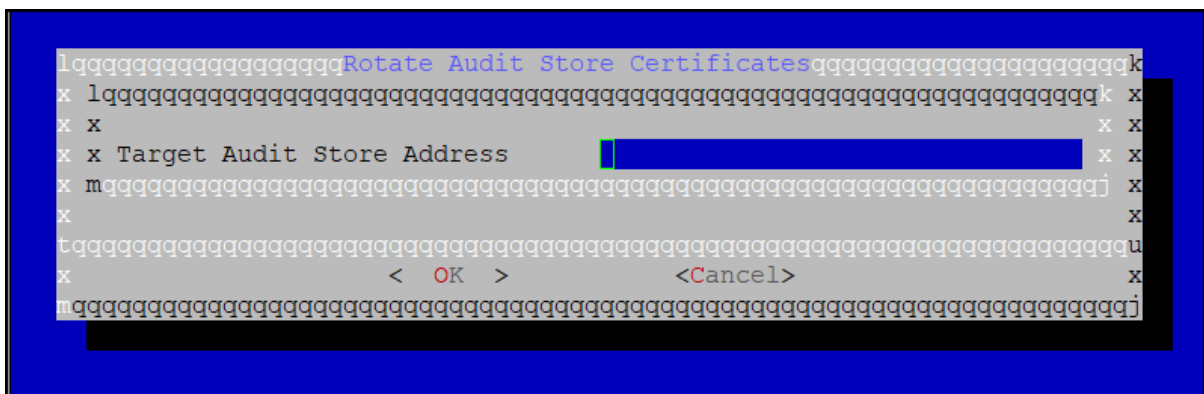


Figure C-8: Target Audit Store Address

- f. Enter the *admin* username and password for the Lead node and select **OK**.

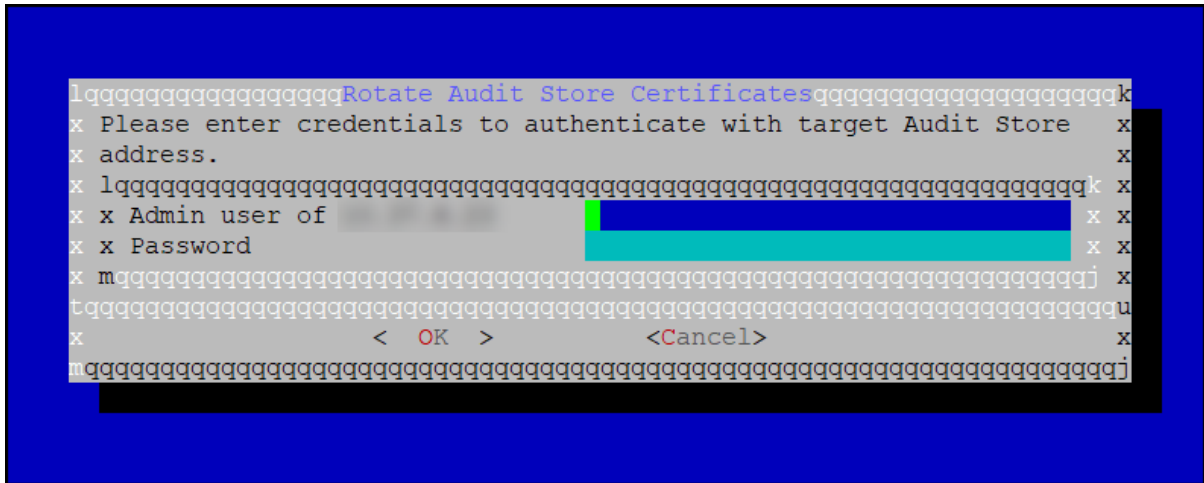


Figure C-9: Admin Credentials

- g. After the rotation is completed without errors, the following screen appears. Select **OK** to go to the CLI menu screen.

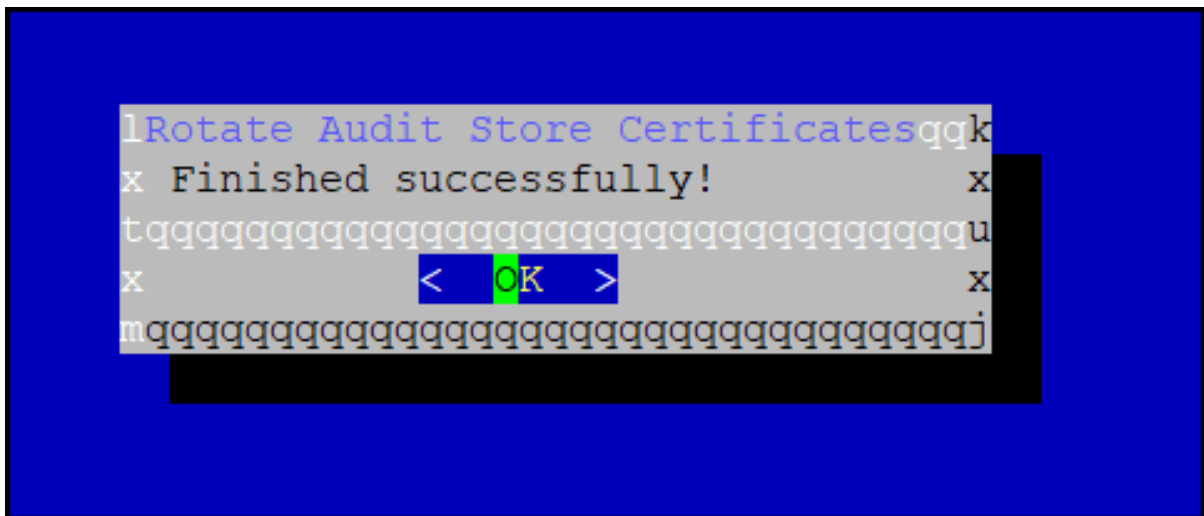


Figure C-10: Rotation Complete

The CLI screen appears.

```
Tools:

  Disable USB Flash Drives
Web-Services Tuning
Service Dispatcher Tuning
AntiVirus
PLUG - Forward logs to Audit Store
-- Analytics Tools --
  Migrate Analytics Configuration
  Migrate Analytics Audits
  Clear Analytics Migration Configuration
-- Cloud Utility AWS Tools --
  CloudWatch Integration
-- Audit Store Tools --
  Rotate Audit Store Certificates
  Apply Audit Store Security Configs
  Set Audit Store Repository Total Memory
```

Figure C-11: Keys Rotated

12. Navigate to **System > Services > Audit Store**.

13. Start the **Audit Store Repository** service.

**Attention:** This step must be performed on the Lead node followed by all the other nodes without any delay. A delay in starting the services on the nodes will result in that node receiving logs. This will lead to inconsistency in the logs across nodes and logs might be lost.

14. Navigate to **System > Services > Audit Store**.

15. Start the **Audit Store Management** service.

**Note:** This step must be performed on the Lead node followed by all the other nodes.

16. Navigate to **Audit Store Management** and confirm that the Audit Store cluster is functional and the Audit Store cluster status is green or yellow as shown in the following figure.

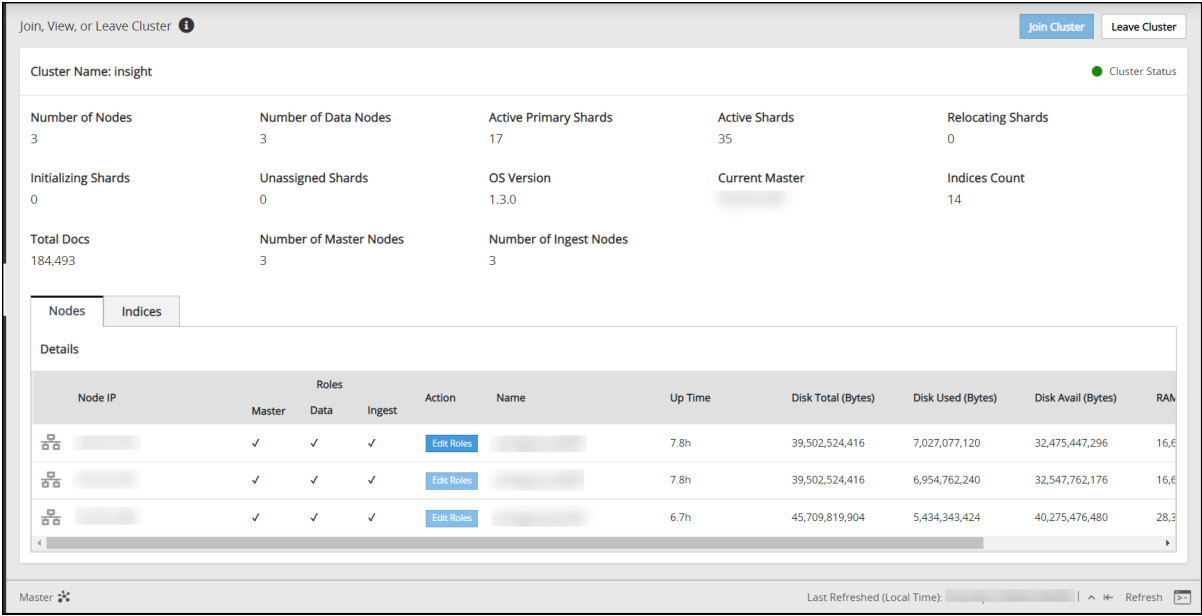


Figure C-12: Audit Store Clustering Started

- 17. Navigate to **System > Services > Misc.**
- 18. Start the **Analytics** service.

**Note:** This step must be performed on the Lead node followed by all the other nodes. The other nodes might not have Analytics installed. In this case, skip this step on those nodes.

- 19. Navigate to **System > Services > Misc.**
- 20. Start the **td-agent** service.

The following figure shows all services that are started.

**Note:** This step must be performed on the Lead node followed by all the other nodes.

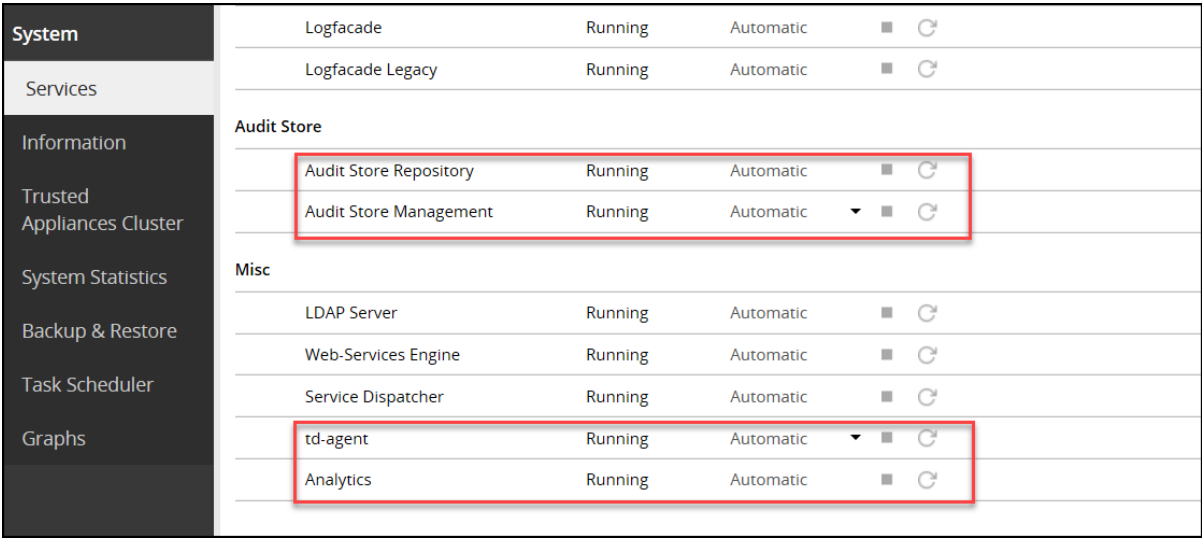


Figure C-13: Services Started

- 21. On the ESA Web UI, navigate to **Audit Store Management.**



22. Verify that the nodes are still a part of the Audit Store cluster.

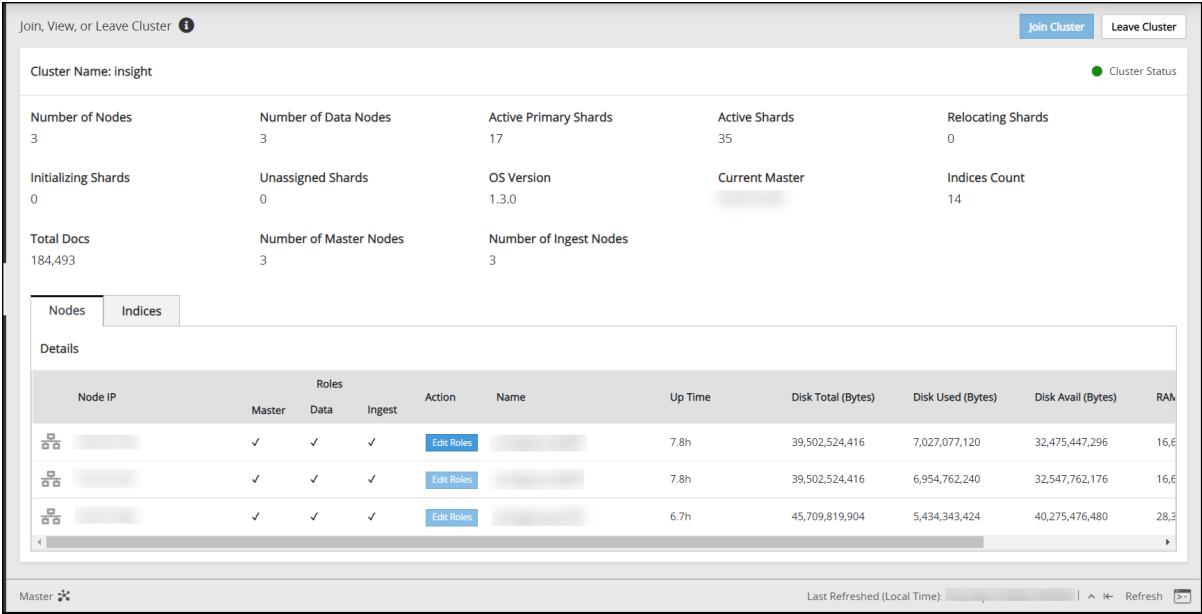


Figure C-14: Audit Store Nodes

# Appendix

## D

### Removing the Audit Store from the ESA

Complete the steps provided in this section to remove the Audit Store from the ESA when you use an external SIEM.

**Caution:** This feature cannot be reinstalled after it is removed.

1. Login to the ESA Web UI.
2. Navigate to **System > Services**.
3. Navigate to **Audit Store**.
4. Set the **Mode** for the following services to **Manual**:
  - **Audit Store Repository**
  - **Audit Store Management**
5. Stop the following services:
  - **Audit Store Repository**
  - **Audit Store Management**
6. Login as an administrator to the ESA CLI Manager.
7. Navigate to **Administration > Add/Remove Services**.
8. Enter the root password and select **OK**.
9. Select **2. Remove already installed applications** and select **OK**.
10. Press the space bar to select the following application from the list:
  - **Audit Store**
11. Select **OK** to uninstall the applications.
12. Disable the scheduled task, that will no longer work, using the following steps.
  - a. Login to the ESA Web UI.
  - b. Navigate to **System > Task Scheduler**.
  - c. Disable the following scheduled tasks by selecting the task, clicking **Edit**, clearing the **Enable** check box, and clicking **Save**:
    - **Update Audit Store Management Unicast Hosts**
    - **Rotate Audit Store Management log file**